



大会

Distr.: General
21 April 2022
Chinese
Original: Arabic/English/French/
Russian/Spanish

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

会员国提交的关于打击为犯罪目的使用信息和通信技术行为全面国际
公约的刑事定罪条款、总则及程序措施和执法条款的提案和材料汇编

摘要

为筹备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，特委会主席在秘书处的支持下编写了本文件。文
件中包含从会员国收到的关于刑事定罪条款（A/AC.291/9）、总则
（A/AC.291/9/Add.1）及程序措施和执法条款（A/AC.291/9/Add.2）的提案。



目录

	页次
一. 导言	3
二. 刑事定罪	3
安哥拉	3
澳大利亚	4
巴西	7
布隆迪	11
加拿大	15
哥伦比亚	17
埃及	18
萨尔瓦多	23
欧洲联盟及其成员国	27
加纳	29
伊朗伊斯兰共和国	35
日本	36
约旦	38
墨西哥	40
新西兰	40
挪威	45
俄罗斯联邦，并代表白俄罗斯、布隆迪、中国、尼加拉瓜和塔吉克斯坦	46
南非	51
瑞士	55
大不列颠及北爱尔兰联合王国	59
坦桑尼亚联合共和国	63
美利坚合众国	64
委内瑞拉玻利瓦尔共和国	69
越南	70

一. 引言

1. 为筹备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，并根据特设委员会在其第一届会议上核准的路线图和工作方式，特别是其中第3和第4段，请会员国向秘书处提供拟在第二届会议期间审议的各章或各条文的文本草案，涉及刑事定罪条款（A/AC.291/9）、总则（A/AC.291/9/Add.1）及关于程序措施和执法的条款（A/AC.291/9/Add.2）。
2. 在此基础上，特委会主席在秘书处的支持下编写了本谈判文件，其中汇编了会员国的提案和材料，重点是第二届会议期间将审议的具体各章。因此，本文件仅载有关于刑事定罪、总则及程序措施和执法各章的具体起草建议或一般性意见，并按会员国提供的并翻译成联合国六种正式语文的内容按章归类。除非另有说明，脚注均含有会员国提供的文本。
3. 如上所述，本文件不载有对其他议题的评论意见或对具体起草建议的解释，这些意见或建议可在原始提交材料中找到，原始提交材料已按收到时的原样和原始版本登载于特设委员会的网站上。
4. 截至2022年4月14日，秘书处共收到24份提交材料，其中代表了54个会员国和欧盟的意见。

二. 刑事定罪

安哥拉

[原件：英文]

[2022年4月8日]

- 公约应将最严重的网络犯罪，特别是影响到关键基础设施的网络犯罪行为作为典型并定为刑事犯罪，将其归类为网络恐怖主义或危害人类罪，并界定调查和起诉网络犯罪代理人的国际合作的优先和紧急规则。
- 公约应将涉及用于资助恐怖主义和洗钱的加密货币和加密资产的网络犯罪行为作为典型并定为刑事犯罪。

刑事定罪

依赖网络实施的犯罪（危害计算机系统和数据的保密性、完整性和可用性的犯罪）：非法访问、非法拦截、破坏计算机数据、计算机破坏、计算机伪造、非法复制计算机程序。

网络工具性犯罪（利用信息和通信技术实施的传统犯罪）：网络骗局、网络钓鱼、网上经济和金融犯罪、网上盗用身份、网上对儿童的性虐待和剥削、网络欺凌、网络跟踪、报复性色情、网络恐怖主义。

可以借助于上述区域和国际法律文书，以构建这些罪行的法律类型概念。¹

¹ 秘书处的说明：此处提及的是安哥拉共和国提交的材料中“序言”副标题下所包含的文书，即：“《非洲联盟网络安全和个人数据保护公约》（《马拉博公约》）、《欧洲委员会网络犯罪公约》（《布达佩斯公约》）、《联合国打击跨国组织犯罪公约》和《联合国反腐败公约》”。

澳大利亚

[原件：英文]
[2022年4月13日]

刑事定罪

新的公约为改进打击网络犯罪方面的国际合作提供了机会，同时确保与现有的国际打击犯罪公约和其他相关文书保持一致，并避免不必要的重复。刑事定罪条款应与现有国际文书保持一致，避免这些文书之间产生冲突。刑事定罪条款还应适当地兼顾尊重法治、人权和基本自由。

澳大利亚认为，新公约提供了一个机会，可以加强全球对打击网络犯罪的协调。这反过来将缩小网络犯罪分子的安全区，并增强执法部门在线打击网络犯罪活动的的能力。

新公约的实质性刑法条款应是具体的，并且明确阐明基本犯罪行为。公约还应适当考虑依赖网络实施的犯罪和借助网络实施的犯罪的上游犯罪和附属责任。这应包括《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》等文书所载刑事责任的标准延伸。

依赖网络实施的犯罪

澳大利亚认为，新的公约应包括对针对计算机系统的犯罪（“依赖网络实施的犯罪”）进行刑事定罪的标准。澳大利亚提议，新公约应包括以下依赖网络实施的犯罪：

- 未经授权非法访问计算机系统的任何部分（包括计算机数据）
- 未经授权非法拦截计算机数据的传输
- 未经授权非法干扰计算机数据（包括删除、损坏、更改或抑制计算机数据）
- 非法干扰计算机系统或网络的运行
- 为实施另一起网络犯罪而制作、提供、传播或获取恶意软件

借助网络实施的犯罪

几乎所有国家的现行国内刑法都足以涵盖常见的犯罪，特别是非法侵入、故意破坏、偷窃、与麻醉品有关的犯罪和其他暴力罪行。

如果在犯罪过程中使用计算机系统并不改变犯罪行为的性质或严重性，则公约就无需仅仅因为在犯罪过程中涉及计算机系统或数字技术而重新设想这些犯罪。

然而，澳大利亚认为，一些“传统”犯罪的实施范围、规模和容易度因信息和通信网络提供的速度、匿名性和广泛覆盖面而急剧增加。这些犯罪被描述为“借助网络实施的”犯罪。公约应明智地处理这些犯罪，制定一个明确的框

架，确定为什么某些犯罪被“网络因素”如此显著地改变，以至于其需要一个新的协调一致的国际标准，将这一行为提升到“传统”犯罪之上。公约不需要为每一种可能包含“网络元素”的现有犯罪设立新的犯罪类别，特别是在被定为犯罪的行为的严重性、规模、范围或容易度没有因该元素而发生重大变化的情况下。

虽然澳大利亚认为公约在纳入任何新的犯罪类别方面应采取克制的做法，但也愿意听取支持将公约覆盖范围从依赖网络实施的犯罪扩大到“借助网络实施的犯罪”的论点。

为此，澳大利亚赞赏地注意到，在特设委员会第一届会议期间，许多国家呼吁应对网上儿童性剥削和性虐待所构成的严重威胁。澳大利亚认为，各国可以在这个问题上建设性地达成共识。认识到这一严重的犯罪，澳大利亚单独提出了一项涉及网上虐待儿童的犯罪的提案，其中包括线上诱拐和直播。

澳大利亚还认为，借助网络实施的欺诈和盗窃，包括与勒索软件有关的勒索，大量增加，这是一个普遍存在的问题，各国可就为公约目的将这种行为定为刑事犯罪达成共识。

将网上虐待儿童罪行定为刑事犯罪

第[A]条——通过计算机系统提供虐待儿童材料

1. 各缔约国应采取必要的此类立法和其他措施，将故意[无合法理由]²实施的下列行为在其国内法中定为刑事犯罪：

(a) 通过计算机系统访问、控制、传输、分发、主动提供、获取、制作或提供虐待儿童材料；³或者

(b) 拥有因第 1(a)项中的行为而产生的虐待儿童材料。

2. 就第[A]条的目的而言，“虐待儿童材料”一词应包括描绘或描述以下内容的材料：被暗示或似乎正在从事性活动或在从事性活动的人面前的儿童或儿童代表；主要出于性目的的儿童性器官⁴的任何代表；酷刑、残忍、不人道或有辱人格的待遇或处罚的受害者。

² 列入这一警告是为了确保该罪行不会无意中涵盖某些合法情况——例如，可能因医疗需要而获取或制作本条款本来将涵盖的材料。

³ “计算机系统”的定义是指任何设备或一组互连或相关的设备，其中一个或多个设备根据程序自动处理数据。这可能包括输入、输出和存储设备。计算机系统还包括独立的系统或其他设备联网的系统。请注意，这一术语（或其定义）可作修改，以确保与公约草案的其他条款保持一致。

自生材料可能包括纯粹自生的材料，以及因被胁迫或勒索而自生的材料。在这些情况下，该条款旨在就刑事定罪提供一个格外谨慎的总体立场，但仍由国内法律制度自行决定其适度和合理的对策。

⁴ 术语出自《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》。

第[B]条——便利通过计算机系统提供虐待儿童材料

1. 各缔约国均应采取可能必要的立法和其他措施，在本国法律中将下述故意[无合法理由]实施的为便利第[A]条所述虐待儿童材料⁵而创建、开发、变更、维护、控制、调节、协助、⁶提供、宣传或推销计算机系统的行为规定为刑事犯罪。
2. 就第 1 款的目的而言，“便利虐待儿童”一词应包括第 1 款中概述的任何行为，其目的是允许个人为自己或其他人获取、传输、分发、主动提供或提供或制作“虐待儿童材料”。

第[C]条——通过计算机系统为性目的而诱骗或招收儿童

各缔约国均应采取可能必要的立法和其他措施，在本国法律中将故意实施的通过[计算机系统]诱拐儿童、向儿童提出性要求、招收儿童或导致儿童遇见、目睹或参与性活动的行为定为刑事犯罪。

第[X]条——与提案有关的一般规定

1. 就第[A、B、C]条的目的而言，“儿童”一词应包括未满 18 岁的所有人员。此外，就第[C]条的目的而言，“儿童”亦包括据信未满 18 岁的人。⁷然而，就第[A、B、C]条的目的而言，缔约国可要求一个较低的年龄限制，但不应低于 16 岁。
2. 就第[A、B、C]条的目的而言，刑事责任应适用于 18 岁及以上的人。各缔约国可随时声明对未满 18 岁的人适用此刑事责任。如果缔约国作出声明，则应确保其国内法中有适当的保障措施保护被指控的儿童，并注意到接受刑事司法程序可能对儿童产生的影响。
3. 如果缔约国寻求根据第[A]条将未满 18 岁的人刑事定罪，则应适当考虑避免对有第[A]条第 2 款所涵盖自生材料的儿童过度定罪，并考虑到有必要尊重其根据《儿童权利公约》及其议定书承担的义务。

相关处罚

我们提议列入一条款，规定缔约国有义务采取必要的立法或其他措施，确保本公约确立的任何刑事犯罪都可受到有效、适度和劝阻性措施的惩罚，其中可包括剥夺自由。

⁵ 依据脚注 2。

⁶ “协助”最终可能会被刑事责任一般规定的延伸所涵盖。在审议这些条款之前保留在此。

⁷ 此处增加“据信”一词旨在涵盖以下情况：相关人员或因为性目的诱拐或招收儿童而被调查的人员秘密地与执法人员在网上进行接触。

巴西

[原件：英文]
[2022年4月8日]

第二章 刑事定罪

第4条 非法访问⁸

各缔约国均应采取必要的立法和其他措施，将未经授权故意访问计算机系统的全部或任何部分的行为确定为其国内法中的刑事犯罪。缔约方可规定犯罪行为是通过违反安全措施意图获取计算机数据或实现其他不诚实意图而实施的，或者涉及与另一计算机系统相连的计算机系统。

第5条 干扰数据⁹

各缔约国均应采取必要的立法和其他措施，将未经授权故意破坏、删除、损坏、更改或抑制计算机数据的行为定为其国内法中的刑事犯罪。缔约方可保留规定条款所述行为造成严重损害的权利。

第6条 干扰系统¹⁰

各缔约国均应采取必要的立法和其他措施，将未经授权通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而故意严重妨碍计算机系统运行的行为定为其国内法中的刑事犯罪。

第7条 非法拦截¹¹

各缔约国均应采取必要的立法和其他措施，将未经授权故意实施的以技术手段拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据的行为定为其国内法中的刑事犯罪，包括载有这类计算机数据的计算机系统的电磁发射。缔约方可规定该罪行是以不诚实的意图而实施的，或者涉及与另一计算机系统相连的计算机系统。

⁸ 来源：《欧洲委员会网络犯罪公约》（《布达佩斯公约》）。

⁹ 来源：《欧洲委员会网络犯罪公约》。

¹⁰ 来源：《欧洲委员会网络犯罪公约》。

¹¹ 来源：《欧洲委员会网络犯罪公约》。

第 8 条

与计算机有关的欺诈¹²

各缔约国均应采取必要的立法和其他措施，将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其国内法中的刑事犯罪：

- (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，在无权的情况下为自己或他人获取经济利益。

第 9 条

非法获取密码和证书¹³

各缔约国均应采取必要的立法和其他措施，将未经授权而故意获取、获得或接收计算机系统的密码或访问证书的行为确定为其国内法中的刑事犯罪。

第 10 条

滥用设备¹⁴

1. 各缔约国均应采取必要的立法和其他措施，将下列未经授权而故意实施的行为确定为其国内法中的刑事犯罪：

- (a) 生产、销售、获取使用、进口、分销或以其他方式提供：
 - (i) 主要为实施按第 4 条至第 9 条所确立的任何犯罪而设计或改装的设备，包括计算机程序；
 - (ii) 计算机密码、访问代码或类似的数据，通过这些数据可以访问整个或部分计算机系统；

意图将其用于实施第 4 条至第 9 条所确立的任何罪行；以及

(b) 拥有上文第 1(a)(i)或(ii)款所述物品，意图将其用于实施第 4 条至第 9 条所确立的任何犯罪。缔约国可依法规定在承担刑事责任之前拥有若干此类物品。

2. 如果本条第 1 款所述的生产、销售、获取使用、进口、分销或以其他方式提供或拥有并非为了实施根据本公约第 4 条至第 9 条确立的犯罪，例如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)(ii)款所述物品的销售、分销或以其他方式提供。

¹² 来源：《欧洲委员会网络犯罪公约》。

¹³ 来源：巴西的原始提案。

¹⁴ 来源：《欧洲委员会网络犯罪公约》

第 11 条

与计算机有关的作假¹⁵

各缔约国均应采取必要的立法和其他措施，将未经授权故意输入、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其国内法中的刑事犯罪，而不论该数据是否可直接阅读和理解。缔约国可以规定在承担刑事责任之前存在欺诈或类似的不诚实意图。

第 12 条

与儿童色情制品有关的犯罪¹⁶

1. 各缔约国均应采取必要的立法和其他措施，将下列未经授权而故意实施的行为确定为其国内法中的刑事犯罪：

- (a) 为通过计算机系统分发目的而制作儿童色情制品；
- (b) 通过计算机系统提供儿童色情制品；
- (c) 通过计算机系统分发或传输儿童色情制品；
- (d) 通过计算机系统为自己或他人获取儿童色情制品；
- (e) 在计算机系统或计算机数据存储介质上拥有儿童色情制品。

2. 就上文第 1 款的目的而言，“儿童色情制品”一词应包括以视觉方式描绘下列内容的色情材料：

- (a) 未成年人参与露骨性行为；
- (b) 看似未成年人参与露骨性行为；
- (c) 显示未成年人参与露骨性行为的真实图像。

3. 就上文第 2 款的目的而言，“未成年人”一词应包括未满 18 岁的所有人员。不过，缔约国可规定一个较低的年龄限制，但不应低于 16 岁。

4. 各缔约国可保留全部或部分不适用第 1 款(d)和(e)项以及第 2 款(b)和(c)项的权利。

第 13 条

鼓励或胁迫自杀¹⁷

各缔约国均应采取必要的立法和其他措施，在其国内法中将以下行为规定为犯罪：在包括互联网在内的信息和电信网络中通过心理或其他压力鼓励或胁迫自杀，包括使未成年人自杀。

¹⁵ 来源：《欧洲委员会网络犯罪公约》。

¹⁶ 来源：《欧洲委员会网络犯罪公约》。

¹⁷ 来源：中国和俄罗斯联邦的提案。

第 14 条

利用信息和通信技术侵犯版权和相关权利¹⁸

各缔约国均应采取必要的立法和其他措施，在其本国法律中将以下行为规定为犯罪或其他非法行为：利用信息和通信技术故意实施的侵犯本国立法所界定的版权和相关权利的行为，包括非法使用受版权保护的计算机系统或数据库的软件以及盗用作者身份的行为。

第 15 条

未遂和协助或教唆¹⁹

1. 各缔约国均应采取必要的立法和其他措施，在其本国法律中将故意实施、协助或教唆实施根据公约第二章确定的任何犯罪的行为规定为刑事犯罪。
2. 各缔约国均应采取必要的立法和其他措施，在其本国法律中将故意实施根据公约第二章确定的任何犯罪未遂规定为刑事犯罪。
3. 各缔约国可保留全部或部分不适用本条第 2 款的权利。

