·情报研究·

论开源情报的渊源、变革及其影响*

梅建明[1] 刘明辉[2]

(1. 上海政法学院 上海 201701; 2. 中国人民公安大学 北京 100038)

摘 要:[**研究目的**] 信息化时代,由于信息的载体形式和技术手段等方面因素的影响,传统的开源情报的地位和作用发生了巨大变化,深入研究开源情报对于理解新时代情报的变革意义重大。[**研究方法**]依据有关文献研究,采用定性研究方法探讨了开源情报的概念、起源发展、知识基础、技术动力和现实影响等问题。[**研究结论**] 数据和信息作为情报的知识基础、基础来源和原始载体极大丰富,人工智能技术等信息化技术改变了传统的情报工作作业方式,开源情报价值得以提升。开源情报已经或将要在国家安全情报思想和理论、情报组织结构、情报工作机制、情报力量建设与资源配置、情报工作技术手段、反情报工作等诸多重大方面产生深刻影响。

关键词:情报;开源情报;人工智能;大数据;国家安全;国家安全情报;情报工作;定性研究方法

中图分类号: D771 **文献标识码:**A **文章编号:**1002-1965(2021)12-0001-07

引用格式:梅建明,刘明辉. 论开源情报的渊源、变革及其影响[J]. 情报杂志,2021,40(12):1-7,102.

On the Origin, Change and Impact of the Open Source Intelligence

Mei Jianming[1] Liu Minghui[2]

(1. Shanghai University of Political Science and Law, Shanghai 201701;
2. People's Public Security University of China, Beijing 100038)

Abstract:[**Research purpose**] In the digital time, the open source intelligence (OSINT), which is used for a long time, is greatly changed due to the factors such as the carrier type of information and the new technology. Thus the study of OSINT has great implications for the change of intelligence in modern time. [**Research method**] This paper explores the issues such as the concept, the origin and development, the knowledge base, the technological stimulant, and the real impacts of OSINT based on relevant literature using the qualitative research method. [**Research conclusion**] This paper concludes while there are plenty of data and information which are the knowledge base, primitive source and carrier agent of intelligence, the artificial intelligence (AI) and other new information technologies are game changer for the traditional intelligence working style. In this context, the value of OSINT increases. The application of OSINT is changing or will change the conception and theory of national security intelligence, the structure of intelligence organization, the working mechanism of intelligence, the intelligence professional education and training, and the budget and technological resources allocation, and counterintelligence.

Key words: intelligence; open source intelligence; artificial intelligence; big data; national security; national security intelligence; intelligence work; qualitative research methods

在信息化时代,虽然传统的电力和机械仍不可或缺,但数据取代了电力机械的核心地位,正发挥着越来越重要的作用。从某种意义上讲,数据就是信息化时代的石油原油。由于作为"石油原油"的数据在数量、类型、传输和更新速度、潜在价值等方面具有的新特性,使传统的开源情报在性质和地位方面发生了变化,在应用领域得到了广泛的拓展。虽然开源情报的应用在伦理、法律等方面仍面临诸多挑战,但其变革性的冲击与影响仍然值得重视与思考。

目前国内学术界对开源情报的研究正处于起步阶段。在知网上以"开源情报"作为篇名检索得到的54篇期刊论文和博硕士学位论文基本都是发表在近五六

收稿日期:2021-09-04 修回日期:2021-10-10

基金项目:**中央高校基本科研业务费重点项目"基于数据技术的恐怖活动人员、组织特征与演化模型构建研究"(编号:2021JKF216)**。

作者简介:**梅建明**,男,1968年生,博士,教授,博士生导师,研究方向:反恐怖、国家安全、情报学;**刘明辉**,男,1986年生,博士,副教授,博士生导师,研究方向:公安情报学。

年之内。这些论文中,付举磊的博士学位论文集中讨论了开源情报在反恐怖工作的应用问题[1]。马增军和邓胜利等重点介绍了美国开源情报发展历程和制度建设[2-3]。杨建英等在国内外有关开源情报研究的基础上,结合开源情报的概念及特点,提出开源情报是中国国家安全情报的主要组成部分[4]。目前国内的文献对于进一步开展开源情报研究起到了较好的铺垫作用,具有开创性和探索性的价值和意义。但总体来看,现有文献对信息化时代开源情报在整个国家安全情报中所具有的价值,特别是以新技术驱动的开源情报将会产生并且能够产生的深远影响,仍然缺乏比较系统的梳理和深入的分析。本文将努力填补现有研究中的不足,将围绕开源情报这个核心主题,介绍其涵义,着重分析开源情报的知识基础、技术动力、理论挑战与现实影响。

