开源情报与公共外交作用的机制、效应与边界

刘成昊[1]

（1.同济大学，上海 200092）

摘　要：平台化传播重塑了国际舆论结构，公共外交由政府主导的单向传播转向多主体参与的网络竞争。开源情报（OSINT）以公开信息为基础，通过核验、推理与可视化呈现形成证据链叙事，并在跨平台扩散与媒体/智库引用过程中进入公共议程，影响国际受众对责任归因与能力评估等关键问题的解释框架。本文在公共外交概念演进与“声誉安全”视角下，选取 MH17 事件中的 Bellingcat 调查与俄乌冲突中 ORYX 可视化战损统计为案例，分析开源情报影响公共外交的机制与边界。研究发现：开源情报的作用不在于简单替代官方叙事，而在于改变叙事竞争的起点——以证据可见性提升解释优势，进而对国家形象与声誉安全产生外溢影响；同时，开源情报亦面临可得性偏差、平台算法放大与工具化的风险。

关键词：开源情报；公共外交；数字传播；国家形象；声誉安全

DOI：doi.org/10.70693/rwsk.v2i3.301

一、研究缘起

开源情报（OSINT）,也就是 Open Source Intelligence。其特点是信息获取的低成本与公开性，特点是可以公开获取，即所谓的“可公开获取”或者“在公共领域的非机密信息来源”。[1]其特点是依托一切公众可以接触到的信息，例如报纸、广播节目、公开演讲、商业卫星图像、论文、社交媒体、博客、各类网站，以及越来越多的其他新鲜事物（如区块链）。这些曾经都基于新闻自由和公民新闻传统。[2]在传统传播结构中，重大国际事件的“事实呈现—解释框架—舆论走向”往往由政府部门与主流媒体主导，公共外交亦主要依赖官方话语、国际传播机构与外交渠道来塑造国家形象。然而，互联网平台与社交媒体降低了信息获取与再生产门槛，公开影像、商业卫星、数据库与社交媒体文本等材料迅速增量，使得事实核验与叙事竞争呈现去中心化趋势。公共外交由此面临两项变化：其一，议程设置主体多元化，非国家行为体在舆论场中获得更大可见度；其二，叙事竞争的核心从把控主流媒体与分发渠道转向提供素材与社交媒体的自发传播。

在此背景下，开源情报逐步从情报领域的工作方法扩展为公共舆论中的知识生产形态。与一般舆论表达不同，OSINT 强调以公开来源材料构建可复核的证据链，并以图像定位、时间线比对、来源核验等方式给出可传播的结论。这种“方法透明—证据可见”的呈现方式，容易在跨国传播中形成较强说服力，并被媒体、研究机构和政策讨论引用，从而对公共外交效果产生外溢影响。

现有研究中，关于 OSINT 的讨论多聚焦其技术路径与安全治理，关于公共外交的研究则集中于软实力、国家形象与数字外交工具。相对而言，OSINT 如何通过证据链叙事改变国际受众认知框架，并进一步影响国家形象与公共外交议程，仍需更具操作性的机制分析。基于此，本文提出研究问题：OSINT 通过何种机制影响公共外交？这种机制在重大国际事件中如何发挥作用？其潜在风险何在？

二、开源情报与公共外交的历史与融合路径

（一）公共外交概念的不断发展

传统的公共外交被定义为政府对非政府的宣传与互动，例如爱德华·R·爱默在被任命未美国新闻署署长时对“公共外交”的定义为“不同于传统外交，不但包括与政府间的互动，而且包括主要是与非政府的个人和组织之间的互动。”[3]这些 20 世纪官员眼中的公共外交是一国政府主导的对另一个主权国家行为体及其内部非主权国家行为体的政治宣传。学界通常认为公共外交这一概念，即“public diplomacy”一词在 20 世纪 60 年代由埃德蒙·古里昂（Edmund Gullion）提出并与默罗公共外交中心的设立相关，其核心意涵是：国家（以及与之相关的社会力量）

作者简介：刘成昊(1998—)，男，硕士研究生，研究方向为国际安全。
通讯作者：刘成昊

如何通过对外传播、公众互动与社会联系来影响海外公众对本国政策与形象的理解。[4]这一早期界定的优点是抓住了公共外交的对象——“外国公众”；但它也造成了一个长期争论：公共外交究竟是外交的延伸，还是包装后的宣传，抑或是一种更强调沟通与关系的治理方式。

