联合国 A/C.3/72/12*

大 会

Distr.: General
16 October 2017
Chinese
Original: Russian

第七十二届会议

第三委员会

议程项目 107

预防犯罪和刑事司法

2017 年 10 月 11 日俄罗斯联邦常驻联合国代表给秘书长的信

我谨随函提交《联合国合作打击网络犯罪公约》草案(见附件)。

请将本函及其附件作为大会议程项目 107 的文件分发为荷。

瓦西里·涅边贾(签名)

* 由于技术原因于 2018 年 1 月 29 日重发。

17-18234 * (C) 141217 310118

2017 年 10 月 11 日俄罗斯联邦常驻联合国代表给秘书长的信的附件

联合国合作打击网络犯罪公约草案

目录

序言

本公约缔约国，

关切信息和通信技术(信通技术)领域的犯罪对社会稳定和安全造成严重问题和威胁，破坏民主体制和价值观、道德观和正义，并对可持续发展和法治产生不利影响，

又关切不当使用信通技术的犯罪为洗钱等其他形式的犯罪活动提供了大量机会，

还关切信通技术犯罪案件涉及巨额资产，可能构成有关国家资源的很大一部分，并且威胁这些国家的政治稳定和可持续发展，

深信信通技术犯罪是影响所有国家社会和经济的跨国现象，因此，开展预防打击信通技术犯罪的国际合作至关重要，

又深信应通过提供技术援助，将各缔约国的信息和电信系统技术水平提升到同等程度，这在加强各国有效预防犯罪和提高信息安全水平的能力方面发挥着重要作用，

决心更有效地预防、发现并制止通过信通技术犯罪而非法获得的资产进行国际转移，并加强在追回资产方面的国际合作，

铭记预防和消除信通技术犯罪是所有国家的责任，各国必须彼此合作，在公共部门以外的个人和团体，如民间社会的支持和参与下，确保这一领域的努力取得成效，因为整个信息环境的总体安全取决于每个国家所作的努力，

深信网络空间的使用应严格依照公认的国际法原则和准则、尊重人权和自由原则以及和平解决争端原则，

铭记每个国家在其领土上对网络空间拥有主权并依照其国内法行使管辖权，

又铭记公平、责任和法律面前人人平等原则，有必要培育不容忍信通技术犯罪的文化，

兹议定如下：

第一章
总则

第一条
宗旨

本公约的宗旨如下：

(a) 促进和加强旨在有效预防和打击信通技术领域犯罪和其他违法行为的措施；

(b) 预防危害信通技术保密性、完整性和可获性的行为以及不当使用信通技术的行为，为此将本公约载述的此类行为定为刑事犯罪，为有效打击此类犯罪和其他违法行为充分授权，为在国内国际两级发现、调查和起诉此类行为提供便利，并做出国际合作安排；

(c) 提高国际合作效率并将之深化，包括在就预防和打击信通技术犯罪问题进行人员培训和提供技术援助领域的合作。

第二条
适用范围

1. 本公约依其规定适用于预防、调查和起诉本公约第六条至第十九条规定的犯罪和其他违法行为，并且适用于采取措施查明、阻止和消除此类行为的后果，包括暂停与实施本公约规定的任何犯罪或其他违法行为所获资产有关的交易，以及扣押、没收和返还此类犯罪所得。

2. 为执行本公约之目的，其中规定的犯罪和其他违法行为不必导致损害，但本公约另有规定的除外。

第三条
保护主权

1. 在履行本公约规定的义务时，缔约国应恪守国家主权原则、各国主权平等原则和不干涉别国内政原则。

2. 本公约不授权缔约国在另一国领土内行使该另一国国内法规定专属于该国当局的管辖权及职能。

第四条
用语

就本公约而言：

(a) “扣押财产”系指按照法院或其他主管当局的命令暂时禁止财产转移、转换、处置或移动，或暂时对财产实施扣留或控制；

(b) “僵尸网络”系指在用户不知情的情况下已被安装恶意软件并受到集中控制的两个或两个以上信通技术装置；

(c) “恶意软件”系指以未经授权修改、破坏、复制和阻拦信息或使信息保护软件失效为目的的软件；

(d) “儿童色情制品”具有 2000 年 5 月 25 日《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》赋予该用语的含义；

(e) “所得”系指直接或间接通过实施本公约和国内法规定的犯罪或其他违法行为而产生或获得的任何财产；

(f) “信息和通信技术”(信通技术)系指为生成、转换、传输、利用和存储信息而相互联接的方法、流程、硬件和软件的集合；

(g) “财产”系指各种资产，不论其为动产或不动产、有形或无形，以及证明对这些资产或其任何组成部分拥有所有权的文件或信息；

(h) “信息”系指任何数据(消息、记录)，不论其呈现形式；

(i) “没收”系指按照法院或其他主管当局的命令，强行剥夺财产而不予补偿；

(j) “关键基础设施”系指为了国家、国防或安全，包括个人安全之利益而开展活动的国家设施、系统和机构；

(k) “有组织犯罪集团”系指由两人或更多人组成、在一段时期内存在并以实施本公约规定的一项或多项犯罪为目的而一致行动的有组织结构的集团；

(l) “服务提供者”系指㈠ 向其所服务的用户提供利用信通技术进行通信的能力的任何公共或私营实体，㈡ 代表一上文㈠中所述实体或使用该实体所提供服务的用户，处理或存储电子信息的任何其他实体；

(m) “垃圾信息”系指向地址列表(数据库)中未向发送方告知消息送达地址、未同意接收消息且无法拒绝发送方发送消息的各方发送的电子消息；

(n) “流量数据”系指与采用信通技术转移数据有关，特别是显示基础网络服务的起点、终点、路由、时间、日期、规模、持续时间和类型的任何电子信息，但不包括被转移数据的内容；

(o) “信通技术装置”系指用于或设计用于自动处理和存储电子信息的硬件组件的集合(组合)体。

第二章
入罪和执法

第一节
法律责任的确立

第五条
法律责任的确立

1. 各缔约国应采取必要立法措施和其他措施，在其国内法中将本公约第六至十二条、第十五条、第十八条和第十九条所述行为规定为犯罪或其他违法行为，并在考虑到具体罪行的公共危险程度及其造成的损害量基础上，适用监禁等刑罚和其他处罚。

2. 各缔约国均应采取必要立法和其他措施，在其国内法中将本公约第十三条、第十四条、第十六条和第十七条所述行为规定为犯罪或其他违法行为。

3. 各缔约国均应采取必要立法和其他措施，在其国内法中将对关键基础设施信通技术装置实施的本公约第六条、第八条、第九条、第十条和第十五条所述行为规定为犯罪。

4. 各缔约国均应确保，本公约第二十条规定负有责任的法人应受到有效、适度和劝阻性处罚，包括金钱处罚。

5. 在不影响一般国际法准则的情况下，本公约不应排除缔约国行使其本国法律规定的刑事管辖权的可能性。

第六条
未经授权访问电子信息

各缔约国均应采取必要立法和其他措施，在其国内法中将故意未经授权访问电子信息的行为规定为犯罪或其他违法行为。

第七条
未经授权截取

各缔约国均应采取必要立法和其他措施，在其国内法中规定，在未经适当授权和(或)违反既定规则的情况下使用技术手段截取非供公众使用的流量技术参数和通过信通技术处理的数据，故意截取电子信息，构成犯罪或其他违法行为。

第八条
未经授权的数据干扰

各缔约国均应采取必要立法和其他措施，在其国内法中将未经授权故意修改、阻拦、破坏或复制电子信息的行为规定为犯罪或其他违法行为。

第九条
阻断信通技术运行

缔约国均应采取必要立法和其他措施，在其国内法中确认，未经授权、故意以阻断信通技术运行为目的的行为构成犯罪或其他违法行为。

第十条
创建、利用和散发恶意软件

1. 各缔约国均应采取必要立法和其他措施，在其国内法中规定，除为研究目的外，故意创建、利用和散发恶意软件的行为构成犯罪或其他违法行为。

2. 各缔约国均应采取必要立法和其他措施，在其国内法中规定，为实施本公约第六至十条所述任何行为之目的而创建或利用僵尸网络，构成犯罪或其他违法行为。

第十一条
散发垃圾信息

各缔约国均应采取必要立法和其他措施，在其国内法中规定，散发垃圾信息构成犯罪或其他违法行为。

第十二条
未经授权贩运装置

各缔约国均应采取必要立法和其他措施，在其国内法中规定，非法制造、出售、为使用而购买、进口、出口或为使用而以其他形式转移主要为实施本公约第六至九条所规定犯罪而设计或改装的装置，构成犯罪或其他违法行为。

