

网络极端主义群体与学校及其他教育机构中的大规模枪击案。 续，第3部分。

续篇，前文：[第1部分](#)、[第2部分](#)。

在教育机构和儿童机构的工作中引入额外的监管措施，并对潜在高风险群体*中的青少年采取公开和隐蔽的干预手段。这应能显著减少“死亡组织”招募人员的潜在受害者总数，进而减少根据这些组织指示并为其利益实施犯罪的犯罪实施者数量。其结果是：在实际开展此项工作的国家中，此类团体的活跃度将降低，其宣扬的极端主义思想的传播速度将减缓，最重要的是，其成员实施的严重及特别严重犯罪案件数量将减少。

如果将这一方法长期融入教育机构及其他儿童机构中心理学家和社会学家的日常工作中，并维持国际监测与协调小组的运作 — 该小组将跟踪局势变化，并据此调整识别与应对策略 — 这将成为遏制威胁的有效手段，并有望在长远看来使局势得到控制。

作为对前述遏制措施的有效补充，以减少招募者潜在的目标人数，我建议学校、其他教育机构以及儿童和青少年聚集场所的管理层，考虑引入CPTED这一要素。

CPTED：“通过环境设计预防犯罪” (Crime Prevention Through Environmental Design) — 一种旨在通过改变犯罪发生的物理环境来降低犯罪率的策略。该理念的核心在于：经过精心设计的物理空间能够预防犯罪、遏制不良行为，并加强社区联系。

该方法在降低教育机构暴力水平方面的有效性，已得到 Safe Havens International (SHI) — 全球历史最悠久、经验最丰富的专家分析机构之一，专门致力于提升教育机构安全水平 — 所开展的多年实践研究证实。

关于CPTED的应用方法及取得的成果，可参阅SHI执行董事迈克尔·多恩 (Michael Dorn) 的[文章](#)，他是教育机构安保与安全领域公认的国际专家。

尽管营造更舒适的心理环境并不能解决所有安全问题，也无法对所有高风险青少年产生确切的影响。但研究表明，采用此类方法能够将部分青少年的焦虑、紧张和攻击性水平降低 10%-15%，这意味着潜在受害者的数量也会随之减少。

而这类在精神和心理上处于脆弱状态的青少年越少，“死亡组织”的招募者就越难吸引和控制他们。

这里涉及简单的数学原理。目前，极端主义团体的“策导者”通过其信息渠道招募了成百上千名青少年，但同意参与实际行动的最多只有几十人，而愿意实施特别严重犯罪的则寥寥无几。只要将最初的数字减少，其余的自然也会随之减少。即使能减少 10%-15%，在这里也算是不错的结果。

遏制威胁的下一阶段，是封锁犯罪分子所使用的网络资源。这里需要明确的是，这一方向在技术实施和法律执行方面都极其复杂。封锁必须精准且有针对性，针对具体社区和个别账号 — 正是通过这些渠道，极端主义材料得以传播，青少年被招募以诱使其参与犯罪和恐怖活动。

在此情况下，犯罪分子利用了若干现有的安全漏洞。我总结出了需要应对的5个主要问题：

1. 在社交网络和即时通讯应用中封禁单个账户较为困难。

仅凭技术和软件手段，在无需社交网络或即时通讯平台管理方介入的情况下，限制单个（或多个）特定账户的访问权限，几乎是不可能的。

2. 获取关于封禁此类网站以及特定个人主页和群组的法院强制执行文书，其法律和行政程序既复杂又耗时。

作为第1点的延续。社交网络和即时通讯应用的管理方在多数情况下虽能认识到威胁的存在，但基于其内部政策，并遵循关于言论自由和信息自由的国家及国际法律法规，会要求执法机关提供证据，且通常需要出示关于封禁账户的法院判决书。获得此类裁决并非易事，而且往往耗时较长，有时甚至需要数周乃至数月，直到执法人员收集到足够的证据提交给法院。