此外，公共外交主体也在变化。正如时代的发展使得大量非国家行为体逐步走上国际关系舞台，对于公共外交的施动者与主体也有了更多的讨论。公共外交一直以来对其主语有不同的观点，部分学者认为，当代新公共外交的对象和执行者都不一定必须为政府机构。正如外交学者保罗·夏普指出：“我们仍不确定‘人民’‘民众’具体指代谁，尤其不清楚‘公共外交中的公众’究竟是谁？”[5]欧洲学者克里斯蒂娜·拉库尔（Christina la Cour）通过分析了威尔逊、哈罗德·尼科尔森、基辛格与约瑟夫·奈的外交著作，分析指出外交文献中“公众”概念的内涵范围总体呈扩展趋势，而公共外交的指涉也从“公开外交行为”演变为外交官直接面向外国公众开展的特殊外交活动形态。[6]

为了避免把公共外交简化为“对外宣传”的同义词，后续研究逐渐把它拆解为可操作的组成部分。较有影响力的一种划分将公共外交概括为五类实践：倾听（收集并理解海外公众意见）、倡导（阐释政策立场）、文化外交、交流项目与国际广播。[7]这一分类背后隐含一个判断：公共外交的有效性不仅取决于“说什么”，也取决于“是否理解对方、能否形成长期信任”。因此，学界对传统公共外交的批评往往集中在两点：一是过度强调单向输出与短期动员，容易滑向宣传；二是忽视倾听与反馈，导致话语与受众经验脱节，从而损耗可信度。

如果说公共外交在 20 世纪是“独自/广播模式”，那么互联网时代的 21 世纪则是“对话/网络模式”。公众不再是被动的信息接收者，同样是信息的生产者和建构者，“数字化公共外交”的概念应运而生——外交机构、民间组织或个人开展的以对象国的公众互联为抓手，以对话、参与和关系建构为目标的对外传播获得。但是由于公众不再是单方面被灌输，他们可以在评论区进行补充、赞成、反对甚至是辟谣，因此新时代的数字化公共外交更注重对受众意见的尊重和反馈，以构建“长效关系”，奉行“客体本位，多元阐释、分布式”的后现代主义逻辑，蕴含解构主义与消解权威的意义。[8]

（二）开源情报的缘起与进入公共外交

开源情报的发展与传媒的发展息息相关，因为开源情报的核心在于利用海量的公开数据来生成有价值的情报。传媒的发展让信息流通的成本不断降低，规模不断扩大，成为了情报的来源；而传媒培养出的公民意识则是开源情报的中坚力量。最初，克里米亚战争，又被称作“第一次电报直播战争”。因为电报让新闻能在数日之内从克里米亚半岛传回伦敦，公众可以通过记者获得大量前线报道，了解到了前线的各类不满与官方宣传的矛盾之处，从而推动了英国的国内政治变化。在第一次世界大战和第二次世界大战期间，尽管信息的传输速度并未显著加快，但是照片资料和影像资料的极大丰富为开源情报提供了素材，而公民识字率的普遍提高则为开源情报分析提供了足够的土壤。特别是在总体战的背景下，各国政府的安全需求催生了庞大的情报需求，而汇总公开数据并进行分析则是最直接的情报手段。在这一时期，1939 年英国政府委托 BBC 成立的 BBC 监控部门（British Broadcasting Corporation Monitoring Service, BBCMS）可以视作最早的有官方支持的开源情报机构。主要通过监听翻译外国广播并制作简报《每日文摘》（Daily Digest）并上报外交部、战争部、MI7、MI9 和美国政府等部门。[9]除此之外，我国的《参考消息》与其 1931 年 11 月开始创刊的前身《无线电材料》（1932 年夏更名为《无线电日讯》）也是采取类似的操作，通过收集到的公开新闻加以编印作为情报资料。