第十三条
与信通技术有关的盗窃

1. 各缔约国均应采取必要立法和其他措施，在其本国法律中规定，采用复制、修改、删除或阻止电子信息或者其他干扰信通技术运行的手段故意盗窃财产的行为构成犯罪或其他违法行为。

2. 各缔约国可保留一项权利，即在与信通技术有关的盗窃行为以其国内法所规定形式实施的情况下，将此类盗窃行为视为加重处罚情节。

第十四条
与儿童色情有关的犯罪

各缔约国均应采取必要立法和其他措施，在其国内法中规定，制作、持有、取得和加工处理以及散发电子形式的儿童色情制品，构成犯罪。

第十五条
与网络钓鱼有关的犯罪

1. 各缔约国均应采取必要立法和其他措施，在其国内法中规定，为非法目的而创建和使用可被误认为用户已知或所信任数据的电子信息，构成犯罪或其他违法行为。

2. 各缔约国可保留一项权利，即可将与该缔约国国内法规定的其他犯罪同时实施的或带有实施这些其他犯罪意图的网络钓鱼行为视作刑事犯罪。

第十六条
与国内法规定受保护数据有关的犯罪

各缔约国均应采取必要立法和其他措施，在其国内法中规定，使用信通技术发布电子信息，如其中包含构成一国机密的数据并有适当标记表明所发布信息是另一缔约国国内法规定保护的信息，则构成犯罪。

第十七条
利用信通技术实施国际法规定为犯罪的行为

1. 各缔约国均应采取必要立法和其他措施，在其国内法中规定，为实施本公约附件一所列任何一项国际条约规定为犯罪的行为而使用信通技术，构成犯罪。

2. 在交存其批准、接受、核准或加入文书之时不是本公约附件一所列的一项条约之缔约方的本公约缔约国可声明，在对该缔约国适用本公约时，应将该条约视为不包含于上述附件。而一旦该条约对该缔约国生效，则声明即失效，且该缔约国应将此事实通知保存人。

3. 若一缔约国不复为本公约附件一所列任何条约的缔约方，则可就该条约作出本条所规定的声明。

第十八条
与信通技术有关的侵犯版权和相关权利行为

1. 各缔约国均应采取必要立法和其他措施，在其国内法中规定，若故意实施该缔约国制定法所规定的侵犯版权和相关权利行为，则构成犯罪或其他违法行为。

2. 各缔约国均应采取必要立法和其他措施，在其国内法中规定，若利用信通技术故意实施该缔约国制定法所规定的侵犯版权行为，则构成犯罪。

第十九条
协助、预备实施犯罪和犯罪未遂

1. 各缔约国均应采取必要立法和其他措施，在其国内法中规定，以任何形式参与实施本公约条款规定为犯罪的行为，例如作为共犯、帮助犯或教唆犯，均构成犯罪。

2. 各缔约国可采取必要立法和其他措施，在其国内法中规定，一个人直接以实施犯罪为目的故意采取行动，即使由于不受该人控制的原因而未实施该罪行，也构成犯罪。

3. 各缔约国可采取必要立法和其他措施，在其国内法中规定，一个人制造或改造犯罪手段或工具、寻找共犯、共谋实施犯罪或以任何其他方式故意为实施犯罪创造条件，即使由于不受该人控制的原因而未实施罪行，也构成犯罪。

第二十条
法人的法律责任

1. 各缔约国均应采取必要立法和其他法律措施，确保能够就因具备下列条件而在法人内部担任领导职位的任何自然人为该法人利益独自或作为相关法人机关一部分实施的本公约所规定刑事犯罪或其他违法行为，追究该法人的法律责任：

(a) 该法人的委托授权书；

(b) 代表该法人作出决定的职权；

(c) 在该法人内部行使控制的职权。

2. 在本条第 1 款已经规定的情况之外，各缔约国还应采取必要措施，确保在以下情况下能够追究法人的法律责任：由于第 1 款所述之自然人对法人缺乏监督或控制，致使根据该法人授权行事的自然人得以为该法人利益实施依本公约条款规定的犯罪或其他违法行为。

3. 以不违反相关缔约国适用的法律原则为限，法人的法律责任可为刑事、民事或行政责任。

4. 法人的这一法律责任不应影响实施犯罪或其他违法行为的自然人的法律责任。

第二节
执法

第二十一条
程序性规定的范围

1. 各缔约国均应采取必要立法和其他措施，为预防、制止和调查犯罪以及进行与犯罪有关的司法程序之目的，确立本节条款所设想的权力和程序。

2. 除本公约第二十八条另有规定外，各缔约国均应将本条第 1 款所述权力和程序适用于：

(a) 本公约第六至十九条规定的刑事犯罪和其他违法行为；

(b) 通过信通技术手段实施的其他刑事犯罪和其他违法行为；

(c) 收集实施刑事犯罪和其他违法行为的证据，包括电子形式的证据。

3. (a) 各缔约国均可作出一项保留，声明该缔约国保留将本公约第二十七条所述措施仅适用于该项保留中具体列明的刑事犯罪或刑事犯罪类别的权利，前提是这些刑事犯罪或刑事犯罪类别范围不得窄于该缔约国对之适用本公约第二十八条所述措施的刑事犯罪范围。各缔约国均应考虑限制适用此项保留，以便本公约第二十七条规定的措施得到最广泛适用；

(b) 若一缔约国在通过本公约之时由于其国内现行制定法的限制而无法将本公约第二十七条和第二十八条所述措施适用于一服务提供者信息系统中正在传输的数据，并且该系统㈠ 仅为一个封闭用户群的利益而运行且㈡ 没有使用信息和电信网络，也不与其他信息系统联接，则该缔约国可保留不对该数据的传输适用上述措施的权利。各缔约国均应考虑限制适用此项保留，以便本公约第二十七条和第二十八条规定的措施得到最广泛适用。

4. 若在一国境内实施的犯罪案件中，被指控的行为人是该国公民并处于该国境内，且没有任何其他国家有任何理由依照本公约的规定行使管辖权，则案件不适用本公约。

第二十二条
条件和保障措施

1. 各缔约国均应确保，确立、执行和适用本节规定的权力和程序须遵循其本国制定法为确保充分保护人权和自由，包括为保护该缔约国根据 1966 年 12 月 16 日《公民权利和政治权利国际公约》及其他适用国际人权文书承担的义务所致权利而规定的条件和保障措施。

2. 考虑到所涉权力和程序的性质，此类条件和保障措施除其他外，应包括司法或其他独立监督、适用理由以及对权力或程序的范围和持续期的限制。

3. 在符合公共利益、特别是司法方面利益的限度内，缔约国应考虑本节所规定的权力和程序对第三方权利、责任及合法利益的影响。

第二十三条
快速保全已存储的计算机数据

1. 各缔约国均应采取必要立法和其他措施，使本国主管当局能够作出适当命令或指示或通过类似手段确保，尤其是在有理由认为数据特别易被删除、复制或修改的情况下确保迅速保全特定计算机数据，包括流量数据。

2. 若一缔约国通过命令个人保全由该人持有或控制的特定已存储数据实施本条第 1 款的规定，则该缔约国应采取必要立法和其他法律措施，要求该人在最长可达 180 天的所需期间内保全这些数据并维护其完整性，以便主管当局寻求予以披露。缔约国可规定，此类命令随后可以延长。

3. 各缔约国均应采取必要立法和其他措施，要求负责保全数据的个人在其国内制定法所规定的期间内对履行此类程序一事保密。

4. 本条所述权力和程序应符合本公约第二十一条和第二十二条的规定。

第二十四条
快速保全和部分披露流量数据

1. 各缔约国均应就本公约第二十三条规定应予保全的流量数据，采取必要立法和其他措施，旨在：

(a) 确保无论有多少服务提供者参与了相关信息传输都有可能迅速保全流量数据；

(b) 确保快速向缔约国主管当局或该当局指定人员披露数量充分的流量数据，以便相关缔约国能够查明服务提供者以及所指信息的传输路由。

2. 本条所述权力和程序的确立应符合本公约第二十一条和第二十二条的规定。

第二十五条
提供令

1. 为本公约第二十一条第 1 款所述目的，各缔约国均应采取必要立法和其他措施，授权其主管当局命令：

(a) 在其境内的一人员提供由该人持有或控制的特定计算机数据；

(b) 在其境内提供服务的服务提供者提交由其持有或控制的用户信息。

2. 本条所述权力和程序的确立应符合本公约第二十一条和第二十二条的规定。

3. 就本条而言，用语“用户信息”系指一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、为此提供的技术支持和服务期；

