网络空间的反恐

恐怖分子和恐怖组织不仅利用互联网和社交媒体实施恐怖行为，还协助开展各种各样的恐怖主义活动，包括煽动、激进化、招募、培训、规划、收集信息、通信、制备和筹资。COVID-19大流行在许多会员国造成封锁和社交距离，互联网的使用也急剧增加，引起了人们对恐怖分子和恐怖组织以及信奉极右(或出于种族或族裔动机)意识形态的个人和团体滥用信息和通信技术(信通技术)的严重关切。反恐委员会在处理这些突出问题的工作中，遵循安全理事会的若干决议，其中包括：

- 安全理事会第1373(2001)号决议，该决议是在2001年9月11日对美国的袭击之后不久通过的，呼吁所有会员国设法加紧和加速交流有关恐怖主义集团使用信通技术的行动情报，并制止招募恐怖分子。
- 安全理事会第1624(2005)号决议，其中要求会员国根据国际法规定的义务，采取必要和适当措施，依法禁止煽动实施恐怖行为，并防止这种行为。
- 安全理事会第2129(2013)号决议，其中指示反恐怖主义委员会执行局(反恐执行局)与会员国、国际、区域和次区域组织、私营部门和民间社会协商，继续处理在恐怖活动中使用信通技术的问题，并就进一步办法向委员会提供建议。
- 安全理事会关于制止外国恐怖主义作战人员流动的第2178(2014)号决议，该决议促请会员国协作采取国家措施，防止恐怖分子利用技术、通信和各种资源来煽动对恐怖行为的支持。同时，各国应尊重人权和基本自由，并确保遵守国际法规定的其他义务。
- 安全理事会在第2322(2016)、2331(2016)、2341(2017)和2396(2017)号决议中，呼吁各国收集和保存数字证据，以便进行调查和起诉，追究恐怖袭击者的责任。
- 安全理事会第2341(2017)、2354(2017)、2395(2017)和2396(2017)号决议确认，需要通过自愿合作发展公私伙伴关系，以解决信通技术被用于恐怖主义目的的问题，包括制定反宣传和技术解决方案，同时尊重人权和基本自由，并确保遵守国内和国际法律。安全理事会第2395(2017)号决议确认了反恐执行局在这方面的工作。
- 安全理事会第2354(2017)号决议规定了实施反宣传的“综合性国际框架”的准则，并向易受极端主义信息影响的受众宣传积极和可信的替代讯息。
- 第2462(2019)号决议注意到利用众筹平台为恐怖主义目的筹集资金，以及利用预

付卡和移动支付或虚拟资产等新兴支付方式转移和转移此类资金的现象。决议还呼吁评估和解决与虚拟资产和新金融工具有关的潜在风险。

此外，反恐委员会通过 2015 年《马德里指导原则》(S/2015/939)和关于 2018 年《关于外国恐怖主义作战人员的指导原则增编》(S/2018/1177)为会员国制定了这一领域的指导。指导原则 13、14、33、43 和 44 侧重于监测和研究通过互联网和其他通信技术传播的恐怖主义内容的方法；鉴于对数字数据的请求增加，审查国家司法协助法律和机制；以及在与外国恐怖主义作战人员有关的案件中收集数字数据和证据。在反恐委员会的政策指导下，反恐执行局关于信通技术的工作侧重于四个支柱：㈠ 将信通技术纳入代表反恐委员会进行的评估访问的主流，以评估会员国执行安全理事会有关决议的情况；㈡ 促进行业自律和公私伙伴关系；㈢ 加强合法获取数字内容的国际合作；㈣ 推广反宣传技术，包括网上技术。

反恐委员会对会员国的评估访问

信通技术被用于恐怖主义目的是反恐委员会执行局代表委员会对会员国进行评估访问的关键专题领域之一，目前正被纳入为应对 COVID-19 大流行而进行的混合访问。执行安理会第 1373(2001)号决议和其他有关决议的技术指南(S/2017/716)以及更新的“反恐委员会访问会员国以监测、推动和协助执行安全理事会第 1373(2001)、1624(2005)、2178(2014)、2396(2017)、2462(2019)和 2482(2019)号决议及安理会其他相关决议的框架文件”(S/2020/731)概述了与信通技术有关的问题。在评估访问期间与会员国讨论的有关信通技术被用于恐怖主义目的的具体问题包括：