3. 管辖权。

正如我在第一、二部分所言，这一威胁具有国际性。近年来，极端分子最常采用的模式是：招募者身处一国，而受害者则在另一国。在此情况下，犯罪分子往往选择那些存在外交分歧且执法机构之间几乎没有合作关系的国家。一个国家的法院判决，对另一个国家而言毫无意义。

4. 程序上的差异。

不同国家的刑事立法各不相同，不同类型的犯罪在定罪要件、类型（类别）、性质和严重程度上也存在差异。在某国被视为特别严重犯罪的行为，在另一国可能仅被视为行政违法行为。某国法律规定某类物品、信息记录及扣押方式可作为法庭证据，而在另一国则不然。

5. 诉讼文书流转的差异。

不同国家在诉讼文书的种类、格式及制作方式，证据的记录与登记方式，对嫌疑人及证人的讯问，以及物证的获取与归卷方面均存在差异。在一个国家收集的证据，仅因格式不符，就可能不被另一个国家的法院采纳，这源于各国在记录具有诉讼意义的事实时，对程序性问题的处理方式存在差异。

这一切既增加了执法人员的工作难度，又为犯罪分子和犯罪团伙的活动提供了便利。但另一方面，也不能通过减少封禁账号的法律依据数量和降低其质量来简化封禁程序。这既会为仅凭怀疑就对信息传播进行毫无依据且缺乏证据的限制提供借口，也会为蓄意滥用职权创造条件。这种情况绝不能发生，合法性是根本基础，必须严格遵守。那么，如何既确保行动的及时性，又严格遵守合法性？这种折中方案是否可能？当然可能，但这需要对现行做法进行根本性的改变。

目前，发送国际请求（即使是在已签署协议的国家之间）也需要数周甚至数月的时间，在此期间，可能会有数百甚至数千名青少年被卷入犯罪网络，并可能发生数十起严重犯罪案件。亟需建立一套国际层面的快速司法响应机制。该机制将使任何参与国的执法人员都能迅速获得具有法律效力的司法执行文书，社交媒体和即时通讯平台的管理方将据此对相关群组 and 用户实施封禁。

为了切实落实这一建议，必须满足以下几个条件：

1. 设立一个高度专业化的国际司法机构，专门审理某一类案件**。该机构不必一定以法院的形式设立，在第一阶段，它可以是一个具有司法职能、以司法形式运作的国际组织，但在法律意义上并非法院。

2. 制定一套统一的国际指控和证据提交格式，供该司法机关审理。

该文件应明确界定：

- 谁有权向该司法机关提出申请；
- 提出何种指控以及基于何种理由；
- 应提交何种申诉文件以及该文件应如何撰写；
- 应提供何种证据、以何种形式提供以及如何获取；
- 应在何时限内审理该申请；
- 该司法机关可作出何种裁决。

3. 依据国际条约，争取与该组织建立合作关系，即使不能涵盖所有，至少也要让那些拥有最主要社交网络、即时通讯软件及其他被用于犯罪目的的信息资源的、规模最大的跨国公司参与其中。合作的核心在于接受并执行该司法组织作出的决定，对那些有充分理由被怀疑从事极端主义、恐怖主义或其他活动，且有充分理由怀疑其实施或诱使他人（尤其是未成年人）实施针对个人、生命或健康、性质极其严重的犯罪行为。

鉴于第1款所述的国际司法机构职能有限且法律权限有限，该机构不必作为独立的国际法主体设立，完全可以作为具有特殊法律地位的现有国际组织之一的下属机构设立。例如，联合国。资金将由缔约国根据单独的国际条约提供。每个缔约国均有权就该司法机关的职权范围向其提起诉讼，并承担缴纳会费以维持其运作以及在其领土内执行该司法机关所作裁决的义务。例如，将该国际司法机构关于限制信息传播的裁决，在程序地位上等同于该国司法体系中法院的判决。