(b) 可从服务协议或安排中获取的用户身份、邮政地址或其他地址、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) 与服务协议或安排有关、涉及信息和通信装置所在位置的任何其他信息。

第二十六条
搜查和扣押已存储或处理的计算机数据

1. 各缔约国均应采取必要立法和其他措施，授权其主管当局寻求访问该国境内的：

(a) 信通技术装置以及其中存储的计算机数据；和

(b) 可能存有所查找计算机数据的计算机数据存储介质。

2. 各缔约国均应采取必要立法和其他措施，确保若其主管当局在根据本条第 1 款(a)项的规定进行搜查时有理由相信所查找的数据存储于该缔约国境内另一信通技术装置内，则该主管当局应能够迅速进行搜查，以访问该另一信通技术装置。

3. 各缔约国均应采取必要立法和其他措施，授权其主管当局扣押在该缔约国境内或其管辖之下的计算机数据，或者通过类似手段保护该数据安全。这些措施应包括提供以下权力：

(a) 扣押用于存储信息的信通技术装置或通过其他手段确保其安全；

(b) 制作并保留这些计算机数据的副本；

(c) 维护已存储的有关计算机数据的完整性；

(d) 从信通技术装置中删除以电子形式存储或处理的数据。

4. 各缔约国均应采取必要立法和其他措施，授权其主管当局根据其国内制定法制定的程序，命令对有关信息系统、信息和电信网络或其部件或其中所含信息所适用的保护措施的运作具有专门知识的人员在实施本条第 1 至 3 款所述措施方面提供必要信息和(或)协助。

5. 本条所述权力和程序的确立应符合本公约第二十一条和第二十二条的规定。

第二十七条
实时收集流量数据

1. 各缔约国均应采取必要立法和其他措施，授权其主管当局：

(a) 运用技术手段收集或记录该缔约国境内与使用信通技术有关的流量数据；及

(b) 要求服务提供者以其拥有的技术能力为限：

㈠ 运用技术手段收集或记录该缔约国境内的流量数据；或

㈡ 配合并协助该缔约国主管当局实时收集或记录该国境内与特定信息有关的流量数据。

2. 若一缔约国由于其国内法律制度由来已久的原则而不能采取本条第 1 款(a)项规定的措施，则可转而采取必要立法和其他措施，确保在其境内运用技术手段实时收集或记录流量数据。

3. 各缔约国均应采取必要立法和其他措施，要求服务提供者对本条所规定任何权力的行使及与之相关的任何信息保密。

4. 本条所述权力和程序应符合本公约第二十一条和第二十二条的规定。

第二十八条
收集通过信通技术传输的信息

1. 各缔约国均应采取必要立法和其他措施，授权其主管当局针对本公约所规定且由其国内制定法所确定的犯罪：

(a) 在该缔约国境内运用技术手段，收集或记录通过信通技术传输的信息；及

(b) 要求服务提供者以其拥有的技术能力为限：

㈠ 在该缔约国境内运用技术手段，收集或记录通过信通技术传输的计算机信息；或

㈡ 配合并协助该缔约国主管当局实时收集或记录该缔约国境内通过信通技术传输的计算机信息。

2. 若一缔约国由于其国内法律制度由来已久的原则而不能采取本条第 1 款(a)项所述措施，则可转而采取必要立法和其他措施，确保在该国境内运用技术手段实时收集或记录其境内通过信通技术传输的计算机信息。

3. 各缔约国均应采取必要立法和其他措施，要求服务提供者对本条所规定任何权力的行使及与之相关的任何信息保密。

4. 本条所述权力和程序应符合本公约第二十一条和第二十二条的规定。

第三节
资产追回

第二十九条
一般规定

缔约国应根据本公约及其国内制定法的规定，为追回资产相互提供最广泛的合作和协助，同时顾及区域、区域间和多边组织打击洗钱的有关举措。

第三十条
预防和发现犯罪所得的转移

1. 缔约国应根据其国内制定法，采取必要措施，在其管辖范围内金融机构的客户和受益所有人据报可能参与实施了本公约规定的犯罪，或者其家庭成员或密切关联人或代表其行事的其他个人可能参与实施了本公约规定的犯罪的情况下，要求这些金融机构核实所涉客户和受益所有人的身份，包括提供其账户信息。

2. 缔约国应根据其国内制定法，采取一切必要措施，要求金融机构对本条第 1 款所述之人曾试图开立或维持的有关账户采取合理控制措施。

3. 应合理设计本条第 1 款和第 2 款所述措施，以期发现可疑交易并向主管当局报告，并且不应将上述措施解释为阻止或禁止金融机构与任何正当客户开展业务。

4. 为了促进执行本条第 1 款和第 2 款规定的措施，各缔约国均应在适当情况下应另一缔约国的请求或主动向其管辖范围内的金融机构通告特定自然人或法人的身份，金融机构则将对这些自然人或法人以及金融机构另行确定身份的其他人的账户适用强化审查。

5. 各缔约国均应采取措施，确保其金融机构在适当期间内对涉及本条第 1 款所述之人的账户和交易保持适足的记录，其中至少应载有关于客户身份的信息以及尽可能载有关于受益所有人身份的信息。

6. 为了预防和发现转移本公约规定的犯罪所得的行为，各缔约国均应采取适当和有效措施，在其监管和监督机构帮助下，防止设立无实体机构且未与一受监管的金融集团建立附属关系的银行。此外，缔约国可考虑要求其金融机构拒绝与此类机构建立或继续保持代理行关系，并防范那些允许无实体机构且未与一受监管的金融集团建立附属关系的银行使用其账户的外国金融机构，不与之建立关系。

7. 各缔约国均应考虑依照其国内制定法，针对据报可能参与实施了本公约条款所规定罪行的相应人员制定有效的财务披露制度，并为不遵守该制度的行为规定适当的制裁措施。各缔约国还应考虑采取必要措施，允许本国主管当局在必要时与其他缔约国主管当局共享这些信息，以便调查并追回本公约规定的犯罪之所得。

第三十一条
直接追回财产的措施

各缔约国均应依照其国内制定法，采取必要立法或其他措施：

(a) 准许另一缔约国、其公民和永久居住在其境内的无国籍人和在其境内设立的或有常驻代表的法人在该缔约国法院提起民事诉讼，确立对通过实施本公约规定的犯罪或其他违法行为取得的财产的所有权；

(b) 准许本国法院下令支付与本公约规定的犯罪或其他违法行为有关的补偿金或损害赔偿金；并

(c) 准许本国法院或主管当局在必须作出关于没收的决定时，确认另一缔约国、其公民和永久居住在其境内的无国籍人以及在其境内设立的或有常驻代表的法人提出的关于他们是通过实施本公约规定的犯罪或其他违法行为取得的财产的合法所有人的权利主张。

第三十二条
通过没收事宜国际合作追回财产的机制

1. 各缔约国为提供与通过实施本公约规定的犯罪取得的财产或用于实施犯罪的工具有关的司法互助，应依照其国内制定法：

(a) 采取必要措施，准许其主管当局执行另一缔约国的法院发布的没收令；

(b) 采取必要措施，准许其主管当局在拥有管辖权的情况下，通过对洗钱犯罪进行裁断，命令没收因本公约规定的犯罪而收到的源自外国的此类财产；

(c) 考虑采取必要措施，在因犯罪行为人死亡、潜逃或缺席而无法予以起诉的案件中或在其他适当情形下，允许不经刑事定罪而没收此类财产。

2. 各缔约国应另一缔约国的请求为其提供司法互助时，应根据其国内制定法：

(a) 采取必要措施，准许本国主管当局根据提出请求的缔约国的法院或主管当局发出的扣押令扣押财产，前提是请求国提供了合理根据，使被请求国相信，有充分理由采取该行动并且最终将对该财产施加本条第 1(a)款所述没收令；

