doi:10.3772/j.issn.2095-915x.2022.01.003

刍议开源军事情报工作的标准构建

黄永勤

国防大学政治学院军事信息与网络舆论系 上海 200433

开放科学（资源服务）标识码（OSID）

摘要：[目的 / 意义] 在“全源情报分析”时代，开源情报已成为军事安全领域关注和应用的重点，研究开源军事情报工作标准构建的思路和内容，为我军情报标准构建提供参考。[方法 / 过程] 基于现有文献和实践经验，论文界定了开源军事情报的概念，构建了开源军事情报工作标准“三层七要素”的框架。[结果 / 结论] 开源军事情报工作标准建设应重点关注：术语和定义、开源军事情报系统、情报工作人员、情报目标和情报需求、任务策划和部署、搜集存储、处理分析、分发利用、情报成果等九个方面核心内容。

关键词：开源军事情报；情报工作；情报标准

中图分类号：G35; G250

Research on the Standard Construction of Open Source Military Intelligence

HUANG Yongqin

Department of Military Information and Public Opinion, Political College of National Defense University PLA, Shanghai 200433, China

Abstract: [Purpose/Significance] In the era of “all source intelligence analysis”, open source intelligence (OSINT) has become the focus of attention and application in the military security field. This paper studies the ideas and contents of the construction for OSINT work standards, so as to provide reference for the construction of military intelligence standards. [Method/Process] Based on the existing literature and practical experience, this paper defines the concept of open source military intelligence, and constructs the framework of open source military intelligence work standard based on “three layers and seven elements”. [Result/Conclusion] The standard construction of open source military intelligence should focus on terms and definitions, open source military intelligence information system, intelligence staff, intelligence objectives and intelligence requirements, mission planning and deployment, collection and storage, processing and analysis, distribution and utilization, and intelligence achievements.

Keywords: Open source military intelligence; intelligence work; intelligence standard

基金项目 国家社科基金军事学青年项目“联合作战中开源军事情报保障研究”（2019-SKJJ-C-064）。

作者简介 黄永勤（1991-），博士研究生，讲师，研究方向：军事信息资源管理、开源情报，E-mail：yqhuang163@163.com。

引用格式 黄永勤 . 刍议开源军事情报工作的标准构建 [J]. 情报工程 , 2022, 8(1): 26-34.

引言

近年来，开源军事情报在国家安全和军队备战打仗等方面的实际效用愈发突出，推进开源军事情报工作的标准化，有利于提升情报工作的法治化、体系化和科学化，使其更好的发挥“尖兵”“耳目”“参谋”之作用；其次，习主席指出：“现代战争中，制信息权成为夺取战场综合控制权的核心”，情报显然是夺取制信息权的关键，而标准化有利于实现联合作战中的数据集成、信息共享和情报融合；最后，标准化能提升智能装备对情报的理解和算力，推动情报工作的智能化发展，最终助力打赢未来智能战争。

开源情报（Open Source Intelligence，简称OSINT）又常被称为公开情报、公开源情报、公开来源情报等，情报界对其概念界定存在一定的差异[1]，一般泛指情报的来源为公开途径。开源军事情报即开源情报在军事领域的具体应用，在概念逻辑上可视为开源情报和军事情报的交集。通过考察军语等相关文献，本文将开源军事情报定义为：为满足军事活动需求而利用公开途径获取的有关国家安全、作战指挥、国防和军队建设等方面的信息，通过鉴别、处理、分析、评估、分发、利用等环节加工而形成的情报、研究判断成果及相关服务。开源军事情报工作即为搜集、鉴别、处理、分析、评估、分发、利用等业务环节的统称。开源军事情报除了具有情报的基本特性外，还具有经济成本低、协作共享强、使用风险低、信息来源广、处理难度大、保护其他情报源等特点。

