联合国 A/CONF.234/11

第十四届联合国预防犯罪和刑事司法大会

Distr.: General
23 January 2020
Chinese
Original: English

2020年4月20日至27日，日本京都

临时议程*项目6

开展国际合作并提供技术援助以预防和应对一切形式的犯罪

讲习班4：目前的犯罪趋势、最近动态和新出现的解决办法，特别是新技术作为犯罪的手段和打击犯罪的工具**

秘书处编写的背景文件

摘要

本背景文件探讨了技术这把双刃剑的影响：它既能促成犯罪，也能有助于预防、侦查和制止犯罪。为此，本文件采取双管齐下的方法来解释新出现的基本二元论：一方面，技术有助于为警务工作、起诉和刑事司法工作顺利取得成果找到解决办法；另一方面，技术在增强犯罪分子和有组织犯罪集团的作案手法方面发挥着邪恶的作用。本文件中所作的分析考虑到了各个具体领域内的发展动态，并涵盖了具有跨领域性质的两个方面：必须开展培训，采取跨学科办法，在各个相关利益攸关方之间实现协同增效，从而了解技术当下能够带来的益处及其在应对未来犯罪威胁方面的潜力；同时也有必要在利用技术打击犯罪时，适当考虑到伦理问题和人权保障措施。

* A/CONF.234/1。

** 联合国秘书处谨此感谢联合国预防犯罪和刑事司法方案网各研究所，特别是韩国犯罪学协会和美国司法部国家司法研究所协助筹备和举办本期讲习班。

V.20-00547 (C) 140220 140220

一. 导言

1. 1997 年，联合国国际药物管制规划署和国际预防犯罪中心合并为药物管制和预防犯罪办事处，并于 2002 年更名为联合国毒品和犯罪问题办公室（毒品和犯罪问题办公室）。正是在 1997 年，一台名为“深蓝”的国际象棋计算机升级版成为第一个在国际象棋锦标赛标准时间控制下的比赛中击败卫冕世界冠军的计算机系统。当时，尽管科技不断进步，但犯罪技术含量仍然相对较低，互联网作为“信息时代”的决定性技术，才刚刚开始对社会产生影响。

2. 在其后二十多年的时间里，互联网以及信息和通信技术的迅速发展促进了经济增长和重要服务的普及，但也为犯罪活动创造了新的机会。犯罪分子已成为新技术和全球化的意外受益者，因为这些发展使他们能够利用跨国活动实施犯罪并从中获利，还能在数字平台上扩大其非法活动和业务，从而降低犯罪风险，特别是被发现的风险。[1]

3. 另一方面，新技术和现有技术也为执法行动、刑事侦查和起诉提供了新的机会。通过技术进步改善公共安全，增强执法机关和刑事司法机关预防和打击犯罪的能力，可能会对实现《2030 年可持续发展议程》的各项目标，特别是可持续发展目标 16 产生积极影响。

4. 2018 年，秘书长成立了数字合作高级别小组，以加强国际合作和多利益攸关方合作，推动开展公开辩论，探讨如何确保人人享有安全和包容的数字未来。该小组在《相互依存的数字时代》报告中也强调了“雅努斯的两副面孔”。如该报告所述，已经证明数字技术可以跨越文化和地理障碍将人们联系起来，从而增进相互理解，并可能促进社会更加和平、团结。然而，也有将数字技术用于侵犯权利、破坏隐私、使社会两极分化和煽动暴力方面的例子。[2]

5. 本背景文件以第十四届预防犯罪大会讨论指南所述讲习班 4 的主题框架为基础，并加以扩展。[3]本背景文件由不同章节组成，每一节都从不同角度反映了同一核心问题：执法机关和刑事司法机关正处于关键时期，因为技术创新快速发展，这既有助于有效开展警务工作，促进解决全面推进法治工作中长期存在的缺陷，同时也更易于在不同领域被用于犯罪活动。[4]

二. 技术作为犯罪手段和打击犯罪的工具

A. 加密货币和虚拟资产

6. 于近年来兴起的加密货币和虚拟资财吸引人们投资于使用相关软件协议建

[1] 尤里·费多托夫，“在短短的二十年里，科技已经成为犯罪的基石”，赫芬顿邮报英国版，2017 年 10 月 23 日。

[2] 见联合国，《相互依存的数字时代》，2019 年 6 月，第 17 页。

[3] A/CONF.234/PM.1，第 161-189 段。

[4] 秘书处就议程项目 6 编写的工作文件（A/CONF.234/7）涵盖了将互联网和数字技术用于恐怖主义目的以及与网络犯罪有关的问题。

设的支付基础设施。[5]加密货币用户可能会出于各种原因认为此种货币值得拥有，同时也可能持有此类资财以进行投机性投资。一些用户试图借此保护更高级别匿名交易的私密性，而另一些用户则只是想避免国家或银行对其合法交易进行监督和（或）控制。[6]加密货币的支持者指出，加密货币的交易费用低于传统银行对国家货币收取的费用，然而任何汇率损失和与加密货币服务提供商相关的费用都可能增加成本。[7]在没有传统银行的地方，加密货币可以提供与传统支付服务相关的功能。[8]最后，由于加密货币通常不是国家货币，所以可便利跨境交易。[9]

7. 尽管如此，许多允许加密货币市场运营的国家都颁布了相关法律，用以预防洗钱、有组织犯罪和资助恐怖主义行为，[10]不过到目前为止，恐怖分子似乎还没有大规模使用加密货币。[11]这一监管趋势是为了应对经常使用加密货币在网上进行非法和黑市购买的情况[12]，以及在洗钱、庞氏骗局、敲诈、勒索（分布式阻断服务攻击的威胁）和欺诈案件中将加密货币作为支付方式。

8. 适用于使用现金洗钱行为的概念同样也适用于使用加密货币的洗钱行为。[13]涉及加密货币的洗钱与传统洗钱有着类似的流程，区别是利用技术来洗钱。[14]此外，加密货币还可能被用于为逃税提供便利。[15]

9. 盗窃加密货币也是一个日益严重的问题。[16]加密货币用户可能成为旨在窃取加密货币的骗局的受害者。[17]此外，针对个人、公司或政府的勒索软件攻击在进

---

[5] Sesha Kethineni 和 Ying Cao，“加密货币和相关犯罪活动的兴起”，《国际刑事司法评论》，2019 年 2 月 6 日；Stearns Broadhead，“当代网络犯罪生态系统：事态和发展动态的多学科概述”，《计算机法律与安全评论》，第 34 卷，第 6 期（2018 年 12 月），第 1180-1196 页。