但是这种传统上的基于开源情报的分析并不参与公开传播，无法做到了对社交媒体的再影响。这也是在互联网之前，这些所谓的开源情报与传统的情报研究无法拉开较大差距的原因，甚至正因为模糊的定位，学术界难以对他们进行有针对性的讨论。此外，尽管伊拉克战争被视作第一次电视直播的战争，但直到此时战场信息的披露仍然是高度依赖政府渠道、政府有权或者有能力限制记者的采编，因此实际上仍然是一种“宣传”而非可互动的“传媒”。

互联网特别是移动互联网对这种政府主导的传播结构产生了冲击，即使战场也不例外。此外，大量廉价的“灰色情报”，如商业卫星图像，也使得情报分析的门槛进一步降低。在这个背景下，民间的爱好者通过自身的专业知识与互联网，就可以极大的填补那些政府主导的机构兴趣之外的空白。开源情报机构也因此应运而生。

传统的情报机构，其服务对象为本国政府部门，本身并不承担信息宣传功能，受本国政府影响，定位是辅助决策的功能。但新时期的开源情报机构特别是民间开源情报机构往往发起者出自兴趣，相对独立，其研究目的也并非干扰决策而是在互联网上进行信息传播，因此天然类似于宣传中的发起者地位。对于这些新一代的开源情报机构而言，其服务对象是互联网平台的支持者与观众，更类似自媒体角色，从而削弱了国家在情报领域与对外宣传中的垄断地位。在这一转向中，“可信度”成为比“声量”更稀缺的资源：谁的解释更能经受质疑、谁更能提供可核验的依据，往往比谁更善于表达立场更重要。

三、开源情报影响公共外交的案例

基于上述历史脉络，本文提出一个可被案例检验的观点：开源情报在公共外交中作为非国家行为体提供了与主权国家宣传例外的可信度，通过公开证据链影响国际受众对事件的解释框架，从而改变国家形象竞争的起点与边界。这一角色带来双重后果：其一，开源情报可能削弱官方叙事的垄断性，使公共外交更难依赖单向话语维持

一致解释，也意味政府部门面临更强的信息核实压力，更倾向于适度公开来争取民主与盟友支持；[10]其二，开源情报机构的“第三方”也可能被国家行为体所利用，——当国家力量通过信息投放、资源支持或议程引导介入其中时，开源情报可能被工具化，反而成为更隐蔽的影响渠道。

（一）MH-17 事件中开源情报机构如何破坏俄罗斯宣传

在 2014 年 MH-17 航班被击落后，俄罗斯官方媒体最初宣布击落的为乌克兰空军 AN-26 运输机，但很快又改称该民航客机为乌克兰空军战斗机击落[11]，并让自媒体宣称“目睹了有乌克兰战斗机”。在同一年成立的民间开源情报机构 Bellingcat 则在 MH-17 事件中第一次展示了开源情报机构对国际关系的影响。Bellingcat 是 2014 年 7 月英国记者希金斯召集化学武器专家丹·卡泽塔、彼 得·朱克斯以及克里斯·布雷斯组成的私营情报调查机构，是一个分工明确、专家云集的核心业务团队、一个依托互联网、保持高热度的信息发布平台和一个规模精干、结构多元的基金会。[12]该组织依托当时俄罗斯媒体暴跌、当地人在社交媒体发布的视频、公开的商业卫星照片，通过对比后确认 MH-17 为被地面射出的防空导弹击落。随后在社交媒体上发起“众筹”式情报征集，带动大量专业人士和热心网友参与，并借助大量收集到的线索信息提出了亲俄武装使用“山毛榉”防空导弹击落的假设，在事件第二天便在官网公布了其初步调查结论。在随后的跟踪报导中逐步锁定俄罗斯国防部发布文件中的事实漏洞。[13]此次事件中 Bellingcat 通过迅速响应并在互联网平台依据开源情报与社区形成互动，占据了宣传优势，破坏了俄罗斯媒体对欧洲的公共外交。