- 与信通技术有关的监管和政策框架
- 打击为恐怖主义目的滥用信通技术的立法
- 使用特殊调查技术监测将信通技术用于恐怖主义目的的能力
- 发现恐怖主义内容和恐怖主义活动的方法；屏蔽、过滤和删除与恐怖主义有关的在线内容的操作做法
- 与私营部门和民间社会(公私伙伴关系)合作，包括通过技术解决办法，打击将信通技术用于恐怖主义目的的行为
- 使用数字证据将恐怖分子绳之以法，包括获取储存在另一司法管辖区(立法、国家

结构、执法层级和司法合作)的数字证据

- 关键基础设施安全和抵御恐怖分子恶意活动的政策，包括通过使用信通技术
- 会员国反恐措施的人权方面，包括对与信通技术有关的表达自由的适当保障。

信通技术问题(数字证据、保护关键基础设施、网上煽动、网上监管等)也被纳入执行情况评估概要和详细执行情况调查电子版，这是委员会及其执行局最近更新的调查工具，托管在一个新的基于云的评估和分析门户中。

与私营部门合作

自 2014 年以来，反恐执行局在反恐委员会的政策指导下，一直在这一领域积极与私营部门接触。2017 年，这种合作在一个名为“技术反恐”的公私伙伴关系中正式确定。这项倡议涉及来自政府、私营部门、贸易协会、民间社会、学术界和多利益攸关方论坛的众多伙伴，旨在支持全球科技行业在尊重人权的同时，应对恐怖分子利用其技术的问题。在与主要利益相关方进行全球磋商的基础上，技术反恐倡议与全球技术部门合作，分享良好做法，包括政策、指导方针、学习材料、实践研讨会和其他工具。另一关键特征是大型平台与较小的平台和初创企业共享支持和专有技术，以避免被恐怖分子利用。

此外，反恐执行局一直是全球互联网反恐论坛的重要合作伙伴，该论坛由脸书、谷歌、微软和推特于 2017 年创立，目前是一个独立的非政府组织。反恐执行局是全球互联网反恐论坛独立咨询委员会的常驻观察员。技术反恐倡议与全球互联网反恐论坛密切合作，支持小型平台和技术解决方案的开发。自 2016 年以来，全球互联网反恐论坛成员已经修改了其使用条款，禁止发布恐怖主义内容或支持联合国安全理事会综合制裁名单上的组织。安理会在第 2617(2021)、2395(2017)和 2396(2017)号决议中确认了全球互联网反恐论坛和技术反恐的发展，并呼吁这些倡议继续努力促进公私合作，以破坏恐怖分子为恐怖主义目的利用互联网的能力。

打击暴力极端主义和恐怖主义宣传

恐怖主义团体成功地将宣传用于多种目的，包括招募人员和促使从激进走向暴力。安全理事会第 2354(2017)号决议以安理会 2016 年 5 月 11 日的主席声明(S/PRST/2016/6)和“综合性国际框架”(S/2017/375)为基础，其中包括法律和执法措施、公私伙伴关系和开展反宣传。该决议

提出了一系列指导方针，除其他外，强调联合国在打击恐怖主义宣传方面的行动应以《联合国宪章》为基础；会员国在打击恐怖主义和助长恐怖主义的暴力极端主义方面负有首要责任；联合国相关实体应确保与反恐能力建设捐助国和受援国加强协调一致；反宣传措施和方案应符合不同背景下的具体情况；所有措施必须符合会员国根据国际法、包括国际人权法、国际难民法和国际人道法所承担的义务；有必要继续研究恐怖主义和暴力极端主义的动因，以便制定重点更明确的反宣传方案。

安理会第 2354(2017)号决议中请反恐委员会“与反恐执行工作队办公室[现为联合国反恐怖主义办公室(反恐办)]协调，并酌情与其他相关非联合国实体协商，查明并汇编反恐怖主义宣传方面的现有良好做法。”反恐委员会还将“继续审查各国为加强执行所采取的法律措施”，“进一步发展公私伙伴关系”，与民间社会组织和宗教行为体开展外联，并与反恐执行局全球研究网络成员和其他方面合作，衡量反宣传的影响和效力。

因此，反恐委员会和反恐执行局在评估会员国执行安理会有关决议的情况时，重视各国是如何采取步骤，制定方案和战略，以根据第 1624(2005)号决议打击煽动行为，根据第 2354(2017)号决议将煽动行为定为犯罪并打击恐怖主义宣传，以及根据第 2178(2014)号决议和其他决议打击暴力极端主义。只要存在漏洞，反恐委员会和反恐执行局就会设法让各国与技术援助提供者一起，在这些领域制定进一步的举措。