[6] Geoff Goodell 和 Tomaso Aaste，“加密货币能保护隐私并符合法律规定吗？”，《区块链前沿》，第 2 卷，第 4 篇（2019 年 5 月），第 1-20 页。

[7] Angela S. M. Irwin 和 Adam B. Turner，“非法比特币交易：在了解何人、何事、何时、何地方面面临的挑战”，《洗钱控制杂志》，第 21 卷，第 3 期（2018 年 7 月），第 297-313 页。

[8] 同上。

[9] Perri Reynolds 和 Angela S. M. Irwin，“追踪数字足迹：比特币系统中的匿名性”，《洗钱控制杂志》，第 20 卷，第 2 期（2017 年 5 月），第 172-189 页。

[10] 美国国会法律图书馆全球法律研究中心，《全球加密货币监管》（2018 年，华盛顿特区），2018 年 6 月。

[11] Cynthia Dion-Schwarz、David Manheim 和 Patrick B. Johnson，《恐怖分子使用加密货币：技术和组织障碍以及未来的威胁》（2019 年，加利福尼亚州圣塔莫妮卡，兰德公司）。

[12] Reynolds 和 Irwin，“追踪数字足迹”；Monica J. Barratt、Jason A. Ferris 和 Adam R. Winstock，“评分更安全？加密市场、社会供应和药物市场暴力”，《国际药物政策杂志》，第 35 卷（2016 年 9 月），第 24-31 页。

[13] Chad Albrecht 等人，“加密货币在洗钱过程中的使用”，《洗钱控制杂志》，第 22 卷，第 2 期（2019 年 5 月），第 210-216 页；Rolf van Wegberg、Jan-Jaap Oerlemans 和 Oskar van Deventer，“比特币洗钱：结果好坏参半？关于利用比特币进行网络犯罪所得洗钱的探索性研究”，《金融犯罪杂志》，第 25 卷，第 2 期（2018 年 6 月），第 419-435 页。

[14] Denis B. Desmond、David Lacey 和 Paul Salmon，“将加密货币洗钱作为复杂的社会技术体系进行评估：系统性文献综述”，《洗钱控制杂志》，第 22 卷，第 3 期（2019 年 7 月），第 480-497 页。

[15] Albrecht 等人，“加密货币在洗钱过程中的使用”；Saman Jafari 等人，“加密货币：对法律体系的挑战”，2018 年 5 月 10 日。

[16] Garrick Hileman 和 Michel Ruchs，《全球加密货币基准研究》（2017 年，大不列颠及北爱尔兰联合王国剑桥，剑桥大学替代金融研究中心）。

[17] Desmond 等人，“将加密货币洗钱作为复杂的社会技术体系进行评估”。

行勒索时往往要求用加密货币支付。

10. 在那些监管力度不足以识别用户身份或实施制裁以及监管漏洞可能被利用的环境中，更容易发生涉及加密货币的犯罪。由于不同国家对加密货币的规定不同，用户在一个国家进行的活动在其他地方可能被视为非法活动。[18]

11. 应考虑并采取若干行动，以预防将加密货币用于犯罪目的。交易去匿名化的方法可以增强威慑力和为侦查职能提供支持。这些方法可能包括制定法规，要求识别信息（“了解客户”规则）[19]或使用机器学习或其他监视技术分析交易以识别非法交易。[20]

12. 识别或有效侦查加密货币计划的知识和技能有限使得有更多机会将加密货币用于非法活动。[21]联合国所做的努力，如为侦查员提供关于加密货币犯罪的培训等，有助于预防和查明此类活动。[22]

13. 加密货币的发行者、监管机构和执法机关在阻止使用加密货币便利犯罪方面发挥着关键作用。必须开发一套强有力的预防和侦查手段，使之能够适应技术变化和加密货币的各种应用，从而最大限度减少犯罪中滥用加密货币构成的威胁。

B. 技术和暗网市场，包括毒品市场

14. 互联网通过明网和黑网为非法买卖商品提供了新的机会。明网（也称“表层网”）系指公众可以获得的、被常用的搜索引擎编入索引的信息，而黑网（或暗网，这两个术语在下文可互换使用）由加密网络的各个暗网组成，使网站所有者和用户可以保持相对匿名且不可追查。[23]

15. 暗网市场（也称“加密市场”）[24]为买家和卖家提供匿名性，在这类市场上，加密货币主要用于支付，以便利武器和非法药物等商品的销售和交易。

16. 欧洲联盟执法合作署（欧警署）指出，被泄露的个人、医疗和金融数据是暗网市场上的重要商品，在欺诈、网络钓鱼、身份盗窃和接管账户等活动中发挥着至关重要的作用。然而，虽然暗网市场上出售一系列假冒和盗版商品，但大多数

---

[18] Angela S. M. Irwin 和 Caitlin Dawson，“追踪网络货币踪迹：侦查勒索软件攻击面临的全球挑战以及监管如何发挥作用”，《洗钱控制杂志》，第 22 卷，第 1 期（2019 年 1 月），第 110-131 页。

[19] 金融行动特别工作组，《关于打击洗钱及资助恐怖主义和扩散的国际标准：金融行动特别工作组的建议》（2012 年，巴黎）。

[20] Irwin 和 Turner，“非法比特币交易”；Goodell 和 Aste，“加密货币能保护隐私并符合法律规定吗？”。

[21] Sesha Kethineni、Yin Cao 和 Cassandra Dodge，“比特币在暗网市场的使用：审视比特币相关犯罪的推动因素”，《美国刑事司法杂志》，第 43 卷，第 2 期（2018 年 6 月），第 141-157 页。

[22] 联合国毒品和犯罪问题办公室（毒品和犯罪问题办公室），“毒品和犯罪问题办公室开展培训，打击加密货币促成的有组织犯罪”，2017 年 5 月 8 日。

[23] Darren Guccione，“何为黑网？如何访问黑网以及从中可以找到什么”，《网络安全状况》，2019 年 7 月 4 日。

[24] Julian Broseus 等人，“研究暗网市场上的非法药物贩运问题：加拿大视角下的结构和组织”，《国际法证科学》，第 264 卷，2016 年 3 月 5 日，第 7 页。