第 16 条

法人责任²⁰

1. 各缔约国均应采取必要的立法和其他措施，以确保在基于下列权利在法人内部担任领导职务的任何自然人单独或作为该法人的一个机构的组成部分而实施根据本公约确立的刑事犯罪的情况下，可追究该法人的刑事犯罪责任。
 - (a) 该法人的代表权；
 - (b) 代表该法人作出决定的职权；
 - (c) 在该法人内部行使控制权的职权。
2. 除本条第 1 款已规定情况之外，各缔约国应采取必要措施确保，如果因第 1 款所述自然人缺乏监督或控制而使自然人在授权范围内行事时能够为法人利益实施根据本公约确立的刑事犯罪，则亦可对法人追究法律责任。
3. 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、民事责任或者行政责任。
4. 法人责任不应影响实施这种犯罪的自然人的刑事责任。

¹⁸ 来源：中国和俄罗斯联邦的提案。

¹⁹ 来源：《欧洲委员会网络犯罪公约》，巴西作了修改。

²⁰ 来源：《欧洲委员会网络犯罪公约》。

第 17 条

制裁和措施²¹

1. 各缔约国均应采取必要的立法和其他措施，以确保对根据公约第二章确立的刑事犯罪可处以有效、适度和劝阻性的制裁，包括剥夺自由。
2. 各缔约国均应当确保使依照第 16 条应当承担责任的法人被处以有效、适度和劝阻性的刑事或者非刑事制裁或措施，包括金钱制裁。

布隆迪

[原件：法文]

[2022 年 4 月 8 日]

第二章. 侵犯计算机数据和系统的保密性、完整性和可用性的犯罪

第 1 节

针对计算机系统保密性的行动

第 2 节

非法访问

本公约缔约国应将未经授权故意访问计算机系统的全部或任何部分的行为确定为其本国法中的刑事犯罪。

第 3 节

干扰计算机系统

本公约缔约国应将未经授权故意破坏、删除、损坏、更改或抑制计算机数据的行为定为其本国法中的刑事犯罪。

第 4 节

干扰数据

本公约缔约国应在不影响其本国法律的情况下，将未经授权通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而故意严重妨碍计算机系统运行的行为定为刑事犯罪。

第 5 节

非法制造、销售、购买、使用、进口、分销或拥有计算机系统和鼓励自杀

本公约缔约国应在不影响其本国法律的情况下，将为实施犯罪而制造、销售、购买、使用、进口、分销或拥有计算机或计算机系统，或提供计算机数据、程序或系统以便他人使用或获得的行为规定为刑事犯罪。

²¹ 来源：《欧洲委员会网络犯罪公约》。

第 6 条

与计算机有关的欺诈

本公约缔约国应在不影响其本国法律的情况下，将下述未经授权故意实施对他人财产造成损害的行为规定为刑事犯罪：(a)通过输入、更改、删除或抑制计算机数据，或(b)以任何形式干扰计算机系统的运行，意图欺诈或犯罪，以为本人或他人获取不正当的经济利益。

§1. 计算机系统中的欺诈

本公约缔约国应在不影响其本国法律的情况下，将下述行为规定为刑事犯罪：通过电子通信手段，使用欺诈手段，获取或企图获取他人的金钱、动产、债券、存款、票据、质押物、收据、弃权书或者全部或部分财产。

§2. 数字身份盗用

本公约缔约国应在不影响其本国法律的情况下，将下述行为规定为刑事犯罪：冒用他人的数字身份，或使用可识别该人身份的一项或多项任何种类的数据，以引起该人的不安，或损害其本人或第三方的名誉、隐私或财产，从而获取利益或误导他人。

§3. 网络钓鱼

本公约缔约国应在不影响其本国法律的情况下，将下述行为规定为刑事犯罪：使用网站或者借助计算机系统发送电子信息，意图从网站访问者或者电子信息接收人处获取机密信息，以便将该信息用于犯罪目的。

§4. 与计算机数据有关的失信

本公约缔约国应在不影响其本国法律的情况下，将下述行为规定为刑事犯罪：以某人将归还或将其用于特定目的为条件而盗用或散失委托他人保管的计算机数据。

§5. 非法接收计算机数据

本公约缔约国应在不影响其本国法律的情况下，将下述行为规定为刑事犯罪：以任何身份，在知晓通过犯罪手段获得的计算机数据是如何获得的情况下，持有该数据。

§6. 勒索计算机数据

本公约缔约国应在不影响其本国法律的情况下，将企图以武力、暴力或胁迫手段获取计算机数据的行为规定为刑事犯罪。

§7. 敲诈和发布谣言

本公约缔约国应在不影响其本国法律的情况下，将下述行为规定为刑事犯罪：以书面或口头进行威胁、发表揭露性或诽谤性言论或勒索或企图勒索计算机数据。

§8. 发送垃圾邮件

本公约缔约国应在不影响其本国法律的情况下，将下列行为规定为刑事犯罪：

1. 使用计算机或计算机系统重复发送未经请求的信息或向大量人员发送这种信息；
2. 使用计算机或计算机系统将接收到的信息转发给多人或将其多次重发给不需要它的人。

第 7 节

与内容有关的犯罪

§1. 与儿童色情有关的犯罪

本公约缔约国应在不影响其本国法律的情况下，将下列未经授权故意实施的行为规定为刑事犯罪：为通过计算机系统传播而制作儿童色情制品；通过计算机系统提供儿童色情制品。

第 8 节

通过计算机系统传播的种族主义或仇外文字和图像

本公约缔约国应在不影响其本国法律的情况下，将利用计算机系统制作、下载、传播或以任何形式提供具有种族主义或仇外性质的思想或理论的文字、信息、照片、图画、录像或任何其他表述的行为规定为刑事犯罪。

第 9 节

利用计算机系统实施的侮辱

本公约缔约国应在不影响其国内法的情况下，将以下行为定为刑事犯罪：以某人属于按种族、肤色、血统、民族或族裔出身或宗教区分的群体为理由对其进行侮辱，或以此作为这其中任何因素的借口，对按任何上述特点区分的群体进行侮辱。

第 10 节

在计算机或计算机系统帮助下实施的与恐怖主义、武器制造或贩运人口或毒品有关的犯罪

§1. 为恐怖主义集团创建或发布网站

本公约缔约国应在不影响其本国法律的情况下，将下列行为规定为刑事犯罪：

1. 借助互联网、计算机或计算机系统创建、发布或使用恐怖主义集团的网站，以便利其领导层或成员的交流；
2. 筹集资金或传播其关于如何开展恐怖主义行动的想法或知识。

§2. 传播破坏方法或手段

本公约缔约国应在不影响其本国法律的情况下，将下述行为规定为刑事犯罪：通过计算机系统向经授权的人员以外的人传播或提供枪支及其零部件和弹药的使用说明或制造方法，其性质足以对人的生命、财产或环境造成损害。

§3. 为贩运人口目的建立或发布网站

本公约缔约国应在不影响本国法律的情况下，将下述行为规定为刑事犯罪：在信息网络、计算机设备或计算机系统中建立或发布用于贩运人口或为此类交易提供便利的网站。

§4. 为贩运或分销毒品或麻醉品目的建立或发布网站

本公约缔约国应在不影响本国法律的情况下，将下述行为规定为刑事犯罪：在信息网络、计算机设备或计算机系统中建立或发布用于贩运或分销毒品或麻醉品或为此类交易提供便利的网站。

第 11 节

计算机相关犯罪团伙

本公约缔约国应在不影响其本国法律的情况下，将故意参与为筹备或实施一项或多项犯罪而组成的社团或形成的阴谋的行为规定为刑事犯罪。

第 12 节

与侵犯知识产权及相关权利有关的犯罪

本公约缔约国应在不影响其本国法律的情况下，将任何侵犯知识产权的行为规定为刑事犯罪。

第三章. 法人责任

本公约缔约国应作出必要的安排，以确保可追究法人对本公约所规定的犯罪的责任。

采取必要的措施，确保法人可以因为在该法人内部工作的自然人缺乏监督或控制而被追究责任。法人的责任可以是刑事、民事或行政责任。

加拿大

[原件：英文]
[2022 年 4 月 9 日]

犯罪

非法访问计算机系统

将以欺诈手段且未经授权访问整个计算机系统或其任何部分的行为定为刑事犯罪。

非法拦截非公用计算机系统的传输

将以下行为定为刑事犯罪：通过任何技术手段，以欺诈手段且未经授权拦截向计算机系统、从计算机系统和在计算机系统中非公开传输计算机数据，包括从携带此类数据的计算机系统中发出的电磁发射。

干扰计算机数据

将未经授权故意破坏、删除、损坏、更改或抑制计算机数据的行为定为刑事犯罪。

干扰计算机系统

将未经授权故意通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而严重妨碍计算机系统运行的行为定为刑事犯罪。

滥用设备

1. 将未经授权故意实施的下列行为定为刑事犯罪：

(a) 生产、销售、获取使用、进口、分销或以其他方式提供：

(i) 主要为实施本公约中所包含的任何网络犯罪而设计或改装的设备，包括计算机程序；

(ii) 计算机密码、访问代码或借由能够访问整个计算机系统或其任何部分的类似数据，意图将此用于实施本公约中所包含的任何网络犯罪；及

(b) 拥有第 1(a)(i)或(ii)款所述物品，意图将其用于实施本公约中所包含的任何网络犯罪。

2. 如果第 1 款所述物品的生产、销售、获取使用、进口、分销或以其他方式提供或拥有并非为了实施本公约中所包含的网络犯罪的目的，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。

与儿童性剥削有关的犯罪

1. 将未经授权故意实施的下列行为确立为刑事犯罪：
 - (a) 为通过计算机系统分发目的而制作儿童性剥削材料；
 - (b) 通过计算机系统宣传或提供儿童性剥削材料；
 - (c) 通过计算机系统分发或传送儿童性剥削材料；
 - (d) 通过计算机系统为自己或他人获取儿童性剥削材料；
 - (e) 在计算机系统或计算机数据存储介质中访问或拥有儿童性剥削材料。
2. 就第 1 款的目的而言，“儿童性剥削材料”一词包括《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》中所定义的儿童色情制品，以及任何：
 - (a) 描述以下内容的视觉材料，包括照片、视频和实时流媒体：
 - (i) 参与性活动或出现在性活动现场的儿童；
 - (ii) 看似儿童参与性活动或出现在性活动现场；
 - (iii) 表现儿童参与性活动或出现在性活动现场的真实图像；
 - (b) 具有下列特点的书面材料：
 - (i) 鼓动与儿童进行性活动；
 - (ii) 为性目的而编写，并以描述与儿童的性活动为主要特点；及
 - (c) 具有以下特点的录音：
 - (i) 鼓动与儿童进行性活动；
 - (ii) 为性目的而录制的，并以描述与儿童的性活动为主要特点。

诱拐和引诱儿童

1. 将未经授权故意实施的下列行为确立为刑事犯罪：
 - (a) 通过计算机系统向儿童或据信是儿童的人传输、分发、出售或提供露骨色情材料；
 - (b) 通过计算机系统与儿童或据信是儿童的人沟通；或者
 - (c) 通过计算机系统与儿童或据信是儿童的人达成协议或作出安排；

为实施本公约、《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》或缔约国国内法确立的任何儿童性剥削犯罪提供便利。
2. 如果一个人已采取合理步骤确定对方不是儿童，则不确立刑事责任。

未经同意传播私密图像（“报复性色情”）

1. 明知图像对象未同意或不顾该人是否同意，未经授权故意通过计算机系统发布、分发、传输、销售、提供或宣传某人的私密图像，应将此类行为定为刑事犯罪。
2. 就第 1 款的目的而言，私密图像指以任何方式，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，暴露其生殖器官、肛区或乳房，或进行露骨的性活动；
 - (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，在罪行实施时，图像对象仍带有合理的隐私期望。
3. 如果未经同意的分享是为了公共利益或具有合法目的，则不确立刑事责任。

哥伦比亚

[原件：西班牙文]

[2022 年 4 月 8 日]

3. 刑事定罪

关于依赖网络实施的犯罪，各会员国均应采取必要的立法和其他措施，在其国内法律制度中将下列行为规定为刑事犯罪：

- (a) 非法访问：未经授权访问计算机系统的全部或任何部分。²²
- (b) 非法拦截：未经授权拦截计算机数据，不论是在其源头或终点或者在计算机系统内，或是在载有此种数据的计算机系统的电磁发射中。²³
- (c) 干扰数据：对计算机数据或信息处理系统或其逻辑组件或部件的损害、破坏、删除、损坏、更改或抑制。²⁴
- (d) 干扰系统：在未经授权的情况下，阻碍计算机系统、其中包含的数据或电信网的运行或正常访问。²⁵
- (e) 滥用设备：为实施本节(a)、(b)、(c)和(d)款所述的任何罪行而生产、采购、拥有或分销或买卖某一设备，包括计算机程序以及计算机密码、访问代码或能够借由访问计算机系统的全部或任何部分的类似数据。²⁶

²² 关于网络犯罪的《布达佩斯公约》第 2 条。符合 2009 年第 1273 号法第 269A 条。

²³ 关于网络犯罪的《布达佩斯公约》第 3 条。符合 2009 年第 1273 号法第 269C 条。

²⁴ 关于网络犯罪的《布达佩斯公约》第 4 条。符合 2009 年第 1273 号法第 269D 条。

²⁵ 关于网络犯罪的《布达佩斯公约》第 5 条。符合 2009 年第 1273 号法第 269B 条。

²⁶ 关于网络犯罪的《布达佩斯公约》第 6 条。

(f) 与计算机有关的伪造：未经授权故意输入、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。²⁷

关于借助网络实施的犯罪，各会员国均应采取必要的立法和其他措施，在其国内法律制度中将下列行为规定为刑事犯罪：

(a) 与儿童性虐待材料有关的犯罪：通过计算机系统制作、提供、分发、传输或采购儿童性虐待材料，或在计算机系统中拥有此类材料。²⁸

(b) 与计算机有关的欺诈：输入、更改、删除或抑制计算机数据，或干扰计算机系统的运行，意图欺诈或犯罪，在未经授权的情况下为自己或他人获取经济利益，从而损害他人的财产。²⁹

(c) 侵犯个人数据：未经授权获取、汇编、删除、提供、出售、交换、发送、购买、拦截、披露、修改或使用文件、档案、数据库或类似介质中的个人数据，以为个人或第三方获取利益。³⁰

自然人以及对法人的金钱制裁。³¹

埃及

[原件：阿拉伯文]

[2022 年 4 月 8 日]

第二章. 刑事定罪、刑事诉讼和执法

第 5 条

刑事定罪

1. 各缔约国均应采取必要的立法措施和其他措施，预防和侦查利用信息和通信技术实施本公约所列犯罪或任何其他犯罪，包括屏蔽和删除与这类犯罪有关的内容、起诉这类犯罪的行为人、引渡犯罪人、促进国际合作程序和收集与这类犯罪有关的证据，同时肯定技术中立原则的重要性。

2. 各缔约国还应采取必要的立法和其他措施将下列行为规定为刑事犯罪：

第 6 条

非法使用或便利非法使用通信和信息服务及技术

通过信息网络或者信息和通信技术，非法使用或者便利他人使用通信服务或者音视频广播频道。

²⁷ 关于网络犯罪的《布达佩斯公约》第 7 条。

²⁸ 关于网络犯罪的《布达佩斯公约》第 9 条。

²⁹ 关于网络犯罪的《布达佩斯公约》第 8 条。

³⁰ 2009 年第 1773 号法第 269F 条。

³¹ 关于网络犯罪的《布达佩斯公约》第 13 条。符合《联合国反腐败公约》第三十条和《联合国打击跨国组织犯罪公约》第十一条。

第 7 条

非法访问和（或）超越访问权限

1. 一个人超过授予其访问网站、私人账户或信息系统的权利的时间限制或访问级别限制。
2. 非法获取、存在于或接触全部或部分信息技术或使其永久化。
3. 如果这种获取、存在、接触或永久化造成下列后果，应加重处罚：
 - (a) 删除、修改、歪曲、复制、转移或销毁保存的数据、电子设备或系统或通信网络，或对用户和受益人造成损害；
 - (b) 获取政府机密信息。

第 8 条

攻击网站设计

非法损坏、扰乱、减缓、扭曲、隐藏或修改公司、机构、组织或自然人的网站设计。

第 9 条

非法拦截

通过任何技术手段对数据流进行有意的、非法的拦截，或中断信息技术数据的传输或接收。

第 10 条

攻击数据完整性

故意非法破坏、删除、妨碍、修改或阻断信息技术数据。

第 11 条

滥用信息技术

生产、销售、购买、进口、分销、提供或拥有任何经设计或改装的工具或软件、密码或借由访问信息系统的类似信息，意图利用其实施本公约所述犯罪，或者创建恶意软件，旨在毁坏、屏蔽、修改、复制或传播数字信息或使数字信息的安全功能失效，但合法研究除外。

第 12 条

伪造

使用信息技术改变数据的实质，意图将数据作为有效数据使用，并造成损害。

第 13 条

欺诈

故意非法地对受益人和用户造成伤害，意图欺诈，以非法方式为行为人或其他人实现利益和好处，包括通过与虚拟货币(数字货币或加密货币)有关的欺诈性电子犯罪。

第 14 条

威胁和勒索

使用信息和通信技术或任何其他技术手段，威胁或勒索某人实施某项行为或不实施某项行为。

第 15 条

色情制品

1. 违反各国的国内法，通过信息和通信技术制作、展示、分发、提供、出版、购买、销售或进口色情材料，意图使妇女或未成年人卖淫或对其进行剥削。
2. 在信息和通信技术或信息和通信技术存储介质上制作、展示、分发、提供、出版、购买、销售或进口描绘儿童或未成年人的色情材料，包括拥有被视为淫秽的描绘儿童或未成年人的材料。

