破坏性社群和游戏，«红海豚» — 学校及其他教育机构面临的新型威胁。

2024年9月，俄罗斯车里雅宾斯克市和巴拉甘斯克市在相隔一周的时间内，接连发生了两起类似的校园袭击事件。两起案件均为校内袭击，均由该校学生实施，所用武器类型（锤子）相同，嫌疑人外貌特征和年龄也相似。两起犯罪均属蓄意犯罪，袭击前均经过精心准备和策划。

总体而言，与其他同类犯罪相比，这两起袭击事件并无特别之处。然而，在第一起袭击事件（2024年9月16日车里雅宾斯克）发生后，多家媒体、社交网络及即时通讯软件上的网络社区，以及部分官员（俄罗斯总统儿童权利事务专员玛丽亚·利沃娃-贝洛娃）和公共组织 （如«安全互联网联盟») 的声明中, 均出现相关信息,
称此次袭击可能并非由实施袭击的青少年个人主动发起，而是为了完成他从名为«红海豚» 的互联网封闭社群组织者那里收到的特定任务，

该群组宣扬极端主义和自杀思想。值得注意的是，关于此类网络群体的信息此前已通过名为 «蓝鲸» 的游戏进入媒体视野。社交媒体上以此命名的群组发布抑郁内容,
群主会给青少年布置任务，而最终任务便是自杀。因此，群组成员被比作搁浅的鲸;
如果青少年拒绝自杀，就会遭到杀害其家人的威胁。该 «游戏»
的活动高峰期出现在2016至2017年，有多名青少年的死亡与之有关。当时，在公众的支持下，执法部门封禁了社交媒体上绝大多数 «蓝鲸» 群组,
警方和调查委员会逮捕了数名群组管理员，并以故意诱使自杀的罪名对他们提起公诉。到2018年，此类团体在互联网和即时通讯软件上的活跃度已大幅下降，几乎销声匿迹。

2024年，局势发生了剧变。社交媒体和即时通讯软件上纷纷涌现出新的群组和频道，这次它们使用了 «红海豚» 这一名称。不仅名称发生了变化，其理念也随之改变。
如果说 «蓝鲸» 组织诱导青少年自残，最终以参与者自杀告终，那么 «红海豚»
则要求成员伤害周围的人, 其最终任务同样是自杀, 但前提是必须先实施大规模杀人。
在车里雅宾斯克和巴拉甘斯克发生袭击事件不久后的2024年10月1日，俄罗斯联邦安全局（FSB）又拘留了一名16岁的青少年，其涉嫌策划在学校实施大规模杀人。媒体指出，该青少年曾加入某个极端主义团体，正是该团体向其灌输了此类思想，但未透露该团体的名称。

我再次强调，今年9月针对学校的袭击事件与 «红海豚» 意识形态之间的关联仅是-种推测, 因为公开渠道中没有相关调查材料,
且调查委员会的官方新闻稿中也未提及这-信息。然而, 考虑到以下事实:
该信息几乎同时从不同渠道传出，且这些渠道消息灵通；此外，无论是最初披露该信息的官员、媒体还是执法机构，均未对此信息予以否认。因此，该信息极有可能属实。但即便该破坏性团体与上述袭击事件无关，也不应低估其未来可能构成的威胁。