(b) 采取必要措施，准许本国主管当局根据请求扣押财产，前提是相关请求提供了合理根据，使被请求国相信，有充足理由采取行动并且最终将对该财产施加本条第 1(a)款所述没收令；

(c) 考虑采取补充措施，准许本国主管当局基于与财产的取得有关的外国逮捕令或刑事指控等依据，为没收目的而对有关财产进行保全。

第三十三条
没收事宜国际合作

1. 一缔约国在收到对本公约规定的一项犯罪拥有管辖权的另一缔约国关于如本公约第三十五条第 1 款所述没收位于被请求国境内、因实施本公约规定的犯罪而取得的财产或犯罪实施工具的请求后，应在根据其国内制定法可能的范围内：

(a) 将该请求提交其主管当局，以便取得没收令并在没收令发出后予以执行；或

(b) 向其主管当局提交提出请求的缔约国境内法院发布的没收令，以期在所请求的范围内，且在与位于被请求国境内因实施本公约规定的犯罪而取得的财产或用于实施该犯罪的工具有关的范围内予以执行。

2. 在对本公约规定的犯罪拥有管辖权的缔约国提出请求后，被请求的缔约国应采取措施，查明或扣押因实施本公约规定的犯罪而取得的财产或本条第 1 款(b)项提及的用于实施该犯罪的工具，以便由提出请求的缔约国命令，或者依照请求国根据本条第 1 款提出的请求，而最终予以没收。

3. 被请求的缔约国应依照其国内制定法以及在该国与提出请求的缔约国关系方面可能约束该国的任何双边或多边协定或安排的规定，作出或采取本条第 1 款和第 2 款规定的决定或行动。

4. 各缔约国均应向联合国秘书长提供该国实施本条规定的法律和法规以及其后各项修正案副本或说明。

5. 若被请求的缔约国未及时收到提出请求的缔约国主管当局的命令或被请求国主管当局作出决定所需的文件，则可拒绝根据本条提交的请求或解除临时措施。

6. 在解除根据本条采取的任何临时措施之前，被请求的缔约国应尽可能向提出请求的缔约国提供一次说明须继续执行临时措施的理由的机会。

7. 不应对本条规定作损害善意第三人权利的解释。

第三十四条
特别合作

若认为披露关于因实施本公约规定的犯罪而产生的财产的信息有可能为接收信息的另一缔约国主管当局提供启动调查或司法程序的理由，或者有可能导致该另一缔约国根据本章规定提出请求，则各缔约国均应在不违背其国内法的情况下努力采取措施，以不妨碍本国主管当局开展的调查或司法程序为前提，主动向该另一缔约国提供该信息。

第三十五条
财产的返还和处置

1. 已按照本章条款没收财产的缔约国应按照本条第 3 款及其国内法处置该财产，包括将财产归还之前的合法所有人。

2. 各缔约国均应采取一切必要立法和其他措施，使本国主管当局能够在考虑到善意第三方权利的基础上，依照其国内法，在根据另一缔约国依照本公约规定提出的请求而采取行动时，返还所没收的财产。

3. 根据本公约第三十三条以及本条第 1 款和第 2 款的规定，被请求的缔约国应：

(a) 在盗用公共财产案件中，向提出请求的缔约国返还已按照本公约第三十三条的规定并根据在请求国境内作出的终局判决而没收的财产，但被请求国可免除关于请求国须作出终局判决的这一要求；

(b) 在所有其他案件中，优先考虑将所没收财产归还给之前的合法所有人或者用于向罪行受害者支付补偿或损害赔偿。

4. 除非缔约国另有决定，否则被请求的缔约国可在适当时扣除为按照本条规定返还或处置所没收财产而开展的调查或司法程序所致合理费用。

5. 缔约国可进行协商并缔结单独协定，以期就所没收财产的最后处置达成互可接受的安排。

第三章
预防和打击网络空间犯罪和其他违法行为的措施

第三十六条
预防和打击与使用信通技术有关的犯罪和其他违法行为的政策和做法

1. 各缔约国均应根据其本国法律制度的根本原则，制订执行或寻求行之有效和协调一致的政策，以打击与使用信通技术有关的犯罪和其他违法行为。

2. 各缔约国均应努力制订和促进行之有效的做法，以预防与使用信通技术有关的犯罪和其他违法行为。

3. 缔约国应在适当情况下，按照本国法律制度的根本原则，相互并与相关国际和区域组织协作，促进和制订本条所述措施。

第三十七条
预防和打击与使用信通技术有关的犯罪和其他违法行为的负责机构

1. 各缔约国均应采取一切必要立法和其他法律措施，指定负责预防和打击与使用信通技术有关犯罪和其他违法行为活动的主管当局，并制订此类主管当局间互动程序。

2. 各缔约国均应将可协助其他缔约国制订和执行预防与使用信通技术有关的犯罪和其他违法行为具体措施的一个或多个主管当局的名称和地址通知联合国秘书长。

第三十八条
私营部门

1. 各缔约国均应根据其国内法根本原则，采取措施预防私营部门中与使用信通技术有关的犯罪和其他违法行为，提高私营部门的信息安全标准，对不遵守这些措施的，在适当情况下施加并适用有效、适度和劝阻性的民事、行政或刑事处罚。

2. 旨在实现上述目标的措施除其他外包括：

(a) 促进执法机构与有关私营实体之间的合作；

(b) 促进制订旨在确保信息安全的标准和程序；

(c) 促进对执法、调查、司法和检察人员的培训方案。

第三十九条
私营信息和电信服务提供者原则和行为守则

1. 位于缔约国境内的各私营信息和电信服务提供者或其集团均应在其权力范围内并依照其所在国的法律采取适当措施，协助以尊重联合国各项根本文书所保障的人权为基础，制定和执行国际网络空间的使用原则和守则。

2. 旨在实现上述目标的措施除其他外包括：

(a) 私营信息和电信服务提供者或其集团之间的合作；

(b) 合作制订各项原则和标准，以期创造建设文明社会的有利环境，使其成为国际网络空间的组成部分。

第四十条
提高公众对网络犯罪的预防意识

1. 各缔约国均应采取适当措施，在其权力范围内，根据其国内法根本原则，促进个人和团体，包括非政府组织和公共组织，积极参与预防与使用信通技术有关的犯罪和其他违法行为，并让公众更加了解这些犯罪行为、其原因和严重性以及构成的威胁。应采取下列措施支持这一参与：

(a) 提供有效的公众获取信息途径；

(b) 开展提高公众认识活动，推动对与使用信通技术有关犯罪和其他违法行为的零容忍；

(c) 开展关于信通技术安全的公众教育培训方案。

2. 各缔约国均应采取适当措施，确保公众了解负责打击与使用信通技术有关的本公约所述犯罪和其他违法行为的相关机构，并提供诉诸这些机构的途径，以利于举报任何可被认为属于本公约规定的犯罪和其他违法行为的事件。

第四章
国际合作

第一节
国际合作与互助的一般原则

第四十一条
国际合作的一般原则

1. 各缔约国应依照本章的规定，按照刑事事务国际合作的有关国际文书、在示范法或共同商定的法律基础上达成的协定以及本国法律，尽可能充分地相互合作，以期预防、制止、发现和调查与使用信通技术有关的犯罪。

2. 若为将一项行动认定为犯罪以便进行国际合作而必须满足相互承认这项要求，则当提出协助请求的缔约国和被请求的缔约国两国制定法都将一个构成犯罪的行动定为刑事犯罪时，无论被请求国的法律与请求国的法律是否将该行动定为相同类别的犯罪或使用相同措辞进行表述，都应视为可适用相互承认要求。

3. 缔约国应在适当且国内法律制度允许的情况下，考虑在调查和起诉与使用信通技术有关的违法行为相关民事和行政案件方面提供互助。

4. 为了缔约国之间司法互助和引渡目的，本公约第六至十八条提及的任何犯罪均不得被视为政治犯罪、与政治犯罪有关的犯罪或出于政治动机的犯罪。因此，不得单纯因为一项犯罪涉及政治犯罪、与政治犯罪有关的犯罪或出于政治动机的犯罪而拒绝与该犯罪有关的司法协助或引渡请求。