第 16 条

与色情制品有关的其他犯罪

性剥削或性骚扰，尤指针对妇女、儿童或未成年人。

第 17 条

鼓励或胁迫自杀

借助信息和通信网络，包括互联网，无论是通过直接互动还是通过现代技术和电子游戏，施加心理或其他压力，鼓励或胁迫包括未成年人在内的人自杀。

第 18 条

未成年人参与实施非法行为

未成年人通过信息和通信技术参与实施危害其生命或身心健康的非法行为。

第 19 条

侵犯隐私

利用信息和通信技术侵犯隐私，包括创建电子邮件、网站或私人账户，并谎称其归为某自然人或法人。

第 20 条

利用信息技术实施的与恐怖主义有关的犯罪

1. 传播、宣传恐怖主义集团思想和原则或为其辩护。
2. 资助或训练恐怖主义行为、便利恐怖主义组织之间的联系或向恐怖主义行为的实施者提供后勤支持。
3. 传播制造爆炸物的方法，特别是用于恐怖主义行为的。
4. 散播冲突、煽动叛乱、仇恨或种族主义。
5. 各国应采取必要措施，通过信息和通信技术防止传播此类内容，包括屏蔽或删除与这些犯罪有关的内容。

第 21 条

包括洗钱在内的金融犯罪

1. 利用信息和通信技术实施金融犯罪，或滥用虚拟货币（数字货币和加密货币）。
2. 进行洗钱活动，请求协助进行洗钱活动，或公布洗钱方法。

第 22 条

非法使用电子支付工具

1. 伪造、捏造或安装任何有助于以任何方式伪造或仿造任何电子支付工具的装置或材料。
2. 挪用、使用或向他人提供任何支付工具的数据，或为他人获取此类数据提供便利。
3. 利用信息网络或信息技术，未经授权获取任何支付工具的号码或数据。
4. 明知是伪造的支付工具而接受改工具。

第 23 条

利用信息技术实施的与有组织或跨国犯罪有关的罪行

1. 推销或贩运麻醉药品或精神药物。
2. 非法分销假冒药品或医疗产品。
3. 偷运移民。
4. 非法贩运人口或人体器官。
5. 非法武器贸易。
6. 非法贩运文化财产。

第 24 条

与侵犯版权及相关权利有关的犯罪

侵犯缔约国法律规定的版权或相关权利，如果侵权行为是故意的。

第 25 条

未经授权访问关键信息基础设施

1. 创建、散播或使用旨在提供对关键信息基础设施的未经授权访问的软件或其他数字信息，包括毁坏、阻断、修改或复制其中所含信息或使其安全功能失效。
2. 违反为存储、处理或传送缔约国国内法所规定关键信息基础设施或信息系统、属于关键信息基础设施的信息和通信网络或对其进行访问的手段中存在的受保护数字信息而制定的媒体使用规则，如果此违反行为损害了关键信息基础设施。

第 26 条

煽动颠覆或武装活动或其他刑事犯罪

通过信息和通信技术发出呼吁，鼓吹针对另一国政权的破坏或武装活动，破坏公共安全和稳定；或犯下可判处至少一年监禁的刑事犯罪。

第 27 条

与极端主义有关的犯罪

利用信息和通信技术或宣传、辩解或提供获取信息和通信技术的途径，传播煽动具有政治、意识形态、社会或族裔动机的非法行为或任何其他鼓吹族裔或宗教仇恨或一般敌意的非法行为的材料。

第 28 条实施或参与实施犯罪未遂

实施公约所列刑事犯罪或实施未遂，和（或）作为共犯参与公约所列刑事犯罪，和（或）组织或指挥他人实施公约所列刑事犯罪。

第 29 条

其他非法行为

本公约不应妨碍缔约国将通过信息和通信技术故意实施的任何其他非法行为规定为刑事犯罪。

第 30 条

法人责任

1. 各缔约国应承诺在不违反其本国法律的情况下，规范法人对其代表以其名义或为其利益实施的犯罪所承担的刑事责任，但不影响对实施犯罪的自然人，包括网站管理人的惩罚。

2. 在不妨碍本公约规定的情况下，服务提供者/网站管理人及其关联人员应遵守以下义务，违反这些义务应被视为犯罪：

(a) 在信息系统日志或信息技术日志中保存和存储下列数据，保存期限为（待定）：

- 能够识别服务用户的数据
- 与在信息系统中处理的内容有关的数据，当这些数据在服务提供者的控制之下时
- 与通信量有关的数据
- 与通信外围设备有关的数据
- 国家为执行本公约而规定的任何其他数据。

(b) 对已保存和存储的数据保密，并禁止在未经主管机关合理命令的情况下披露此类数据，包括其任何服务用户的个人数据、与其用户以及同其用户有通信联系的个人或实体访问的网站和私人账户有关的任何数据或信息；

(c) 确保数据和信息的安全，以保持其机密性并保护数据和信息不被渗透或损坏的方式；

(d) 向其服务的用户和任何主管当局提供对下列数据和信息的方便、直接和持续的访问：

- 服务提供者的名称和地址
- 服务提供者的联系信息，包括其电子邮件地址
- 对服务提供者及监督服务提供者的主管机关予以确定的许可证数据

(e) 应国家指定的主管当局的要求，提供使此类当局能够行使其权力所需的所有技术能力。

萨尔瓦多

[原件：西班牙文]

[2022年4月12日]

关于刑事定罪的规定

各国应采取适当的立法和其他措施，在其本国法中将下列行为定为刑事犯罪，在考虑到受害者人数和所造成损害的程度的情况下，施加刑事和其他制裁，包括监禁：

非法访问

未经适当授权，故意访问计算机系统的全部或任何部分。这不适用于合法和可核查的经授权测试或调查活动，只要它们不造成严重的间接损害。

非法拦截

在未经适当授权的情况下，故意无权实施的以技术手段拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据，包括载有这类计算机数据的计算机系统的电磁发射。

干扰数据

在未经适当授权的情况下，故意无权破坏、删除、损坏、更改或抑制计算机数据。

干扰计算机系统

未经授权故意通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而严重妨碍计算机系统运行。

滥用设备

故意未经授权生产、销售、获取使用、进口、分销或提供主要为实施本公约所列任何犯罪而设计或改装的任何设备，包括计算机程序；或密码、访问代码或借由能够访问整个计算机系统或其任何部分的类似数据，意图实施本公约所确立的任何犯罪。这不适用于合法和可核查的经授权测试或调查活动，只要它们不造成严重的间接损害。

与计算机有关的伪造

未经授权故意输入、更改、删除或抑制计算机数据，造成不真实的数据，不论该数据是否可直接阅读和理解。要求有欺诈意图或类似的不诚实意图，才可追究刑事责任。

利用信息和通信技术实施的欺诈

故意未经授权通过输入、更改、删除或抑制计算机数据或者干扰计算机系统的运行，以欺诈或不诚实的意图为自己或他人获取经济利益，从而对他人财产造成损害的行为。

与含有虐待儿童内容的材料相关的犯罪

故意未经授权实施以下行为：制作、复制、分发、出版、进口、出口、提供、资助、销售、营销、传播或在任何类型的技术设备或介质上拥有此类内容。

侵犯知识产权及相关权利

有预谋地通过使用信息和通信技术实施的侵犯缔约国立法所界定的知识产权和相关权利的行为，包括非法使用受版权保护的计算机程序和数据库，以及剽窃。

协助或教唆及未遂

作为共犯、协助者或教唆者或者以任何其他身份参与犯罪；实施根据本公约确立的犯罪的任何未遂或准备。

责任

各缔约国均应采取符合本国法律原则的必要措施，以确保因参与法人内部担任领导职务的任何自然人单独或作为该法人的一个机构的组成部分为法人利益实施的根据本公约确立的犯罪，而追究该法人的责任，其中自然人的权力基于：该法人的代表权；代表该法人作出决定的职权；在该法人内部行使控制权的职权。

除前款已规定情况之外，各缔约国应采取必要措施，确保如果因前款所述自然人缺乏监督或控制而使自然人在授权范围内行事时能够为法人利益实施本公约所规定的犯罪，则亦可对该法人追究责任。

在不违反缔约国法律原则的情况下，此类责任可以是刑事责任、民事责任或者行政责任。此类责任不应影响实施这种犯罪的自然人的刑事责任。

各缔约国均应当特别确保使依照本公约应当承担责任的法人受到有效、适度和劝阻性的刑事或者非刑事制裁，包括金钱制裁。

起诉、审判和制裁

各缔约国均应当使实施根据本公约条款确立的犯罪受到与其严重性相当的制裁。

为因本公约所涵盖的犯罪起诉某人而行使本国法律规定的法律裁量权时，各缔约国均应努力确保针对这些犯罪的执法措施取得最大成效，并适当考虑到震慑此种犯罪的必要性。

就根据本公约条款确立的犯罪而言，各缔约国均应当根据本国法律并在适当尊重辩护方权利的情况下采取适当措施，力求确保关于保外候审或者上诉的裁决所规定的条件已经考虑到确保被告人在其后的刑事诉讼中出庭的需要。

各缔约国均应确保其法院和其他主管当局在考虑早释或假释已被判定犯有本公约所涵盖的犯罪者的可能性时，顾及此种犯罪的严重性。

各缔约国均应在适当情况下在其本国法律中对于本公约所涵盖的任何犯罪规定一个较长的追诉时效期限，并在被指控犯罪的人逃避司法处置时规定更长的期限。

本公约的任何规定概不影响下述原则：对于根据本公约确立的犯罪以及适用的法律例外或者决定行为合法性的其他法律原则，只应当由缔约国本国法律加以阐明，而且对于这种犯罪应当根据缔约国本国法律予以起诉和惩罚。

洗刷通过利用信息和通信技术实施犯罪的所得

各缔约国均应当根据本国法律的基本原则，采取必要的立法和其他措施，将故意实施的下列行为定为刑事犯罪：

(a) 明知财产为犯罪所得，为隐瞒或者掩饰该财产的非来源，或者为协助任何参与实施上游犯罪者逃避其行为的法律后果而转换或者转移该财产；

(b) 明知财产为犯罪所得而隐瞒或者掩饰该财产的真实性质、来源、位置、处置、转移、所有权或与之有关的权利；

(c) 在得到财产时，明知其为犯罪所得而仍获取、占有或者使用；

(d) 对本公约所确立的任何犯罪的参与、协同或者共谋实施、实施未遂以及协助、教唆、便利和参谋实施。

为实施或适用本款的规定，各缔约国均应努力：

(a) 将本款的规定适用于范围最为广泛的上游犯罪；

(b) 将根据本公约条款确立的犯罪列为上游犯罪。缔约国立法中如果列出具体上游犯罪清单，则至少应在这类清单中列出与有组织犯罪集团有关的范围全面的各种犯罪；

(c) 就(b)项的目的而言，上游犯罪应包括在有关缔约国司法管辖权范围之内和之外发生的犯罪。然而，如果犯罪发生在一缔约国司法管辖权范围之外，则只有当该行为根据其发生地所在国法律为刑事犯罪，而且根据实施或者适用本条的缔约国的法律该行为若发生在该国也为刑事犯罪时，才构成上游犯罪；

(d) 各缔约国均应当向联合国秘书长提供其实施本条的法律以及这类法律随后的任何修改的副本或说明。

妨碍司法

各缔约国均应采取必要的立法和其他措施，将下列故意实施的行为确定刑事犯罪：

(a) 在涉及本公约所涵盖的犯罪的诉讼中使用暴力、威胁或恐吓，或许诺、提议给予或给予不正当好处，以诱使提供虚假证言或干扰证言或证据的提供；

(b) 使用暴力、威胁或恐吓，干扰司法或执法人员针对本公约所涵盖的犯罪执行公务。本项中的规定概不应影响缔约国制定保护其他类别公职人员的立法的权利。

管辖权

各缔约国应采取必要的措施，在下列情况下确立其对根据本公约确立的犯罪的管辖权：

- (a) 犯罪发生在该缔约国的领域内；
- (b) 犯罪发生在当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。

在下列情况下，缔约国也可以确立对任何这些犯罪的管辖权：

- (a) 犯罪系针对该缔约国的国民；
- (b) 犯罪者为该缔约国的国民或在该国境内有惯常居所的无国籍人；
- (c) 犯罪系针对某缔约国。

各缔约国均应采取必要的措施，在被指控犯罪人在其领域内而其仅因该人为本国国民而不予引渡时，确立本国对根据本公约确立的犯罪的管辖权。

如果根据前款行使其管辖权的缔约国被告知或者通过其他途径获悉另一缔约国正在对同一行为进行侦查、起诉或者审判程序，这些缔约国的主管机关应当酌情相互磋商，以便协调行动。

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根据其国内法确立的任何刑事管辖权。

欧洲联盟及其成员国

[原件：英文]

[2022年4月6日]

第二章

刑事定罪和执法

第5条

非法访问

1. 各缔约国均应采取必要的立法和其他措施，将违反安全措施而未经授权故意访问计算机系统的全部或任何部分的行为确定为刑事犯罪。
2. 缔约国可规定犯罪行为的实施是意图获取计算机数据或实现其他不诚实意图，或者涉及与另一计算机系统相连的计算机系统。

第6条

非法拦截

1. 各缔约国均应采取必要的立法和其他措施，将故意实施的以技术手段无权拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据的行为规定为刑事犯罪，包括来自载有这类计算机数据的计算机系统的电磁发射。

2. 缔约国可规定该罪行是以不诚实的意图实施的，或与另一计算机系统相连的计算机系统有关。

第 7 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，将未经授权故意破坏、删除、损坏、更改或抑制计算机数据的行为定为刑事犯罪。
2. 缔约国可规定第 1 款所述行为造成严重损害。

第 8 条

非法干扰系统

各缔约国均应采取可能必要的立法和其他措施，将故意实施的通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而未经授权严重妨碍计算机系统运行的行为规定为刑事犯罪。

第 9 条

滥用设备

1. 各缔约国均应采取必要的立法和其他措施，将下列未经授权故意实施的行为确定刑事犯罪：
 - (a) 生产、销售、获取使用、进口、分销或以其他方式提供：
 - (i) 主要为实施本公约第 5 条至第 8 条所确立的任何犯罪而设计或改装的设备，包括计算机程序；
 - (ii) 计算机密码、访问代码或类似的数据，通过这些数据可以访问整个或部分计算机系统；
 意图将其用于实施本公约第 5 条至第 8 条所确立的任何罪行；及
 - (b) 拥有上文第 1(a)(i)或(ii)款所述物品，意图将其用于实施本公约第 5 条至第 8 条所确立的任何犯罪。缔约国可规定在承担刑事责任之前占有若干此类物品。
2. 如果本条第 1 款所述的生产、销售、获取使用、进口、分销或以其他方式提供或拥有并非为了实施根据本公约第 5 条至第 8 条确立的犯罪，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. 各缔约国可不适用本条第 1 款，只要不涉及本条第 1a.ii 款所述物品的销售、分销或以其他方式提供。

第 10 条

未遂及协助与教唆

1. 各缔约国均应采取必要的立法和其他措施，将故意实施、协助或教唆实施本公约第 5 条至第 9 条确定的任何犯罪行为规定为刑事犯罪。

2. 各缔约国均应采取必要的立法和其他措施，将故意实施本公约第 5 条至第 9 条确定的任何犯罪未遂规定为刑事犯罪。

第 11 条

法人责任

1. 各缔约国均应当采取符合其法律原则的必要立法和其他措施，确保可以因根据本公约第 5 条至第 10 条确立的刑事犯罪追究法人的责任。

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、民事责任或者行政责任。

3. 法人责任不应影响实施这种犯罪的自然人的刑事责任。

第 12 条

起诉、审判和制裁

1. 各缔约国均应使实施根据本公约第 5 条至第 10 条确立的犯罪的自然人和法人受到有效、适度和劝阻性制裁。

2. 为因本公约所涵盖的犯罪起诉某人而行使本国法律规定的任何法律裁量权时，各缔约国均应努力确保针对这些犯罪的执法措施取得最大成效，并适当考虑到震慑此种犯罪的必要性。

3. 各缔约国均应建立和保持有效的、以法治为基础的国家刑事司法系统，以确保任何因本公约所涵盖的犯罪而被起诉的人都被绳之以法，同时确保充分保护人权和基本自由，包括公正审判权和辩护方的权利。

加纳

[原件：英文]

[2022 年 4 月 12 日]

第二章. 关于刑事定罪的规定³²

依赖网络实施的犯罪：侵犯计算机系统和数据保密性、完整性和可用性的犯罪行为

第 5 条

未经授权访问计算机系统

各缔约国应采取必要的立法和其他措施，将故意实施的以下行为定为刑事犯罪：未经授权或超过授权访问整个计算机系统或其任何部分。缔约国可规定犯罪行为的实施是通过违反安全措施而意图获取计算机数据或实现其他不诚实意图，或者涉及与另一计算机系统相连的计算机系统。