1 开源情报的涵义、渊源与发展

1.1 涵义 开源情报就是通过分析公开渠道获取的信息所得到的情报。对于开源情报的内涵,需要进一步明确的问题有以下几点:

a. 开源情报与其他类型情报之间的根本区别。两者之间的根本区别就是情报来源的不同。不少研究把开源情报与信号情报、人力情报、图像情报等情报形式并列在一起,实际上,其中隐含的前提条件就是:只要来源是公开渠道获得的信息,无论这种信息的表现形式是信号的,还是图像的,那么,这种信息加工而成的情报就是开源情报。

b. 开源情报遵循情报生成的基本规律,即开源情报在生成过程,也会经历从情报需求、信息收集、信息处理、分析研判、传递与共享、反馈与评估等一系列环节。这一系列环节构成了情报生成的闭环。这个生成过程,有的学者或部门称之为情报循环(Intelligence Cycle),但有的机构(如美国国防部)称之为情报过程(Intelligence Process)。无论对开源情报这个过程冠以何种名称,实际上都揭示出开源情报与其他情报一样,都是一种动态过程的产物。

c. 开源情报具备情报的普遍属性。这种属性主要表现在:第一,情报是为决策服务的。开源情报与其他形式的情报一样,服务于决策者的特定需求,需要在某些特定事项上回答"是什么"(陈述)、"为什么"(解释)、"怎么样"(预测)、"可以怎么办"(应对)等问题。艾伦·杜勒斯总结发现"预先获得信息的愿望毫无疑问源于人类生存本能。统治者会向自己提出许多问题——下面会发生什么?我的事业如何才能兴盛?我应该采取什么行动?我的敌人有多强大?他们准备怎样反对我?"[5]情报就是围绕这类问题,努力给决策者提供"怎么办"的答案。开源情报也是为决策服务的,这种性质与定位并没有改变。第二,情报具有使用权和所有权,且两者相对独立。开源情报作为一种情报形式,其成果是专业人员创造性分析的结果。作为一种智力劳动的成果,开源情报与其他类型的情报一样,具有权属特性。一般来说,其所有权属于制造开源情报的组织或个人,其使用权一般限于决策者以及相关范围的组织或人员。在情报共享的背景下,相关的人员或组织共享的实际上是情报的使用权。第三,情报在一定范围内需要保密的属性。虽然开源情报来自于公开渠道的信息,但开源情报作为情报过程的最终产品形式,它并非是任何人可以知悉的。开源情报与其他形式的情报一样,也有需要保密的属性。

1.2 渊源与发展 开源情报并非新鲜事物,开源情报作为一种专业化的情报,其最早且成规模的应用可追溯到美国、英国二战前的情报工作。在美国,肇始于1941年的美国"外国广播情报服务局"(Foreign Broadcast Intelligence Service,缩写为FBIS)就是一个典型的开展开源情报搜集工作的机构。该机构成立之初名为"外国广播监听局"(Foreign Broadcast Monitoring Service,缩写为FBMS),隶属于美国联邦通讯委员会。二战末期,该机构划归为美国陆军部。1947年,美国《国家安全法》通过后,中央情报局成立,"外国广播监听局"(FBMS)更名为后来长期使用的名字,即"外国广播情报服务局"(FBIS)。冷战时期,"外国广播情报服务局"(FBIS)通过监听、翻译、分析苏联东欧国家的广播和其他公开媒体信息,获取开源情报,以支持美国政府领导人的决策。2005年,美国成立了由国家情报总监领导的"开源情报中心"。该中心的主体就是"外国广播情报服务局"(FBIS)。

与美国的情况类似,英国在二战前夕于1939年建立了"英国广播公司监听部"(BBC Monitoring Service,缩写为BBCM)。该机构的最初职责就是为了应对日益增长的轴心国的战争威胁,通过全天候地监听世界各地(重点是欧洲地区)的广播,搜集有关国家正发生的事件的信息,并向有关人员和机构提供最新情况报告。该机构提供的信息快速、及时、准确,其作用和价值日益显现,成为英国政府掌握世界最新动态的重要渠道,以至于当时的英国首相丘吉尔经常深更半夜打电话给相关人员,问:"这家伙(指希特勒)又在说什么呢?"

"英国广播公司监听部"自成立至今,作为英国政府开展开源情报工作的重要机构,发挥着重要作用。目前,该机构对全球150多个国家、100多种不同语言的3 000多个不同的媒体(广播、电视、报刊、互联网和新闻机构等)进行全天候的监听、监测,搜集这些公开