该司法机构本身在组织规模和人员编制上不会过大。申请的审理和裁决将采取合议制，我认为合议庭应由3名法官组成，他们将在60小时内接收、研究、审理每一份提交的申请并作出裁决。在个别紧急情况下，则应在12小时内完成。将根据公认的国内法和国际法规范，对指控的真实性及证据的说服力进行评估。因此，法官必须具备国际法领域的相关知识，并拥有充分的实践经验来应用这些法律。

平均而言，一个合议庭每周可审理最多4起申请。在当前情况下，平均工作量约为每月100起申请。需要说明的是，该机构仅会处理信息安全领域中极小一部分的犯罪案件。这些案件涉及极端主义、恐怖主义或其他性质的直接、明显的威胁，且与实施或诱使他人（尤其是未成年人）实施针对个人、生命或健康、性质极其严重的犯罪行为有关。此类犯罪目前数量虽不多，但属于危害社会最严重的类别，因此需要采取最迅速的遏制措施。

根据初步数据，该司法机构的总编制人数（不仅包括法官，还包括行政和技术人员）将约为200人。对于一个国际组织而言，这一规模并不大；只要有至少30个成员国参与，其资金筹措成本也不会很高。

主要难题在于说服那些拥有主要社交网络、即时通讯软件及其他信息资源的大型跨国企业 - 这些平台在多数情况下被用于犯罪目的 - 认识到合作的重要性。

因为只有这样，才能充分发挥此类系统的核心优势 - 快速响应能力。

迅速封堵极端主义内容的传播渠道，将能大幅遏制破坏性群体的活动能力，最重要的是，这将使非法活动的指挥协调体系难以运作，甚至在某些情况下彻底瓦解该体系。

当前，青少年正被积极利用来组织大规模骚乱，这一问题显得尤为紧迫。[早在2023年](#)，当俄罗斯及几个邻国发生由“私兵组织‘列丹’”亚文化群体实施的大规模斗殴和骚乱时，我就曾就此撰文。当时我曾推测，这些事件并非偶然，我们所目睹的并非自发事件，而是经过精心策划和操控的过程。如今，我们在美国也能看到类似的情况，那里正掀起一波此类犯罪浪潮，甚至已被冠以《Teen Takeover》之名。此外，欧洲也记录到了类似的大规模袭击事件，尽管规模较小。

对已发生事件的分析表明，煽动实施违法行为、通报集合地点，以及确定袭击目标、时间和地点等行为，均是通过社交媒体群组、聊天群以及即时通讯软件中的频道进行的。

在第三部分的结尾，我想重申，“死亡小组”及其他网络破坏性群体的威胁早已成为国际性问题。信息技术以及通信形式和方式的发展，抹去了国家与大陆之间的边界。遗憾的是，犯罪分子和极端分子正积极利用这一点，他们的群体迅速演变为跨国性质。在这种情况下，那种“各人自扫门前雪”的自主安全体系已无用武之地。只有通过国际合作，凝聚力量，采取主动、预防和先发制人的行动，才能应对这些威胁。这样，我们就有充分的把握在这场为孩子安全未来而战的较量中取得胜利。

在下一篇文章中，我将继续就打击“死亡小组”的活动提出我的建议。这将标志着第二阶段的结束，该阶段致力于制定有效的应用解决方案，其实施将有助于遏制信息传播和招募活动，从而减少新成员流入极端主义团体，并过渡到第三阶段 — 具体的反制战术措施。

* 该小组成员的心理类型，以及其识别和干预方法，将由行为分析专家共同制定，依据是国际工作组在工作中收集的个人信息经处理后的结果。详情见第2部分。

** 在初期阶段。然而，鉴于信息技术领域跨国威胁的日益增长与发展，设立此类司法机构在未来具有广阔的发展前景，其管辖范围有望扩展至其他类别的犯罪。

本文最初发表于2026年09月15日

作者：罗曼·格里申