目前有关情报标准的研究较分散，有少量成果关注具体类型的情报标准，如威胁情报标准[2]；也有部分文献探索情报业务工作中某个具体细节方面的标准，如情报分析师职业能力标准[3]、情报产品质量标准[4]等；公开的情报相关标准较少，仅有《水文情报预报规范》（GB/T 22482-2008）等。总体而言，情报标准方面的学术研究成果较少，且多以介绍国外成果为主，对我国相关的实践经验缺乏总结。本文以“开源军事情报”这一专业科目为例，探索情报工作标准问题，基于以下三方面考虑：（1）现有情报标准基本以通用的情报工作流程进行构建，这种设计思路基于时间（纵向）维度，符合业务工作实际，具有很强的指导意义和实践价值，但存在一定的局限性，即虽体现了情报业务工作流程的普遍性却忽略了具体情报科目的特殊性。笔者认为在现有标准体系基础上兼顾专业（横向）维度进行针对性探索和完善具有重要意义，如目前公开的外军相关成果中，美军针对“网络安全威胁情报”制定了专门的MITRE系列标准、STIX标准、TI标准、TAXII标准等；英军针对“地理空间情报”发布了专门的标准*Defense Standard 00-102*：*MOD GEOINT Standards*。显然，开源军事情报区别于传统的信号情报（SIGINT）、测量与特征情报（MASINT）等，具有一定的独特性，为其制定专门的标准具有现实需求。（2）外军现有相关成果一方面催人奋进填补缺陷，另一方面也给我军的标准化工作提供了理论参考。北约《开源情报手册》[5]将其视为“全源情报分析（All-Source Intelligence Analysis）”中的“第一诉诸源”和“地基”，该手册从信息发现、鉴别、浓缩、综述与述评分发等方面阐述了开

doi:10.3772/j.issn.2095-915x.2022.01.003

源情报工作的流程；美军的《开源情报：专业手册》[6]在信息源、开源情报与军事能力、分析人员等方面的论述颇受业界认可；美陆军野战条令《开源情报》[7]（FMI 2-22.9）阐释的“行动计划与准备”“情报生产”“信息搜集与处理”三大开源情报工作流程也极具实践特色。（3）互联网飞速发展衍生的社交媒体、流媒体等开源平台成为情报界的新战场，北约《开源情报手册》更将“开源情报”上升为新的情报科目，但我军对此的理论和实践探索还比较欠缺。笔者有幸参与了国家军用标准的一些研制工作，结合课题研究和业务工作经验，希望文章能抛砖引玉引起更多专家和同行的关注，也希望研究成果能为开源军事情报标准的具体制定提供参考。

1 开源军事情报工作标准的框架构建

推进开源军事情报工作标准建设，核心任务是依据现有情报标准体系，立足情报需求、作战流程、工作实际和开源军事情报的特点，建立完善运行规则，使之体系化、标准化、科学化。笔者吸收了前文提及的北约和美军有关开源情报相关条令、手册中的内容框架、情报来源、情报人员、情报计划、情报生产等方面的成果，也反思了其在当下的适用性和情报要素方面存在的弊端，如当前互联网已成为开源情报的主要来源，对统一集成的情报系统需求强烈，而上述成果几乎未涉及。论文主要采用“理论—实践”双螺旋循环上升的研究思路，广泛吸收现有的理论成果，突出目标需求导向、情报组织严密、情报界与决策界彼此相对独立等我军开源情报工作的特点，纠正当前存在的情报分析量化不足、情报系统集成不够、情报规划随意等问题。综上，本文总结了开源军事情报工作标准的框架，其包含“三层”（理论层、基础层、实践层）和“七要素”（基本理论、情报组织、情报人员、情报系统、目标需求、情报流程、情报成果），如图 1 所示。