渠道的信息,对全球的重大事件进行分析,服务于政府领导人和相关机构[6]。

除了美国、英国之外,一些国际组织也十分重视开源情报工作。例如,国际刑警组织(Interpol)强调开源情报应用于对恐怖主义、网络犯罪、贩运人口犯罪等类型案件的侦查,并在培训课程中开设了开源情报理论与方法的模块。加拿大政府捐赠 200 万欧元给国际刑警组织,要求国际刑警组织为东盟国家(ASEAN)提供为期四年(2017-2021 年)的反恐侦查培训计划。该计划的主要任务就是如何利用开源情报并结合国际刑警组织的内部数据库开展反恐侦查工作[7]。类似地,欧洲警察组织(Europol)和欧盟执法培训署(European Union Agency for Law Enforcement Training)也在执法实务和培训工作中重视开源情报的应用。例如,欧洲警察组织于 2016 年在海牙举行了专门讨论开源情报的专题会议,来自美国和欧盟成员国的 100 多名代表讨论了开源情报打击各类跨国犯罪问题;欧盟执法培训署为欧盟成员国的执法部门提供专门化的开源情报培训课程。北约(NATO)在 2001 年就制定了专门的《北约开源情报手册》(NATO Open Source Intelligence Handbook),该手册详细提出了实施开源情报工作的步骤与要求[8]。北约于 2002 年又发表了另外两个指导性的资料(《北约开源情报读者参考》和《从互联网获取情报》)用以指导北约内部的开源情报工作。

2　大数据与信息源:信息化时代开源情报的知识基础

尽管开源情报由来已久,但信息化时代的到来,特别是互联网的应用与普及,以及信息科学技术的发展与应用,使开源情报开始进入一个新阶段。也正是从这个角度上讲,开源情报与几十年前的情况相比,已经发生了巨大变化。美国兰德公司于 2018 年发表了一篇报告,题为《为国防服务的第二代开源情报》[9]。从信息源的来源和特点等方面看,当今时代的开源情报在已非第一代的开源情报所能比肩。在传统的开源情报中,开源情报基本来源于传统的纸质媒体(报刊、图书、档案资料等),以纸质信息来源为基础的开源情报也只不过是以搜集者和分析者所能见到和看到的为限。“简言之,你之所见就是你之所得,仅此而已。”[10]信息化时代多样化的信息源和大数据构成了第二代开源情报的知识基础。

2.1　开源情报的信息源　信息化时代,传统的纸质媒体仍然可以成为开源情报的信息来源,但建构在信息技术基础之上的其他类型的信息载体构成了开源情报更为丰富的信息来源。开源情报的信息源从信息来源的形态看,主要包括两大类:一类是传统的纸质媒体;另一类是建构在互联网技术之上的各类平台。后者主要有浅网、深网、暗网等。开源情报的信息源从信息提供者的性质看,可以来自不同性质的渠道,主要有政府机构、军方、执法部门、民众、媒体、商界、学术界等[11]。

2.2　数据与大数据　作为记录和传递信息的基本载体和基本单元,数据是关于特定对象(人、事、物等)的可以观测到的定性或定量特征性符号。信息时代的数据与人类社会之前的数据相比较,具有根本性的质的差别。信息时代的数据具有大数据的特点。所谓大数据就是指人们无法在一定时间内用常规方法进行收集、处理和管理的复杂数据集合。大数据技术,是指从各种各样类型的数据中,快速获得有价值信息的能力和方法。大数据具有 5V 特点,即在 Volume(大量)、Velocity(高速)、Variety(多样化)、Value(价值)、Veracity(可信度)等五个方面与传统社会的数据相比,具有十分明显的特点。

3　人工智能:信息化时代开源情报的关键技术动力

人工智能(Artificial Intelligence,英文缩写为 AI)是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。无论是作为一门理论或一种方法,还是作为一项技术及应用,人工智能被认为是 21 世纪最重要的关键领域之一。

3.1　大数据与人工智能之间具有密切的关系　从一定意义上讲,两者之间是一种相互促进的共生关系。一方面,大数据需要人工智能。由于大数据具有价值密度的稀疏性,从价值稀疏的大数据中发现真正有价值的知识,离开了人工智能,就很难实现。另一方面,人工智能也离不开大数据。正是通过大数据的不断训练,人工智能的规则体系才能不断建立,人工智能发现知识的能力才能不断得到提高。最终,人工智能才能成为基于数据,但却又能超越数据并具有类人化能力的技术。

3.2　人工智能的影响　如同原油不会直接驱动车辆一样,数据也不能直接成为信息化时代的生产力和战斗力。信息化时代,人工智能技术是把数据转化为生产力和战斗力的关键技术之一。

人工智能不仅全面地影响着人类社会生产与生活的方方面面,也对国家安全产生重要而且深刻的影响。早在 20 世纪 90 年代,经过第一次海湾战争之后,西方国家从海湾战争的经验中发现,人类社会的战争冲突模式由于人工智能技术的应用,正发生着根本性的变化,传统的战争冲突模式进入了一种新的智能化战争形态。在这种智能化战争(即 Hyperwar)中,传统的人