³² 本节的案文主要摘自《欧洲委员会网络犯罪公约》、《非洲联盟网络安全和个人数据保护公约》、《2008 年电子交易法》（第 772 号法）和《2020 年网络安全法》（第 1038 号法）。这些文书构成了加纳的网络犯罪立法框架。

第 6 条

未经授权访问关键信息基础设施

各缔约国应采取必要的立法和其他措施，将故意实施的以下行为定为刑事犯罪：未经授权进入整个关键信息基础设施或其任何部分。

第 7 条

未经授权拦截

各缔约国均应采取必要的立法和其他措施，在其国内法中将故意实施的以技术手段未经授权拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据的行为规定为刑事犯罪，包括来自载有这类计算机数据的计算机系统的电磁发射。

缔约国可规定该罪行是以不诚实的意图实施的，或与另一计算机系统相连的计算机系统有关。

第 8 条

干扰数据

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意破坏、删除、损坏、更改、复制或抑制计算机数据的行为定为其国内法中的刑事犯罪。
2. 缔约国可保留对第 1 款所述行为造成严重损害作出规定的权利。

第 9 条

干扰系统

各缔约国均应采取必要的立法和其他措施，将通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而未经授权故意严重妨碍计算机系统运行的行为定为其国内法中的刑事犯罪。

第 10 条

滥用设备

1. 各缔约国均应采取必要的立法和其他措施，将下列未经授权而故意实施的行为确定为其国内法中的刑事犯罪：
 - (a) 生产、销售、获取使用、进口、分销或以其他方式提供：
 - (i) 主要为实施按第 5 条至第 9 条确立的任何犯罪而设计或改装的设备，包括计算机程序；
 - (ii) 计算机密码、访问代码或借由能够访问整个计算机系统或其任何部分的类似数据，意图将其用于实施第 5 条至第 9 条所确立的任何犯罪；及
 - (b) 拥有上文第 1(a)(i)或(ii)款所述物品，意图将其用于实施第 5 条至第 9 条所确立的任何犯罪。缔约国可依法规定在承担刑事责任之前拥有若干此类物品。

2. 如果本条第 1 款所述的生产、销售、获取使用、进口、分销或以其他方式提供或拥有并非为了实施根据本公约第 5 条至第 9 条确立的犯罪，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)(ii)款所述物品的销售、分销或以其他方式提供。

借助网络实施的犯罪：由于计算机系统的出现，其范围、速度和影响都有所增加的犯罪³³

第 11 条

与计算机有关的伪造

各缔约国均应采取必要的立法和其他措施，将以下行为定为其国内法中的刑事犯罪：未经授权故意输入、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，而不论该数据是否可直接阅读和理解。缔约国可规定在承担刑事责任之前存在欺诈意图或类似的不诚实意图。

第 12 条

与计算机有关的欺诈

各缔约国均应采取必要的立法和其他措施，在其国内法中将通过以下方式未经授权故意造成他人财产损失的行为确定为刑事犯罪：

- (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，未经授权为自己或他人获取经济利益。

针对儿童的犯罪

第 13 条

与网上性剥削和性虐待儿童有关的犯罪

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意实施的下列行为确定为其国内法中的刑事犯罪：

- (a) 为通过计算机系统发布和分发目的而制作儿童性剥削和性虐待材料；
- (b) 为自己或他人获取儿童性剥削和性虐待材料；
- (c) 通过计算机系统或电子设备提供儿童性剥削和性虐待材料；
- (d) 通过计算机或电子设备发布、分发、流播（包括直播）、传输儿童性剥削和性虐待材料或；

³³ 与计算机有关的欺诈、伪造和针对儿童的犯罪符合《欧洲委员会网络犯罪公约》、《非洲联盟网络安全和个人数据保护公约》和《2020 年网络安全法》（第 1038 号法）。

(e) 在计算机系统或在计算机上或在电子记录存储介质中拥有儿童性剥削和性虐待材料。

2. 就第(1)分节(c)项的目的而言，如果某人实施下列行为，则该人就是发布儿童性剥削和性虐待材料：

- (a) 将其拥有的儿童性剥削和性虐待材料出售给他人；或者
- (b) 暴露或提供儿童性剥削和性虐待材料以供他人获取。

3. 就本节的目的而言，儿童性剥削和性虐待材料包括描绘或描述以下内容的实体图像、视觉记录、视频、音频、实时流媒体材料、绘图或文本：

- (a) 儿童参与露骨或暗示性行为；
- (b) 貌似儿童的人参与露骨或暗示性行为；
- (c) 表现儿童参与露骨或暗示性行为的图像；
- (d) 儿童露骨性图像；
- (e) 实时观看儿童性剥削和性虐待的过程或材料，往往涉及引导虐待的罪犯；
- (f) 任何鼓动或劝告与儿童进行非法性活动的书面材料、视觉表现或音频记录；
- (g) 任何其主要特征是描述为性目的而与儿童进行非法性活动的书面材料；
- (h) 任何其主要特征是描述为性目的而与儿童进行非法性活动的音频记录。

第 14 条

为性虐待而与儿童打交道

各缔约国均应采取必要的立法和其他措施，将故意使用下列手段而实施的行为确定为其国内法中的刑事犯罪：

- (a) 计算机在线服务；
- (b) 互联网服务；
- (c) 本地公告栏服务；或者
- (d) 能够进行电子数据存储或传输的任何其他设备；

诱惑、招揽、引诱、诱拐或怂恿，或企图诱惑、招揽、引诱、诱拐或怂恿儿童或其认为是儿童的人，以方便、鼓励、提供或招揽任何儿童进行非法性行为或与任何儿童进行非法性行为，或对这种行为的视觉描述。

第 15 条

对儿童的网络跟踪

各缔约国应采取必要的立法和其他措施，在其国内法中将下述故意实施的行为定为刑事犯罪：使用计算机在线服务、互联网服务或当地互联网公告栏服务或任何其他电子设备，以汇编、传送、发布、复制、购买、出售、接收、交换或传播儿童的姓名、电话号码、电子邮件地址、居住地址、照片、身体描述、特征或任何其他可识别儿童身份的信息，推动安排与儿童会面以进行性交、露骨性行为或非法性活动。

其他网上性犯罪³⁴

第 16 条

性勒索

1. 各缔约国均应采取必要的立法和其他措施，在其国内法中将下述故意实施的行为确定为刑事犯罪：威胁以邮寄、电子邮件、文本分发或者以电子手段或其他方式传输参与露骨性行为的他人的私人图像或动态图像，其具体意图是：

(a) 骚扰、威胁、胁迫、恐吓或对该人施加任何不正当影响，特别是为了勒索金钱或其他报酬，或强迫受害人参与违背其意愿的性活动；或者

(b) 实际勒索金钱或其他报酬，或强迫受害人参与违背其意愿的性活动。

2. 各缔约国应采取必要的立法和其他措施，在其国内法中将下述故意实施的行为确定为刑事犯罪：威胁以邮寄、电子邮件、文本分发或者以电子手段或其他方式传输参与露骨性行为的儿童的私人图像或动态图像，其具体意图是

(a) 骚扰、威胁、胁迫、恐吓或对儿童施加任何不正当影响，特别是为了勒索金钱或其他报酬，或强迫受害人参与违背其意愿的性活动；或者

(b) 实际勒索金钱或其他报酬，或强迫受害人参与违背其意愿的性活动。

3. 就第 1 和 2 款的目的而言，私密图像可包括对他人的生殖器或肛区裸露或仅有内衣覆盖的描绘；或者对未被覆盖或透过衣物清晰可见的乳晕顶部以下乳房的描绘。

第 17 条

未经同意分享私密图像

1. 各缔约国应采取必要的立法和其他措施，在其国内法中将以下行为定为刑事犯罪：未经私密图像中所描绘的人的同意，故意传播或故意促使他人传播另一个可识别身份的人的私密图像或被禁止的视频记录，意图造成严重的精神痛苦，并且在制作图像或录像时和（或）在犯罪时有理由期望得到隐私。

2. 在本节中，“严重的精神痛苦”包括任何导致精神反应以及身体疼痛的故意行为，精神反应包括恐惧、紧张、悲伤、焦虑、担忧、屈辱、震惊、羞辱和侮辱。

³⁴ 与《网络安全法》的规定一致。

第 18 条

威胁传播被禁止的私密图像或视频记录

各缔约国应采取可能必要的立法和其他措施，在其国内法中将下述故意实施的行为定为刑事犯罪：以一种会导致对方在所有情况下合理产生痛苦的方式，威胁传播他人被禁止的亲密图像或视频记录，并且威胁的方式会导致对方在所有情况下合理地产生对正在实施的威胁的恐惧。

第 19 条

与侵犯版权及相关权利有关的犯罪³⁵

1. 各缔约国应采取必要的立法和其他措施，根据其按照《保护文学和艺术作品伯尔尼公约》1971 年 7 月 24 日巴黎文本、《与贸易有关的知识产权协定》和《世界知识产权组织（知识产权组织）版权条约》所承担的义务，在其国内法中将故意以商业规模并借助计算机系统实施的侵犯该缔约国法律所界定的版权的行为定为刑事犯罪，但上述公约等文书所赋予的任何精神权利除外。
2. 各缔约国应采取必要的立法和其他措施，根据其在《保护表演者、唱片制作者和广播组织的国际公约》（《罗马公约》）、《与贸易有关的知识产权协定》和《世界知识产权组织表演和录音制品条约》下所承担的义务，在其国内法中将故意以商业规模并借助计算机系统实施的侵犯该缔约国法律所界定的相关权利的行为定为刑事犯罪，但上述公约等文书所赋予的任何精神权利除外。
3. 缔约国可保留在有限的情况下不根据本条第 1 款和第 2 款追究刑事责任的权利，但须有其他有效的补救措施可用，而且此种保留不减损本条第 1 款和第 2 款所述国际文书中规定的缔约国的国际义务。

第 20 条

未遂和协助或教唆

1. 各缔约国均应采取必要的立法和其他措施，在本国法律中将故意协助或教唆实施根据本公约第 5 条至第 19 条确立的任何犯罪行为规定为蓄意犯下该罪行的刑事犯罪。
2. 各缔约国均应采取必要的立法和其他措施，在其本国法律中将故意实施根据第 7 条至第 9 条、第 11 条、第 12 条、第 13 条第 1(a)、(b)和(e)款、第 14 条、第 15 条、第 16 条和第 17 条确立的任何犯罪的未遂规定为刑事犯罪。

第 21 条

法人责任

1. 各缔约国均应采取必要的立法和其他措施，以确保可以因法人内部担任领导职务的任何自然人单独或作为该法人的一个机构的组成部分为法人利益实施的根据本公约确立的刑事犯罪而追究该法人的责任，其中自然人的权力基于：

³⁵ 与《欧洲委员会网络犯罪公约》和《非洲联盟网络安全和个人数据保护公约》一致。

- (a) 该法人的代表权；
 - (b) 代表该法人作出决定的职权；
 - (c) 在该法人内部行使控制权的职权。
2. 除本条第 1 款已规定情况之外，各缔约国均应采取必要措施确保，如果因第 1 款所述自然人缺乏监督或控制而使自然人在授权范围内行事时能够为法人利益实施根据本公约确立的刑事犯罪，则亦可对法人追究责任。
 3. 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、民事责任或者行政责任。
 4. 法人责任不应当影响实施这种犯罪的自然人的刑事责任。

第 22 条

制裁和措施

1. 各缔约国均应采取必要的立法和其他措施，以确保对根据第 5 条至第 20 条确立的刑事犯罪可处以有效、适度和劝阻性的制裁，包括剥夺自由。
2. 各缔约国均应当确保使依照第 21 条应当承担责任的法人被处以有效、适度和劝阻性的刑事或者非刑事制裁或措施，包括金钱制裁。

伊朗伊斯兰共和国

[原件：英文]

[2022 年 4 月 8 日]

2. 刑事定罪

越来越多的情况是，犯罪分子不仅针对信通技术设备，而且还通过这些设备组织和实施非法活动。尽管通过滥用信通技术实施的犯罪行为可被定为犯罪，反之亦然，但在某些情况下，犯罪的严重性和其他因素要求将通过使用信通技术实施的非法行为定为刑事犯罪。当信通技术的使用加剧了犯罪行为，特别加剧了对受害者造成的伤害程度时，情况尤其如此。因此，除了依赖信通技术实施的犯罪外，公约还应将通过这些技术实施的犯罪定为刑事犯罪。然而，从法律角度看，这可能需要采取逐案办法，因为各种形式的犯罪可能反映出不同的要素以及犯罪行为和犯罪意图。在采取确定罪行的措施时，应适当考虑到国内法律制度的基本原则。

还应规定法人的责任，以确保对犯罪活动作出全面应对，并剥夺犯罪者在法律实体的掩护下的行动自由。这类措施应使法人对故意或以其他方式知情地参与实施根据公约确立的犯罪承担责任。

日本

[原件：英文]
[2022 年 4 月 8 日]

1. 刑事定罪**1.1. 依赖网络实施的犯罪**

1.1.1. 日本认识到，特设委员会在对依赖网络实施的犯罪进行刑事定罪方面存在普遍共识，主要包括侵犯计算机数据和系统的保密性、完整性和可用性的犯罪。基于这一认识，日本支持将依赖网络实施的犯罪定为刑事犯罪。

1.1.2. 我们认为，为应对当今各会员国重视的挑战而需要被定为刑事犯罪的许多行为，如勒索软件攻击和对关键基础设施的计算机系统的攻击，都属于依赖网络实施的犯罪的范围。这种依赖网络实施的犯罪可能包括非法访问、非法拦截、干扰计算机数据或计算机系统以及滥用设备等。

1.1.3. 日本认识到，必须对针对信息基础设施和设备的计算机系统的攻击采取反制措施。然而，由于这些攻击，如通过黑客手段窃取或更改数据，可被视为属于依赖网络实施的犯罪的范围，因此没有必要将这些犯罪作为信息基础设施或设备的特有问题来处理。同样，由于必须使即将出台的公约在未来长期适用，应当注意，如果关于刑事定罪的条款过于侧重于个别的作案手法，则这些条款将失去其通用性。此外，重要的是，这项新公约应规定尽可能多的会员国能够遵守和执行的基本和必要条款。有鉴于此，讨论应从非法访问等常见的网络犯罪开始。应当认真考虑是否有必要在关于常见网络犯罪的条款之外，制定一项关于攻击信息基础设施和设备的计算机系统的具体条款，以避免刑事定罪条款之间的重复。

1.1.4. 此外，还需避免因刑事定罪范围过宽而对技术开发等合法经营和活动产生寒蝉效应或执法当局滥用权力的风险。例如，在将非法访问定为刑事犯罪时，可能要求访问行为没有合法的理由，并意识到这一点，以避免追究绝对责任。

1.1.5. 此外，对未遂罪或协助和伙同作案犯罪规定统一的惩罚，或规定在不足以构成未遂的准备或共谋阶段进行处罚，将是对各个国家国内刑事立法的过度干预。将这些罪行定为刑事犯罪的问题应由各会员国的国家立法决定。关于打击具有跨国性质的网络犯罪的对策，非常重要是不能为网络犯罪创造庇护所。因此，有必要避免规定此类条款，由于会员国之间不可避免地存在基本法律概念上的差异，此类条款会限制能够缔结新公约的会员国数量。

1.2. 表达自由

1.2.1. 在考虑将网络空间活动定为刑事犯罪时，应参考国际人权条约。在确定哪些行为可根据新公约被定为借助网络实施的犯罪时，特别是在将与互联网上的有害内容有关的行为定为刑事犯罪时，会员国不得忘记保护表达自由的重要性。

1.2.2. 例如，《公民及政治权利国际公约》第十九条第二款规定，发表自由之权利“包括以语言、文字或出版物、艺术或自己选择之其他方式，不分国界，寻求、接受及传播各种消息及思想之自由”。在牢记第十九条第三款规定了对这项权利的某些限制的同时，我们必须确保考虑到每个会员国的实际情况，为国内法律的制定留有余地，以便与学术研究、文化和艺术活动以及新闻有关的权利和自由不受不公正的侵犯。

1.2.3. 为了保护表达自由，有必要避免对表达活动造成寒蝉效应。因此，对与互联网上的有害内容有关的行为进行刑事定罪，只应在所有会员国能够就此类行为的定义达成一致并且有可证明的理由需要进行处罚的情况下进行。

1.2.4. 为了使这项公约成为尽可能多的会员国能够缔结的条约，并等待国际和国家讨论成熟，我们认为，最有希望的选项之一是将与有害内容有关的行为的刑事定罪留给未来的附加议定书。

1.3. 利用网络空间的传统犯罪

1.3.1. 关于与恐怖主义有关的犯罪、与枪支有关的犯罪和与毒品有关的犯罪，即使是通过使用互联网实施的此类犯罪，也可能构成公约规定的罪行，《联合国打击跨国有组织犯罪公约》等现有条约也可能适用。

1.3.2. 应认真考虑将这些行为定为刑事犯罪，以免重复上述现有努力。还应参考现有条约制定过程中的讨论情况，以避免将有意不纳入这些条约的条款简单地以不同形式纳入本公约。