这个破坏性群体的存在本身毋庸置疑，它确实存在（通过在即时通讯软件和社交媒体上进行相关搜索不难验证，此外也有不少关于此主题的记者调查报道），
其信息网络已覆盖多个国家，这意味着其向全球蔓延只是时间问题（我预测大约2-3个月）。
如果这种«游戏»广泛传播，它将在教育机构中催生出-种新型的大规模杀人犯。目前，我们主要面临两种此类罪犯：
1. «校园杀手»（通常被称为«校园枪手»，无论使用何种武器) —
因个人动机实施大规模杀戮，动机多种多样：报复，个人敌意，精神失常，模仿其他杀手，«上帝情结»等。此类犯罪占绝大多数，超过93%。
2. «恐怖分子» - 此类犯罪目前仅占总数的不到7% (249起中的16起)，
但就受害者人数而言，它们属于最危险的类型，占受害者总数的42.6%（4,064人中的1,732人）。此类犯罪由恐怖组织成员（包括其支持者及意识形态狂热分子）实施，旨在维护该组织利益，既可能遵照领导者的直接命令，也可能出于个人主动。
在此情况下，出现了一种第三类类型，姑且称之为 «受操控（或受控制）的杀手» — 此类杀手在学校（幼儿园、大专院校、大学）实施大规模杀戮，是出于完成游戏任务或遵照 «幕后操控者» 的指示，既无直接的个人动机， 也不代表恐怖组织的利益。其任务是前往教育机构实施大规模杀戮，并在最后自杀。这个青少年已无所顾忌，没有任何制约因素。

如何应对这一现象？

在这种情况下，那些策划并运营«红海豚»，«蓝鲸»
及类似群组的极端分子所采取的策略转变，本身已为犯罪分子埋下了严重的隐患，我们可以利用这一点来打击他们。
关键在于，«红海豚»与«蓝鲸»的主要区别在于：在新版«游戏»中，
参与其中的青少年必须执行«监护人»布置的任务，
这些任务的本质是实施违法行为，但不再针对自身（如«蓝鲸»中那样)，
而是针对第三方个人或组织。
任务形式多样，包括损坏或毁坏财物、对他人实施侮辱性行为或造成轻微伤害。
在第一阶段，这些任务的后果尚不严重，例如在墙上涂写侮辱性字句、砸碎窗户、焚烧信箱里的信件、损坏汽车轮胎、向路人泼水或泼洒无害但令人不快的液体，或是泼洒泥浆， 辱骂、嘲笑、扯掉他人头上的帽子以及类似的轻微违法行为。
在任务的第二阶段，任务难度和危害社会程度都会增加，青少年必须实施更严重的违法行为，例如纵火焚烧车辆或建筑物、杀害动物、使用非法但危险的武器对路人造成中度或更严重的伤害 （气动、冷兵器、非致命性、冲击性、气体类、自制武器）。

在第三阶段，参与者将面临 «不可逆转点», 即涉及严重犯罪类别的任务, 例如对他人造成身体伤害，但必须以隐蔽的方式进行，例如：
将人推向驶过的汽车或火车、从桥上或窗户推下，破坏铁路轨道或地铁设施，纵火焚烧有人在场的建筑物、儿童或医疗机构。
在所有三个阶段，违法行为都必须通过摄像头进行视频记录，并将任务完成后的录像发送给 «监护人», 青少年需通过社交媒体和即时通讯软件上的封闭群组进行提交。实际上，青少年是在自拍有损声誉的素材，一旦他们试图退出 «游戏» 并拒绝实施违法行为，这些素材就会被用来勒索他们。
第四阶段，即最后阶段，是实施大规模杀人，随后由执行者自杀。考虑到参与者的年龄，最后行动的地点通常选在他们就读的学校，潜在受害者则是他们身边的人，包括同学和老师。
我再次重申此前所言：所谓参与极端主义组织 «红海豚»
正是导致2024年9月俄罗斯车里雅宾斯克和巴拉甘斯克两座城市发生两起校园袭击事件的动机 —这仅仅是一种推测。 官方媒体尚未公布支持这一说法的直接证据。
执法部门既未正式证实这一事实，但也未予以否认。尽管如此，我认为 «红海豚» 或 «蓝鲸» 这类极端主义团体，对民众的安全-尤其是儿童的安全 -
构成了直接且明显的威胁。
这意味着必须采取先发制人的行动，制定应对该威胁的战术方案，包括预防措施以及遏制直接袭击的措施。

