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。续篇，第二部分。

正如我在本文第一部分所写，网络极端主义群体的威胁是严重且真实的，这一点已毋庸置疑。我还要补充的是，仅在过去一个月内，执法部门就提出了这些群体涉嫌参与另外三起袭击事件的推测：
2026年6月22日，菲律宾塔克洛班；
2026年7月6日，马来西亚班廷；
2026年7月8日，德国肖恩豪。
目前，政界人士和政府官员已承认这一威胁确实存在，并要求警方采取紧急应对措施。然而，这一问题已无快速有效的解决方案。几年前，当这些团伙开始转变其意识形态，从敲诈勒索和诈骗转向组织大规模杀戮和骚乱时，本还有解决的可能。但当时人们低估了这一威胁，如今已错失良机。
在当前形势下，需要采取截然不同的应对方式 — 这绝非旨在追求短期“惊艳效果”的虚幻计划，而是需要一套战略体系，不仅要遏制当前形式的威胁，更要针对其可能的发展方向和形态进行应对。
为了构建这样的应对体系，我建议采用“敌对环境”模型。这是什么呢？请试着将犯罪不视为一种社会现象，而是一个有生命的有机体。只有当环境条件有利时，这种生物体才会积极地生长、发展和繁殖。在这样的环境中，气候条件舒适，水源和食物充足，且不存在（或极少存在）来自掠食者或自然灾害的威胁。在这种情况下，该物种的种群数量将不断增长，并不断向新的领地扩张。
结论很简单：既然犯罪率在上升，就说明其生存环境有利，犯罪现象正在发展。该怎么办？应制定相应的应对策略，使犯罪的生存环境不再舒适，而是变得充满敌意且具有攻击性，使其在其中几乎没有生存的机会。

第一阶段：信息收集。

必须始终从这一点入手，关键在于弄清你面对的是谁，对方的目标是什么，其行动方式如何，以及具备哪些能力。掌握关于对手尽可能多、可靠且客观的信息，就等于成功了一半。这样一来，就能理解其逻辑并解释其行为，这意味着对方的行为变得可预测，其后续行动可以被预判并加以防范。
起点在于那些幸存的犯罪嫌疑人所作的证词 —
他们所犯的罪行是出于网络极端主义团体的利益并遵照其指示实施的。作为直接参与者，他们经历了从招募到执行最终任务的整个事件链。他们知晓许多内情，但问题在于 — 他们是否愿意分享这些信息？必须认识到，在与律师和父母沟通后，
他们会试图把自己塑造成受害者，声称自己是无意为之，是在胁迫下行动，或是受到人身伤害威胁或被曝光不利材料的威胁。他们在调查过程中所作陈述中，可信信息仅占30%至40%。他们全都受到了惩罚，有人被判处实际监禁，有人因年龄原因被判处缓刑，此外还受到限制性措施。我认为，在判决生效后，在（合理范围内）放宽处罚条件并保证匿名的前提下，可以邀请他们再次作证。此过程不具有诉讼程序性质，并将邀请心理学和法医精神病学专家参与。