（二）ORYX 在俄乌冲突中的可视化战损统计

在 2022 年至今的俄乌冲突中，开源情报机构则一度以其开放、即时、可追溯成为了各国媒体的引用来源，甚至成为了部分国家政府的参考。这主要原因在于，战争本身作为一种高度不透明且复杂的活动，所有参与方都天然的有隐瞒自身和夸大对手损失的利益，交战国自身都很难准确掌握前线战损的情况下，更不用说作为第三方的其他国家——从这个角度来说，各国政府内部的智库与民间机构一样，主要信息来源都是基于开源信息。在本次俄乌冲突中，最为知名的开源情报机构则是 ORYX，该组织创始人 Stijn Mitzer 和 Joost Oliemans 曾为 Bellingcat 工作过。该组织自叙利亚战争开始便尝试以交战双方基础士兵在社交媒体上发布的战果视频为依据，结合其他信源，统计各类装备的损失情况。该组织在俄乌冲突期间建立了著名的俄乌双方战损数据库，精确到每一架飞机、每一辆坦克与每一门火炮的损失情况，并依据损失等级分为受损 (damaged) 、全损 (destroyed) 、放弃 (abandoned) 和被俘 (captured) ，并附有相关图像作为损失证据。[14]该组织的统计不仅在 2022 年年初扭转了外界对于俄军的过高估计的刻板印象，还成为了欧洲大部分媒体乃至政府智库评估俄罗斯损失的参考数据。美国 CSIS 智库指出，ORYX 的所有损失数据都附有影像资料，可以视作双方损失的“下限”。[15]

从公共外交的角度来说，ORYX 为代表的开源情报机构在全球互联网时代提供了超越交战国的第三方视角。通过对开源信息的有效利用，国家可以更好地理解外国公众的舆论和情绪，评估自身传播策略的效果，并据此调整公共外交的叙事和重点；反之，那些缺乏事实依据的宣传则可能因为被揭穿而对当事国的公共外交产生负面影响，特别是对“声誉安全”而言。部分研究指出，国家拥有更正向、更可见的国际声誉，会在危机中更容易获得外部同情/支持与韧性。[16]在这个框架下，开源情报机构对公共外交的影响不仅仅是为各国民众提供了第三方叙事，更关键的在于，通过改变了为外部受众对于一国声誉的判断，从而在深层次上对他国的“声誉安全”产生威胁。

不过，ORYX 为代表的开源情报组织也面临另外的问题：如果作为信息来源的社交平台被政府机构有意大规模投放虚假信息时，准确性和即时性是否会受影响？此外，战场存在不同情况的信息管制，这就使得大多数战果的发布并不及时，因此其研究价值会受到一定限制；开源情报更是只能推测“已损失”，而对未损失部分则难以进行推测。[17]

（三）对开源情报机构的削弱与利用

开源情报机构对公共外交的影响也体现在信息战和国家信誉等领域。在当前大国竞争的背景下，开源情报机构已成为信息战和影响力操作的重要工具。战争的本质决定了没有人能完全了解当前局势，因为相关方可能不希望公众了解其行动，且事件的复杂性使得实时追踪所有信息变得不可能，这就是所谓的“战争迷雾”。[18]因此，当政府部门发起信息污染或直接参与开源情报机构工作时，开源情报机构参与的公共外交又回到了政府主导的传统公共外交范畴。

在政府主导的开源情报机构中，俄罗斯的 Rybar 最具有代表性，也是政府部门伪装性第三方的代表案例。Rybar 频道在 Telegram 上有 110 多万订阅，并被其他媒体广泛引用转发。其创始人为米哈伊尔·谢尔盖耶维奇·兹文丘克（俄语：МихаилСергеевич Звинчук），曾在俄罗斯国防部新闻处工作，他一直隐瞒自己的身份直到被俄罗斯独立新闻媒体《贝尔》（The Bell）揭露。事实上，rybar 表面是一个私人的开源情报分析者，但其实有约 40 名雇员并收到瓦格纳控制者普里戈津的资金支持。[19]

政府部门还可以在不参与开源情报机构运作的情况下利用它们，当政府的宣传策略与开源情报组织的判断基本吻合时，开源情报组织就是政府组织的天然盟友。这种支持并非简单的用来进行舆论宣传，有的时候还负有“泄

露机密”的责任来避免政府部门暴露自身情报来源。官方自己的私密情报可靠性更高但更加敏感，而开源情报机构有助于避免政府陷入“披露困境”和权衡。在第三方和受影响的利益相关者（如互联网服务提供商和社交媒体公司）的帮助下，政府可以在秘密情报的指导下更容易地利用经过验证的开源情报机构来揭露对手的军事、网络和信息行动。[20]