预防：

这项工作需分为三个关键方向, 并同步推进各项任务，唯有如此, 威胁预防才能有效：

方向1 - 识别潜在受害者：

«致命寻宝» 这一剧本本身 — 这些极端主义团体的组织者强迫受害者参与其中 — 存在严重的漏洞，若能妥善利用，便可迅速识别并阻止被卷入破坏性活动的青少年。
正如我之前所述，该剧本设定了4个阶段，任务的难度和危害社会程度逐级递增，且这些违规行为必须通过视频记录并公开实施，这正是其漏洞所在。问题在于，落入犯罪团伙网罗的通常是那些此前不曾有此类不良倾向、未曾违法犯罪且从未因故被警方处理过的青少年。
据我咨询过的心理学家分析，如果不先完成前三个阶段，就无法执行最终任务，即实施大规模杀人并随后自杀。因为正是通过执行这一系列难度和危害性逐渐升级的任, 青少年才会形成并固化下这种强迫性念头：即实施伴随自杀的大规模杀人。在倒数第二阶段犯下严重罪行时，孩子便越过了某种 «不可逆转的临界点»。 此外, 将已实施的违法行为录制成视频（这是参与的必要条件）并将其作为报告提交给监管者，若参与者突然决定放弃执行最终任务并终止 «致命任务», 这便为监管者提供了额外的把柄，用于对参与者进行勒索及其他形式的心理施压。

这一特点可用于在犯罪准备阶段就迅速识别潜在的连环杀手。具体该如何操作？首先，应格外关注那些行为毫无缘由地发生剧烈变化的青少年（主要年龄段为12至16岁）。一个明显的迹象表明，青少年可能已受到某个破坏性团体的外部操控，即此前性格内向、害羞的孩子（据心理学家称，最容易受到此类影响的青少年通常具有以下人格特征：敏感型的被动内向者、 忧郁型），且听话顺从，
却突然开始做出与其性格不符的行为及轻微违法行为，而他无法或不愿解释这些行为的动机。
在这种情况下，必须请专业人员介入，包括儿童心理学家、社会教育工作者以及犯罪心理学家。我相信，对于相关领域的专家而言，将青少年行为的变化与极端主义团体(如果确实存在这种关联）联系起来并不困难。若确认存在这种关联，警方及其他执法机构代表应介入处理。与此同时，心理学家和社会教育工作者对该青少年及其家庭的工作不应就此停止，关键在于查明并消除促使该青少年投身于破坏性团体的诱因。此外，对每起此类案件的深入研究，将有助于更详细地了解犯罪分子诱使儿童加入极端主义团体的手段。对这类信息的系统化整理与分析，将有助于今后制定更有效的机制，以识别青少年行为受«外部操控»的情况，并更有效地打击此类犯罪。
谁应该负责此事？这是一项综合性任务，所有与«高风险群体»
中的儿童有直接或间接联系的人都应参与其中。首先是孩子的父母和监护人、教师和学校工作人员、体育教练、儿科医生、警察以及教育机构的安保人员，甚至包括校车司机。所有这些人都必须知道，需要关注孩子哪些外在表现和行为异常，以及该向谁求助。 因此，必须制定一套明确的跨部门协作流程，并据此出台规范性文件，
以确定此类应对措施的形式与程序。所采取的措施既应包括公开手段，也应包含非公开手段，并运用所有可行的行为矫正手段。

第二方面 — 信息安全：

青少年加入破坏性群体的过程，大多数情况下遵循以下两种模式之一：
1. 主动型（自发型）- 青少年通过自行搜索（利用其他资源的链接，
话题标签或特定搜索词）在社交网络或即时通讯软件中找到极端主义社群，
提交加入申请，通过身份验证（在某些群组中，
这是一个相当复杂且漫长的多阶段过程)，随后会被分配一名«导师»，
该导师将开始向其布置任务并实施监控，直至最终阶段；
2. 被动型 — 青少年在其社交媒体主页上发布特定话题标签，破坏性群体的«导师»（招募者）会对此作出反应，并主动与其建立联系。后续流程与第一种模式相同，
包括身份验证、分配«导师»以及执行任务。
要建立信息反制体系，首先必须让社交媒体和即时通讯平台的所有者就封禁此类群组和账号的程序达成一致。此类群组或个人的行为显然属于违法。在任何国家的刑法中，诱使未成年人参与违法活动并导致其自杀均属犯罪。然而，任何犯罪行为或至少犯