类观察、分析、决策和行动模式由于人工智能技术的应用而被改变[12]。实际上,人工智能技术改变的不仅仅只有军事冲突模式。美国著名智库布鲁金斯学会在2018年发表的一份报告中,对人工智能在金融、国家安全、健康执法、交通等不同领域的革命性影响进行了初步分析[13]。

3.3 **人工智能驱动的开源情报** 如前所述,具有5V特点的大数据是一个巨大的宝藏。但是,如何把这个宝藏开发出来服务于情报和国家安全工作呢?显然,用传统的情报工作的作业方式几乎难以完成这项艰巨的任务。但人工智能技术的到来,为开源情报工作带来了颠覆性的技术手段。这种颠覆性的技术手段所具有的意义就如同大规模机械化的生产对传统农耕社会的农业生产所具有的意义一样,在生产效率、生产方式、生产组织等方面都会产生意义深远的影响。

3.3.1 人工智能驱动的开源情报流程 人工智能驱动的开源情报体现在开源情报流程的各个环节中(特别是在信息收集、信息处理、分析研判环节),人工智能的驱动都会带来显著的增益效果。在信息收集方面,人工智能有助于从海量数据中收集任何与情报需求相关的信息;在信息处理方面,利用人工智能的图像处理、语言翻译等技术,对收集到的信息进行清洗、甄别、比对、分类等各种处理;在分析研判方面,人工智能技术中基于特定规则生成的算法和模型可以对所收集和处理的信息做出进一步判别,发现其中的奇异特征,提炼出看似无用的海量信息之间的关联关系。

3.3.2 人工智能驱动的开源情报主要应用 人工智能驱动的开源情报可以应用于许多领域。主持应用开源情报的组织和部门既有政府部门,也有私营部门。在政府部门主持的开源情报应用方面,最主要的应用是由军队、安全和执法部门开展的。其中,典型的应用有通过开源情报实施战区人文地理和安全风险态势评估、开源反情报工作、防大规模杀伤性武器扩散、跨国人道主义救援、反恐、反诈骗、网络安全与打击网络犯罪、打击贩运人口犯罪等。私营部门的开源情报主要体现为基于开源信息的企业竞争情报以及反病毒及网络安全、商业零售、保险等行业针对客户群、产品和市场的分析和应用。

4 国家安全情报的变革:开源情报的现实影响

尽管信息化时代以人工智能驱动下的开源情报从未来发展趋势上,引发了一些值得关注的问题,这些问题需要从理论上进行更进一步的探索与研究,但是,从现实和积极的角度看,人工智能驱动的开源情报所具有的变革性意义和影响也值得关注和期待。人工智能驱动的开源情报如同催化剂,在国家安全情报的诸多重大领域(如国家安全情报思想和理论、情报组织结构、情报工作机制、情报力量建设与资源配置、情报工作技术手段、反情报工作等)都会产生深刻影响。

4.1 **对国家安全情报思想和理论的影响** “所有的公开信息都是情报‘磨坊’的‘谷物’。情报机构需要这些信息,但是训练有素的工作人员必须首先对信息进行挑选,这样才能在浩如烟海的信息中发现真正有价值的。”[5]虽然开源情报对情报工作不可或缺,但开源情报的地位、作用并没有得到应有的认可与重视。以美国为例,“9·11事件”之后美国国内一系列对情报机构的问责和反思都表明:即使在情报机构内部,长期以来,很多人只是把开源情报看作是比秘密情报地位要低下的附属品[14]。兰德公司的资深专家丹尼尔·埃尔斯伯格(Daniel Ellsberg)在研究了美国越战的决策过程和决策模式后,他这样教训越战时担任总统国家安全顾问的亨利·基辛格,他说“危险的是,你会变成一个白痴。你会变得无法向世界上大多数人学习,不管他们在他们特定的领域多么有经验,可能比你强得多。这都是因为你盲目地相信那些狭隘的、经常错误的秘密信息。”[15]在美国和其他许多国家,对秘密情报的信任、依赖根深蒂固,甚至演变成情报系统内部的一种“秘密崇拜”的亚文化。

但在比较开源情报与秘密情报之间的地位方面,实际情况是什么样呢?在1947年美国参议院举行的听证会上,艾伦·杜勒斯揭示了情报工作的秘密,他说:“由于外在的光环和神秘性,由秘密手段和秘密特工获取的秘密情报通常被过分地强调了。在和平时代,大量的情报能通过公开渠道获得。”杜勒斯甚至提出了一个“80%规则”,即80%的情报可以通过公开渠道获得。杜勒斯的这个原则,后来在美国及其他地方的情报工作中得到进一步验证。美国中央情报局长期负责追踪本·拉登的小组承认:涉及本·拉登的情报中,90%的情报来自于开源渠道。欧洲警察组织(Europol)甚至认为超过95%的反恐情报来自于开源渠道。类似地,北约认为80%的军控和防武器扩散方面的情报来自于开源渠道。2005年,时任美国中央情报局副局长助理的威廉·诺尔特(William Nolte)宣称美国情报机构处理的信息中,95%~98%的信息来自于开源渠道。著名的冷战理论的炮制者、美国外交官乔治·凯南曾于1997年就秘密情报和开源情报问题发表了类似的见解。他说:“基于我过去70多年的职业生涯(先作为政府官员,之后45年作为历史学家),我坚信我们政府在关于世界实务方面对秘密情报的需求被过分强调了。我想说我们需要知道的情报中,超过95%的情报可以通过认真、有效地从相关国家的图书馆或文献收藏中分析公开、合法的信息而获得。”[16]