非法交易仍然在表层网上进行。[25]在黑网上，人们越来越多地通过操纵比赛和赌博来完成洗钱过程，跨国有组织犯罪集团尤其如此。[26]第十四届预防犯罪大会欧洲区域筹备会议也强调需要解决利用暗网实施仇恨犯罪的问题。[27]

17. 在毒品领域，《2019 年世界毒品问题报告》指出，从长期来看，通过暗网购买毒品的现象日益增多，不过在 2018-2019 年期间，这种现象似乎有所下降。《2019 年全球毒品情况调查》的数据表明，通过暗网购买毒品是近年来才出现的现象，在 2019 年报称通过暗网购买毒品的人群中，有 48%的人在前两年开始出于此种目的使用暗网，而再往前推两年，有 29%的人开始出于此种目的使用暗网。[28]

18. 暗网毒品市场可能会导致吸毒模式和流行率发生变化，[29]因为它们可降低买家和卖家的某些风险，例如在销售毒品的社区出现的暴力冲突、[30]胁迫和逮捕风险。[31]然而，基于互联网的毒品销售本身也存在风险。最大的风险很可能发生在相关的“线下”活动期间。[32]基于互联网的毒品销售也可能导致过量使用的增加，使得实验更加便利，高效毒品更易获取。[33]

19. 在捣毁大型暗网市场方面已取得了令人瞩目的成就。然而，欧警署指出，犯罪分子正在探索规避执法行动的替代手段。一种新的趋势是出现了一种商业模式，在这种模式下，犯罪分子在不同在线平台上使用多个身份，从而便利多个人而不是一个人的操作。[34]

20. 对黑网进行侦查面临许多挑战。一个主要问题是，暗网中的信息未编入索引，因此侦查员无法使用搜索引擎或关键词轻易找到这些信息。此外，犯罪分子还利用分散的平台托管他们的网络服务器，从而使得服务激增，也更难被发现。[35]

21. 另一方面，执法机关也有机会监控暗网市场，并开展在线侦查。[36]在这种情

[25] 欧洲联盟执法合作署（欧警署），欧洲网络犯罪中心，《2018 年互联网有组织犯罪威胁评估》（2018 年，海牙），第 49 页。

[26] Robin Cartwright 和 France Cleland Bones，《跨国有组织犯罪和对私营部门的影响：隐藏的军营》（2017 年，日内瓦，全球打击跨国有组织犯罪倡议），第 29 页。

[27] 见 A/CONF.234/RPM.5/1，第 36(g)段。

[28] 《2019 年世界毒品问题报告：全球毒品供需情况概览》（联合国出版物，出售品编号：C.19.XI.8（第二分册））。

[29] Judith Aldridge 和 David DéCary-Hétu，“隐藏的批发：网上药物加密市场的药物扩散能力”，《国际药物政策杂志》，第 35 卷，2016 年 9 月，第 12 页。

[30] Julia Buxton 和 Tim Bingham，《暗网毒品市场的兴起和挑战》，政策简报，第 7 期（2015 年 1 月，英国斯旺西，全球药物政策观察站），第 1-24 页。

[31] Buxton 和 Bingham，《暗网毒品市场的兴起和挑战》。另见 David DéCary-Hétu、Masarah Paquet-Clouston 和 Judith Aldridge，“迈向国际化？加密市场药物供应商承担的风险”，《国际药物政策杂志》，第 35 卷，2016 年 9 月，第 71 页。

[32] Judith Aldridge 和 Rebecca Askew，“交付困境：药物加密市场用户如何识别并设法降低其被执法机关发现的风险”，《国际药物政策杂志》，第 41 卷，2017 年 3 月，第 101-109 页。

[33] Nathaniel Popper，“类阿片经销商使用黑网邮寄致命毒品”，《纽约时报》，2017 年 6 月 10 日。

[34] 欧警署，欧洲网络犯罪中心，《2019 年互联网有组织犯罪威胁评估》（2019 年，海牙），第 45 页。

[35] 国际刑事警察组织（国际刑警组织），“创新报告：匿名网络与暗网”（2018 年 9 月），第 12-13 页。

[36] 欧洲毒品和毒品致瘾监测中心与欧警署，《毒品和暗网：从执法、研究和政策角度进行分析》（2017 年，卢森堡），第 60 页及其后各页。

况下，一系列工具可提供解决办法，包括可用于定期自动编制在线数据索引的网络爬巡软件，用于搜索海量数据集的数据挖掘工具，用于追踪支付路径的加密货币分析工具，以及用于追踪证据的区块链软件等。[37]技术援助很重要，毒品和犯罪问题办公室一直积极开展重点关注黑网侦查手段的培训活动。

C. 枪支：技术相关的安全威胁

1. 枪支制造中的高科技聚合物

22. 工业聚合物必将在军火工业中发挥越来越重要的作用，并对有效执行《联合国打击跨国有组织犯罪公约关于打击非法制造和贩运枪支及其零部件和弹药的补充议定书》中所载关于枪支追查和记录保存的规定构成挑战。这种工业聚合物的出现削弱了主管机关充分发现、侦查和起诉相关犯罪的能力。

23. 《小武器管制执行工作模块简编》汇编了小武器管制方面不具约束力的良好做法，该简编建立在以下相关国际文书成果的基础上：《枪支议定书》、《小武器行动纲领》和相关的《国际追查文书》和《武器贸易条约》，可以帮助各国应对聚合物框架和接收器带来的挑战。

2. 模块化武器

24. 新技术和现有法律漏洞导致合法和非法市场充斥着改进、改装和制造套件，使拥有极少技术知识的枪支所有者能够改造其枪支，甚至生产功能齐全的枪支。

25. 《枪支议定书》适用于“零部件”，但其标识要求（第 8 条）仅适用于“枪支”。这个问题在模块化武器方面尤其严重。[38]应对这一挑战可能需要采取一些措施，例如为所有枪支，无论是标准枪支还是模块化枪支，确定一个控制部件，用于标识、保存记录和追查；确定应在控制部件上标记哪些信息以避免序号重复；就追查用途的独特识别提供指导，尤其是模块化武器的独特标识。[39]

3. 增材制造（3D 打印）

26. 增材制造，俗称三维打印或 3D 打印，是一项新兴技术，在短期和长期内可对地方、国家和国际安全产生影响。增材制造的发展和推广可显著加速武器扩散，并可能对日常犯罪产生重大影响。另外，3D 打印枪支可能会对枪支登记和执照发放制度以及警方侦查所用的弹道数据库的效力产生负面影响。