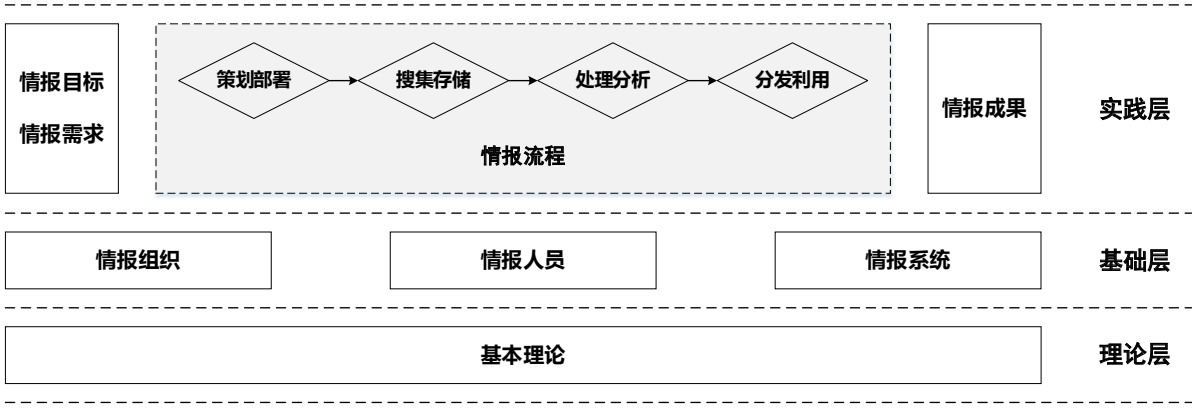

图 1 开源军事情报标准框架

（1）理论层。主要用于厘清开源军事情报涉及的理论问题，具体包括相关的术语和定义、特点、原则、参考引用的相关标准、使用范围等。理论层包含了国内外学术研究和军事应用的最

新成果，凝聚了学界、情报业界和情报使用者对相关问题的共识，是开源军事情报标准制定的理论基础和科学指导。

（2）基础层。主要包括情报组织、情报人员和情报系统三个方面，其共同构成开源军事情报工作的实体基础，具体而言：一是情报组织，主要明晰从事开源军事情报工作的业务机构、隶属关系、职能范围、领导管理机制、工作制度等。二是情报人员，主要明确从事开源军事情报工作的人员身份、工作职责、权利义务、能力要求等，开源军事情报的特点决定了其对工作人员的密级要求相对较低，因此世界各国军队从事此项工作的人员类别较丰富，主要包括现役军人、文职人员、合同劳务人员、高校和研究院所的领域专家、合作企业和智库等。三是情报系统，一方面开源军事情报来源逐步从传统纸质媒介等实体资源向以大数据为代表的网络数字资源转变，情报来源多源、异构、海量等特点决定了其对集成情报系统的需求；另一方面区别于传统人力情报等科目，开源军事情报具有很强的协作共享性，统一的情报系统是实现这一功能的关键。因此，为提高情报处理和服务效率，及时充分的保障联合情报需求，实现情报积累、协作、共享和智能化处理，探索情报精准高效融入作战指挥数据链，构建统一集成的开源军事情报系统已成为业界的共识。

（3）实践层。主要指具体的情报业务工作，包括情报目标和需求、情报流程和情报成果三方面内容，具体而言：一是情报目标和情报需求，从时间维度看既包括针对特定目标对象的长期情报需求，也包括临时的情报任务、情报需求反馈等；从应用层级看，既可以是涉及对象国战略层面的政治情报，也可以是战术层面的网络舆情，还可以是作战对手的武器装备科技情报。二是情报流程，卫星图像情报、信号情报等情报类型在搜集、处理、分发等环节中各平台是相对独立的，而开源情报系统一般集搜集、处理、分析、分发、反馈等功能于一体，部分业务流程的界限变得模糊，依据业务实际，本文将开源军事情报工作分为策划部署、搜集存储、处理分析、分发利用四个主要环节。三是情报成果，除了传统情报整编形成的动态要报、综合报告等情报成果外，开源军事情报成果中还有大量的情报资料成果和服务，如原始开源数据服务、情报资料汇编、特定目标情报资料数据库、武器装备和语种字典等。

2 开源军事情报工作标准的核心内容

在现有情报标准的内容体例之下，结合前文标准框架构建思路的论述，开源军事情报工作标准应重点规范以下几个方面。

（1）术语和定义。对开源军事情报的相关概念进行明确界定，便于形成共同话语体系。涉及的概念比如开源中心、网络情报、新媒体情报、社交媒体情报、流媒体情报、灰色文献、可能性、置信度、话报、简报、报告、情报保障等。在其他相关标准中已经界定的概念，可直接引用。

（2）开源军事情报系统。除了遵循相关的军用信息技术标准，还应理清以下要素：一是系统构建原则，比如体系设计原则、灵活开放原则、个性定制原则、互联共享原则、

doi:10.3772/j.issn.2095-915x.2022.01.003

集中控制原则等。二是按现有标准规范硬件、软件、体系架构、数据资源、运行平台等技术体系。三是数据库建设，按任务类型、需求紧急程度、情报对象等多维度构建情报资料数据库，利用最优技术实现信息的高效组织和检索。四是权限控制，合理规范用户和工作人员权限，既确保安全又兼顾资源利用最大化。五是业务集成，现有系统大多实现了信息搜集、预处理、存储、初步分析、报告自动生成等环节的集成，要依据需求把握集成与分割的范围，保证灵活性。六是安全拓展，兼顾开源军事情报的开放性，留有新资源、新需求的整合接口，兼具新技术和工具的拓展应用能力，如云处理、知识图谱、语义网检索、异地容灾备份、情报智能分析等。