因此,在国家安全情报的思想和理论中,需要结合当今世界的技术创新,分析总结各国情报工作的经验教训,回答一系列重要问题:开源情报是否是情报?如果是,开源情报到底有何价值?秘密情报和开源情报之间的关系到底如何?如何总结和评价秘密情报和开源情报在冷战和后冷战时代的关系、地位与作用?信息化时代的新技术对秘密情报和开源情报及其相互关系到底会产生什么影响?秘密情报与开源情报之间的这种关系,如何会进一步影响情报工作的其他方面(如情报机构的职责和任务、反情报工作等)?诸如此类。在我们围绕这些问题进行理论研究,探讨未来国家安全情报的特点、趋势与规律的时候,我们也可以围绕这些问题对正在发生的变化进行初步的观察和分析。

4.2　**对情报组织结构的影响**　在一些国家,开源情报对情报组织结构的影响是以对情报工作的检讨、对开源情报地位的认可等为条件和先导的。例如,在美国,过去二十多年中,美国多次对情报系统进行问责、检讨。1996 年美国国会成立的阿思平-布朗委员会(Aspin-Brown Commission)就美国情报体系在冷战后的效能进行评估时,指出虽然互联网上的信息非常丰富信息,随手可得,但情报系统并没有让情报分析人员充分利用这些公开信息。在开源情报工作方面,情报体系思想保守,动作缓慢,不能跟随时代的步伐。2004 年"9·11 事件调查委员会"和 2005 年"大规模杀伤性武器委员会"分别发布的两份报告,仍然明确指出了美国情报体系在开源情报工作中存在的问题。正是意识到这些问题的存在及其带来的严重影响,美国国会于 2004 年通过的《情报改革和防范恐怖主义法案》明确要求在美国情报系统中成立开源情报中心。2005 年,美国开源情报中心成立,隶属于中央情报局。此外,美国还设立了负责开源情报工作的国家情报副总监助理的高级职位。类似地,澳大利亚于 2001 年 8 月建立了开源情报中心,隶属于澳大利亚国家情报办公室。如前所述,英国广播公司实际上也有从事专门开展开源情报工作的部门"英国广播公司监听部"。从公开的管理体制上讲,该部门并不是英国情报系统的成员,但是,它的经费有相当一部分来自于英国政府。总体来看,一些国家已经根据当今时代开源情报的地位和作用在组织结构上调整了传统的情报系统,加大了开源情报工作的力度。

4.3　**对情报工作机制的影响**　情报工作机制是情报系统内部单位之间和情报系统与外部单位之间围绕情报流程的各个环节及相关内容形成的固定工作关系。从最广泛的意义上讲,开源情报可以成为当今时代实现全面变革的催化剂。它不仅可以改变全球范围的安全以及相关的其他问题(如贫困问题、武器扩散问题等),也可以在一个国家内部的许多方面产生变革性的影响。罗伯特·斯蒂尔(Robert David Steele)在一篇文章中指出:依靠开源情报可以建设一个属于人民、依靠人民、为了人民的"智慧国家"(Smart Nation)。开源情报通过在国家安全、情报、政府、选举制度等方面发挥催化作用,促使国家变得更智慧、更安全、更高效[11]。在这样的变革过程中,无论是情报系统内部单位之间,还是情报系统与外部单位之间的工作机制都会受到影响并发生变化。

4.3.1　在工作重点上,情报系统内部需要围绕开源情报和秘密情报的关系重新调整彼此之间的工作关系,改变过去长期以来开源情报只是作为附属情报地位的尴尬局面,并进一步地改变情报流程各个环节的工作关系。

4.3.2　在工作关系上,共享与合作关系成为支撑情报系统内部单位、情报系统与外部(政府其他部门、民众、社会组织与团体、媒体等)之间的主流工作关系。在秘密情报作为核心情报形式的环境中,保密导致隔离,垄断阻碍共享。但开源情报在理念、性质、内在动力等方面所具有的变革性特点,必然冲击以秘密情报为核心的工作机制,必然要求建立真正属于人民(主体性)、依靠人民(手段性)和为了人民(目的性)的新机制,这种新机制应当是以共享与合作为主要形式,而不是垄断与隔离。开源情报是所有类型的情报中,唯一一个可以在没有许可的情况下,同时获取所有语言已知信息的学科,可以利用所有可用的专业知识和人力,并产生可以与任何人共享的情报[11]。开源情报的这种特点使得它具有与其他类型的情报相比,更为独特的价值。