第四十二条
司法互助的一般原则

1. 缔约国应提供司法互助，以便就与使用信通技术有关犯罪和其他违法行为开展调查或司法程序。

2. 各缔约国还应采取一切必要立法和其他措施，遵守本公约第四十七条、第四十八条、第五十至五十四条和第五十七条规定的义务。各缔约国还应考虑延长(或免除)时限，以防止逃避责任。

3. 在紧急情况下，各缔约国可采用传真或电子邮件等快速通信方式，发出司法互助请求或相关函件，前提是上述快速通信方式须提供适当程度的安全保障及核证(包括根据需要使用加密)，而若被请求的缔约国提出要求，还应随后提交正式确认。被请求国应采用任何快速通信方式接收并答复请求。被请求国可保留转发在收到最初请求后所作答复的权利。

4. 除非本章条款另有具体规定，否则司法互助应遵循被请求国的法律或适用的司法互助协定的规定，包括被请求国可能援引的不合作理由清单。

第四十三条
管辖权

1. 各缔约国应采取一切必要措施，对符合以下条件的本公约规定的犯罪和其他违法行为确立管辖权：

(a) 发生在该缔约国境内；或

(b) 发生在罪行实施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. 在不违反本公约第三条规定的情况下，缔约国在下列情况下还可对上述任何犯罪和其他违法行为确立管辖权：

(a) 实施对象是该缔约国国民、在其境内永久居住的无国籍人、在其境内设立或有常驻代表的法人、或者该缔约国的外交使团或领事馆；或

(b) 实施者是该缔约国国民或在其境内有惯常居所的无国籍人；或

(c) 罪行是针对该缔约国实施的。

3. 为本公约第四十八条之目的，各缔约国均应采取一切必要措施，在被指控的犯罪行为人位于该国境内并且该国仅以被指控人是其本国国民或由其授予难民地位之人为由而不予引渡时，确立该国对本公约所规定犯罪的管辖权。

4. 在本条第 1 款和第 2 款规定的情况下，不引渡其境内被指控的行为人的缔约国，无论犯罪是否发生在该缔约国境内，都毫无例外应不加拖延地将案件提交其主管当局，以便依照该国法律进行法律诉讼。

5. 若根据本条第 1 款或第 2 款行使其管辖权的缔约国被告知或以其他方式获知任何其他缔约国正在对同一行为开展调查、起诉或进行司法程序，则这些缔约国的主管当局应适当相互协商，以期协调行动。

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。

第四十四条
主动提供信息

1. 缔约国若认为披露其在调查期间收集到的信息可能会帮助另一缔约国就本公约规定的犯罪或其他违法行为启动或者进行调查或司法程序，或者可能导致该另一缔约国按照本章规定提出合作请求，则可依照其国内法，未经另一缔约国事先请求，将这些信息转给该另一缔约国。

2. 相关缔约国在提供信息之前可要求对信息进行保密或规定信息使用的特定条件。若接收信息的缔约国不同意这一请求，则应通知提供信息的缔约国，由提供国决定是否仍将提供该信息。若接收国根据上述条件接受信息，则上述条件对接收国具有约束力。

第四十五条
移交刑事诉讼程序

缔约国如认为在涉及多个司法管辖区的具体案件中，向另一缔约国移交与本公约所规定犯罪有关的刑事诉讼程序有利于妥当司法，则应考虑移交诉讼程序，以确保合并审理刑事案件。

第四十六条
在无适用的国际协定情况下发出互助请求的程序

1. 若提出请求的缔约国和被请求的缔约国之间没有司法互助条约或协定，则适用本条第 2 至 8 款的规定。若存在这样的条约或协定，则本条规定不适用，除非有关缔约国同意适用本条的下列任何或所有规定，替代上述文书。

2. (a) 各缔约国均应指定一个中央主管当局或数个主管当局负责传送、答复、批准，或向主管当局转交司法互助请求；

(b) 上文(a)项提及的中央主管当局或数个主管当局应相互直接沟通；

(c) 各缔约国于签署本公约时或交存其批准、接受、核准或加入文书时，应将该国依照本款规定指定的主管当局名称和地址告知联合国秘书长；

(d) 联合国秘书长应编制并定期更新载列各缔约国指定的中央主管当局的登记册。各缔约国均应定期确保登记册载有最新信息。

3. 被请求的主管当局在准予司法互助请求时，应适用其本国法律。如提出请求的主管当局要求适用请求国的法律程序，则在请求国法律程序不违反被请求国制定法的前提下，可适用请求国的法律程序。

4. 被请求的缔约国除了第四十三条第 4 款规定的拒绝理由外，还可以在以下情况下拒绝提供法律协助：

(a) 被请求国认为，请求所涉犯罪是针对该国的犯罪或是与此有关的犯罪；

(b) 被请求国认为执行该请求将损害其主权、安全、公共秩序或其他重大利益。

5. 若应请求而采取的措施会妨碍被请求的缔约国主管当局正在开展的刑事调查或司法程序，则被请求国可推迟采取这些措施。

6. 在拒绝或推迟提供司法协助之前，被请求的缔约国应在视需要与请求国协商之后，考虑部分准予请求或在设定其认为适当的条件基础上准予请求。

7. 被请求的缔约国应将司法协助请求的处置结果尽快通知提出请求的缔约国。若拒绝请求或推迟准予，则应将拒绝或推迟的原因告知请求国。被请求国还应告知请求国请求不会得到准予或很可能在推迟相当长时间后才会准予的原因。

8. 提出请求的缔约国可要求被请求的缔约国对按照本章规定所提请求之事实和请求的事由保密，但以不影响该请求的实施为限。若被请求国不能遵守保密要求，则应立即告知请求国；请求国随后应决定是否仍然提出该请求。

第四十七条
保密和信息使用限制

1. 若提出请求的缔约国和被请求的缔约国之间没有基于示范法或共同商定的法律而达成的司法互助条约或协定，则适用本条规定。若存在这样的条约或协定或法律，则本条规定不适用，除非有关缔约国同意适用本条的下列任何或所有规定，以之替代上述文书。

2. 针对请求，被请求的缔约国可以为提供信息或材料设定条件：

(a) 对信息或材料进行保密，若不接受这些条件，则不准予司法互助请求；

(b) 不得为请求中未提及的其他调查或法律程序的目的披露这些信息或材料。

3. 若提出请求的缔约国不能遵守本条第 2 款所述的任何条件，则应立即通知对方请求国；对方缔约国随后应决定是否能够提供信息。若请求国同意遵守条件，则该条件对该缔约国具有约束力。

4. 以本条第 2 款所述条件为前提提供信息或数据的任何缔约国均可要求对方缔约国明确说明使用该信息或材料的任何规定条件。

第四十八条
引渡

1. 对于根据本公约确定的犯罪，当被请求引渡之人处于被请求的缔约国境内时，应适用本条规定，条件是引渡请求所涉犯罪根据提出请求的缔约国和被请求国各自的国内法律，均应受到至少为期一年的监禁或更重的处罚。

2. 本公约第六至二十条规定的各项刑事犯罪均应被视为缔约国间任何现行引渡条约规定的可引渡犯罪。缔约国承诺将这些犯罪作为可引渡的犯罪列入它们今后将缔结的任何引渡条约。若缔约国国内法允许，则在以本公约作为引渡依据时，本公约规定的任何犯罪均不得被视为政治犯罪。

3. 若引渡请求涉及多项单独罪行，其中至少有一项是本条规定的可引渡犯罪，而其他罪行因适用的处罚而不可引渡，但仍被视为本公约规定的犯罪，则被请求的缔约国也可对这些犯罪适用本条规定。

4. 以订有条约为引渡条件的缔约国若收到未与之订有引渡条约的另一缔约国的引渡请求，则可将本公约视为就本条所适用的任何犯罪进行引渡的法律依据。

5. 以订有条约为引渡条件的缔约国应：

(a) 于交存本公约批准书、接受书、核准书或者加入书时通知联合国秘书长，说明该国是否将适用本公约，将之作为其与本公约其他缔约国进行引渡合作的法律依据；及

(b) 若不以本公约作为引渡合作的法律依据予以适用，则应在适当情况下寻求与本公约其他缔约国缔结引渡条约，以适用本条规定。

6. 不以订有条约为引渡条件的缔约国应承认本条所适用的犯罪是这些缔约国之间可相互引渡的犯罪。

7. 引渡应符合被请求的缔约国国内法或相关引渡条约所规定的条件，其中包括引渡的最低限度处罚要求和被请求国可据以拒绝引渡的理由。

8. 对于本条所适用的任何犯罪，缔约国应在符合其国内法的情况下，努力加快引渡程序并简化与之有关的证据要求。

9. 被请求的缔约国在不违背其国内法及其引渡条约的规定情况下，可在认定情况需要而且紧迫时，根据提出请求的缔约国的请求，对被请求国境内的被请求引渡之人进行拘押或采取其他适当措施确保在进行引渡程序时该人在场。