27. 《枪支议定书》关于非法制造枪支的第 3 条(d)项和第 5 条第 1 款(a)项将适用于采用 3D 打印技术生产的枪支，与适用于传统制造枪支的方式相同。然而，

[37] 国际刑警组织，“创新报告”，第 14 页。另见 Shira Stein，“改进执法，使用加密货币抓捕罪犯”，《证券监管和法律报告》，49 SRLR 1029（2017 年，弗吉尼亚州阿灵顿，国家事务出版公司）。

[38] Giacomo Persi Paoli，“从枪支到武器系统：标识、记录保存和追查模块化设计的挑战和影响”，载于《曲线背后：新技术、新控制挑战》，《小武器调查》的专题文件，第 32 期，Benjamin King 和 Glenn McDonald 编辑。（2015 年，日内瓦，《小武器调查》），第 23 页。

[39] 同上，第 40 页。

下载数字化文件用于 3D 打印枪支似乎超出了议定书的范围，这种情况亟需法律对策。

28. 许多关于无许可证生产、制造和持有枪支的现行法律和罪行都涉及 3D 打印枪支，但不一定涉及持有或散发设计文件。[40]对于向可能希望使用增材制造技术生产枪支者提供器械的第三方，涉及非法制造枪支问题的法律可能需要确定其罪责。[41]

29. 全面的监管办法必须涵盖国内和国际行为体，以及公共和私营部门。增材制造的双重用途潜力使得人们在限制推广这项技术的同时肯定也会限制它的众多益处。[42]与任何新兴技术一样，就这项技术为执法人员提供培训和教育将非常重要。

4. 黑网中的枪支贩运

30. 黑网有可能成为有组织犯罪集团和希望匿名或非法购买枪支的个人的首选平台。[43]联合国裁军事务厅于 2018 年提交给大会第一委员会一份研究报告，该报告是基于兰德欧洲公司 2017 年进行的一项更大的研究项目编写的。[44]针对该报告，有人指出，迫切需要开展新的国际合作，以打击因黑网的匿名性而可能进行的非法武器销售。[45]

31. 在黑网上进行武器销售的比例似乎比其他非法物品的比例低。[46]最近一项仅关注黑网上武器相关清单的研究发现，枪支清单最常见，占黑网上所有清单的 42%；其次是与武器相关的数字产品，占比 27%；弹药等其他产品占 22%。[47]

32. 了解黑网上非法武器贸易的规模和范围对于更好地了解执法机关所面临威胁和受到影响的严重程度至关重要。在国家一级，政策制定者需要确保执法机关人员配备适当、训练有素且装备齐全，足以应对相关挑战。现有的国际法律框架，特别是《有组织犯罪公约》及其《枪支议定书》，可以为采取全面办法应对这一现象提供基础。需要深入分析《枪支议定书》（第 15 条）和《武器贸易条约》（第 10 条）规定的现行经纪活动条例是否适用。[48]

---

[40] 国际刑警组织创新论文，“3D 和 4D 打印”，国际刑警组织全球创新中心，2018 年，第 6 页。

[41] N. R. Jenzen-Jones，“小武器和增材制造：对 3D 打印枪支及其零部件的评估”，载于《曲线背后：新技术、新控制挑战》，《小武器调查》的专题文件，第 32 期，Benjamin King 和 Glenn McDonald 编辑。（2015 年，日内瓦，《小武器调查》），第 63-64 页。

[42] Trevor Johnston、Troy D. Smith 和 J. Luke Irwin，“2040 年的增材制造：强大的推动力、破坏性威胁”，文件编号：PE-283-RC（2018 年，加利福尼亚州圣塔莫尼卡，兰德公司），第 17 页。

[43] 兰德欧洲，“黑网上的国际武器贸易”（2019 年），“调查结果”章节，第 8 段。

[44] Giacomo Persi Paoli 等人，《幕后：黑网上的枪支、爆炸物和弹药非法贸易》（2017 年，加利福尼亚州圣塔莫尼卡，兰德公司）。

[45] Giacomo Persi Paoli，《黑网上的小武器和轻武器贸易》，联合国裁军事务厅（裁军厅）《专题文件》，第 32 期（联合国出版物，出售品编号：C.19.XI.1），第 9 页。

[46] Damien Rhumorbarbe 等人，“加密市场网上武器贩运的特征”，《国际法证科学》，第 283 卷，2018 年 12 月，第 16-20 页。

[47] 兰德欧洲，“黑网上的国际武器贸易”（2019 年），“调查结果”章节，第 4 段。

[48] Simonetta Grassi 和 Mareike Buettner，“附件：国际法律文书概览及其对黑网非法枪支贩运的适用性”，载于 Paoli 等人，《幕后》，第 101 页。

5. 致命性自主武器

33. 尽管官方未承认存在完全自主武器，但是利用人工智能控制此类武器的观点已经引发了激烈的辩论。2016 年，禁止或限制使用某些可被认为具有过分伤害力或滥杀滥伤作用的常规武器公约缔约国第五次审议大会成立了致命性自主武器系统领域的新技术问题政府专家组。在 2019 年的会议上，专家组建议缔约国核可专家组确认的指导原则。[49]

D. 贩运人口

34. 过去几年的研究和直接证据表明，人贩在犯罪的所有阶段，包括招募、控制和剥削受害者的过程中都使用了技术。

35. 人贩利用技术的一个原因是，技术能帮助他们匿名操作并隐藏其身份。此外，加密货币使人贩可以进行金融交易，并匿名转移犯罪所得。另一个原因是，技术为人贩招募和剥削受害者提供了便利。在线分类广告和社交网站可以被用作“贩运人口的渠道”。[50]

36. 此外，滥用技术使人贩更容易与用户进行交易，进入新的市场，以及扩大犯罪活动。人贩可以通过直播开拓更广阔的客户市场，而这些客户可能从未与受害者有过现实接触。[51]

37. 此外，滥用技术可以帮助人贩控制和胁迫受害者。人贩可能会利用位置跟踪技术来便利对受害者进行剥削。即使受害者已经逃脱了人贩的控制，施虐者仍可以使用受害者手机上的位置追踪器发现他们的行踪，从而跟踪他们。

38. 同时，执法机关已经使用位置跟踪技术来侦查可疑人贩或参与贩运网络的其他个人的位置。同样，也可能利用受害者的位置跟踪数据，因为受害者可能被视为“行走的证据数据库”。[52]