4.3.3　在工作内容上,数据、信息、情报、知识、权力之间的关系被重新定义和构造。人工智能驱动的开源情报在信息化时代的广泛应用,不仅加速了从数据、信息向情报、知识,最终向权力的转化速度和转换形式,也将缩小、弥合在工业化社会数据、信息、情报、知识和权力等要素之间存在的巨大鸿沟。共享与合作机制下对数据、信息、情报和知识的利用,应当以形成民主化和法治化的权力架构为途径;而民主化和法治化的权力架构,必然也会要求对数据、信息、情报的共享与合作成为新时代国家安全情报建设的重要命题。

4.3.4　在规范化机制上,人工智能驱动的开源情报将推动情报工作机制走向以问责、透明为核心的法治化规范渠道。开源情报将变革情报系统的内部文化,冲击情报系统内部的以保密为手段搞情报神秘主义的组织文化传统和组织文化屏障。法治社会治理之下的情报将随着开源情报的广泛应用,最终必然走向

更加强调问责和透明的规范化渠道。否则,人工智能驱动的开源情报不会带来属于人民、依靠人民和为了人民的美好国家。

4.4　**对情报力量建设与资源配置的影响**　情报工作长期以来是一项高度保密性、高度专业化的工作。在情报工作中,人力、资金、技术等资源的投入很高,各种资源在不同情报领域和情报流程的不同环节的配置也不一样。在人工智能驱动的开源情报发展过程中,情报力量建设及资金投入、技术研发和保障等方面,都会发生较大变化。

4.4.1　对情报力量建设的影响　对情报力量建设的影响主要表现在情报工作人员的专业构成比例、情报工作人员的选拔和教育培训课程设置、情报力量的社会面和阵地布局等。在前面介绍的美国"外国广播情报服务局"(FBIS)和"英国广播公司监听部"(BBCM)都有大量的语言翻译雇员,他们负责把大量的非英文资料翻译成英文资料。很显然,随着人工智能技术的发展,大量的翻译工作将由机器翻译完成。从事开源情报工作的人员中,作为语言专家或翻译人员的比例将下降。就整个情报系统的人员构成情况来说,人工智能驱动的开源情报也会对原有的情报工作人员在情报、隐蔽行动、反情报等不同领域的人员配备产生影响。在人员选拔和教育培训课程设置方面,虽然缺乏系统的资料分析世界主要国家情报教育和培训的课程设置情况,甚至"五眼联盟"内部的情报教育和训练课程体系也难以详尽分析[17]。尽管如此,从可以掌握的部分资料可以发现:自"9·11事件"之后,在美国以及"五眼联盟"的其他国家,情报教育训练的课程内容中,社会人文学科知识的重要性得以显现。例如,美国陆军基于人类学、社会学、政治学、语言学等学科的知识提出了"人文地形系统"(Human Terrain System)的概念,并于2007年开始直到2014年为止,美军先后向阿富汗、伊拉克地区部署了31支"人文地形小组",这支队伍的年度经费为1.5亿美元。美军认为"人文地形系统"实际上是一种情报赋能的工作,通过帮助战场指挥官认识作战地区的人文地理特点,增强对战场环境的理解。美军在德克萨斯州的利文沃斯堡开展"人文地理系统"战斗小组的培训,其培训内容涉及田野研究方法、人文社会科学基础理论、作战参谋业务、武器和装备使用等[18]。由此可见,随着作战任务的多样化,以开源情报为支撑的战场决策和作战行动,要求更新传统的情报教育训练形式和内容。开源情报工作也要求在情报力量布局中,增加对社会面和外围阵地的布局,同时也应改变情报系统在社会面阵地和力量的使用方法、使用形式,以适应信息化时代的情报工作需要和特点。例如,2014年俄罗斯成功吞并克里米亚,其中一个很重要的做法就是俄罗斯有效地通过开源情报和战略沟通手段赢得了在乌克兰的俄罗斯裔人的支持,为俄罗斯吞并克里米亚创造了积极的社会氛围和条件。

4.4.2　对资金投入的影响　情报作为辅助决策的工具,国家安全情报是围绕各种安全问题开展的工作,其中既有秘密的,也有公开的。但各种安全问题与秘密情报和开源情报的关联性到底有多高呢?根据联合国2004年发布的报告《一个更安全的世界:我们的共同责任》,罗伯特·斯蒂尔(Robert David Steele)列出了开源情报与联合国报告所关注的安全问题的关联度(见表1)。依据表中的数据,可以发现在解释各种安全问题上,开源情报可以发挥很高的效力。