10. 若一缔约国不引渡在其境内被发现的、与本条所适用犯罪有关的被指控犯罪行为人，在寻求引渡的缔约国提出请求后，该国毫无例外地有义务将案件提交其本国主管当局进行起诉，不得不当拖延。主管当局应作出决定并进行诉讼程序，其方式与根据该缔约国国内法处理性质严重的任何其他犯罪所采用的方式相同。有关缔约国应相互合作，特别是在程序和证据事项上进行合作，以确保该诉讼的效率。

11. 若一缔约国国内法规定，允许引渡或移交其国民的条件是，该人将被送还本国以便按照引渡或移交请求所涉及的审判或诉讼作出的判决服刑，并且该缔约国和请求引渡该人的缔约国也同意该程序以及它们可能认为适当的其他条件，则这种有条件引渡或移交即充分履行了本条第 10 款规定的义务。

12. 在对任何人就本条所适用的任何犯罪进行诉讼时，应确保其在诉讼的所有阶段受到公平对待，包括享有其所在国国内法所提供的一切权利和保障。

13. 不得将本公约的任何条款解释为施加在下列情况下的引渡义务：被请求的缔约国有充分理由认为提出引渡请求的目的是以某人的性别、种族、宗教、国籍或族裔为由对其进行起诉或惩处，或者认为遵从该请求将使该人的处境因上述任一原因而受到损害。

14. 被请求的缔约国在拒绝引渡前应在适当情况下与提出请求的缔约国协商，使后者有充分机会陈述自己的意见并提供与请求书中陈述的事实有关的信息。

15. 缔约国应寻求缔结双边和多边协定或安排，以执行引渡或加强引渡的成效。

第四十九条
被判刑人员的移交

缔约国可考虑缔结双边或多边协定或安排，将犯有本公约规定的罪行而被判处监禁或以其他形式剥夺自由的人员移送至缔约国本国境内服满刑期。

第五十条
快速保全电子信息

1. 一缔约国可请另一缔约国发布命令或以其他方式迅速保全在该另一缔约国境内利用信通技术保存或处理的信息，为此请求国须在司法互助框架内发出搜查、扣押或以其他方式保全该信息的请求。

2. 根据本条第 1 款提出的信息保全请求应具体说明：

(a) 提出请求的主管当局的名称；

(b) 概述请求所涉基本事实以及有关的调查、起诉或司法程序的性质；

(c) 拟保全的电子信息及其与相关犯罪之间的关系；

(d) 可用于确定信息保管人或信通技术装置位置的任何可获数据；

(e) 保全信息的理由；

(f) 缔约国打算在司法互助框架内提出的搜查、扣押或类似保全信息请求的函件。

3. 收到另一缔约国的请求后，被请求的缔约国应采取适当措施，根据其本国内法迅速保全本条第 1 款具体规定的信息。被请求国可全部或部分执行请求，以确保保全信息，即使构成请求理由的行为在被请求国不被定为刑事犯罪。

4. 若被请求的缔约国认为执行请求可能损害其主权、安全或其他基本利益，则可拒绝保全信息的请求。

5. 若被请求的缔约国认为执行本条第 1 款所述请求无法确保将来保全信息或将会危及保密性或给调查、起诉或司法程序造成其他损害，则应立即通知提出请求的缔约国。请求国应根据该通知决定该请求是否应予执行。

6. 应本条第 1 款所述请求而实行的任何保全在期间上不得少于 180 天，以便提出请求的缔约国能够提交搜查、扣押或以其他方式保全信息的请求。在收到请求后，被请求的缔约国应在就该请求作出决定前，保全相关信息。

第五十一条
加快披露已保全的流量数据

1. 若在执行依照本公约第五十条提出的保全信息请求过程中，被请求的缔约国发现另一国家境内的一服务提供者参与传输该信息，则被请求国应迅速向提出请求的缔约国披露充足的流量数据，以确定该服务提供者的身份并查明所请求保全信息的传输路径。

2. 若被请求的缔约国认为执行请求可能损害其主权、安全或其他基本利益，则可拒绝保全信息的请求。

第五十二条
执法合作

1. 缔约国应在符合其国内法律制度和行政管理制度的情况下相互密切合作，以加强执法行动的成效，打击本公约规定的犯罪。各缔约国尤其应采取有效措施，目的是：

(a) 加强并在必要时建立各国主管当局、机构和部门之间的沟通渠道，以促进安全、迅速地交换有关本公约所规定犯罪的各个方面信息，有关缔约国认为适当时还可包括与其他犯罪活动的联系的有关信息；

(b) 同其他缔约国合作，就本公约规定的犯罪进行调查，目的是查明：

㈠ 涉嫌参与犯罪之人的身份、行踪和活动，或其他相关人员的所在地点；

㈡ 犯罪所得或因实施犯罪而取得的财产的去向；

㈢ 用于或企图用于实施犯罪的财产、设备或其他工具的去向；

(c) 提供用于实施犯罪的物品，包括犯罪工具；因犯罪而获取的物品或作为犯罪报偿的物品；行为人用采取这种方式取得的物品所换取的物品；可能在刑事案件中具有证据价值的物品；

(d) 视情况与其他缔约国就实施本公约规定的犯罪所采用的具体手段和方法交换信息，其中包括利用虚假身份；虚假、变造或伪造的文件；或其他掩盖违法活动的手段；

(e) 促进各缔约国主管当局、机构和部门之间有效协调，并推动交换工作人员和其他专家，包括根据有关缔约国之间的双边协定和安排派出联络官员；

(f) 交换重要情报，采取协调一致的措施，以尽早发现本公约规定的犯罪。

2. 为执行本公约，缔约国应考虑订立关于其执法机构间直接合作的双边或多边协定或安排，并在已有此类协定或安排的情况下考虑对其进行修正。若有关缔约国之间没有此类协定或安排，则缔约国可考虑以本公约为依据，就本公约规定的犯罪开展相互执法合作。凡在适当情况下，缔约国均应充分利用各种协定或安排，包括国际或区域组织机制，加强缔约国执法机构之间的合作。

第五十三条
实时收集流量数据方面的互助

1. 缔约国应根据另一缔约国提出的请求，在其境内或受其管辖的领土内实时收集流量数据，然后根据其国内法律规定的程序，基于相关理由(如有)传输所收集的信息。

2. 各缔约国均应考虑就其国内法律规定应实时收集流量数据的犯罪和其他违法行为提供司法互助。

3. 根据本条第 1 款发出的请求应具体说明：

(a) 提出请求的主管当局的名称；

(b) 概述请求所涉基本事实以及有关的调查、起诉或司法程序的性质；

(c) 需要收集流量数据的有关电子信息及其与相关犯罪或其他违法行为的关系；

(d) 可用于确定信息所有人/使用人以及信通技术装置位置的任何可获数据；

(e) 收集流量数据的期间；

(f) 收集流量数据的原因；

(g) 选择指定期间收集流量数据的原因。

第五十四条
收集电子信息方面的互助

缔约国应在其本国境内或受其管辖的领土内，依照其国内法规定的程序，实时收集通过信通技术传输的电子信息。缔约国应根据其国内法和已有的司法互助协定，向另一缔约国提供这些信息。

第五十五条
联合调查

缔约国应考虑缔结双边或多边协定或安排，以便有关主管当局可据以设立联合调查机构，处理作为一国或多国境内调查、起诉或司法程序事由的案件。若无此类协定或安排，则可逐案商定开展联合调查。参与调查的各缔约国应确保调查实施地所在的缔约国主权受到充分尊重。

第五十六条
特殊侦查手段

1. 为有效打击与使用信通技术有关的犯罪，各缔约国均应在其国内法的根本原则允许的范围内，以其国内法规定的条件为限，尽其所能采取必要措施，允许其主管当局在其境内适当使用电子监视或其他形式的监视以及卧底行动等特殊侦查手段，使得通过这些方法收集的证据可为法院所接受。