39. 在打击贩运工作中使用技术干预措施需要跨部门协作。信息和通信技术行业和国际组织已开展合作，探讨如何利用技术预防贩运人口，并帮助受害者康复。“打击贩运技术”是由领先的技术公司、学术机构和国际移民组织组成的联盟，该联盟提供了一份用于打击人口贩运的技术解决方案清单。[53]

40. 所有相关行为体的能力建设对于应对利用技术贩运人口带来的挑战至关重要。必须认真考虑从业人员打击人口贩运所用技术的开发、使用、维护、监测和

---

[49] CCW/GGE.1/2019/3, 附件四。

[50] Mark Latonero，《网络人口贩运：社交网站和在线分类广告的作用》，传播领导力和政策中心系列研究（2011 年 9 月，洛杉矶南加州大学），第 8 页。

[51] 打击贩运人口机构间协调小组，“人口贩运与技术：趋势、挑战和机遇”，问题简报，第 7 期（2019 年），第 1-2 页。

[52] Felicity Gerry、Julia Muraszkiewicz 和 Niovi Vavoula，“技术在打击人口贩运中的作用：对隐私和数据保护问题的思考”，《计算机法律与安全评论》，第 32 卷，第 2 期（2016 年 4 月），第 210-211 页。

[53] 商务社会责任国际协会，“打击贩运技术联盟确定的技术工具和举措清单”，2019 年 1 月 15 日。

评价。[54]然而，相关工具的开发人员需要预测并顾及存在被贩运风险的用户之间的差异。[55]

E. 偷运移民

41. 信息和通信技术已成为移民和招募者广泛使用的重要工具，用于传递有关路线、服务和价格的信息。[56]此外，社交媒体增强了偷运者为应对过境国执法机关的对策而改变路线的能力，从而提高了偷运活动的成效，并对调查和起诉此类罪行造成阻碍。[57]

42. 移动技术的快速发展可能会对移民和偷运者之间的关系产生影响。在若干 Facebook 群中，移民可以核实某些偷运者的可靠性，并分享信息，告知谁是最佳联系人。这被称为“信任度等级体系”。[58]

43. 技术也可以用于金融支付，因为主要通过在线支付系统向偷运者付款。加密货币可能使偷运者更容易接收、隐藏和转移资金。这种货币可以帮助洗钱，并通过提供匿名性和减少携带大量现金的需要，帮助偷运者免遭调查和逮捕。

44. 技术还在提供欺诈性差旅证件或身份证件方面发挥重要作用，为偷运移民提供便利。各种类型的设备被用于伪造、变造或复制护照。在某些情况下，技术先进的工具被用于高水准的造假（“镜像级”护照）。[59]

45. 然而，可以从多个角度看待技术创新，而不仅仅是从偷运者获益的角度。数字化还缩小了偷运者赖以生存的信息鸿沟。互联网可用于帮助移民与提供支持和信息的社交网络建立起联系。技术驱动的转变呈现的最新趋势是，越来越多的移民在整个移民过程中自给自足，对偷运者的依赖减少。这使移民具有更多的自主权，并使他们不那么容易受到剥削。[60]

46. 移民使用社交媒体的方式因他们的国籍、种族、原籍地区和教育背景以及他们使用互联网的情况而异。[61]有证据表明，移民群体之间存在数字鸿沟，这是由他们实际获取和使用数字技术、有效使用不同技术所需的技能以及支付服务费用的能力方面的不平等造成的。[62]

---

[54] 打击人口贩运机构间协调小组，“人口贩运与技术”，第 4 页。

[55] 见 Mark Latonero、Bronwyn Wex 和 Meredith Dank，《网络社会中的技术和劳动力贩运：总述、新兴创新和菲律宾案例研究》（2015 年，洛杉矶，南加州大学安纳堡传播领导力和政策中心），第 11 页。

[56] 欧警署和国际刑警组织，“偷运移民网络：执行摘要”（2016 年 5 月），第 8 页。

[57] CTOC/COP/WG.7/2018/2，第 25 段。

[58] Judith Zijlstra 和 Ilse van Liempt，“智能（手机）旅行：了解移动技术在非常规移民旅程中的使用和对其的影响”，《国际移民与边境研究杂志》，第 3 卷，第 2 和 3 期（2017 年 3 月），第 176-177 页。

[59] 毒品和犯罪问题办公室东南亚和太平洋区域办事处，《东南亚偷运移民的推动因素：伪造证件、洗钱和腐败》（2019 年，曼谷），第 26 页。

[60] 毒品和犯罪问题办公室，《多哈宣言》，高等教育，“教育促进正义”大学模块系列，贩运人口和偷运移民，“模块 14：网络犯罪、贩运人口和偷运移民之间的联系——偷运移民采用的技术”。可查阅：www.unodc.org/e4j/。

[61] 欧盟委员会，“使用社交媒体打击偷运移民”，欧洲移民网通报（2016 年 9 月）。

[62] Alam Khorshed 和 Sophia Imran，“难民移民的数字鸿沟和社会包容：澳大利亚地区的案例”，《信息技术与人》，第 28 卷，第 2 期（2015 年 6 月），第 344 页及其后各页。

47. 从执法的角度来看，人们越来越关心找到利用技术破坏偷渡移民网络的方法。此外，使用从社交媒体和（或）通过使用技术获得的证据可支撑被偷运移民在相关刑事诉讼中的证词。

48. 适当使用技术有助于各国政府、私营部门和非政府组织在各自的职权范围内预防和减少偷运移民活动。因此，必须提高刑事司法对策的有效性，并与在线服务提供商建立激励机制和伙伴关系，以便更好地监测、发现和举报偷运相关内容。

F. 网上虐待和剥削儿童

49. 虽然儿童性虐待和性剥削在互联网出现之前就已经存在，但这些罪行的线上形式使犯罪者能够彼此互动，并在网上获得儿童性剥削材料。此外，越来越多的年幼儿童可以上网，相较于线下环境，这让犯罪者有机会更容易接触到儿童，进而对相关犯罪的作案手法产生相当大的影响。

50. 技术的进步在对儿童商业性剥削方面起着重要作用。参与儿童色情旅游的游客可以利用云计算来存储图像或视频，从而避免与现实中运送儿童性剥削材料相关的风险。此外，移动电话技术将儿童性剥削和性虐待的组织者、受害者和消费者联系起来，降低了生产者和分销商当面进行交易的必要性，进而使他们更加不易被发现。