1.4. 有待考虑的可能的借助网络实施的犯罪

关于有害内容（见上文 1.2）以外的借助网络实施的犯罪，在所有会员国能够就此类行为的定义达成一致并且有可证明的理由需要进行惩罚的前提下，一些借助网络实施的犯罪被确认为本公约下规定的重大刑事犯罪，则能够就其刑事定罪问题进行讨论。这类借助网络实施的犯罪包括因使用计算机而扩大范围、加快速度和扩大损害规模的犯罪。这些犯罪可能包括以下罪行。

1.4.1. 与计算机有关的伪造

难以用人体感官来检测计算机数据伪造。此外，在当今世界，由于许多商业流程都是通过计算机进行的，所以破坏对计算机数据的信任也会产生巨大的社会影响。因此，日本可以支持将未经授权故意输入、更改、删除或抑制计算机数据造成数据不真实的行为定为刑事犯罪。

1.4.2 与计算机有关的欺诈

通过伪造计算机数据或干扰计算机系统的运行而实施的计算机数据欺诈很容易针对各种目标而实施，并可能在许多会员国造成严重的财产损失。因此，我们可以支持将通过对计算机数据的任何输入、更改、删除或抑制，或者以欺诈或不诚实的意图干扰计算机系统的运行而造成他人财产损失的行为，定为刑事犯罪。

1.4.3 侵犯版权

在互联网上，数据可以被复制，内容可以被轻易复制，而且这些内容传播速度很快，这就会增加侵犯版权的程度。我们认为，参照现有与版权有关的国际协定，将故意以商业规模和利用计算机系统实施的侵犯版权和相关权利的行为定为刑事犯罪，这会大有裨益。

1.4.4 儿童性虐待和性剥削

制作和传播儿童性虐待材料是极其恶意的行为，会对被描绘儿童的身心健康产生有害影响，严重侵犯他们的人权。儿童性虐待材料一旦通过互联网传播，就很难删除，并将继续对儿童的健康成长产生严重影响。从保护儿童人权的角度来看，我们支持将制作和传播在视觉上描绘儿童从事露骨性行为的材料定为刑事犯罪。

尽管如此，我们认为，考虑到现实存在的未成年人不受直接虐待以及表达自由的重要性，应认真考虑将表现一个貌似未成年的人或不存在的儿童从事露骨性行为的真实图像视为儿童性虐待材料，并将与这些图像相关的罪行定为刑事犯罪。

1.5. 法人责任

如果法人组织广泛犯下与其业务有关的网络犯罪，在责任可以是各会员国法律原则下的刑事、民事或行政责任的情况下，我们支持在一定程度上规定此类法人的责任。刑事、民事和行政事项之间的角色分工以及制裁的必要性是应留给每个会员国的国内立法来处理的问题，因为需要根据每个会员国的国家结构以及与每个会员国网络部门以外的治理的平等性来考虑这些问题。

约旦

[原件：阿拉伯文]

[2022年4月7日]

约旦哈希姆王国提议，应根据公约草案将下列行为定为刑事犯罪：

- 未经授权或违反授权，以任何方式非法访问信息网络、信息系统或其任何部分。如果非法访问属于官方、公共、安全、金融或银行机构的信息网络、信息系统或其任何部分，以及非法访问影响国家安全、国家外交关系、公共安全或国民经济的关键基础设施和不向公众提供的数据或信息，则应加重对该罪行的处罚。
- 非法拦截数据流量。
- 通过信息网络或信息系统侵犯与电子支付方式、执行电子金融或银行交易或者转移资金有关的数据或信息。
- 电子欺诈。
- IP 地址欺诈。

- 通过信息系统、网络或网站进行性剥削。
- 通过信息系统、网络或网站散布谣言或虚假消息。
- 利用信息网络或网站发表与侮辱宗教或国家有关的仇恨言论或采取此类行动。
- 通过植入或引入恶意软件非法干扰信息系统或信息网络。
- 以窃取登录数据或个人信息或收取非法捐款为目的，创建与真实网站相似的网站，误导或欺骗用户。
- 发送电子邮件或文本信息，旨在窃取数据、传播恶意软件或试图访问不允许访问的网络或信息系统为目的，以达到网络钓鱼的目的。
- 在社交媒体网站上创建虚假页面、群组或账户，以误导或欺骗用户、收集非法捐款或从事电子乞讨。
- 以用户的设备为目标，在用户不知情的情况下创建一个信息网络，用于拒绝信任的攻击或非法目的。
- 利用或企图利用信息网络或系统中的安全漏洞，意图对其进行渗透或者窃取、破坏或修改数据。
- 未经许可扫描或试图扫描互联网协议或网络访问端口，意图收集信息或识别安全漏洞。
- 未经授权使用硬件或软件来猜测密码或用户名。
- 使用人工智能技术实施非法行为。
- 与冒充有关的行为。
- 与侵犯隐私有关的行为。
- 与知识产权和软件盗版有关的行为。
- 构成对供应链攻击的行为。
- 与服务提供者未经授权使用数据有关的行为。
- 与传播、支持或宣传恐怖主义意识形态有关的行为。
- 与为恐怖主义目的使用信息和通信技术有关的行为。
- 与电子欺诈有关的行为。
- 与通过电子手段销售或贩运毒品有关的行为。
- 与利用电子手段洗钱有关的行为。

墨西哥

[原件：英文]
[2022 年 4 月 13 日]

刑事定罪

国家管辖权将是界定刑事定罪义务的基本要素。在这方面，墨西哥认为，《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》提供了可延伸适用于打击与使用信息和通信技术有关的犯罪的条款示例，但与云端信息有关的案件除外，这些案件需要根据最近的具体调查经验作进一步分析和讨论。

刑事定罪的一个出发点应该是在公约中考虑那些被国际法承认为犯罪的行为，特别是在联合国框架内通过的其他条约所规定的条款中，这些行为是通过信息和通信技术、电子和数字手段实施的。因此，建议加入以下条款：

“缔约国承认，就本公约的目的而言，现行国际法承认的利用信息技术和电子手段实施的所有犯罪行为均为犯罪。”

在其他刑事犯罪中，对墨西哥政府来说，至关重要的是将与儿童性剥削有关的犯罪以及与利用信息和通信技术实施性别暴力有关的犯罪包括在内。

建议列入加强调查和起诉的执行要素；然后有必要考虑列入附件，其中列有指明处理信息共享请求所需数据的模板。

由于不指望列出所有类型的刑事犯罪，而主要是依赖网络实施的犯罪，为了防止与国家法律不一致或重复，建议列入一项缔约国的一般性承诺，以便在必要时协调其立法。

“本公约的任何内容概不应影响现行国际法下各国和个人旨在防止和打击为犯罪目的使用信息和通信技术的权利、义务和责任。”

“在旨在执行本公约的所有行动中，应首要考虑本公约所确认犯罪的受害者（个人、机构和组织）的最佳利益。”

新西兰

[原件：英文]
[2022 年 4 月 8 日]

刑事定罪条款

1. 在第一届会议期间，我们听到了对在本公约中纳入针对网络犯罪的条款的广泛支持，没有反对意见，特别是依赖网络实施的犯罪和有限的借助网络实施的犯罪。

2. 在本文件附件 1 中，我们提出了一份刑事定罪条款清单，新西兰认为这些条款最有可能达成共识，因此，鉴于资源和时间有限，应成为特设委员会关注的重点。我们还提供了一些案文建议，以协助起草工作，这些建议主要来自其他相关国际文书，如《联合国打击跨国有组织犯罪公约》、《联合国反腐败公约》和《欧洲委员会网络犯罪公约》（《布达佩斯公约》）。

3. 新西兰支持列入一项关于管辖权的规定，在适用情况下反映现有文书，如《联合国反腐败公约》第四十二条，并增加一些内容，要求各缔约国在犯罪或犯罪的任何部分发生在其境内时行使管辖权，以反映网络犯罪可能发生在网络空间，但犯罪人、受害人、数据和所使用的计算机系统有可能在不同的管辖区的这一现实。

附件 1——刑事定罪条款

非法访问计算机系统

各缔约国均应采取必要的立法和其他措施，将未经授权故意访问计算机系统的全部或任何部分的行为确定为其国内法中的刑事犯罪。缔约国可规定犯罪行为的实施是通过违反安全措施意图获取计算机数据或实现其他不诚实意图，或者涉及与另一计算机系统相连的计算机系统。

非法拦截计算机数据

各缔约国均应采取必要的立法和其他措施，在其国内法中将未经授权故意以技术手段拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据的行为规定为刑事犯罪，包括来自载有这类计算机数据的计算机系统的电磁发射。缔约国可规定该罪行是以不诚实的意图实施的，或者涉及与另一计算机系统相连的计算机系统。

干扰计算机数据

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意破坏、删除、损坏、更改或抑制计算机数据的行为定为其国内法中的刑事犯罪。
2. 缔约国可保留对第 1 款所述行为造成严重损害进行规定的权利。

干扰计算机的运行

各缔约国均应采取可能必要的立法和其他措施，在其国内法中将故意实施的通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而未经授权严重妨碍计算机系统运行的行为规定为刑事犯罪。

滥用设备或计算机程序

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意实施的下列行为确定为其国内法中的刑事犯罪：
 - (a) 生产、销售、获取使用、进口、分销或以其他方式提供：
 - (i) 主要为实施根据[相关条款]所确立的任何犯罪而设计或改装的设备，包括计算机程序；
 - (ii) 计算机密码、访问代码或借由能够访问整个计算机系统或其任何部分的类似数据，意图将其用于实施[相关条款]所确立的任何犯罪；及

(b) 拥有上文第(a)(i)或(ii)款所述物品，意图将其用于实施[相关条款]所确立的任何犯罪。缔约国可依法规定在承担刑事责任之前拥有若干此类物品。

2. 如果本条第1款所述的生产、销售、获取使用、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]确立的犯罪，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)(ii)款所述物品的销售、分销或以其他方式提供。

将网络勒索定为刑事犯罪

1. 新西兰将支持列入一项规定，将下列行为定为刑事犯罪：

(a) 勒索计算机系统的用户以解锁数据；

(b) 以未经授权发布数据或个人信息为威胁，勒索计算机系统用户。

2. 新西兰期待与各位同事合作，为这一犯罪行为制定确切的措辞。

与计算机有关的欺诈

各缔约国均应采取必要的立法和其他措施，将未经授权通过以下方式故意造成他人财产损失的行为确定为其国内法中的刑事犯罪：

(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，在未经授权情况下为自己或他人获取经济利益。

与计算机有关的伪造

各缔约国均应采取必要的立法和其他措施，将未经授权故意输入、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其国内法中的刑事犯罪，而不论该数据是否可直接阅读和理解。缔约方可以规定在承担刑事责任之前存在欺诈或类似的不诚实意图。

利用计算机系统对儿童进行性剥削

1. 我们期待与同事合作，制定有效且全面的刑事定罪条款，打击网上对儿童的性剥削和性虐待。

2. 这类犯罪行为至少应包括与使用计算机系统从事下列活动有关的犯罪：

(a) 制作儿童性剥削材料；

(b) 提供儿童性剥削材料；

(c) 分发或传播儿童性剥削材料；

- (d) 为自己或他人获取儿童性剥削材料；
- (e) 拥有儿童性剥削材料；
- (f) 为性剥削为目的诱拐儿童。

未经同意发布或分发私密视觉记录

1. 各缔约国均应采取必要的立法和其他措施，在本国法中将下列情况下无合理理由而利用计算机系统转移、发送、发布、传播或以其他方式交流被害人的私密录像的行为确定为刑事犯罪——

- (a) 明知受害人不同意发布；或
- (b) 不顾及受害人是否同意发布。

2. 为明确起见，未满 16 岁的儿童或青少年不能同意发布以他们为对象的私密视觉记录。

参与和未遂

1. 各缔约国均应采取必要的立法和其他措施，根据本国法将以共犯、从犯或者教唆犯等任何身份参与根据本公约确立的犯罪定为刑事犯罪。
2. 各缔约国均可以采取必要的立法和其他措施，根据本国法将实施根据本公约确立的犯罪的任何未遂和中止规定为刑事犯罪。
3. 各缔约国均可以采取必要的立法和其他措施，根据本国法律将为实施根据本公约确立的犯罪进行预备的行为规定为刑事犯罪。

法人责任

1. 各缔约国均应当采取符合其法律原则的必要措施，确定法人参与根据本公约确立的犯罪应当承担的责任。
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、民事责任或者行政责任。
3. 法人责任不应当影响实施这种犯罪的自然人的刑事责任。
4. 各缔约国均应当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者非刑事制裁，包括金钱制裁。
5. 法人应受保护，免于为出于善意而作出或不作出的行为承担责任：
 - (a) 在履行或打算履行本公约所规定的义务时；或
 - (b) 在行使或打算行使根据本公约赋予的职能或权力时。

将洗钱定为刑事犯罪

1. 各缔约国均应当根据本国法律的基本原则采取必要的立法和其他措施，将故意实施的下列行为定为刑事犯罪：

(a)(i) 明知财产为网络犯罪所得，为隐瞒或者掩饰该财产的非来源，或者为协助任何参与实施上游犯罪者逃避其行为的法律后果而转换或者转移该财产；

(ii) 明知财产为网络犯罪所得，隐瞒或者掩饰该财产的真实性质、来源、位置、处置、转移、所有权或者有关的权利；

(b) 在符合本国法律制度基本概念的情况下：

(i) 在得到财产时，明知其为网络犯罪所得而仍获取、占有或者使用；

(ii) 对本条所确立的任何犯罪的参与、协同或者共谋实施、实施未遂以及协助、教唆、便利和参谋实施；

2. 为实施或者适用本条第 1 款：

(a) 各缔约国均应当寻求将本条第 1 款适用于范围最为广泛的上游犯罪；

(b) 各缔约国均应将[本公约有关条款确立的相关犯罪和]根据本公约[有关条款]确立的犯罪列为上游犯罪。缔约国立法中如果明确列出上游犯罪清单，则至少应在这类清单中列出[与网络犯罪有关的范围全面的各种犯罪]；

(c) 就(b)项的目的而言，上游犯罪应包括在有关缔约国司法管辖权范围之内和之外发生的犯罪。然而，如果犯罪发生在一缔约国司法管辖权范围之外，则只有当该行为根据其发生地所在国法律为犯罪，而且根据实施或者适用本条的缔约国的法律该行为若发生在该国也为犯罪时，才构成上游犯罪；

(d) 各缔约国均应当向联合国秘书长提供其实施本条的法律以及这类法律随后的任何修改的副本或说明；

(e) 如果缔约国本国法律基本原则要求，则可以规定本条第 1 款所列犯罪不适用于实施上游犯罪的人；

(f) 本条第 1 款所规定的作为犯罪要素的明知、故意或目的可根据客观实际情况推定。

妨碍司法

各缔约国均应采取必要的立法措施和其他措施，将故意实施的下列行为规定为刑事犯罪：

(a) 在涉及本公约所涵盖的犯罪的诉讼中使用暴力、威胁或恐吓，或许诺、提议给予或给予不正当好处，以诱使提供虚假证言或干扰证言或证据的提供；

(b) 使用暴力、威胁或恐吓，干扰司法或执法人员针对本公约所涵盖的犯罪执行公务。本项规定概不应影响缔约国制定保护其他类别公职人员的立法权利。

挪威

[原件：英文]
[2022 年 4 月 8 日]

刑事定罪

1. 我们应当建议，公约将依赖网络实施的犯罪定为刑事犯罪。尽管网络犯罪每天都在发展，但国家和国际机构设法查明了核心的、反复出现的行为类型。如今，许多会员国已经将这些犯罪定为刑事犯罪。在这方面，挪威王国政府建议至少考虑以下依赖网络实施的犯罪：

- 非法访问，即未经授权访问计算机或计算机系统
- 非法拦截，即实时非法拦截通信内容或与通信相关的流量数据
- 干扰数据或系统，即恶意软件、拒绝服务攻击、勒索软件以及删除或修改数据
- 滥用设备，即贩运或使用允许获取资源的信用数据、密码和个人信息

2. 我们希望保持清单简短。

3. 公约还应避免与其他法律文书所涉及的罪行重复。

4. 案文应该是技术中性的。

5. 除了依赖网络实施的犯罪的简短清单外，公约还应包括与儿童性虐待材料相关犯罪有关的条款。

俄罗斯联邦，并代表白俄罗斯、布隆迪、中国、尼加拉瓜和塔吉克斯坦

[原件：俄文]
[2022 年 4 月 7 日]

第二章 刑事定罪、刑事诉讼和执法

第 1 节 责任的确定

第 5 条 责任的确定

各缔约国均应采取必要的立法和其他措施，在本国法中至少将本公约第 6 条、第 7 条、第 9-12 条、第 14-17 条、第 19 条、第 20 条、第 22-26 条和第 28 条所设想的行为定为犯罪，同时考虑到某一行为对公众造成的危险程度和损害程度，适用包括监禁在内的刑事和其他处罚。

第 6 条 非法获取数字信息

各缔约国均应采取必要的立法和其他措施，在本国法中将故意非法获取数字信息并导致其被销毁、屏蔽、修改或复制的行为规定为犯罪。

第 7 条 非法拦截

各缔约国均应采取必要的立法和其他措施，在本国法中将未经适当授权且（或）违反既定规则而故意拦截数字信息的行为定为犯罪，包括使用技术手段拦截非公共用途的流量数据和通过信息和通信技术处理的数据的行为。