（3）情报工作人员。正如美国国家安全局情报专家 David T. Moore[8] 所言：“情报由情报工作人员独立生产，保证情报工作人员的分工与其能力、技能、知识相匹配，是情报改革战略的核心环节”。目前关于情报工作人员职业胜任力的成果不少，相关标准如美国国家情报办公室 2008 年发布的情报界第 610 号指令（ICD 610）《情报界工作人员胜任能力目录》（2010 年修订）、美国国防情报局联合军事情报训练中心 2008 年发布的《国防情报局分析师培训需求和胜任能力》、美国国防部国防文职情报人员系统发布的《国防文职情报人员系统：设计、实施和影响的独立评估》、美国执法情报分析师国际协会 2004 年制定的《执法分析标准》（2012 年修订）等均可作为参考。开源军事情报工作人员的职业素养可从政治素质、保密意识、沟通协作能力、学科知识（特定目标知识、国家政略和战略、国际关系、政策法规、军事知识、情报理论等）、情报业务技能（批判思维、搜集、处理、分析、撰写报告等）、个性特征（性格、快速学习能力、创造力、灵活性、责任感、领导力等）等方面进行规范。此外，还应对情报工作人员的招募、培训、等级、职业规划、岗位职责、奖惩机制、福利待遇等方面进行规范。

（4）情报目标和情报需求。1994 年时任美国国家情报委员会主席的 Joseph Nye 博士曾指出：“情报搜集和分析工作是‘智力拼图’（Jigsaw Puzzle Analogy）模式，而开源情报是‘拼图的外围信息’，没有开源情报既无法开始拼图也无法最终完成拼图”[9]。开源军事情报的目标和需求便是“拼图的起点之起点”，需把握三个关键点：一是情报需求发起者和情报任务领受者，为帮助发起者全面表达需求、领受者准确理解任务，可对相关协调工作机制进行标准化，如规范交接形式、参会人员、需求文书等。二是情报目标，可参照国军标《作战目标分类》进行分类阐释。三是情报需求，规范具体的情报内容、时限、周期等需求要素。

（5）任务策划和部署。筹划和落实开源军事情报的任务需要梳理以下内容：一是需求优先级，可从重要程度和紧急程度两个维度进行考量，优先保障重要且紧急的目标任务。二是开源军事情报成果的定密机制，这将影响成果的内容、详略程度、分发范围等。三是分发范围，明确使用对象，了解使用者对结果形式的偏好、术语的理解等。四是时限，包括情报的覆盖时间、成果提交时间、动态跟踪周期频率等。五是成果分发，涉及成果的通用格式、分发方式等。六是人员分工和协作，如人员业务分工、情报

源搜集分工、与需求者沟通协作与反馈等。七是搜集分析方案，如确定搜集的社交媒体平台、关键词、人物等要素，明确分析方法、工具等。八是风险管理，包含判断是否为敌方释放的假情报、与其他科目情报印证时开源军事情报的置信度等。

（6）搜集存储。重点规范以下几个方面：一是搜集方式，明确人工搜集、搜索引擎、网络爬虫、专业领域数据库、众包搜集等各种方式的要求和原则。二是情报来源，Steele R D[10]曾针对美军开源情报的来源提出了信息闭联（Information Continuum）的思想，其提出了包括学校（原文主要指语言类院校提供的翻译服务）、大学、图书馆、企业、私人侦探和信息经纪人、媒体、政府、国防部门、情报部门9个来源。随着社交媒体平台成为越来越重要的情报源，兰德公司[11]2018年发布的《为国防事业定义第二代开源情报》报告指出当下开源情报的三大来源为新媒体、灰色文献和社交媒体。综上，本文认为可从文献情报资源、网络情报资源、实物情报资源、言语情报资源、其他情报资源五个类目进行梳理和规范。三是信息内容，依据任务锁定重点关注的账号、栏目、网站、信息发布规律等，规范元数据如题名、内容、发布时间、互动内容等。四是初步鉴别，依据个人经验和现有情报对搜集的信息进行初步鉴别，包括真伪性、可信度、完整性等方面的初步判断和筛选。五是信息存储，规范信息存储的格式、位置、容灾备份制度等。