罪意图都需要证据支持。为此，警方或其他执法机构的法律顾问应制定专门的《信息安全威胁应急响应规程》*，用于查明、收集并记录能证实传播此类信息的群组管理员或账号持有者存在犯罪意图的相关事实。需要说明的是，该规程所指的证据收集并非为了提起指控或立案，而是为了封堵极端主义信息的来源。阻止破坏性信息的传播至关重要，必须剥夺极端分子操控儿童行为的工具。尽管客观而言，完全剥夺犯罪分子招募新受害者的能力是不可能的，但大幅增加其操作难度却是完全可行的。

* 理想情况下，应以国际标准制定此类协议（因为该威胁早已具有国际性质，且其危险程度仍在持续 上升），并采用统一的格式和实施程序。 通过联合国安理会专门机构或国际刑警组织等国际执 法机构推广其应用，将能显著提升全球范围内应对这一 威胁的效能。

对于信息安全战略而言，最重要的是它必须采取主动进攻的姿态。执法机关以及教育、儿童监护和福利部门，应以最积极的方式对信息资源进行监控，既可独立开展，也可根据热心市民的举报进行。查明具有破坏性的资源，进行核查，记录其所有者的犯罪意图（如有），并在上述信息安全规程的框架内，运用一切可用的法律手段，对其进行及时封锁。在具备技术和法律条件的情况下，追究创建和管理含有破坏性内容的互联网资源人员的法律责任。

3. 对潜在威胁进行持续监测、预测和建模

这项任务主要应由执法机构的分析专家来完成。既要分析关于已发生事件的来报信息，也要评估潜在威胁。鉴于局势不断变化，必须持续调整第一和第二方面的预防措施。犯罪分子在应对措施实施后会迅速改变策略，因此不仅要应对其当前行动，更要预测其可能采取的步骤。基于此类预测，制定并实施预防性措施，以遏制其可能的行动。最佳解决方案可能是以国际形式建立一个常设的信息分析小组。

防范直接袭击。

尽管采取了各种预测和防范潜在威胁的措施，但仍无法完全避免针对性的大规模杀戮企图。遗憾的是，迄今为止尚未建立起100%有效的安防系统。所有现有的预测和预防此类威胁的方法，只能将此类袭击的发生概率及其造成的损害降低到可接受的限度，并将可能的受害者人数降至最低。

仅凭一篇文章，无法详尽阐述如何预防和制止在学校、其他教育机构以及儿童聚集场所发生的群体性杀戮企图。这是一个极其广阔的研究课题，我目前正在完成相关研究，并将于近期着手开展专门针对这一问题的项目。

这是一个复杂的多层次预防与应对体系，旨在应对教育机构当前及未来可能面临的安全威胁。我早在2019年就曾尝试构建此类模型，并在该文中进行了阐述，此后该文又经过数次修订补充。新项目将具有更大的规模，并包含更多具体的措施和建议，但这目前仅是未来的规划。

2. «恐怖分子» — 其犯罪行为受特定意识形态驱使，并追求该极端主义意识形态（或恐怖组织，运动）所宣扬的目标。

第三种新型类型，我称之为 «受控自杀者»，其目标是完成 «策导者» 的任务 — 尽管他不知道策导者的真实身份和动机 — 然后自杀。

令人深感遗憾的是，这种实施大规模杀戮的方式对恐怖组织及其他激进极端组织极具吸引力，这些组织显然会在不久的将来试图发展并利用这种手段来实现其犯罪目的。

统计数据来源:《学校及其他教育机构发生的犯罪和恐怖主义行为手册》

本文最初发表于2024年10月23日

作者：罗曼 • 格里申