第 8 条 非法干扰数字信息

各缔约国均应采取必要的立法和其他措施，在本国法中将故意非法干扰数字信息并导致其被损坏、删除、改变、屏蔽、修改或复制的行为规定为犯罪或其他非法行为。

第 9 条 破坏信息和通信网络

各缔约国均应采取必要的立法和其他措施，在本国法中将以破坏信息和通信网络为目的、造成或威胁造成严重后果的故意非法行为规定为犯罪。

第 10 条

制作、使用和传播恶意软件

1. 各缔约国均应采取必要的立法和其他措施，在本国法中将下述行为规定为犯罪：故意制作（包括改编）、使用和传播恶意软件，旨在未经授权破坏、屏蔽、修改、复制或传播数字信息，或使其安全功能失效，但合法研究除外。
2. 各缔约国均应采取必要的立法和其他措施，在本国法中将为实施本公约第 6-12 条和第 14 条所设想的任何行为而制作或利用僵尸网络的行为规定为犯罪或其他非法行为。

第 11 条

非法干扰关键信息基础设施

1. 各缔约国均应采取必要的立法和其他措施，在本国法律中将以下行为规定为犯罪：在知情的情况下故意制作、传播和（或）使用软件或其他数字信息，旨在非法干扰关键信息基础设施，包括软件或其他数字信息，以销毁、屏蔽、修改、复制其中所载信息，或者使其安全功能失效。
2. 各缔约国均应采取必要的立法和其他措施，在本国法中将下列行为规定为犯罪：违反为储存、处理和传送关键信息基础设施或属于关键信息基础设施的信息系统或信息和通信网络中所载受保护数字信息而制定的媒体操作规则，或违反获取这些信息的规则，且这种违反行为损害了关键信息基础设施。

第 12 条

未经授权获取个人数据

各缔约国均应采取必要的立法和其他措施，在本国法中将未经授权获取个人数据以销毁、修改或复制该数据的行为规定为犯罪。

第 13 条

非法贩运设备

各缔约国均应采取必要的立法和其他措施，在本国法律中将以下行为规定为犯罪或其他非法行为：非法制造、销售、购买以供使用、进口、出口或以其他方式转让以供使用主要为实施本公约第 6 条至第 12 条所确立的任何犯罪而设计或改装的设备。

如果设备的制造、销售、购买以供使用、进口、出口或以其他方式转让以供使用与计算机系统的授权试验或保护相关，则本条规定不适用。

第 14 条

信息和通信技术相关的偷窃

1. 各缔约国均应当采取必要的立法和其他措施，在本国法律中将盗窃财产或者非法取得财产权利规定为犯罪，包括通过破坏、屏蔽、修改或者复制数字信息或者以其他方式干扰信息和通信技术的运行等欺诈手段。

2. 各缔约国均可保留权利，将与信息和通信技术有关的财产盗窃或非法获取财产权利，包括通过欺诈手段，视为以本国法所界定的形式实施的从重处罚情节。

第 15 条

与制作和传播带有未成年人色情图像的材料或物品有关的信息和通信技术相关犯罪

1. 各缔约国均应采取必要的立法和其他措施，在本国法中将未经授权故意且非法实施的下列行为确定为犯罪：

(a) 制作儿童色情制品，用于通过包括互联网在内的信息和通信网络传播；

(b) 通过包括互联网在内的信息和通信网络提供儿童色情制品；

(c) 利用包括互联网在内的信息和通信网络传播、传送、公开展示或宣传儿童色情制品；

(d) 利用信息和通信技术为自己或他人获取儿童色情制品；

(e) 在计算机系统或电子数字数据存储装置上拥有儿童色情制品。

2. 就本条第 1 款的目的而言，“儿童色情制品”一词应包括以视觉方式描绘下列内容的色情材料：

(a) 未成年人参与露骨性行为；

(b) 貌似未成年的人参与露骨性行为；

(c) 显示未成年人参与露骨性行为的真实图像。

就本条的目的而言，“未成年人”一词应包括不满 18 岁的所有人员。不过，缔约国可规定一个较低的年龄限制，但不应低于 16 岁。

第 16 条

鼓励或胁迫自杀

各缔约国应采取必要的立法和其他措施，在其国内法中将在包括互联网在内的信息和电信网络中通过心理或其他压力鼓励或胁迫自杀，包括使未成年人自杀，定为犯罪。

第 17 条

涉及未成年人参与实施危害其生命或健康的非法行为的犯罪

各缔约国均应采取必要的立法和其他措施，在本国法中将利用信息和通信技术使未成年人参与实施危及生命的非法行为规定为犯罪，但本公约第 16 条规定的行为除外。

第 18 条

制作和使用数字信息以误导用户

1. 各缔约国均应采取必要的立法和其他措施，在本国法中将下列行为规定为犯罪或其他非法行为：故意非法制作和使用能被误认为是用户已知并信任的数字信息，造成重大损害。
2. 如果此类行为与该缔约国国内法规定的其他犯罪相结合实施，或涉及实施此类犯罪的蓄意意图，各缔约国可保留将此类行为视为刑事犯罪的权利。

第 19 条

煽动颠覆或武装活动

各缔约国均应采取必要的立法和其他措施，在本国法中将利用信息和通信技术为旨在暴力推翻另一国政府的颠覆或武装活动而发出的号召定为犯罪。

第 20 条

与恐怖主义活动有关的犯罪

各缔约国均应采取必要的立法和其他措施，在本国法律中将以下行为定为犯罪：利用信息和通信技术发出号召，以实施恐怖主义活动，煽动、招募或以其他方式参与恐怖主义活动，为恐怖主义进行宣传和辩护，或者为资助恐怖主义而筹集或提供资金。

第 21 条

与极端主义有关的犯罪

1. 各缔约国均应采取必要的立法和其他措施，在国内法中将以下行为定为犯罪或其他非法行为：利用信息和通信技术，分发煽动出于政治、意识形态、社会、种族、族裔或宗教仇恨或敌意的非法行为的材料，为这种行为进行宣传和辩护，或提供获取这种材料的途径。
2. 各缔约国均应采取必要的立法和其他措施，在本国法律中将利用信息和通信技术以种族、族裔、语言、血统或宗教信仰为由侮辱某一个人或群体的行为定为犯罪或其他非法行为。

第 22 条

与分销麻醉药品和精神药物有关的犯罪

各缔约国均应采取必要的立法和其他措施，在本国法中将利用信息和通信技术故意非法贩运麻醉药品和精神药物以及制造这些药物所需的材料定为犯罪。

第 23 条

与贩运武器有关的犯罪

各缔约国均应采取必要的立法和其他措施，在本国法中将利用信息和通信技术故意非法贩运武器、弹药、爆炸装置和爆炸物质定为犯罪。

第 24 条

为纳粹主义平反、为灭绝种族或危害和平与人类罪辩护

各缔约国均应采取必要的立法和其他措施，在本国法律中将以下行为定为犯罪：利用信息和通信技术故意传播否认或认可与 1945 年 8 月 8 日《伦敦协定》设立的国际军事法庭的判决书所确定的种族灭绝或危害和平与人类罪相当的行为或为此类行为辩护的材料。

第 25 条

非法分销假冒药品或医疗产品

各缔约国均应采取必要的立法和其他措施，在本国法中将利用信息和通信技术故意非法分销假冒药品或医疗产品定为犯罪。

第 26 条

利用信息和通信技术实施国际法确立为犯罪的行为

1. 各缔约国均应采取必要的立法和其他措施，在本国法中将使用信息和通信技术实施根据本公约附件³⁶所列任何国际协定构成犯罪的行为定为犯罪。
2. 非本公约附件所列协定的缔约国的国家在交存其批准书、接受书、核准书或加入书时，可以声明，在对该缔约国适用本公约时，应将该协定视为未列入上述附件。一旦协定对缔约国生效，则该声明立即失效，缔约国应将此情况通知保存人。
3. 若缔约国不再是本公约附件所列协定的缔约国，则可按照上文第 2 款的规定就该协定发表声明。

第 27 条

利用信息和通信技术侵犯版权和相关权利

各缔约国均应采取必要的立法和其他措施，在其本国法律中将利用信息和通信技术故意实施的侵犯本国立法所界定的版权和相关权利的行为，包括非法使用受版权保护的计算机系统或数据库的软件以及盗用作者身份的行为，定为犯罪或其他非法行为。

第 28 条

协助、预备和企图实施犯罪

1. 各缔约国均应采取必要的立法和其他措施，在其本国法中将实施根据本公约确定的任何犯罪的预备和未遂规定为犯罪。
2. 各缔约国均应考虑采取必要的立法和其他措施，在本国法中将下述行为规定为犯罪：在由于实施者不可控的原因而未实施犯罪的情况下，制造或改装犯罪工具和其他犯罪手段、教唆共犯、共谋实施犯罪或为实施本公约确立的犯罪故意创造条件的任何其他行为。

³⁶ 秘书处的说明：请参看 A/75/980 号文件的附件。

3. 各缔约国均应根据本国法律采取必要的立法和其他措施，确定参与实施根据本公约确立的犯罪的组织者、教唆者或协助者的责任，以及根据本公约确立的犯罪的实际犯罪人的责任，并加强对有组织集团和犯罪团伙等集体犯罪的追责。

第 29 条

其他违法行为

本公约不应排除缔约国将通过信息和通信技术故意实施的造成重大损害的任何其他非法行为定为犯罪。

第 30 条

法人责任

1. 各缔约国均应采取必要的立法和其他法律措施，确保当任何自然人单独或作为有关法人的实体的一部分为法人的利益而实施刑事犯罪或其他非法行为，并通过以下方式在该法人中担任领导职位时，可追究法人的责任：

- (a) 该法人的授权书；
- (b) 代表该法人作出决定的职权；
- (c) 在该法人内部行使控制权的职权。

2. 除本条第 1 款已规定情况之外，各缔约国应采取必要的措施确保，如果因第 1 款所述自然人缺乏监督或控制而使自然人在职权范围内行事时能够为法人利益实施根据本公约规定的刑事犯罪或其他非法行为，则亦可对法人追究责任。

3. 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、民事责任或者行政责任。各缔约国均应确保使应当承担责任的法人受到有效、适度和劝阻性的制裁，包括金钱制裁。

4. 此类法人责任不应影响实施犯罪或其他非法行为的自然人的责任。

南非

[原件：英文]

[2022 年 4 月 14 日]

第二章. 刑事定罪

第 5 条：非法访问

各缔约国均应采取必要的立法和其他措施，将故意且不合法地非法访问计算机系统的全部或任何部分的行为确定为其国内法中的刑事犯罪。缔约国可规定犯罪行为的实施是通过违反安全措施意图不合法地获取计算机数据或实现其他不诚实意图，或者涉及与另一计算机系统相连的计算机系统。

第 6 条：非法拦截

各缔约国均应采取必要的立法和其他措施，在其国内法中将故意且非法地实施的以技术手段无权拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据的行为规定为刑事犯罪，包括来自载有这类计算机数据的计算机系统的电磁发射。缔约国可规定该罪行是以不诚实的意图实施的，或者涉及与另一计算机系统相连的计算机系统。

第 7 条：未经授权干扰数字信息

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意且非法地破坏、删除、损坏、更改或抑制计算机数据的行为定为其国内法中的刑事犯罪。
2. 缔约国可保留对第 1 款所述行为（对自然人、法人和缔约国经济）造成严重损害作出规定的权利。

第 8 条：对信息和通信网络的系统干扰和破坏

各缔约国均应采取必要的立法和其他措施，在其国内法中将故意且非法地通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而未经授权严重妨碍计算机系统运行的行为规定为刑事犯罪。

第 9 条：设备的创建、使用和分发

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意且非法实施的下列行为确定为其国内法中的刑事犯罪：
 - (a) 生产、销售、获取使用、进口、分销或以其他方式提供：
 - (i) 主要为实施按第 5 条至第 26 条所确立的任何犯罪而设计或改装的设备，包括计算机程序；
 - (ii) 计算机密码、访问代码或借由能够访问整个计算机系统或其任何部分的类似数据，意图将其用于实施第 5 条至第 26 条所确立的任何犯罪；及
 - (b) 拥有上文第 1(a)(i)或(ii)款所述物品，意图将其用于实施第 5 条至第 26 条所确立的任何犯罪。缔约国可依法规定在承担刑事责任之前拥有若干此类物品。
2. 如果本条第 1 款所述的生产、销售、获取使用、进口、分销或以其他方式提供或拥有并非为了实施根据本公约第 5 条至第 26 条确立的犯罪，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)(ii)款所述物品的销售、分销或以其他方式提供。

第 10 条：借助网络实施的伪造

各缔约国均应采取必要的立法和其他措施，将未经授权故意且非法输入、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其国内法中的刑事犯罪，而不论该数据是否可直接阅读和理解。缔约方可以规定在承担刑事责任之前存在欺诈或类似的不诚实意图。

第 11 条：借助网络实施的欺诈

各缔约国均应采取必要的立法和其他措施，将未经授权通过以下方式故意且非法地造成他人财产损失的行为确定为其国内法中的刑事犯罪：

- (a) 对计算机数据的任何输入、更改、删除或抑制；
- (b) 干扰计算机系统的运行，其欺诈或不诚实意图是在未经授权的情况下为自己或他人获取经济利益。

第 12 条：与儿童性虐待材料有关的犯罪

1. 各缔约国应采取必要的立法和其他措施，将故意且非法实施的下列行为在其国内法中定为刑事犯罪：

- (a) 制作儿童性虐待材料，意图通过计算机系统或信息和通信技术传播；
- (b) 通过计算机系统或信息和通信技术提供儿童性虐待材料；
- (c) 通过计算机系统或信息和通信技术分发或传送儿童性虐待材料；
- (d) 通过计算机系统或信息和通信技术为自己或他人获取儿童性虐待材料；
- (e) 在计算机系统或信息和通信技术中或在计算机数据存储介质上拥有儿童性虐待材料。

2. 就上文第 1 款的目的而言，“儿童性虐待材料”一词应包括以视觉方式描绘下列内容的材料：

- (a) 未成年人参与露骨性行为；
- (b) 貌似未成年的人参与露骨性行为；及
- (c) 显示未成年人参与露骨性行为的真实图像。

3. 就第 2 款的目的而言，“未成年人”一词应包括不满 18 岁的所有人员。不过，缔约国可要求一个较低的年龄限制，但不应低于 16 岁。

第 13 条：与侵犯版权及相关权利有关的犯罪

1. 各缔约国均应采取必要的立法和其他措施，根据其在各种国际条约和协定下承担的义务，在其国内法中将故意以商业规模借助计算机系统或信息和通信技术侵犯该缔约国法律所定义的版权的行为确定为刑事犯罪，但这些公约赋予的任何精神权利除外。

2. 各缔约国应采取必要的立法和其他措施，根据其在《保护表演者、录音制品制作者和广播组织国际公约》（《罗马公约》）、《与贸易有关的知识产权协定》和《世界知识产权组织表演和录音制品条约》下所承担的义务，在其国内法中将故意以商业规模并借助计算机系统实施的侵犯该缔约国法律所界定的相关权利的行为定为刑事犯罪，但这类公约所赋予的任何精神权利除外。
3. 缔约国可保留在有限的情况下不根据本条第 1 款和第 2 款追究刑事责任的权利，但须有其他有效的补救措施可用，而且此种保留不减损本条第 1 款和第 2 款所述国际文书中规定的缔约国的国际义务。

第 14 条：与分销麻醉药品和精神药物有关的犯罪

各缔约国均应采取必要的立法和其他措施，在本国法中将涉及使用信息和通信技术而助长贩运麻醉药品、精神药物及其制造所需材料的行为规定为刑事犯罪。

第 15 条：保护举报人

各缔约国均应当考虑在本国法律制度中纳入适当措施，以便对出于合理理由善意向主管机关举报关于根据本公约确立的涉及使用信息和通信技术的犯罪的任何事实的任何人员提供保护，使其不致受到任何不公正的待遇。

各缔约国均应考虑，在其国内立法中纳入对任何在与有关执法机构互动时提供充分配合并本着诚意的人的免于被起诉的保障，但须满足缔约国通过的标准/条件。

第 16 条：与执法机关的配合

1. 各缔约国均应当采取适当措施，鼓励参与或者曾经参与实施根据本公约确立的涉及使用信息和通信技术犯罪的人，出于善意提供有助于主管机关侦查和取证的信息，并为主管机关提供可能有助于剥夺罪犯的犯罪所得并追回这种所得的实际具体帮助。
2. 对于在根据本公约确立的任何涉及使用信息和通信技术的犯罪的侦查或者起诉中出于善意提供实质性配合的被告人，各缔约国均应当考虑就适当情况下减轻处罚的可能性作出规定。
3. 对于在根据本公约确立的涉及使用信息和通信技术的犯罪的侦查或者起诉中出于善意提供实质性配合的人，各缔约国均应当考虑根据本国法律的基本原则就允许不予起诉的可能性作出规定。
4. 应当按本公约第 22 条的规定变通适用为这类人员提供的保护。
5. 如果本条第 1 款所述的、处于某一缔约国的人员能够给予另一缔约国主管机关以实质性配合，有关缔约国可以考虑根据本国法订立关于由对方缔约国提供本条第 2 款和第 3 款所述待遇的协定或者安排。
6. 各缔约国均应根据其本国法的基本原则，保存一份登记册，其中载有其管辖范围内所有域名注册商、加密资产交易商和加密资产的可识别信息，并将此类信息提供给主管机关，以供调查和取证之用。