51. 借助信息和通信技术虐待和剥削儿童的主要形式包括接触色情制品、线上诱拐和线上性招揽骚扰，其中许多剥削行为的特点是与儿童发生不当性行为。毒品和犯罪问题办公室的一项相关研究提请人们注意虐待和剥削儿童的新形式，如用户生成的内容、包括色情短信在内的自创内容、直播性虐待和“定制”的儿童性虐待材料。[63]

52. 欧洲刑警组织称，直播性虐待已成为既定威胁，直播渠道为社交媒体应用程序、视频聊天应用程序、游戏平台和网络聊天室。此外，直播性虐待的载体似乎正在从电脑转向智能手机和平板电脑，使用的网络则从有线互联网转向 Wi-Fi 和移动互联网。[64]

53. 在网上散发儿童性剥削材料的最大威胁之一是暗网的使用越来越多。据因特网监视基金会称，用“数字通道”方法隐藏儿童性虐待图像的伪装网站仍然是重大问题。此外，该基金会发现，近年来儿童性虐待网站的数量稳步增加：从 2015 年的 68,092 个增加至 2018 年的 105,047 个。[65]

54. 此外，随着网上儿童性犯罪者采用的技术日益先进，他们将继续寻找新的方法来避免被发现。最近，他们借助具有端到端加密功能的移动通讯应用程序，从大型论坛转向了小型用户群。

55. 一些国家没有监管新型虐待儿童行为的适用法律规定，在保护儿童和界定同意年龄的法律方面存在差异，这些都是重大问题，降低了成功发现、侦查和起诉相关行为的可能性。

---

[63] 毒品和犯罪问题办公室，《关于新信息技术对虐待和剥削儿童行为的影响的研究》（2015 年，维也纳），第 21 页及其后各页。

[64] 欧洲刑警组织，《2018 年互联网有组织犯罪威胁评估》，第 35 页。

[65] 因特网监视基金会，《曾几何时》（2018 年，英国剑桥），第 19 和 43 页。

56. 技术也可能为执法机关提供解决相关问题的方法。[66]数据挖掘和分析等方法和手段的创新改进了法证过程，从而推进侦查。由于儿童性剥削会对儿童造成创伤以及儿童证人的年龄和脆弱性，在使用依托信息技术的手段时应尊重保护人权的边界。

57. 还建立了能上传儿童性虐待材料以供侦查之用的数据库，如国际刑事警察组织的国际儿童性剥削数据库。在美利坚合众国，国家失踪和被剥削儿童中心的数据库是儿童性虐待材料的中央储存库。[67]

58. 为有效打击借助信息和通信技术的儿童虐待和剥削行为，需要采用多利益攸关方办法，即纳入儿童、家庭、社区、政府、民间社会和私营部门，让他们积极参与其中。[68]

G. 人工智能和机器人

59. 在互联网和移动技术引发“第三次工业革命”后，大数据驱动的[69]人工智能技术正在催生“第四次工业革命”。尽管这可能有利于全球发展和社会变革，有助于实现可持续发展目标，但也出现了法律、伦理和社会问题与挑战。在执法领域，人工智能进步所带来的机遇与风险并存，因此需要采取战略性办法，加大努力，投入更多资源。[70]

60. 第十四届预防犯罪大会的几乎所有区域筹备会议都强调，务必探索各种方式方法，让刑事司法和执法从业人员在打击犯罪的过程中使用并充分利用不断发展的技术，如人工智能以及大数据等信息和通信技术。[71]

61. 除其他外，会议也就以下问题进行了相关讨论：使用人工智能进行虚拟尸检、助力警方优化资源的犯罪预测系统、行为侦查工具、尊重隐私的基于区块链的可追溯性方法，以及自动巡逻车。[72]此外，由于人工智能技术的进步，机器人变得“更聪明”，并能够取代人类发挥很多作用、完成很多任务，因此，越来越多的执法机关将此类先进技术运用到各项行动中。各国机器人技术的使用程度各异，因为一些国家在研究和使用这类技术方面比其他国家更先进。[73]

62. 人工智能和机器学习似乎提供了日益有效的反洗钱工具。就像帮助网上零售商锁定目标客户的算法一样，人工智能和机器学习通过解读表明犯罪活动的信号

---

[66] Victoria Brains，“网上儿童性剥削：采取最佳国际对策”，社会科学研究网电子期刊，2018 年 8 月 29 日。

[67] 毒品和犯罪问题办公室，《多哈宣言》，高等教育，“教育促进正义”大学模块系列，网络犯罪，“模块 12：人际网络犯罪——网上儿童性剥削和性虐待”。可查阅：www.unodc.org/e4j/。

[68] 毒品和犯罪问题办公室，《关于新信息技术影响的研究》。

[69] Victor Mayer-Schönberger 和 Kenneth Cukier，《大数据：一场将改变我们的生活、工作和思维方式的革命》（2013 年，伦敦，约翰·默里出版社）。

[70] 联合国区域间犯罪和司法研究所（犯罪司法所）在海牙设立了人工智能和机器人中心，作为人工智能和机器人相关事项方面的国际资源。

[71] A/CONF.234/RPM.1/1，第 61(J)段；A/CONF.234/RPM.2/1，第 79(k)段；A/CONF.234/RPM.3/1，第 56(f)段；A/CONF.234/RPM.4/1，第 57(e)段；

[72] 国际刑警组织和犯罪司法所，“将人工智能和机器人技术用于执法”（2019 年，意大利都灵），第 5 页。

[73] 同上，第 6 页。

和分析海量数据，能够以更可靠的方式帮助制定更具洞察力且更准确的尽职调查政策。此外，机器学习越来越多地被社交媒体平台用于屏蔽非法内容和假新闻。企业一直将人工智能用于高风险管理，并通过反应迅速的欺诈侦查来预防和预测犯罪。

63. 然而，人工智能在很大程度上是一把双刃剑，因为它既可以使执法机关处理警务任务的方式发生巨大变化，也会增强犯罪集团和恐怖主义集团的作案手法，甚至可能导致出现新的犯罪形式。[74]在这场堪称“适者生存”的斗争中，优先事项可以概括为：推动警务工作人工智能化，以打击人工智能犯罪。[75]

H. 刑事事项和技术使用方面的国际合作

64. 刑事事项国际合作领域正在开展一场讨论，即中央机关如何才能通过运用现代技术充分受益。在政策方面，2016 年联合国打击跨国有组织犯罪公约缔约方会议鼓励缔约国最充分、最有效地利用现有技术便利中央机关之间的合作。[76]