（7）处理分析。将公开获取的数据和信息加工提炼成为可用的情报是开源军事情报工作最核心的环节，主要关注以下要点：一是应急预案，合理匹配处理分析能力和时限因素等，遇到数据信息量超出内部处理容量时，可按应急预案协调外部力量共享处理。二是预处理，开源信息数据量大、质量参差不齐，需要规范对信息全面性的核查、可靠性的初步研判、无关数据（如网页广告等）的清洗、待分析数据的预处理、情报信息的标引和著录等工作。三是初步分析，对时效性强的动态情报需求，通过快速分析获得情报，并将情报（甚至是原始数据信息）分发给指挥官和需求者。四是评估研究，针对综合性强的战略情报、目标情报等，多数时候需要联合相关领域专家共同分析研究。五是分析方法和工具，为确保软件安全可靠应制定禁用平台、工具的清单。六是分析要求和标准，美国国家情报总监办公室2007年制定并于2015年重新修订的第203号情报界指令（ICD 203）《情报分析标准》[12]从“客观、准确、及时、独立、有见地”五个方面规范了情报分析的标准，极具参考价值，该标准符合美国的情报文化，且面向所有情报科目，针对性较欠缺。如表1所示，本文吸收了ICD 203关于情报分析“客观、准确、及时、独立”的部分思想，同时结合开源军事情报的特点和我军的工作实践进行了针对性的改进、细化和阐释。如开源情报具有来源广、数据量丰富等特点，实践中需突出情报分析的全面性，因此在分析要求中增加了“分析全面”的指标并进行了标准细化；对“科学客观”要求补充了构建开源情报系统、合理使用软件工具、开展情报协作等细化标准；对“立场中立”要求补充了准确领会意图、与决策层保持适当距离等符合我军情报文化的细化标准。

doi:10.3772/j.issn.2095-915x.2022.01.003

（8）分发利用。指以规范的格式，通过任务确立的通信方式，及时将情报分析结果提供给需求者利用。应注意以下工作：一是规范分发的步骤和方式，如寄送、印发、电子邮件、指挥专网传递等；二是建立分发前的自我审查机制；三是建立合理的反馈机制，包括不同阶段的需求反馈和成果分发后的整体评价；四是建立情报撤回机制，便于及时纠正发现的错误和数据更新带来的结论变化；五是建立应急分发机制，针对动态任务、紧急作战需求等建立联合共享的应急分发机制，确保情报准确及时送达。

表 1 开源军事情报分析要求和标准

情报分析要求	情报分析标准细化
1.科学客观	• 分类描述各类来源及比重，对搜集的全面性量化说明 • 描述分析方法的科学性和可信度，兼顾领域专家经验揭示 • 情报分析假设合理、论证清晰、工具使用得当 • 纳入相关甚至对立的观点，克服认知缺陷 • 警惕已有立场和主观偏见，避免先入为主 • 保持开放理念，随事态发展、数据扩充及时更新结论 • 保持协作原则，依托开源情报系统多团队协作分析
2.立场中立	• 准确理解上级情报意图，但与决策层保持适当距离 • 不受特定用户、政治议程和观点的影响 • 不为特定政策偏好辩护，维持客观中立 • 说明与用户的相关性并陈述对情报分析结论的影响
3.注重时效	• 依据优先级处理重要紧急情报 • 合理设置数据搜集工具（如网络爬虫）的更新和响应时间 • 情报成果按权限及时分发 • 有价值情报持续跟踪和反馈
4.数据准确	• 对数据来源、真伪鉴定、噪音处理、情报印证等量化说明 • 建立原始开源数据核实、评估及责任倒查机制 • 存疑数据和矛盾信息核实并标注 • 说明和解释与主要分析判断相关数据的准确性 • 对灰色文献应特别说明和标识
5.分析全面	• 明确分析层级[13]（战略、战役、战术、技术）并进行分析方案设计 • 数据源涵盖纸质、电子、言语等多渠道多类型公开来源 • 基于现有所有情报来源进行分析 • 对评估结论及其置信度量化描述，可参照ICD 203设置的七个数据区间 • 视情运用有效的可视化图表 • 分析研判保持连贯性，如有变化应作出说明 • 对重要网络舆情等动向情报的“转折点”信息应作特别说明