有的时候政府可以利用开源情报的研判逻辑，在源头上故意披露部分信息来产生宣传效果。例如 2025 年美军空袭伊朗核设施的“午夜之锤”行动中，就使用大批机群经美国本土从美国西侧进入太平洋，通过民众在互联网平台讨论与开源情报机构分析，营造出美军将从“太平洋-印度洋”进入对伊朗威慑/打击的航线的假象，实际的打击机群则悄无声息的从美国东侧进入大西洋执行打击任务。在开源信息与开源情报机构的作用下，军事行动会把“公众可见的开源信号”纳入欺骗设计：通过诱饵航迹与信息披露节奏管理，既影响对手的态势判断，也影响国际舆论对行动的预期。

结语

本文围绕“开源情报如何影响公共外交”这一问题，梳理了公共外交从政府主导的单向传播向平台化、多主体互动竞争的结构转型。与传统意义上以权威背书为主的对外叙事不同，开源情报机构以公开来源信息为材料，通过定位、核验与链条化的证据型叙事，从而在责任归因与能力评估等关键议题上影响国际受众的解释框架。公共外交竞争因此不再仅取决于传播渠道与话语技巧，更取决于能否在公开环境中提供经得起对照的证据资源与一致解释。

以 MH17 事件与俄乌冲突为例可以看到，OSINT 的影响并不主要表现为替代官方叙事，而更常表现为改变叙事竞争的起点：在责任议题上，通过公开证据链推动责任框架趋于固化；在战争态势议题上，通过可视化战损清单与规则化统计提供事实核查与战损证据的事实基准，不仅影响外界对交战双方实际军事实力的评估，更深刻影响到当事国的声誉安全。这种基于证据可见性的认知变化，会进一步回流到国家形象与声誉安全层面，为政府主导的公共外交带来深刻影响。

同时，本文指出开源情报机构并非等于客观事实，其“第三方”的地位是一种叙事的信誉，既可能削弱官方叙事的垄断性，也可能被国家行为体通过资源支持、议程引导或信息投放加以工具化；在行动层面，国家亦可能主动把可观察的开源信号纳入欺骗与保密设计，以制造噪声、延缓对手判断并塑造公众预期。加之公开信息存在可得性偏差与平台算法放大，开源情报机构在提升核验水平的同时，也可能引入新的误导路径。因此，相关分析不宜停留在技术层面，更需要把它放回平台化传播结构与可信度政治之中加以理解。

面向数字公共外交实践，本文的启示在于：其一，应强化对开源情报生态与证据链叙事的研判能力，将跨源核验、可视化呈现与解释一致性纳入对外传播准备；其二，应提升公共外交的“证据表达”能力，在公开环境中以可核验方式回应争议议题，降低单向声明被再解构的空间；其三，应建立对伪装性第三方与信息污染的识别机制，关注开源信号被操纵的可能，以减少声誉风险的长期积累。受限于篇幅，本文未能对不同平台的扩散机制与受众分层接受进行系统比较，后续研究可进一步从跨平台引用链条、受众分群与政策反馈机制等方向深化。

参考文献：

[1] Hatfield J M. There is no such thing as open source intelligence[J]. International journal of intelligence and CounterIntelligence, 2024, 37(2): 397-418.

[2] Hatfield J M. Intelligence under democracy and authoritarianism: a philosophical analysis[J]. Intelligence and National Security, 2022, 37(6): 903-919.

[3] 仇朝兵.美国"公共外交"及若干相关概念辨析[J].现代传播：中国传媒大学学报, 2021, 43(5):7.

[4] Cull N J. Public diplomacy before Gullion: The evolution of a phrase[M]//Routledge handbook of public diplomacy. Routledge, 2008: 39-43.

[5] Sharp P. Diplomatic theory of international relations[M]. Cambridge University Press, 2009.

[6] La Cour C. The evolution of the ‘public’ in Diplomacy [J]. Place Branding and Public Diplomacy, 2018, 14(1): 22–35.

[7] Cull N J. Public diplomacy: Taxonomies and histories[J]. The annals of the American academy of political and social science, 2008, 616(1): 31-54.

[8]史安斌,张耀钟.数字化公共外交:理念,实践与策略的演进[J].青年记者, 2020(7):4.