65. 加强国际合作的必要性日益凸显，但这取决于是否有资源，包括“技术资源”，例如用于安全传输信息的网络、促进通信的设备（如电话会议和视频会议）以及用于跟踪收到和发出的请求的案件管理系统。资源需求的增加还可能与更高效地处理涉及电子证据的司法协助请求有关（例如通过在中央机关内设立专门机构进行处理）。

66. 从会员国各不相同的能力水平可以看出，会员国中央机关的案件管理情况明显反映了本国整个刑事司法体制机制的进步、发展或缺陷。许多国家依然用硬拷贝形式保存档案，这可能使搜索这些档案和向请求国提供相关文件成为一项艰巨的任务。另一些国家则采用现代技术，利用电子平台来管理收到和发出的司法协助请求，或汇编案件和趋势方面的统计数据。[77]

67. 第十四届预防犯罪大会拉丁美洲和加勒比区域筹备会议讨论了该区域某些国家以电子方式发送司法协助请求的问题，并强调这是一种良好做法。[78]筹备会议建议，除其他因素外，各国应该在考虑到中央机关之间根据国家法律以电子方式发送国际合作请求的协定的情况下，促进对技术的利用，以使刑事事项方面的国际合作更加有效。[79]

68. 毒品和犯罪问题办公室已采取行动促进国际合作，包括借助量身定制的工具和技术创新：知识管理门户网站“打击犯罪信息与法律网络共享平台”（夏洛克数

[74] 2018 年的一份报告研究了滥用人工智能的犯罪行为，并确定了三大类相关威胁：(a)与数字安全有关的威胁；(b)与人身安全有关的威胁；(c)与政治安全有关的威胁（假新闻和自动化虚假信息泛滥，或影响投票行为并可能有损维持真实公开讨论的能力的扩大影响力活动）。见 Miles Brundage 等人，《人工智能的恶意使用：预测、预防和缓解》（2018 年 2 月）。

[75] 国际刑警组织创新论文，“人工智能”，国际刑警组织全球创新中心，2018 年，第 2 页。

[76] 会议第 8/1 号决议。

[77] 亚洲开发银行和经济合作与发展组织，《亚洲及太平洋司法协助：31 个法域的经验》（2017 年），第 31 页。

[78] A/CONF.234/RPM.3/1，第 72 段；

[79] 同上，第 79(n)段。

据库）、国家主管机关名录和新开发版本的司法协助请求撰写工具。[80]

69. 毒品和犯罪问题办公室一直积极支持各项政府间进程，其中，涉及电子证据的国际合作已成为政策和法律优先事项。这类进程的实例包括全面研究网络犯罪问题不限成员名额政府间专家组、[81]2018 年 5 月举行的预防犯罪和刑事司法委员会第二十七届会议关于网络犯罪的专题讨论，[82]以及有组织犯罪公约缔约方大会国际合作工作组的相关工作。

I. 伦理考量因素：程序和人权保障措施

70. 技术工具可以作为有效切入点，解决与犯罪有关的威胁。然而，在具体应用这些工具时应当谨慎，确保以负责任和合乎伦理的方式使用，避免意外后果。这一点尤为重要，因为当前和未来的许多技术可能会对个人隐私和公民自由产生严重影响。

71. 例如，执法专业人员目前使用面部识别软件来更快地识别嫌疑人。然而，批评人士担心，这可能会导致政府滥用监控、企业操纵以及隐私终结。此外，生物识别系统的数据保留特性可能会因潜在的数据滥用而危及隐私。[83]

72. 另一个实例是预测性警务或预测分析。过去几年，越来越多的执法机关采用软件来分析统计数据，识别各种活动和案件之间的联系，甚至预测下一次威胁会在哪里出现。然而，其风险在于，使用预测性警务技术进行特征分析可能会导致将个人和群体污名化，从而导致基于算法的各种歧视。[84]

73. 在人口贩运领域以及在探索技术的利用与人权和数据保护之间的相互作用时，必须确保加强对受害者的保护。[85]在设计打击贩运的解决办法时，应予以认真监督，以免侵犯隐私权或不当地针对某些群体，[86]同时确保受害者也能安全地获取技术。[87]

74. 另一个重要因素是落实程序方面的保障措施，使得通过特殊侦查手段（包括使用技术的手段）获取的证据在法庭上可被采纳。特殊侦查手段的使用须遵守国内法律和适用的多边文书的相关规定。[88]在大多数法域，在收集证据时，需严格遵守防止可能滥用权力的保障措施，包括对这些手段的使用进行司法监督或独立

[80] 可查阅：www.unodc.org/mla/en/index.html。

[81] 毒品和犯罪问题办公室，网络犯罪，“涉及简易爆炸装置的网络犯罪问题会议”。可查阅：www.unodc.org。

[82] 见该专题讨论指南（E/CN.15/2018/6）。

[83] Max Snijder，《生物识别技术、监视和隐私》（2016 年，意大利伊斯普拉，关键基础设施保护欧洲参考网应用生物识别技术促进关键基础设施安全主题小组），第 4 页及其后各页。

[84] 见 Eva Schlehahn 等人，“预测性警务的益处和陷阱”，载于《2015 年欧洲情报与安全信息学会议》，Joel Brynielsson 和 Moi Hoon Yap 编辑（2015 年，新泽西州皮斯卡塔韦，电气和电子工程师学会），第 145-148 页；Albert Meijer 和 Martinjn Wessels，“预测性警务：利弊综述”，《国际公共管理杂志》，第 42 卷，第 12 期（2019 年 2 月）。

[85] 见打击人口贩运机构间协调小组，“人口贩运与技术”，第 5 页。

[86] Mark Latonero 等人，《移动设备的兴起与技术辅助贩运的扩散》，技术与人口贩运系列研究（2012 年 11 月），第 38 页。

[87] Gerry、Muraszkiewicz 和 Vavoula，“技术在打击人口贩运中的作用”，第 211 页。

[88] 见《联合国打击跨国有组织犯罪公约》第 20 条和《联合国反腐败公约》第五十条。

监督，以及遵守合法性、辅助性和相称性原则。[89]电子证据必须符合既定程序，以便其可被采纳。[90]对在加密货币法证侦查中获得证据的可采性适用国内程序法和国家判例的一般原则是具有挑战性的新领域，需要进一步审议和分享经验。[91]