（9）情报成果。情报成果对构建联合作战态势图极为重要，其可以是搜集平台直达指挥官的实时或近实时数据链，也可以是一份分析后的标准报告。该环节需思考以下问题：一是

类型规范，依据情报需求明确成果类型，如对象国概略情况、目标人物社交媒体动向情报、敌军武器装备评估情报等。二是形式规范，对不同形式情报成果如话报（口头报告）、简报、报告的总体要求、适用目标、用户受众等进行规范。三是内容规范，明确不同形式情报成果的格式规范、内容构成、数据来源的评价、不确定性问题的重点阐述、存疑问题的标注、不同结论的置信度量化描述等。四是知悉范围，正确标识公开信息、涉密和非涉密信息，同时遵循相应知悉范围的分发利用机制。五是评估监管，包括质量标准体系、定期评估计划、评估形式和参与者、自我审查、用户反馈、同行评议、主管机构监管、评估成果教育推广等机制。

4 结语

决胜千里，情报先行，将情报融入联合作战指挥体系的使命重大，而标准化是实现这一目标的核心路径。本文构建了开源军事情报工作标准“三层七要素”的框架，该框架跳出了传统仅以“情报流程”构建通用情报标准的思路，将情报组织、情报人员、情报系统、情报目标等内容纳入了标准化范畴。同时，框架可进一步落地为标准的具体内容，如“理论层”对应的就是相关的概念、术语、特点等，“基础层”可细化为情报系统、情报组织、体制机制、人员能力素质等，该框架可为特定科目情报工作的标准化提供借鉴。论文还进一步从术语和定义、开源军事情报系统、情报工作人员、情报目标和情报需求、任务策划和部署、搜集存储、处理分析、分发利用、情报成果等九个方面详述了开源军事情报工作标准建设的核心内容。值得指出的是，开源军事情报工作标准化建设任重道远，可供参考的研究成果和最佳实践较少，需在业务工作中摸索前进。同时需关注：

（1）明晰开源军事情报工作标准化的原则，重点把握集中领导、协调共享、开放灵敏等原则。

（2）把握开源军事情报工作标准化的特点，重视开源情报覆盖层级深范围广、数据混杂性强、情报业务兼具科学性和经验性等特点。

（3）掌握开源军事情报工作标准化的方法，目前情报领域立标常用的方法包括需求牵引法、顶层设计法、文献保证法等。

参 考 文 献

[1] 董尹 , 赵小康 . 公开源情报研究综述 [J]. 情报理论与实践 , 2013, 36(1):119-123+118.

[2] 石志鑫 , 马瑜汝 , 张悦 , 等 . 威胁情报相关标准综述 [J]. 信息安全研究 , 2019, 5(7):560-569.

[3] 谢晓专 . 情报分析师职业胜任力通用标准比较研究 [J]. 情报杂志 , 2017, 36(2):25-31+39.

[4] 谢晓专 . 美国情报产品标准与质量控制机制研究 [J]. 图书情报工作 , 2019, 63(18):87-98.

[5] NATO. Open Source Intelligence Handbook[M/OL]. (2001-11) [2021-05-26]. http://oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef-759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf

[6] Joint Military Intelligence Training Center. Open Source Intelligence: Professional Handbook[S]. 1996

[7] US Army Training and Doctrine Command. Open Source Intelligence（FMI 2-22.9）[S]. 2008.

doi:10.3772/j.issn.2095-915x.2022.01.003

[8] David T. Moore. Species of competencies for intelligence analysis[J/OL]. [2021-03-16]. http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.177.8743&rep=rep1&type=pdf.

[9] Steele R D. Intelligence analysis and assessment: the producer/policy-maker relationship in a changing world[C]. Canadian Intelligence conference, 1994:10-27.

[10] Steele R D. The importance of open source intelligence to the military[J]. International Journal of Intelligence & Counterintelligence, 1995, 8(4):457-470.

[11] RAND. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise[R/OL]. (2018-5-17) [2021-03-16]. https://www.rand.org/pubs/research_reports/RR1964.html.

[12] ICD 203.Analytic standards[S/OL]. (2015-1-2)[2021-02-16]. https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

[13] 中国社会科学情报社会 . 图书馆、情报与文献学研究的新视野（11）[M]. 北京：中国书籍出版社 , 2019:154-162.