[9] 郑一卉.BBC 的外媒监测及其启示[J].对外传播, 2015(5):3.DOI:CNKI:SUN:DWDC.0.2015-05-032.

[10] Office of the Director of National Intelligence; Central Intelligence Agency. The IC OSINT Strategy 2024–2026

[11] Катастрофа MH17: как менялись версии российских СМИ https://www.bbc.com/russian/features-37496581, 访问时间 2025 年 11 月 18 日。

[12] 李景龙,周伟.基于网络的开源情报调查方法创新与应用——以英国私营情报调查机构"摇铃猫"为例[J].情报杂志, 2023, 42(2):5.

Bradbury D. In plain view: Open source Intelligence [J]. Computer Fraud & Security, 2011, 2011(4): 5–9.
[13] Das russische Verteidigungsministerium legt neue Beweise vor, die belegen, dass ihre früheren Beweise gefälscht waren
https://www.bellingcat.com/news/uk-and-europe/2016/09/27/das-russische-verteidigungsministerium-legt-neue-beweise-vor-die-belegen-dass-ihre-fruheren-beweise-gefalscht-waren/ 访问时间 2025 年 12 月 26 日。
[14] Attack On Europe: Documenting Russian Equipment Losses During The Russian Invasion Of Ukraine https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html 访问时间 2023 年 11 月 19 日。
Ayhan K J. The boundaries of public diplomacy and nonstate actors: A taxonomy of perspectives[J]. International Studies Perspectives, 2019, 20(1): 63-83.
[15] Bergmann M, Snegovaya M, Dolbaia T, et al. Out of Stock?: Assessing the Impact of Sanctions on Russia's Defense Industry[M]. Center for Strategic & International Studies, 2023.
[16] Sukhorolskyi P, Sukhorolska I M. The public diplomacy of Ukraine in wartime: a path to reputational security [J]. Eastern Journal of European Studies, 2024, 15(Special Issue): 268–291.
[17] Teagan J. Forecasting Russian Equipment Losses Using Time Series and Deep Learning Models [Z]. arXiv, 2025(2025).
[18] Niu J, Stillman M, Seeberger P, et al. A dataset of Open Source Intelligence (OSINT) Tweets about the Russo-Ukrainian war[J]. arXiv preprint arXiv:2409.01052, 2024.
[19] Ирина Панкратова.“ Создатель «Рыбаря». Продолжение расследования The Bell “ https://thebell.io/sozdatel-rybarya-prodolzhenie-rassledovaniya-the-bell 访问时间 2025 年 12 月 29 日。
[20]Dylan H, Maguire T J. Secret intelligence and public diplomacy in the Ukraine war[M]//Survival: August-September 2022. Routledge, 2023: 33-74.

The Mechanisms, Effects, and Boundaries of Open-Source Intelligence and Public Diplomacy

Liu Chenghao[1]

[1] Tongji University, Shanghai 200092, China

Abstract: Platform-based communication has reshaped the production and diffusion of international public opinion, pushing public diplomacy from state-centered one-way messaging toward a competitive, multi-actor networked arena. In this context, open-source intelligence (OSINT) leverages publicly available information to produce evidence-based narratives through searching, verification, and chain-of-evidence presentation. Once amplified through cross-platform circulation and repeated citation by media and think tanks, such narratives can enter the public agenda and affect how international audiences interpret key issues such as attribution of responsibility and assessments of military capability. Drawing on the evolution of public diplomacy and the perspective of reputational security, this article examines two cases—the Bellingcat investigation of the MH17 incident and Oryx’s visualized equipment-loss database in the Russia–Ukraine war—to analyze the mechanisms and boundaries of OSINT’s influence on public diplomacy. The findings suggest that OSINT does not simply replace official narratives; rather, it changes the starting point of narrative competition by increasing explanatory advantage through evidential visibility, thereby generating spillover effects on national image and reputational security. Meanwhile, OSINT is constrained by availability bias, algorithmic amplification, and the risk that its “third-party” appearance may be instrumentalized. The article concludes with practical implications for evidence-based communication, cross-source verification, and risk identification in digital public diplomacy.

Keywords: OSINT; Public Diplomacy; Platform-based Communication; National Image; Reputational Security