表1　开源情报与各类安全问题的关联度

安全问题类别	开源情报相关性(%)
经济与社会问题:	95
贫困	99
传染病	95
环境恶化	90
国家间冲突	75
国家内部冲突:	90
内战	80
种族屠杀	95
其他大规模暴	95
大规模杀伤性武器	75
恐怖主义	80
跨国有组织犯罪	80

据此,罗伯特·斯蒂尔估计,开源情报与这些全球性威胁相关的平均功用为82.5%,非常接近前文提到的杜勒斯所讲的"80%规则"。但是,实际情况(特别是资金配置上)并非与这个规则的要求一致。以美国为例,美国每年至少花费8 500亿美元来收集秘密情报,而秘密情报在整个情报中所占的比重大约只有5%,而用于开源情报方面的资金只占有很小的比例。所以,他进一步强调,许多国家把99.9%的情报资金用于秘密情报工作,而将不到1%的情报资金用于开源情报,这种做法实际上近乎是一种疯狂,当然也是一种腐败[11]。

很显然,按照"80%规则"实现对情报资金的合理配置,目前许多国家的情报资金配置方式应当得到纠正。用于开源情报工作的经费应当占有更大的比例。

4.4.3　对技术研发和保障的影响　在2018年举办的一个会议上,美国特朗普政府时期的国家情报总监丹·科茨(Dan Coats)断言:在应对当前技术变革带来的机遇和挑战过程中,美国情报系统的变革是革命性的,而非渐进性的。情报系统必须善于并且快速采用各种创新性的技术。美国传统基金会于2005年发布的一篇报告中结合反恐怖工作需要,提出未来的创新性关键技术有:系统集成技术、非致命武器技术、纳米技术、激光定向能技术、生物特征识别、数据挖

掘[19]。实际上,自 20 世纪 90 年代前后,美国就着手实施了在情报系统探索应用新技术的研发项目。如美国国防高级研究计划署(DARPA)于 2002 年启动的“反恐怖信息战项目”(简称 TIA,)、美国联邦民航局于 1996 年启动的“计算机辅助下的旅客预审系统”(简称 CAPPS)、美国国家安全局于 2002 年启动的“源于超级数据的新情报”(简称 NIMD)、美国移民海关执法局于 2001 年启动的用于实现对访美的外国留学生和访问学者进行监控和管理等目的的“监测留学生和访问学者信息系统”(SEVIS)。截至 2004 年,美国政府大约有 52 个部门,实施了至少 199 个数据挖掘类的项目。其中,14 个项目是以国家安全和反恐为主要目的的。这些项目应用的关键核心技术就是以大数据应用为方向,以数据挖掘、机器学习、人工智能等技术群为内容的信息科学技术。特别是“9·11 事件”之后,为了平息民众对情报部门的不满与批评,美国加大了此类项目建设的力度,特别强调运用信息科学技术收集和挖掘开源情报,以提升其反恐和安全情报能力。这些研发计划与创新实践项目,极大地推动了美国情报体系,特别是反恐情报体系的重塑[20]。

4.5　对反情报工作的影响　兵者,诡道也。”《孙子兵法》的经典名言深刻揭示了在战争中灵活运用多种策略的重要性。在现代战争中,这些策略包含了情报战和心理战。由于互联网及其他信息网络和媒体渠道是开源情报的主要信息来源渠道,因此,信息化时代,网络空间就成为情报战和心理战的重要战场。网络空间的情报战和心理战是传统情报战和心理战在信息化时代的拓展和升级。在新的技术条件下,人工智能驱动的开源情报在反情报工作中的一个重要作用就是帮助核实秘密情报的真实性。反情报工作中的很多情报都是秘密渠道获得的,这些秘密情报常常难以得到有效的核实和验证。开源情报为核实和验证反情报工作中大量使用的秘密情报提供了一种新的渠道。开源情报在反情报工作中的重要作用更突出地表现在开源情报为甄别网络虚假信息提供新的方法。信息化时代网络空间的各种信息丰富多样,但其中各种虚假信息以及欺骗行动也层出不穷。这些虚假信息既有故意捏造的,也有因其他原因导致的信息失真、信息碎片等问题;既有个人制造的虚假信息,也有国家或组织机构有组织、有规模制造和传播的虚假信息。基于这些虚假信息,别有用心的国家、组织或个人可以采取进一步的欺骗行动。因此,甄别虚假信息是保持自身信息优势、削弱敌人信息战和情报战能力的首要任务。开源情报能够利用不同渠道的信息来源对特定信息的来源、传播、内容、受众等进行分析,从而有效甄别虚假信息,锁定虚假信息的制造者并揭示其行为意图。