第 17 条：管辖权

1. 各缔约国均应当采取必要的措施，在下列情况下确立对根据本公约确立的涉及使用信息和通信技术的犯罪的管辖权：

(a) 犯罪发生在该缔约国管辖范围内；或者

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

2. 在不违背本公约第 4 条的情况下，缔约国还可以在下列情况下对任何此种涉及使用信息和通信技术的犯罪确立其管辖权：

(a) 犯罪系针对该缔约国国民；或者

(b) 犯罪者为该缔约国国民或在其境内有惯常居所的无国籍人；或者

(c) 犯罪发生在本国领域以外，是根据本公约第 17 条第 1(b)(ii)款确立的犯罪，其目的是在其领域内实施根据本公约第 15 条确立的涉及使用信息和通信技术的犯罪；或者

(d) 犯罪是针对某缔约国实施的，或对该缔约国的事务有直接影响。

3. 为了本公约[关于引渡]的条款的目的，各缔约国均应当采取必要措施，在被指控的犯罪人在其领域内而其仅因该人为本国国民而不予引渡时，确立本国对根据本公约确立的涉及使用信息和通信技术的犯罪的管辖权。

4. 各缔约国还可以采取必要的措施，在被指控的犯罪人在其领域内而其不引渡该人时，确立本国对根据本公约确立的涉及使用信息和通信技术的犯罪的管辖权。

5. 如果根据本条第 1 款或者第 2 款行使管辖权的缔约国被告知或者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、起诉或者司法程序，这些缔约国的主管机关应当酌情相互磋商，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根据本国法确立的任何刑事管辖权。

瑞士

[原件：英文]
[2022 年 4 月 8 日]

2.2 关于刑事定罪的规定

a. 侵犯计算机数据和系统保密性、完整性和可用性的犯罪

非法访问

各缔约国均应采取必要的立法和其他措施，将未经授权故意访问计算机系统的全部或任何部分的行为确定为其国内法中的刑事犯罪。缔约国可规定犯罪行为的实施是通过违反安全措施意图获取计算机数据或实现其他不诚实意图，或者涉及与另一计算机系统相连的计算机系统。

非法拦截

各缔约国均应采取必要的立法和其他措施，在其国内法中将未经授权故意以技术手段无权拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据的行为规定为刑事犯罪，包括来自载有这类计算机数据的计算机系统的电磁发射。缔约方可规定该罪行是以不诚实的意图实施的，或者涉及与另一计算机系统相连的计算机系统。

干扰数据

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意破坏、删除、损坏、更改或抑制计算机数据的行为定为其国内法中的刑事犯罪。
2. 缔约国可保留对第 1 款所述行为造成严重损害进行规定的权利。

干扰系统

各缔约国均应采取可能必要的立法和其他措施，在其国内法中将故意通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而未经授权严重妨碍计算机系统运行的行为规定为刑事犯罪。

滥用设备

1. 各缔约国均应采取必要的立法和其他措施，将下列将未经授权而故意实施的行为确定为其国内法中的刑事犯罪：
 - (a) 生产、销售、获取使用、进口、分销或以其他方式提供：
 - (i) 主要为实施根据本公约关于非法访问、非法拦截、数据干扰或系统干扰的规定所确立的任何犯罪而设计或改造的设备，包括计算机程序；
 - (ii) 计算机密码、访问代码或能够借由访问计算机系统的全部或任何部分的类似数据，意图将其用于实施本公约关于非法访问、非法拦截、数据干扰或系统干扰的规定所确立的任何犯罪；及
 - (b) 持有上文第 1(a)(i)或(ii)款所述物品，意图将其用于实施根据本公约关于非法访问、非法拦截、数据干扰或系统干扰的规定确立的任何犯罪。缔约国可规定在承担刑事责任之前拥有若干此类物品。
2. 如果本条第 1 款所述的生产、销售、获取使用、进口、分销或以其他方式提供或拥有并非为了实施根据本公约关于非法访问、非法拦截、数据干扰或系统干扰的规定所确立的犯罪，例如是用于计算机系统的授权测试或保护，则不应将本条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)(ii)款所述物品的销售、分销或以其他方式提供。

b. 与计算机有关的犯罪

与计算机有关的伪造

各缔约国均应采取必要的立法和其他措施，将未经授权故意输入、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其国内法中的刑事犯罪，而不论该数据是否可直接阅读和理解。缔约方可以规定在承担刑事责任之前存在欺诈或类似的不诚实意图。

与计算机有关的欺诈

各缔约国均应采取必要的立法和其他措施，将通过以下方式未经授权而故意造成他人财产损失的行为确定为其国内法中的刑事犯罪：

(a) 对计算机数据的任何输入、更改、删除或抑制；

(b) 干扰计算机系统的运行，其欺诈或不诚实意图是在未经授权的情况下为自己或他人获取经济利益。

c. 与内容有关的犯罪

与儿童性剥削和性虐待材料有关的犯罪

1. 各缔约国均应采取必要的立法和其他措施，将下列未经授权而故意实施的行为确定为其国内法中的刑事犯罪：

(a) 为通过计算机系统分发而制作儿童性剥削和性虐待材料；

(b) 通过计算机系统提供儿童性剥削和性虐待材料；

(c) 通过计算机系统分发或传送儿童性剥削和性虐待材料；

(d) 通过计算机系统为自己或他人获取儿童性剥削和性虐待材料；

(e) 在计算机系统或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 款目的而言，“儿童性剥削和性虐待材料”一词应包括以视觉方式描绘下列内容的材料：

(a) 未成年人参与露骨性行为；

(b) 貌似未成年的人参与露骨性行为；

(c) 显示未成年人参与露骨性行为的真实图像。

3. 就第 2 款的目的而言，“未成年人”一词应包括不满 18 岁的所有人员。不过，缔约国可要求一个较低的年龄限制，但不应低于 16 岁。

4. 各缔约国可保留全部或部分不适用第 1 款(d)和(e)项以及第 2 款(b)和(c)项的权利。

d. 附带责任和制裁

未遂和协助或教唆

1. 各缔约国均应采取可能必要的立法和其他措施，在本国法律中将故意实施的下述行为规定为刑事犯罪：协助或教唆实施根据本公约刑事定罪条款确立的任何犯罪，意图实施此种犯罪。
2. 各缔约国均应采取必要的立法和其他措施，在其本国法中将故意实施根据本公约刑事定罪条款确立的任何犯罪的未遂规定为刑事犯罪。
3. 各缔约国可保留全部或部分不适用本条第 2 款的权利。

法人责任

1. 各缔约国均应采取必要的立法和其他措施，以确保在基于下列权力在法人内部担任领导职务的任何自然人单独或作为该法人的一个机构的组成部分而为法人利益实施根据本公约关于刑事定罪的规定确立的刑事犯罪的情况下，可追究该法人的刑事犯罪责任。
 - (a) 该法人的代表权；
 - (b) 代表该法人作出决定的职权；
 - (c) 在该法人内部行使控制权的职权。
2. 除本条第 1 款已规定情况之外，如果因第 1 款所述自然人缺乏监督或控制而使自然人在授权范围内行事时能够为法人利益实施根据本公约确立的刑事犯罪，则亦可对法人追究责任。
3. 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、民事责任或者行政责任。
4. 法人责任不应当影响实施这种犯罪的自然人的刑事责任。

制裁和措施

1. 各缔约国均应采取必要的立法和其他措施，以确保对根据公约关于刑事定罪的规定确立的刑事犯罪可处以有效、适度和劝阻性的制裁，包括剥夺自由。
2. 各缔约国均应当确保使依照本公约关于法人责任的规定应当承担责任的法人被处以有效、适度和劝阻性的刑事或者非刑事制裁或措施，包括金钱制裁。

大不列颠及北爱尔兰联合王国

[原件：英文]

[2022 年 4 月 12 日]

章次——刑事定罪

依赖网络实施的犯罪

联合王国认为，公约必须包括依赖网络实施的犯罪，其描述和定义必须为所有缔约国所接受，并与这一领域的现有国际协定相一致。

第 5 条

非法访问

各缔约国均应采取必要的立法和其他措施，将未经授权故意访问计算机系统的全部或任何部分的行为确定为其国内法中的刑事犯罪。缔约国可规定犯罪行为的实施是通过违反安全措施意图获取计算机数据或实现其他不诚实意图，或者涉及与另一计算机系统相连的计算机系统。

第 6 条

非法拦截

各缔约国均应采取必要的立法和其他措施，在其国内法中将故意实施的以技术手段未经授权拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据的行为规定为刑事犯罪，包括来自载有这类计算机数据的计算机系统的电磁发射。缔约方可要求该罪行是以不诚实的意图实施的，或者涉及与另一计算机系统相连的计算机系统。

第 7 条

干扰数据

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意破坏、删除、损坏、更改或抑制计算机数据的行为定为其国内法中的刑事犯罪。
2. 缔约方可保留对第 1 款所述行为造成严重损害进行规定的权利。

第 8 条

干扰系统

各缔约国均应采取可能必要的立法和其他措施，在其国内法中将故意通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而未经授权严重妨碍计算机系统运行的行为规定为刑事犯罪。

第 9 条

滥用设备

1. 各缔约国均应采取必要的立法和其他措施，将下列将未经授权而故意实施的行为确定为其国内法中的刑事犯罪：

(a) 生产、销售、获取使用、进口、分销或以其他方式提供：

(i) 主要为实施根据各节所确立的任何犯罪而设计或改装的设备，包括计算机程序；

(ii) 计算机密码、访问代码或借由能够访问整个计算机系统或其任何部分的类似数据，意图将其用于实施本节另外四条所确立的任何犯罪；及

(b) 拥有上文第 1(a)(i)或(ii)款所述物品，意图将其用于实施本节另外四条所确立的任何犯罪。缔约国可依法规定在承担刑事责任之前拥有若干此类物品。

2. 如果本条第 1 款所述的生产、销售、获取使用、进口、分销或以其他方式提供或拥有并非为了实施根据关于非法访问、非法拦截、数据干扰和系统干扰的条款所确立的犯罪，例如是用于计算机系统的授权测试或保护，则不应将本条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)(ii)款所述物品的销售、分销或以其他方式提供。

借助网络实施的犯罪

联合国亦认为，如果犯罪主要在网上进行，计算机改变了犯罪的规模和速度，以及犯罪的定义得到普遍理解，则应列入借助网络实施的犯罪。

第 10 条

欺诈

各缔约国应采取必要的立法修改和其他措施，将全部或部分在网上实施的一般欺诈犯罪确定为其国内法中的刑事犯罪。这包括但不限于通过互联网或其他借助网络的/数字方式，以下列方法在国内和跨境开展的活动：

(a) 通过虚假陈述进行欺诈；

(b) 通过不披露信息进行欺诈；

(c) 通过滥用职权进行欺诈，具有欺诈或不诚实的意图，以给他人造成损失或使他人获得金钱或其他财产。

第 11 条

与在线儿童性剥削和性虐待有关的犯罪，包括儿童性剥削和性虐待材料和线上诱拐

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意实施的下列行为确定为其国内法中的刑事犯罪：

(a) 为通过计算机系统分发而制作儿童性剥削和性虐待材料；

(b) 通过计算机系统提供儿童性剥削和性虐待材料；

(c) 通过计算机系统分发或传送儿童性剥削和性虐待材料；

- (d) 通过计算机系统为自己或他人获取儿童性剥削和性虐待材料；
 - (e) 在计算机系统或计算机数据存储介质中拥有儿童性剥削和性虐待材料；
 - (f) 在计算机系统或计算机数据存储上观看儿童性剥削和性虐待材料；
2. 就上文第 1 款目的而言，“儿童性剥削和性虐待材料”一词应包括以视觉方式描绘下列内容的材料：
- (a) 未成年人参与真实或模拟的露骨性行为；
 - (b) 貌似未成年的人参与真实或模拟的露骨性行为；
 - (c) 显示未成年人参与真实或模拟的露骨性行为的真实图像；
 - (d) 主要为性目的而对未成年人的性器官进行的任何描述。
3. 就上文第 2 款目的而言，“未成年人”一词应包括不满 18 岁的所有人员。不过，缔约国可要求一个较低的年龄限制，但不应低于 16 岁。
4. 各缔约国可保留全部或部分不适用第 1 款(d)和(e)项以及第 2 款(b)和(c)项的权利。

第 12 条

与侵犯版权及相关权利有关的犯罪

1. 各缔约国应采取必要的立法和其他措施，根据其按照《保护文学和艺术作品伯尔尼公约》1971 年 7 月 24 日巴黎文本、《与贸易有关的知识产权协定》和《世界知识产权组织（知识产权组织）版权条约》所承担的义务，在其国内法中将故意以商业规模并借助计算机系统实施的侵犯该缔约国法律所界定的版权的行为定为刑事犯罪，但上述公约和协定所赋予的任何精神权利除外。
2. 各缔约国应采取必要的立法和其他措施，根据其在《保护表演者、唱片制作者和广播组织的国际公约》（《罗马公约》）、《与贸易有关的知识产权协定》和《世界知识产权组织表演和录音制品条约》下所承担的义务，在其国内法中将故意以商业规模并借助计算机系统实施的侵犯该缔约国法律所界定的相关权利的行为定为刑事犯罪，但上述公约和协定所赋予的任何精神权利除外。
3. 缔约国可保留在有限的情况下不根据本条第 1 款和第 2 款追究刑事责任的权利，但须有其他有效的补救措施可用，而且此种保留不减损本条第 1 款和第 2 款所述国际文书中规定的缔约国的国际义务。

第 13 条

未遂、协助和教唆

1. 各缔约国均应采取必要的立法和其他措施，在本国法律中将故意实施、协助或教唆实施根据[本公约]确立的任何犯罪行为规定为蓄意犯下该罪行的刑事犯罪。

2. 各缔约国均应采取必要的立法和其他措施，在其本国法律中将故意实施根据本公约确定的任何犯罪的未遂规定为刑事犯罪。
3. 各缔约方可保留全部或部分不适用本条第 2 款的权利。

第 14 条

起诉、审判和制裁

1. 各缔约国均应当使根据本公约确立的犯罪受到与其严重性相当的制裁。
2. 为因本公约所涵盖的犯罪起诉某人而行使本国法规定的任何法律裁量权时，各缔约国均应努力确保针对这些犯罪的执法措施取得最大成效，并适当考虑到震慑此种犯罪的必要性。
3. 就根据本公约确立的犯罪而言，各缔约国均应当根据本国法律并在适当尊重辩护方权利的情况下采取适当措施，力求确保关于保外候审或者上诉的裁决所规定的条件已经考虑到对确保被告人在其后的刑事诉讼中出庭的需要。
4. 各缔约国均应确保其法院和其他主管当局在考虑早释或假释已被判定犯有本公约所涵盖的犯罪者的可能性时，顾及此种犯罪的严重性。
5. 各缔约国均应在适当情况下在其本国法律中对于本公约所涵盖的任何犯罪规定一个较长的追诉时效期限，并在被指控犯罪的人逃避司法处置时规定更长的期限。
6. 本公约的任何规定概不影响下述原则：对于根据本公约确立的犯罪以及适用的法定抗辩事由或者决定行为合法性的其他法律原则，只应当由缔约国本国法加以阐明，而且对于这种犯罪应当根据缔约国本国法予以起诉和惩罚。

第 15 条

管辖权

1. 各缔约国应采取必要的措施，在下列情况下确立其对根据本公约确立的犯罪的管辖权：
 - (a) 犯罪发生在该缔约国领域内；或者
 - (b) 犯罪发生在当时悬挂该缔约国国旗的船只或已根据该缔约国法律注册的航空器内。
2. 在不违背本公约相关条款规定的情况下，缔约国还可以在下列情况下对任何此种犯罪确立其管辖权：
 - (a) 犯罪系针对该缔约国的国民；或者
 - (b) 犯罪者为该缔约国的国民或在其境内有惯常居所的无国籍人；或者
 - (c) 犯罪系针对该缔约国。
3. 为了本公约与引渡相关的任何条款的目的，各缔约国均可采取必要的措施，在被指控犯罪人在其领域内而其仅因该人为本国国民而不予引渡时，确立本国对根据本公约确立的犯罪的管辖权。

4. 各缔约国还可以采取必要的措施，在被指控犯罪人在其领域内而其不引渡该人时确立本国对根据本公约确立的犯罪的管辖权。
5. 如果根据本条第1款或者第2款行使管辖权的缔约国被告知或者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、起诉或者审判程序，这些缔约国的主管机关应当酌情相互磋商，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根据本国法律确立的任何刑事管辖权。

补充意见

联合王国认为，使用数字技术与未成年人进行性交往，或意图鼓励未成年人进行性交往或活动，以及为获得性满足而进行的交往，应被定为刑事犯罪，我们将在谈判期间提供有关这方面的案文。