75. 随着执法部门日益普遍地使用人工智能和机器人，确保这种使用合乎伦理也日益重要。已采取“软法”性质的举措，最大限度地减少由执法机关使用人工智能系统导致的侵犯基本权利的风险，并从整体上降低与合乎伦理地使用人工智能和机器人相关的法律责任的模糊性。[92]

76. 然而，根本的问题是，整个社会是否已经充分准备好接受诸如建立一个广泛的监视设备网络的做法，即使这是出于公共安全和安保的考虑。[93]关于技术的决定应该基于就其成本、效益和适用规范开展的广泛社会对话。说服公众相信技术在执法和刑事司法领域的益处是一般性讨论的一部分，需要持续进行，以确保主管机关不会失去其有责任保护的社区和公民的信任。这场讨论也应该回应“问题的另一面”，即批评的声音：越是依赖技术就越可能加深对强制性监视和控制策略的依赖。[94]

77. 数字合作问题高级别小组建议秘书长就现有国际人权协定和标准如何适用于新型和新兴的数字技术对各个机构进行审查。应邀请民间社会、政府、私营部门和公众就如何在数字时代以积极和透明的方式应用现有人权文书提出意见。[95]

78. 在技术似乎可能与隐私或其他人权发生冲突的情况下，需要以平衡的方法来寻找解决办法。为了避免将技术用作可能侵犯基本权利的“特洛伊木马”，需要持续监测技术发展并评估其影响。

三. 结论和建议

79. 我们可以从希腊神话中汲取灵感，提出这样的问题：技术最终是预防犯罪的灵丹妙药（一种声称可以治愈所有疾病的药物，以医神阿斯克勒庇俄斯之女的名字命名）吗？还是一个潘多拉魔盒，人们逐渐发现它会在增加犯罪机会方面产生严重影响（类似于潘多拉打开盒子释放出所有邪恶的神话）？

---

[89] 关于欧洲人权法院的相关判例，见 Dimosthenis Chrysikos，“第五十条：特殊侦查手段”，载于《〈联合国反腐败公约〉评注》，Cecily Rose、Michael Kubiciel 和 Oliver Landwehr 编辑，牛津国际法律评论丛书（2019 年，牛津，牛津大学出版社），第 507 页及其后各页。

[90] E/CN.15/2018/6，第 30 段。

[91] Michael Fröwis 等人，“维护加密货币法证侦查的证据价值”（2019 年）。

[92] 电气和电子工程师协会在全球发布了一份关于自主和智能系统伦理（合乎伦理的设计）的论文，旨在使技术符合道德价值和伦理原则。见电气和电子工程师协会自主和智能系统伦理全球倡议，《合乎伦理的设计：在利用自主和智能系统时优先考虑人类福祉的愿景》（2019 年，新泽西州皮斯卡塔韦）。

[93] 国际刑警组织和犯罪司法所，“将人工智能和机器人技术用于执法”（2019 年，意大利都灵），第 14 页。

[94] James Byrne 和 Gary Max，“预防犯罪和警务方面的技术创新：关于实施和影响的研究综述”，《凯尔斯政治研究》，第 20 卷，第 3 期（2011 年），第 30 页。

[95] 联合国，《相互依存的数字时代：联合国秘书长关于数字合作高级别小组的报告》（2019 年 6 月），建议 3A。

80. 这个问题的答案并非摩尼教式的非黑即白。技术带给我们的必然好坏参半。执法机关和刑事司法机关受益于技术的进步。同时，技术创新的激增也为犯罪活动猖獗提供了沃土。由于现代技术的各种应用，“犯罪格局”已经发生了巨大变化，主管机关需要与时俱进。

81. 犯罪分子和法治捍卫者之间正在进行的较量结果如何，将在很大程度上取决于是否投资开展培训，以及是否不断调整预防犯罪和刑事司法策略以应对新出现的挑战，同时还要考虑到伦理和人权因素。

82. 第十四届联合国预防犯罪和刑事司法大会不妨审议以下建议：

(a) 会员国应明确并弥补其法律制度方面的缺口，以确保有效侦查和起诉技术辅助的犯罪行为，包括出台新法律和（或）使用技术上中立的措辞更新现有法律，以及加强国际合作；

(b) 会员国应促进和扩大与包括国际和区域组织、民间社会、私营部门和学术界在内的各利益攸关方之间的伙伴关系和协同增效作用，以加强执法和刑事司法领域的研究、创新、开发和技术应用；

(c) 会员国应明确和评估涉及虚拟资财服务提供商的活动或业务中存在的洗钱和资助恐怖主义风险；采用基于风险的办法，确保预防或减少洗钱和资助恐怖主义的措施与确定的风险相称；并要求虚拟资财服务提供商明确、评估并采取有效行动减轻洗钱和资助恐怖主义风险；

(d) 会员国应增加对相关培训的投资，以提高在侦查期间有效解决加密货币所引发问题的能力；

(e) 会员国应在其法律中列入关于拥有、出版和转让可用于最终制造枪支的数字材料的规定，并开展能力建设活动，以提高预防、侦查、调查和起诉这些行为以及暗网枪支贩运的技能；

(f) 毒品和犯罪问题办公室应继续推动从业人员团体定期召开会议，以确保侦查员了解枪支制造和转让的新型作案手法以及相应的侦查手段；

(g) 会员国应特别注意提升所有相关部门主管机关的专门知识和能力，以便最有效地利用技术打击人口贩运，同时保护受害者的权利；

(h) 毒品和犯罪问题办公室应进一步向会员国提供技术指导和支持，使其能够更有效地找到并落实以技术为基础的刑事司法系统措施，以预防、侦查和起诉贩运人口和偷运移民行为；

(i) 会员国应采取立法或其他措施，协助互联网服务和接入提供商及其他有关实体查明儿童性剥削和性虐待材料，并确保举报和删除这类材料；

(j) 会员国应落实各项相关政策并分享最佳做法，包括受害者帮扶方案和将性别考量纳入主流方面的政策和最佳做法，以保护儿童免受性剥削和性虐待；

(k) 会员国应提高对恶意使用人工智能所带来风险的认识，持续监测新技术的发展，以确保防范、问责、透明和廉正；推广使用这些技术的伦理标准；并确保公民和社区对这些技术的使用充满信心和信任；

(l) 会员国应与毒品和犯罪问题办公室及其他国际组织合作，推进技术援助和培训，以提高从业人员和中央主管机关在利用技术加快国际合作方面的能力。