2. 为调查本公约规定的犯罪，鼓励缔约国在必要时缔结适当的双边或多边协定或安排，以便在国际一级合作中使用上述特殊侦查手段。此类协定或安排的缔结和执行应完全符合各国主权平等原则，执行时应严格遵守协定或安排的条款。

3. 若无本条第 2 款所述协定或安排，则应逐案作出在国际一级使用特殊侦查手段的决定，必要时可考虑到所涉缔约国达成的资金安排以及关于行使管辖权的谅解。

第五十七条
24/7 网络

1. 各缔约国均应指定一个每周七天每天 24 小时可用的联络点，以确保为涉及计算机系统和数据的刑事犯罪调查、起诉或司法程序或为以电子方式收集与刑事犯罪有关的证据提供紧急协助。这种协助应包括促进采取下列措施，或在其国内法和惯例允许的情况下直接执行下列措施：

(a) 提供技术咨询意见；

(b) 保全数据，以收集证据并继而按照其国内法和现有司法互助协定提供法律信息。

2. 各缔约国均应采取措施，确保提供训练有素的人员和设备，以促进该网络的运作。

第二节
技术援助和培训

第五十八条
技术援助的一般原则

1. 缔约国应尽其所能，特别是为了有利于发展中国家打击信通技术犯罪的计划和方案，考虑相互提供最广泛的技术援助，包括在本公约第六十条提及的领域中提供实质支持和培训，并提供培训和援助及互相交流相关经验和专门知识，以促进缔约国之间在引渡和司法互助方面的国际合作。

2. 缔约国应根据需要加强努力，实现国际组织和区域组织以及有关双边和多边协定和安排框架内业务和培训活动的成效最大化。

3. 缔约国应考虑根据请求相互协助，对各自境内实施的信通技术犯罪的类型、原因及后果进行评价、分析和研究，以期在各主管当局、社会和私营部门参与下，拟订打击这些类别犯罪的战略和行动计划。

4. 缔约国应考虑建立自愿机制，以期通过技术援助方案和项目为发展中国家和经济转型国家的努力提供资助。

5. 缔约国应委托联合国毒品和犯罪问题办公室向缔约国提供专业技术援助，以期推动执行打击信通技术犯罪的方案和项目。

第五十九条
培训

1. 各缔约国均应根据需要拟订、实施或改进对其负责预防和打击信通技术犯罪的人员进行培训的具体方案。这些培训方案除其他外可包括以下领域：

(a) 采取有效措施，包括使用电子证据收集和侦查手段，预防、发现和调查并且惩处和打击信通技术犯罪；

(b) 进行能力建设，促进打击信通技术犯罪的战略性政策制定和规划工作；

(c) 对主管当局工作人员进行关于编写符合本公约要求的司法互助请求的培训；

(d) 预防本公约所规定犯罪的所得被转移，并且追回此类所得；

(e) 发现并阻拦与转移本公约所规定犯罪的所得有关的交易；

(f) 监视本公约所规定犯罪的所得去向以及用以转移、藏匿或掩饰此类所得的方法；

(g) 采取适当、高效的法律和行政机制及方法，为扣押本公约所规定犯罪的所得提供便利；

(h) 采取措施保护与司法机关合作的受害人和证人；及

(i) 为工作人员提供本国法规、国际条例和语言培训。

2. 缔约国应委托联合国毒品和犯罪问题办公室向缔约国提供专业培训援助，以期推动执行打击信通技术犯罪的国家方案和项目。

第六十条
交换信息

1. 各缔约国均应考虑在征询有关专家意见后，分析其境内信通技术犯罪的趋势以及此类犯罪的实施情形。

2. 缔约国应考虑散发与信通技术犯罪有关的统计数字和分析，以期尽可能拟订通用定义、标准和方法，包括在预防和打击信通技术犯罪方面的最佳做法，并彼此以及通过国际和区域组织分享。

3. 各缔约国均应考虑对其打击信通技术犯罪的政策和实际措施进行监测，并对这些政策措施的成效进行评估。

第五章
执行机制

第六十一条
公约缔约国会议

1. 兹设立本公约缔约国会议，以增进缔约国的能力及缔约国间的合作，从而实现本公约设定的目标，促进和审查公约的执行。

2. 联合国秘书长应不迟于本公约生效一年之日召集缔约国会议。此后，应依照缔约国会议通过的议事规则，举行缔约国会议的常会。

3. 缔约国会议应通过议事规则以及本条所列活动的运行所应遵循的规则，包括接纳观察员、观察员参与活动以及支付开展活动费用方面的规则。

4. 缔约国会议应为实现本条第 1 款所述目标商定相关活动、程序和工作方法，其中包括：

(a) 通过鼓励自愿捐助等方式，促进缔约国按照本公约第五十九条和第六十条以及第二至五章的规定开展活动；

(b) 促进缔约国之间就信通技术犯罪的模式和趋势以及预防和打击此类犯罪的成功做法及追回犯罪所得交流信息，采取的方式除其他外，包括公布本条所述相关信息；

(c) 与有关国际和区域组织和机制以及非政府组织开展合作；

(d) 适当利用其他打击和预防信通技术犯罪国际和区域机制提供的相关信息，以避免不必要的工作重复；

(e) 由公约缔约国定期审查本公约的执行情况；

(f) 为改进本公约及其执行提出建议；

(g) 查明缔约国在执行本公约方面的技术援助需求，并就此建议采取缔约国会议认为必要的任何行动。

5. 为了本条第 4 款的目的，缔约国会议应通过缔约国提供的信息和缔约国会议可能建立的补充审查机制，对缔约国为执行本公约所采取的措施以及执行过程中所遇到的困难获得必要的了解。

6. 各缔约国均应按照缔约国会议的要求，向缔约国会议提供信息，说明该国执行本公约的方案、计划和做法以及立法和行政措施。缔约国会议应当审查接收信息并就信息采取行动的最有效方式，这些信息除其他外，包括来自缔约国和有关国际组织的信息。对经正式认可的非政府组织按照将由缔约国会议决定的程序提供的投入，也可予以审议。

7. 根据本条第 4 至 6 款，缔约国会议应在其认为必要时建立任何适当机制或机构，以协助有效执行本公约。

第六十二条
打击信通技术犯罪国际技术委员会

1. 缔约国会议应依照本公约的规定，创设和组建打击信通技术犯罪国际技术委员会，协助各国审查公约执行情况。

2. 委员会应是一常设机构，由 23 名成员组成，按照混合代表制原则设立：三分之二的成员代表缔约国会议，其余三分之一的成员代表国际电信联盟的理事机构。

3. 委员会成员由在外交、国际法、通信技术或相关研究方面具有丰富直接经验的专家担任。

4. 委员会成员任期五年，可以连任。

5. 委员会应每年至少举行一次届会，届会应在设于联合国毒品和犯罪问题办公室的委员会总部举行，或在缔约国会议指示或核准的时间和地点举行。

6. 委员会应通过其议事规则，由缔约国会议核准。

7. 委员会应评估信通技术领域的技术进步。

8. 委员会应通过缔约国会议，向缔约国和有关国际组织报告其工作结果。

9. 如有必要，委员会将就修正本公约技术附件向缔约国会议提出建议。关于这些建议的决定应协商一致作出。

10. 经委员会建议，缔约国会议可建议缔约国修正本公约的技术附件。

第六十三条
秘书处

1. 联合国秘书长应为公约缔约国会议提供必要的秘书处服务。

2. 秘书处应：

(a) 为缔约国会议的届会和国际技术委员会的届会做出安排并提供必要服务；

(b) 应缔约国请求，协助其向缔约国会议提供信息；及

(c) 确保与其他有关国际和区域组织秘书处进行必要协调。

第六章
最后条款

第六十四条
公约的执行

1. 各缔约国均应根据其国内法的根本原则采取必要措施，包括立法和行政措施，以切实履行其根据本公约所承担的义务。

2. 为预防和打击信通技术犯罪，各缔约国均可采取比本公约的规定更为严格或严厉的措施。

第六十五条
争端解决

1. 缔约国应努力通过谈判解决与本公约的解释或适用有关的争端。

2. 两个或两个以上缔约国对于本公约的解释或适用发生任何争端，在合理时间内不能通过谈判解决的，应经其中一方请求而交付仲裁。若自请求交付仲裁之日起六个月内这些缔约国不能就仲裁安排达成协议，则其中任何一方均可依照《国际法院规约》请求将争端提交国际法院。