贩运和性剥削妇女和女童是一种危害特别大的犯罪，受害者在受剥削期间遭受了大量虐待，造成了非常严重的身体和精神伤害。由于这种剥削大部分是在网上安排和促成的，因此这是一个全球问题，联合王国认为，我们需要对这一威胁采取统一的做法。联合王国支持在本公约中列入一项条款，将现代奴役和贩运人口，包括通过成人服务网站（ASW）进行的贩运和性剥削，定为刑事犯罪。

联合王国认为，未经授权分享私密图像所造成的伤害要求我们采取协调一致的方法来防止这种滥用，包括通过删除这种图像，以及确保对那些分享未经授权图像的人进行有效惩罚。联合王国希望列入应对这种危害的条款。

坦桑尼亚联合共和国

[原件：英文]
[2022年4月11日]

4. 刑事定罪

最近，由于技术发展，全世界犯罪集团为犯罪目的使用信息和通信技术的情况呈指数级增长。

4.1 罪行清单

由于这一挑战，坦桑尼亚联合共和国认为，各缔约国有必要采取必要的立法和其他措施，将故意和蓄意实施的下列行为规定为刑事犯罪，但不仅限于下列行为：

- (a) 非法访问；
- (b) 非法拦截；
- (c) 非法破坏电子数据和计算机系统；
- (d) 数据间谍活动；

- (e) 非法干扰系统；
- (f) 为犯罪目的而拥有非法设备和（或）软件；
- (g) 与计算机有关的伪造和欺诈；
- (h) 色情制品和儿童色情制品；
- (i) 与身份有关的犯罪；
- (j) 发布虚假信息；
- (k) 种族主义和仇外材料；
- (l) 种族灭绝和危害人类罪；
- (m) 网络欺凌；
- (n) 未遂、协助和教唆；
- (o) 参加有组织犯罪集团。

4.2 法人责任

坦桑尼亚联合共和国提议，公约应要求会员国在其国内立法中列入规定法人对公约所确立的犯罪承担责任的条款。这种责任可延伸到代表公司或在公司掩护下行事的自然人。

美利坚合众国

[原件：英文]

[2022年4月8日]

刑事定罪

将网络犯罪定为刑事犯罪

“非法访问”

各缔约国均应采取必要的立法和其他措施，将未经授权故意访问计算机系统的全部或任何部分的行为确定为刑事犯罪。缔约国可规定犯罪行为的实施是通过违反安全措施意图获取计算机数据或实现其他不诚实意图，或者涉及与另一计算机系统相连的计算机系统。

“非法拦截”

各缔约国均应采取必要的立法和其他措施，将未经授权故意以技术手段拦截向计算机系统、从计算机系统或在计算机系统内传输的非公开计算机数据的行为规定为刑事犯罪，包括来自载有这类计算机数据的计算机系统的电磁发射。缔约国可规定该罪行是以不诚实的意图实施的，或者涉及与另一计算机系统相连的计算机系统。

“干扰数据”

1. 各缔约国均应采取必要的立法和其他措施，将未经授权故意破坏、删除、损坏、更改或抑制计算机数据的行为定为刑事犯罪。
2. 缔约国可保留对第 1 款所述行为造成严重损害进行规定的权利。

“干扰系统”

各缔约国均应采取可能必要的立法和其他措施，将故意实施的通过输入、传输、破坏、删除、损坏、更改或抑制计算机数据而未经授权严重妨碍计算机系统运行的行为规定为刑事犯罪。

“滥用设备”

1. 各缔约国均应采取必要的立法和其他措施，将下列未经授权故意实施的行为确定刑事犯罪：
 - (a) 生产、销售、获取使用、进口、分销或以其他方式提供：
 - (i) 主要为实施根据本章前述条款所确立的任何犯罪而设计或改装的设备，包括计算机程序；
 - (ii) 计算机密码、访问代码或类似的数据，通过这些数据可以访问整个或部分计算机系统；

意图将其用于实施本章前述条款所确立的任何罪行；及

(b) 拥有上文第 1(a)(i)或(ii)款所述物品，意图将其用于实施本章前述条款所确立的任何犯罪。缔约国可依法规定在承担刑事责任之前拥有若干此类物品。

2. 如果本条第 1 款所述的生产、销售、获取使用、进口、分销或以其他方式提供或拥有并非为了实施根据本章前条确立的犯罪，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)(ii)款所述物品的销售、分销或以其他方式提供。

“与计算机有关的伪造”

各缔约国均应采取必要的立法和其他措施，将未经授权故意输入、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行为定为刑事犯罪，而不论该数据是否可直接阅读和理解。缔约国可规定在承担刑事责任之前存在欺诈或类似的不诚实意图。

“与计算机有关的欺诈”

各缔约国均应采取必要的立法和其他措施，将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，在未经授权的情况下为自己或他人获取经济利益。

“涉及儿童性虐待材料的计算机相关犯罪”

1. 各缔约国均应采取必要的立法或其他措施，确保将在知情的情况下通过计算机系统实施的下列行为定为刑事犯罪：

- (a) 制作儿童性虐待材料；
- (b) 导致直播儿童参与露骨的性行为；
- (c) 提供儿童性虐待材料；
- (d) 分发或传送儿童性虐待材料；
- (e) 为自己或他人获取儿童性虐待材料；
- (f) 拥有儿童性虐待材料；

(g) 在知情的情况下通过信息和通信技术获取儿童性虐待材料，或观看儿童参与露骨性行为的直播。

2. 各缔约国均应采取必要的立法或其他措施，将在知情情况下利用信息和通信技术劝说、诱导、怂恿或胁迫儿童或据信是儿童的人参与任何非法性活动的行为定为刑事犯罪。各缔约国均应采取必要的立法或其他措施，以确保其国内法不要求该个人是与儿童亲自见面。

“与侵犯版权及相关权利有关的计算机相关犯罪”

1. 各缔约国应采取必要的立法和其他措施，根据其按照《保护文学和艺术作品伯尔尼公约》1971年7月24日巴黎文本、《与贸易有关的知识产权协定》和《世界知识产权组织（知识产权组织）版权条约》所承担的义务，将故意以商业规模并借助计算机系统实施的侵犯该缔约国法律所界定的版权的行为定为刑事犯罪，但上述公约和协定所赋予的任何精神权利除外。

2. 各缔约国应采取必要的立法和其他措施，根据其在《保护表演者、唱片制作者和广播组织的国际公约》（《罗马公约》）、《与贸易有关的知识产权协定》和《世界知识产权组织表演和录音制品条约》下所承担的义务，在其国内法中将故意以商业规模并借助计算机系统实施的侵犯该缔约国法律所界定的相关权利的行为定为刑事犯罪，但上述公约和协定所赋予的任何精神权利除外。

3. 缔约国可保留在有限的情况下不根据本条第1款和第2款追究刑事责任的权利，但须有其他有效的补救措施可用，而且此种保留不减损本条第1款和第2款所述国际文书中规定的缔约国的国际义务。

“参与和未遂”³⁷

1. 各缔约国均应采取必要的立法和其他措施，根据本国法将以共犯、从犯或者教唆犯等任何身份参与根据本公约确立的犯罪定为刑事犯罪。
2. 各缔约国均可以采取必要的立法和其他措施，根据本国法将实施根据本公约确立的犯罪的任何未遂和中止规定为刑事犯罪。
3. 各缔约国均可以采取必要的立法和其他措施，根据本国法将为实施根据本公约确立的犯罪进行预备的行为规定为刑事犯罪。

法人责任³⁸

1. 各缔约国均应当采取符合其法律原则的必要措施，确定法人对根据本公约确立的犯罪应当承担的责任。
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、民事责任或者行政责任。
3. 法人责任不应影响实施这种犯罪的自然人的刑事责任。
4. 各缔约国均应当特别确保使依照本条应当承担责任的法人受到有效、适度 and 劝阻性的刑事或者非刑事制裁，包括金钱制裁。

起诉、审判和制裁³⁹

1. 各缔约国均应当使根据本公约刑事定罪条款确立的犯罪受到与其严重性相当的制裁。
2. 为因本公约所涵盖的犯罪起诉某人而行使本国法律规定的任何法律裁量权时，各缔约国均应努力确保针对这些犯罪的执法措施取得最大成效，并适当考虑到震慑此种犯罪的必要性。
3. 就根据本公约刑事定罪条款确立的犯罪而言，各缔约国均应当根据本国法律并在适当尊重辩护方权利的情况下采取适当措施，力求确保关于保外候审或者上诉的裁决所规定的条件已经考虑到对确保被告人在其后的刑事诉讼中出庭的需要。
4. 各缔约国均应确保其法院和其他主管当局在考虑早释或假释已被判定犯有本公约所涵盖的犯罪者的可能性时，顾及此种犯罪的严重性。
5. 各缔约国均应在适当情况下在其本国法律中对于本公约所涵盖的任何犯罪规定一个较长的追诉时效期限，并在被指控犯罪的人逃避司法处置时规定更长的期限。
6. 本公约的任何规定概不影响下述原则：对于根据本公约确立的犯罪以及适用的法定抗辩事由或者决定行为合法性的其他法律原则，只应当由缔约国本国法加以阐明，而且对于这种犯罪应当根据缔约国本国法予以起诉和惩罚。

³⁷ 《联合国反腐败公约》，第二十七条。

³⁸ 《联合国打击跨国有组织犯罪公约》第十条和《联合国反腐败公约》第二十六条。

³⁹ 《联合国打击跨国有组织犯罪公约》第十一条。

洗刷网络犯罪所得行为的刑事定罪⁴⁰

1. 各缔约国均应当根据本国法律的基本原则，采取必要的立法和其他措施，将故意实施的下列行为定为刑事犯罪：

(a)(i) 明知财产为犯罪所得，为隐瞒或者掩饰该财产的非法来源，或者为协助任何参与实施上游犯罪者逃避其行为的法律后果而转换或者转移该财产；

(ii) 明知财产为犯罪所得而隐瞒或者掩饰该财产的真实性质、来源、位置、处置、转移、所有权或者有关的权利；

(b) 在符合本国法律制度基本概念的情况下：

(i) 在得到财产时，明知其为犯罪所得而仍获取、占有或者使用；

(ii) 对本条所确立的任何犯罪的参与、协同或者共谋实施、实施未遂以及协助、教唆、便利和参谋实施。

2. 为实施或者适用本条第 1 款：

(a) 各缔约国均应根据本公约刑事定罪条款确立的犯罪列为上游犯罪。缔约国立法中如果明确列出上游犯罪清单，则至少应包括本公约中规定的犯罪。

(b) 就(b)项的目的而言，上游犯罪应包括在有关缔约国司法管辖权范围之内和之外发生的犯罪。然而，如果犯罪发生在一缔约国司法管辖权范围之外，则只有当该行为根据其发生地所在国法律为犯罪，而且根据实施或者适用本条的缔约国的法律该行为若发生在该国也为犯罪时，才构成上游犯罪；

(c) 各缔约国均应当向联合国秘书长提供其实施本条的法律以及这类法律随后的任何修改的副本或说明；

(d) 如果缔约国本国法律基本原则要求，则可以规定本条第 1 款所列犯罪不适用于实施上游犯罪的人；

(e) 本条第 1 款所规定的作为犯罪要素的明知、故意或目的可根据客观实际情况推定。

妨害司法的刑事定罪⁴¹

各缔约国均应采取必要的立法措施和其他措施，将故意实施的下列行为规定为刑事犯罪：

(a) 在涉及本公约所涵盖的犯罪的诉讼中使用暴力、威胁或恐吓，或许诺、提议给予或给予不正当好处，以诱使提供虚假证言或干扰证言或证据的提供；

(b) 使用暴力、威胁或恐吓，干扰司法或执法人员针对本公约所涵盖的犯罪执行公务。本项规定概不应影响缔约国制定保护其他类别公职人员的立法的权利。

⁴⁰ 改编自《联合国打击跨国有组织犯罪公约》第六条。

⁴¹ 《联合国打击跨国有组织犯罪公约》第二十三条。

委内瑞拉玻利瓦尔共和国

[原件：西班牙文]

[2022 年 4 月 13 日]

5. 刑事定罪

公约将责成缔约国确立刑事犯罪和其他犯罪，以便在公约所界定的行为根据国内法尚不构成犯罪的情况下，涵盖与使用信息和通信技术有关的广泛非法行为。在某些情况下，各国在法律义务确定罪行，而在另一些情况下，为了考虑到各国立法的差异，各国在义务制定有关立法。

因此，必须明确界定利用信息和通信技术实施的并在国际社会得到广泛承认的犯罪活动。该公约应提供一个前瞻性框架，以期协调刑事定罪，满足当前和未来的信息和通信技术发展需求，并打击犯罪。

鉴于上述情况，各缔约国应采取必要的立法、政策和其他措施，以确定有关犯罪。因此，公约应载有条款确保需要调整其国家立法和计划的国家有时间这样做，并得到必要的支持。

公约所涵盖的主要犯罪应包括以下内容：

- 未经适当授权获取数字信息，而这种获取导致该信息被破坏、屏蔽或修改
- 未经适当授权和（或）违反既定规则，有预谋地拦截数字信息，包括通过使用技术手段拦截流量数据和以信息和通信技术手段处理的非公共用途数据
- 通过破坏、删除、更改、屏蔽或修改数字信息来非法操纵数字信息
- 有预谋的非法行为，意图导致信息和通信网络发生故障，引起或有风险造成严重后果
- 使用和分发恶意软件，意图未经授权破坏、屏蔽、修改或传播数字信息，或使安全功能失效
- 故意和有预谋地创建、分发和（或）使用软件或其他数字信息，意图非法操纵关键信息基础设施，包括破坏、屏蔽或修改其中所含信息或使安全功能失效
- 在知情的情况下故意制作、传播和（或）使用软件或其他数字信息，旨在非法干扰关键信息基础设施，包括软件或其他数字信息，以销毁、屏蔽、修改或复制其中所载信息，或者使其安全功能失效
- 违反用来存储、处理和传送关键信息基础设施或信息系统所载受保护数字信息的方式、或属于关键信息基础设施的信息系统或信息和通信网络的操作规则，或违反访问它们的规则，如果此类违规行为损坏了关键信息基础设施。

- 盗窃财产或非法获取财产权利，包括通过破坏、屏蔽或修改数字信息或以其他方式干扰信息和通信技术运营的欺诈手段
- 以信息和通信技术手段发出的旨在暴力推翻另一国政府的颠覆或武装活动的呼吁
- 以信息和通信技术手段发出呼吁，煽动、招募人员从事或以其他方式参与恐怖主义活动，为恐怖主义进行宣传和辩护，或为资助恐怖主义筹集或提供资金
- 利用信息和通信技术手段贩运麻醉药品和精神药物及其制造所需材料
- 利用信息和通信技术贩运武器、弹药、爆炸装置和爆炸物
- 未经授权以销毁、修改、复制或共享为目的获取个人数据
- 与制作和传播带有未成年人色情图像的材料或物品有关的信息和通信技术相关犯罪
- 涉及未成年人参与危害其生命或健康的非法行为的犯罪

越南

[原件：英文]

[2022 年 4 月 12 日]

第二章. 刑事定罪

5. 各会员国均应采取必要的立法和其他措施，将未经授权故意实施的下列行为确定为刑事犯罪：

- (a) 制造、交易、转让旨在攻击计算机网络、电信网或电子设备的工具、设备或软件，以用于本公约所管辖的犯罪活动；
- (b) 传播对计算机网络、电信网或者电子设备有害的软件程序；
- (c) 删除、破坏或修改软件程序或数字数据；
- (d) 阻碍计算机网络、电信网或者电子设备的数据传输；
- (e) 妨碍或者干扰计算机网络、电信网或者电子设备的正常运行；
- (f) 通过绕过安全或保护系统、滥用他人的管理权或任何其他方式控制或干扰电子设备的运行；
- (g) 窃取、修改、破坏或伪造信息或数据；
- (h) 将计算机网络、电信网或电子设备用于以下目的：
 - (i) 利用组织或者个人的银行账户或银行卡信息非法侵占资产；
 - (ii) 制造、持有、交易、使用伪造的银行卡，非法侵占资产；

- (iii) 擅自进入政府机构、组织和个人账户，非法侵占资产；
 - (iv) 在电子商务、电子支付、网上货币交易、网上集资、网上多层级营销或网上证券交易中实施以侵占财产为目的的欺诈；
 - (v) 以侵占财产为目的，擅自开办或者提供电信或互联网服务；
 - (i) 收集、持有、买卖、转让或公开个人和组织的银行账户信息。
 - (j) 未经所有者同意，买卖、转让、修改、公开政府机构、组织或个人的私密信息；
 - (k) 利用网络空间、信息技术或电子设备实施恐怖主义行为或资助恐怖主义。
6. 本公约的任何规定均不应阻止会员国采取必要的立法和其他措施，将涉及为犯罪目的使用信息和通信技术的任何其他行为定为刑事犯罪。
7. 本公约的任何规定概不影响下述原则：对于根据本公约确立的犯罪以及适用的法定抗辩事由或者决定行为合法性的其他法律原则，只应当由会员国本国法加以阐明，而且对于这种犯罪应当根据会员国本国法予以起诉和惩罚。
-