5　结束语

信息化时代,情报工作的环境和技术条件发生了重大变化。数据和信息作为情报的知识基础、基础来源和原始载体极大丰富,以人工智能技术为核心的技术改变了传统的情报工作作业方式,开源情报的作用和价值凸显。开源情报在国家安全情报思想和理论、情报组织结构、情报工作机制、情报力量建设与资源配置、情报工作技术手段、反情报工作等诸多重大方面正在或将要产生深刻影响。我们也应当认识到,以人工智能驱动的开源情报也提出了一些新问题值得进一步的思考和分析。比如,广泛的开源情报应用意味着人类社会是否进入了一个以人工智能和其他高技术应用为特点的监控型社会?在社交媒体和互联网中广泛传播的虚假信息对开源情报的真实性提出了严峻的挑战,围绕虚假信息展开的信息战和情报战是否意味着现代社会生活在虚幻和真实之间始终是一种纠结难逃的困境?当开源情报的共享与透明成为极为普遍的趋势的时候,传统的公权顶层决策者垄断情报的事实被打破,政府其他部门,甚至私营部门也可以利用公开信息获得相应的开源情报,这种趋势是否意味着情报的私有化至少在有些国家会成为情报体制的新特点?限于篇幅,本文不去深入讨论这些问题。但无论如何,当今时代开源情报所带来的影响和随之产生的各种问题的确值得关注、思考和研究。

参 考 文 献

[1] 付举磊. 基于开源情报的恐怖活动及反恐策略研究[D]. 长沙:国防科学技术大学,2014.

[2] 马增军,王　净. 美军开源情报发展历程及任务管理体系综述[J]. 现代情报,2015,35(7):172-176.

[3] 邓胜利,王子叶,杨璐伊. 美国开源情报的产生与发展[J]. 保密工作,2020(4):50-51.

[4] 杨建英,余至诚. 开源情报在中国国家安全情报中的地位和作用分析[J]. 情报杂志,2019,38(10):21-26,145.

[5] 艾伦·杜勒斯. 情报术[M]. 陈秋慧,译. 北京:金城出版社,2014,1.

[6] BBC. History of the BBC [EB/OL]. [2021-08-22]. https://www.bbc.com/historyofthebbc/anniversaries/august/bbc-monitoring.

[7] Interpol. Training southeast asian countries to exploit online data in counter-terrorism investigations[EB/OL]. [2021-08-22]. https://www.interpol.int/en/Crimes/Terrorism/Counter-terrorism-projects/Project-Trace2

[8] NATO. Open source intelligence handbook [EB/OL]. [2021-08-22]. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf.

(下转第 102 页)

(上接第7页)

[9] Heather J. Williams, Ilana Blum. Defining second generation open source intelligence (OSINT) for the defense enterprise [EB/OL]. [2021-08-22]. https://www.rand.org/pubs/research_reports/RR1964.html.

[10] Stewart K B. The tao of open source intelligence [M]. IT Governance Publishing, 2015:2-3.

[11] Robert David Steele. Open source intelligence [M]//Loch Johnson. Handbook of Intelligence Studies. NY: Routledge, 2007:129-147.

[12] Eric H. Arnett. Welcome to hyperwar [J]. Bulletin of the Atomic Scientists, 1992, 48(7): 14-21.

[13] Darrell M. West, John R. Allen. How artificial intelligence is transforming the world [EB/OL]. [2021-08-22]. www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/.

[14] Richard A. Best, Jr. Alfred Cumming. Open source intelligence (OSINT): Issues for congress [EB/OL]. [2021-08-22]. https://sgp.fas.org/crs/intel/RL34270.pdf.

[15] Daniel Ellsberg. Secrets: A memoir of vietnam and the pentagon papers paperback [M]. Penguin, 2003:237-239.

[16] Christopher Hobbs, Matthew Moran, Daniel Salisbury. Open source intelligence in the Twenty-First Century: New approaches and opportunities [M]. Palgrave Macmillan UK, 2014:9-11.

[17] Patrick F. Walsh. Teaching intelligence in the twenty-first century: Towards an evidence-based approach for curriculum design [J]. Intelligence and National Security, 2017, 32(7): 1005-1021.

[18] US Army HQ. Military intelligence professional bulletin: Human terrain system [EB/OL]. [2021-08-22]. https://irp.fas.org/agency/army/mipb/2011_04.pdf.

[19] James Jay Carafano. The future of anti-terrorism technologies [EB/OL]. [2021-08-22]. https://www.heritage.org/homeland-security/report/the-future-anti-terrorism-technologies.

[20] 梅建明. 信息化时代反恐情报工作的创新、挑战与启示:基于对美国的分析[J]. 情报杂志,2020,39(11):1-8.

(责编/校对:刘影梅)