反恐委员会和反恐执行局致力于确保其工作与支持的工作相协调，包括通过反恐执行局参与《联合国全球反恐协调契约》。

数字证据

反恐工作的一个重要部分是促进基于法治的有效刑事司法对策。在实践中，会员国在试图获得可接受的证据，以帮助在司法程序中起诉恐怖主义嫌疑人并确保其定罪方面面临重大挑战。外国恐怖主义作战人员及其回返者和迁移者的情况是一项特别严峻的挑战。由于与外国恐怖主义作战人员活动有关的信息往往在战场上，文职检察官和调查人员可能无法获得。因此，对外国恐怖主义作战人员的起诉可能取决于使用基于互联网的证据或数字证据，并可能需要既定法律框架中未规定的司法合作形式。反恐执行局鉴于这些挑战，并根据第 2322(2016)、2331(2016)、2341(2017)和 2396(2017)号决议以及上述《关于外国恐怖主义作战人员的指导原则》和 2018 年

增编采取行动，与国际检察官协会以及联合国毒品和犯罪问题办公室共同发起一项全球倡议，除其他外，加强中央机关、检察官和调查人员在跨境反恐调查框架内保存和获取电子证据的能力。

数据保护和隐私

随着反恐措施越来越多地提出与隐私和数据保护有关的挑战，专家们认识到，私营公司和政府缺乏数据保护法律框架和指导，无法解决法律注册标准、数据保留或删除政策、数据处理、数据共享、防止滥用数据、数据安全、验证和监督等技术问题。这对国际合作和国际数据共享造成了严重阻碍，因为许多国家的法律禁止与数据保护制度较弱的国家共享受保护的个人数据。另外，新的发展，如人工智能领域的进步(如机器学习)和对这种技术工具的日益依赖，使得开发这种指南变得必不可少。反恐执行局正与毒品和犯罪问题办公室以及反恐办一起，在《全球反恐协调契约》的反恐和打击资助恐怖主义行为的刑事司法和法律对策工作组框架内，共同领导一个关于制定数据保护规则的建议立法规定和现有良好做法汇编的项目，以促进国际反恐合作。

人工智能

从通信服务提供商的自动内容审核到生物识别技术的使用，人工智能在反恐中的应用十分广泛。机器学习和决策被视为极其强大的监视和调查工具，但也是对享有公民权利和政治权利(包括隐私和表达自由，以及种族和性别歧视方面)的严重威胁。反恐执行局一直在与活跃在这一领域的各种伙伴合作，特别是联合国区域间犯罪和司法研究所(犯罪司法所)及世界经济论坛。此外，反恐执行局一直在关注科技平台(包括全球互联网反恐论坛公司)使用人工智能驱动的算法来支持其内容审核工作的发展。秘书长数字合作路线图指出了人工智能对促进和平的重要性，并注意到反恐执行局就若干与人工智能有关的事项开展的工作。反恐执行局就路线图的执行向秘书长办公厅提供咨询意见。

新的金融工具

采用分散分布式结构的新技术，如“区块链”相关技术，可被各方用于和用作杠杆进行传

统金融网络以外各类资产的兑换、移动、提取或报账。比特币等虚拟资产允许在国际上匿名转移资金，众所周知，这种资金越来越多地被用于资助恐怖主义。在全球范围内，众筹技巧的使用也是一种公认的资助恐怖主义风险。众筹是企业、组织或个人在互联网上通过捐赠或投资向多个个人筹集资金的一种方式。反恐执行局在打击资助恐怖主义行为的工作中，日益关注与新技术(包括虚拟资产和众筹平台)有关的资助恐怖主义风险，以及与私营部门建立相关有效伙伴关系的必要性。反恐执行局通过以下方式监测和分析这一领域的最新趋势：与会员国对话(包括在打击资助恐怖主义行为评估框架内)；参加相关专家论坛(包括金融行动特别工作组的专门项目)；与关于伊黎伊斯兰国(达伊沙)、基地组织和塔利班及关联个人和实体的第 1526(2004)和 2253(2015)号决议所设分析支助和制裁监测组及其他相关伙伴进行交流；与私营部门和民间社会组织协商)；以及持续研究(包括通过全球反恐怖主义研究网络)。根据第 2462(2019)号决议，反恐执行局还与各国合作，确保各国对虚拟资产服务提供商适用基于风险的打击资助恐怖主义行为条例、监测和监督。