第二个与第一个同等重要的方向，应与前者并行推进 —
即寻找那些未实施犯罪的潜在实施者。这些人同样曾被招募、接受过培训，但最终未实施犯罪；包括那些在最后一刻主动拒绝的人，以及在准备阶段被制止的人。这项工作应以匿名方式进行，且不涉及任何诉讼程序，并需借助专业人员的协助。
关键是要弄清楚犯罪分子究竟是如何、在何处以及依据哪些标准物色受害者，以及他们选择潜在招募对象的原理。他们是如何与极端主义网络的负责人建立联系的？是他们主动寻求接触，还是招募者主动接触了他们？此外，还需要了解对潜在受害者进行道德和心理操控的具体方式。细节至关重要，我确信招募者不会立即向被招募者透露自己隶属于极端主义组织和运动，也不会透露针对这些青少年的真实目的。这是向专家提出的核心问题，我不认为对方会为每个青少年配备一名专业心理学家，或是拥有对外情报机构实际工作经验的招募人员。很可能，他们利用的是那些接受过一定培训但仅限于速成课程的人员。这些人按照特定的模式运作，类似于网络上的激进销售手段，网络诈骗分子也采用类似的套路。
如果参考那些已公开的零星信息，极端主义团体所采用的招募体系与“伊斯兰国”（ISIS）招募人员所采用的体系非常相似。
假设：根据对现有信息的分析，他们有针对性地、精准地开展行动，利用现成的潜在受害者名单，这些受害者是处于道德和心理脆弱状态、易受蛊惑、容易被操控的青少年。他们通过合法和半合法途径获取这些名单，即通过空壳公司向专门为在社交媒体上销售商品和服务的公司收集目标受众数据的信息分析机构下单购买。在这种情况下，他们可能会将自己对上述目标受众的真实兴趣伪装成寻找潜在客户，例如为个人成长课程、心理咨询服务、交友网站、非正式社群周边商品等寻找客户。但在不久的将来（或许现在就已经如此），这种做法将不再必要，基于人工智能的专用搜索程序将能够完成此类数据的收集和初步处理。
第三个方向是处理数字痕迹，分析已被删除的群组、频道、网站及其他网络社区的内容。当法院或授权监管机构（各国情况各异）封禁具有破坏性的网络社区时，其内容往往会直接消失，这导致了宝贵分析信息的流失。有必要为电信运营商和托管服务提供商制定一项服务规程，规定：在封锁之前，所有元数据（帖子、评论、话题标签、时间戳、参与者等）均应予以保存，并移交专门的执法部门（稍后将详细说明）以供后续分析。这对于专家而言，就像是“解剖数字尸体”的过程，可以获取大量有用的信息，包括行动侦察性质和诉讼取证性质的信息。
必须尽可能多地收集极端分子使用的方案，包括细节以及他们用于寻找、接触和处理受害者的详细行动流程。
将所有这些材料提交给专家 — 犯罪学家、心理学家和精神科医生 —
进行分析。根据他们的结论，可以了解：
- 寻找和选择受害者的原则；
- 所使用的信息来源及收集方式；
- 对受害者进行操控时采用的剧本和模板；
- 施加精神心理压力的方法；
- 联系方式及其他控制受害者的手段。

该阶段预期成果：

利用收集到的数据，将能够构建潜在受害者的统计模型：年龄、性别、家庭特征（完整家庭或由单亲抚养、社会地位、收入水平、宗教信仰、父母的教育理念及参与孩子生活的程度等），

智力与身体发育水平、对学习、政治、宗教、体育、文化的态度、兴趣爱好、道德心理特征及其他补充信息。

该模型将有助于识别并清晰描述最易受伤害的青少年群体。相关信息需发送至学校、学院及其他教育机构以及儿童聚集场所，供教师、心理学家、社会工作者及相关警察部门人员在实践中使用。

建立合理的潜在受害者“风险群体”名单，对其进行监控，并向其父母（监护人）通报潜在威胁，这是预防工作的首要且有效的环节，将显著降低极端主义招募者的活动成效。这将起到有效的遏制作用，并能大幅减缓威胁的蔓延。

该阶段工作组织的特点：

为了最有效、最全面地收集信息，必须以国际形式组织这一过程。

需要成立一个国际信息分析小组，成员包括来自不同国家的专家、分析师和专业人士，尤其是那些已经遭受网络“死亡小组”*犯罪分子侵害的国家。

如果每个国家都单独收集信息，而不与其他国家整合，就无法建立有效的统计模型。所有的分析都将基于极其匮乏且不完整的数据。结果，我们得到的将不是一种有效遏制威胁的工具，而是一个措辞模糊、充斥着空泛套话的通用模板，几乎无法用于实际操作。坦率地说，这正是我们目前所面临的现状。需要提醒的是，我们面对的是一种国际性威胁，其运作模式是：策划者位于一国，招募者位于另一国，督导者位于第三国，最终执行者位于第四国。若仅凭“各顾各”的原则与之对抗，我们将再次失败。收集和处理的信息越多，专家的结论就越准确、越详细。因此，必须协同行动，只有这样才能确保取得积极成果。

个人感想：我想再次呼吁各位同仁，是时候停止政治争斗，重新以专业人士的姿态行事了。在涉及儿童安全的问题上，绝不应因无端借口而产生分歧。正如各位所见，犯罪分子不会将儿童分为“好”与“坏”，他们会残害并杀害所有人，无论其国籍、种族、宗教或政治立场如何。

在下一篇文章中，我将继续就打击“死亡小组”活动提出建议。这将是第二阶段，重点在于制定有效的应用解决方案，通过实施这些方案，将阻碍信息传播和招募活动，从而减少新成员流入极端主义团体。

* 该名称由媒体记者杜撰， 他们曾就互联网上的极端主义和破坏性社群进行过报道。本文及后续内容中将沿用这一称谓，特指那些在社交媒体和即时通讯软件上鼓吹暴力、诱导青少年实施自杀、大规模杀人及其他严重犯罪的群体。

本文最初发表于2026年07月24日
作者：罗曼·格里申