3. 各缔约国在签署、批准、接受、核准或加入本公约时，均可声明不受本条第2款的约束。而对于作出此项保留的任何缔约国而言，其他缔约国也不受本条第2款的约束。

4. 凡根据本条第3款作出保留的缔约国，均可随时通知联合国秘书长撤销该项保留。

第六十六条
签署、批准、接受、核准和加入

1. 本公约向所有国家开放供签署。

2. 本公约还应开放供区域组织签署，条件是该组织至少有一个成员已按照本条第 1 款规定签署本公约。本公约须经批准、接受或核准。批准书、接受书或核准书应交存联合国秘书长。

第六十七条
生效

1. 本公约应于第三十份批准、接受、核准或加入文书交存之日后第九十天生效。为本款的目的，区域经济一体化组织交存的任何文书均不得在该组织成员国所交存文书以外另行计算。

2. 对于在第三十份批准、接受、核准或加入文书交存后批准、接受、核准或加入本公约的缔约国或区域经济一体化组织，本公约应于该国或该组织交存有关文书之日后第三十天生效，或于本公约根据本条第 1 款生效之日生效，以时间较后者为准。

第六十八条
修正

1. 本公约生效五年后，缔约国可提出修正案并送交联合国秘书长备案。联合国秘书长应立即将所提修正案通报各缔约国和缔约国会议，以进行审议并作出决定。缔约国会议应尽力就每项修正案达成协商一致。若为达成协商一致作出一切努力后仍未达成一致意见，作为最后手段，须有缔约国三分之二多数票方可通过修正案。

2. 区域经济一体化组织对其权限范围内的事项行使本条规定的表决权时，其票数等同于该组织中同时也是本公约缔约国的成员国数目。若这些组织的成员国行使表决权，则这些组织不得行使表决权，反之亦然。

3. 根据本条第 1 款通过的修正案须经缔约国批准、接受或核准。

4. 根据本条第 1 款通过的修正案，应于缔约国向联合国秘书长交存批准、接受或核准该修正案的文书之日起九十天后对该缔约国生效。

5. 修正案一经生效，即对已表示同意受其约束的缔约国具有约束力。其他缔约国则仍受本公约原条款和该国之前批准、接受或核准的任何修正案的约束。

第六十九条
保留

各缔约国均可在签署或交存其批准书或加入书之时，以书面通知联合国秘书长的方式，声明其将行使就本公约的适用作出保留的权利。对就第十四条、第十六条、第十七条和第四十八条第 10 款作出的保留将不予接受。

第七十条
附件一的修正

1. 任何缔约国均可提议修正本公约附件一载列的国际法律文书清单。

2. 秘书处应负责监测新通过的可能影响本公约适用范围的国际法律文书，并向缔约国会议下次届会提交对附件一的拟议修正案。

3. 拟议修正案应仅涉及已生效且与国际犯罪直接相关的普遍性和区域性国际法律文书。

4. 秘书长应向缔约国转递依照本条第 1 款规定提议的修正案草案。若自修正案草案转递之日起六个月内，已批准本公约的缔约国总数中有三分之一的国家通知秘书长，表示反对该修正案生效，则该修正案不得生效。

5. 若自修正案草案转递之日起六个月内，已批准本公约的缔约国总数中不足三分之一的国家向秘书长提出反对修正案生效的意见，则在六个月的提出反对期结束后三十天时，该修正案对未提出反对的缔约国生效。

6. 缔约国会议通过一项修正案须经已批准本公约的所有缔约国三分之二多数投票赞成。修正案在其通过之日后三十天时，对已表示同意适用该修正案的缔约国生效。

7. 若一项修正案依照本条规定生效之后，任何缔约国向秘书长发出反对该修正案的通知，则对该缔约国而言，该修正案将在相关缔约国通知秘书长该国接受该修正案之日后三十天时生效。

第七十一条
退约

1. 缔约国可书面通知联合国秘书长的方式，退出本公约。退约应自秘书长收到通知之日起一年后生效。

2. 区域经济一体化组织自其所有成员国均已退出本公约之时起，不再是本公约缔约方。

第七十二条
保存人和语文

1. 兹指定联合国秘书长为本公约的保存人。

2. 本公约正本应交存于联合国秘书长，其阿拉伯文、中文、英文、法文、俄文和西班牙文文本同等作准。

兹由经各国政府正式授权的下列署名全权代表签署本公约，以昭信守。

附件一

1. 《关于在航空器内的犯罪和犯有某些其他行为的公约》(1963 年 9 月 14 日，东京)

2. 《关于制止非法劫持航空器的公约》(1970 年 12 月 16 日，海牙)

3. 《关于防止和惩处侵害应受国际保护人员包括外交代表的罪行的公约》(1973 年 12 月 14 日，纽约)

4. 《反对劫持人质国际公约》(1979 年 12 月 17 日，纽约)

5. 《核材料实物保护公约》(1980 年 3 月 3 日，维也纳)

6. 《制止危及海上航行安全非法行为公约》(1988 年 3 月 10 日，罗马)

7. 《制止恐怖主义爆炸的国际公约》(1997 年 12 月 15 日，纽约)

8. 《制止向恐怖主义提供资助的国际公约》(1999 年 12 月 9 日，纽约)

9. 《制止核恐怖主义行为国际公约》(2005 年 4 月 13 日，纽约)

10. 《反恐司法互助和引渡公约》(2008 年 5 月 16 日，纽约)

11. 《联合国打击跨国有组织犯罪公约》(2000 年 11 月 15 日，纽约)

12. 《联合国反腐败公约》(2003 年 10 月 31 日，纽约)

13. 《制止与国际民用航空有关的非法行为的公约》(2010 年 9 月 10 日，北京)[取代 1971 年《制止危害民用航空安全非法行为公约》]

14. 《麻醉品单一公约》(1961 年 3 月 30 日，纽约)

15. 《精神药物公约》(1971 年 2 月 21 日，维也纳)

16. 《联合国禁止非法贩运麻醉药品和精神药物公约》(1988 年 12 月 19 日，维也纳)

技术附件

种类	名称	说明
1. 软件	蠕虫	一种通过局域和全球计算机网络传播的恶意程序
	病毒	一种自我复制的恶意程序
	特洛伊木马	一种在系统中执行未经授权功能的恶意程序
	ROOTKIT	一种在系统中隐藏入侵者或恶意程序的程序或程序包
	BOOTKIT	一种修改主引导记录引导扇区的程序
	漏洞利用	一种利用软件漏洞来攻击计算机系统的程序或命令序列。攻击的目的可能是控制系统(特权提升)或导致系统故障(拒绝服务攻击)
	构造器	用于开发恶意程序的程序
	加密程序	一种用于隐藏恶意软件的程序
	后门	一种用于秘密控制计算机的恶意软件
	暴力破解器	一种用于破解密码的程序
	键盘记录器	一种用于记录按键的恶意程序
	嗅探器	一种分析网络流量的工具
	注册机	密钥生成器
	流量生成器	一种伪造流量的恶意程序
	自动点击器	一种模拟横幅广告并点击的恶意程序
2. 硬件	侧录器	一种记录信用卡磁条信息以供复制的可贴附装置
	编码器(阅读器)	一种阅读/记录磁条信息的装置
	凸字打码机	一种用于给塑料卡片压制凸字的装置
3. 特殊情报技术工具	SITT 1	用于秘密获取和记录声音信息的装置
	SITT 2	用于秘密观察和记录图像的装置
	SITT 3	用于窃听电话的装置
	SITT 4	用于从信道中秘密获取和记录信息的装置
	SITT 5	用于秘密控制电子邮件所发信息和传输的装置
	SITT 6	用于秘密检查物项和文件的装置
	SITT 7	用于秘密进入和检查房地、车辆和其他设施的装置

种类	名称	说明
	SITT 8	用于秘密控制车辆和其他物项的装置
	SITT 9	用于从存储、处理和转移信息的技术媒介中秘密获得(修改、擦除)信息的装置
	SITT 10	用于秘密检查身份的装置