侦察监视与情报研究丛书

美国陆军开源情报手册

马增军 耿卫 王净 李丹浓 编译

知远战略与防务研究所

侦察监视与情报研究丛书

内部资料 仅供学习

美国陆军开源情报手册

马增军 耿卫 王净 李丹浓 编译

知远战略与防务研究所

目录

CONTENTS

第一部分

美国陆军野战条令：开源情报

前言

本手册（FMI 2-22.9，2008 年版）加速推动了条令的交付使用，该条令已获提议者批准，用于训练和作战。本手册建立了对陆军公开来源情报 (open source intelligence，OSINT，以下简称开源情报) 工作的共识。作为暂行的条令，它为陆军开源情报训练、构想、装备和力量结构等方面的分析和发展起到了催化作用。它把开源情报作为一个情报门类的特性，在陆军情报条令和联合出版物 JP2 － 0《联合作战情报支援纲要》中相统一起来。

本手册取代了陆军野战条令 FM 2 － 0 中对开源情报的定义和阐述，提供了陆军开源情报工作的基本原则、专用术语，以及初始的战术、技术与程序（tactics，techniques，and procedures，TTP）。

第一章提供了对开源情报的介绍。

第二章描述了陆军开源情报的基本原则、行动和机构。

第三章至第五章提供了开源情报行动的初始战术、技术与程序。

附录提供了对各章节中所提及信息的支持和相关的拓展信息。

除非另有说明，否则本手册适用于现役陆军、陆军国民警卫队 / 美国陆军国民警卫队、美国陆军预备役。

本手册可为负责制定条令和战术、技术与程序、作战物资和部队结

构、以及情报工作训练的人员提供参考，同样可为国家、联合、跨机构、其他军种，以及多国或合作伙伴的情报人员提供参考。

本出版物的提议者是美国陆军训练与条令司令部（United States Army Training and Doctrine Command），准备机构是美国陆军情报中心条令部（Directorate of Doctrine, US Army Intelligence Center）。有关意见和建议可填写到陆军部2028号表格（对出版物的修改意见空白表），直接发送给司令官，收件方：ATZS — FDD — D (FMI 2 — 22.9)，美国陆军情报中心，瓦丘卡堡Cibeque街550号，AZ 85613 — 7017。请按照陆军部表格2028号的格式填写，或提交电子版表格。

除非另作说明，本出版物中带有男性含义的名词和代词并不专门指男性。

选用的联合或陆军定义的术语在术语表和正文中均有标识。术语表列出了本手册使用的大部分术语，这些术语联合定义或陆军定义。由本手册提倡的术语在术语表中用“•”号作了标记。这些术语及其定义将沿用到陆军野战条令FM 1 — 02的下一个版本中。对于文中显示的其他术语定义，采用了斜体字，并注明了提出该定义的出版物。

第一章 概述

200多年来，美国军队的专业人员通过搜集、翻译和研究大量文章、书籍和期刊，来获取对外国领土和军队的了解。然而，公开信息作为情报的一种来源，在陆军情报工作中往往被忽视。本手册力图让陆军重新认识到公开来源的价值，建立对开源情报的共识，探索系统地搜集、处理和分析公开可得信息的有效途径。

在过去的二十年里，计算机和互联网技术呈指数式增长，士兵们通过指尖能获得的公开信息和处理能力超过了以往任何时候。文化、经济、地理、军事和政治等方面的各种知识，曾经是老学者们的专属，现在的高校毕业生就能轻易获得。对情报人员来说，这些技术使他们能够获取可满足单位情报需求的大量信息。然而，我们对保密数据库和外部支援的过度依赖，往往使我们的士兵在面对从公开来源获取的海量非保密信息时，表现得不知所措。下面的例子说明了这一点。

我将在几个月后被派往萨尔瓦多，担任驻当地任务部队负责情报的代理参谋官，我需要为特遣部队指挥官搜集一些关于这个国家和当地形势的信息。尽管曾在“自由伊拉克”服役过，我还是不知道如何去搜集这些信息，因为当我们被派往伊拉克时，关于这个国家的基本情

况几乎已经呈现在我们眼前。

——工程大队代理情报参谋军士

从萨尔瓦多到伊拉克，对美国陆军来说是世界上完全不同的两个作战环境。对这些不同的作战环境来说，开源情报的发展和运用不是奢侈品，而是必需品。在我们可能要实施的军事行动中，我们需要了解关于作战环境的物理和人为因素，公开来源能提供大量此类信息。事实上，我们对于这些环境的认知，多数基于我们通过教育、旅行、新闻节目和学者获取的公开可得信息。

美国陆军情报与安全司令部 (Intelligence and Security Command，INSCOM) 下属的亚洲研究特遣队论证了持续性开源情报工作的特征和能力。从 1947 年起，该特遣队就开始搜集、处理和分析公开可得信息，以获取中国、朝鲜及其他潜在对手的军事能力、部署和战备等情报。同样也涉及到这些地区的经济、环境、政治和社会状况等领域。

最近几年，亚洲研究特遣队报告了 2004 年台湾总统选举导致两岸关系高度紧张、针对美国的安全威胁、针对 2004 年 12 月印尼大海啸的联合人道主义救援行动、以及 2005 年 8 月中俄“和平使命 2005”联合反恐演习中所用到的战略和战术等情报。

还有许多证据表明，开源情报分析和报告具有极高的价值。亚洲研究特遣队自 2003 年以来的情报信息报告中，已经收到 28 份“非常重要”的评估性情报，这些情报分别来自国防情报局（Defense Intelligence Agency，DIA）、国家地面情报中心（National Ground Intelligence Center，NGIC）、以及美国空军的国家航空航天情报中心（Air Force's National Airand Space IntelligenceCenter，NASIC）等机构，内容涉及从朝鲜的地下设施到中国人民解放军空军航空航天科技发展等各方面。

在战术层面，一些单位把他们的资产编组成开源情报部门。以下是来自2005年第3步兵师部署至伊拉克的例子，它说明了情报人员如何适应新任务并获得成功。在这个例子中，连指挥官把通用地面站（common ground station，CGS）小组编成开源情报小组。

该小组有4到5个校译人员（其中2人为美国籍公民），以及源源不断的来自广播、电视和报纸的报告，通过分析每天能生产出一份带分析意见的情况汇总。该小组的办公设备由一台连接到当地和国际信号的电视、一台连接到非敏感互联网协议路由器网络的手提电脑、一台调幅调频收音机，以及每天10到15份的当天新闻报纸组成。此外，他们还准备了一台摄像录像机和数字视频播放器，用来研究不开放的宣传媒体和其它媒体。他们明白当地新闻报道对旅战斗队取得战役胜利的重要性，坚持对当地的重要新闻进行深入彻底的研究。他们的产品被旅战斗队战术行动中心的情报、监视与侦察组用以作进一步的分析研究，经旅战斗队的情报参谋官分发给营团级和师级单位。

——旅战斗队军情连连长，上尉

本手册可作为定义和描述美国陆军开源情报工作的媒介。陆军和其它情报机构都在努力整合及同步各指挥层级的开源情报工作，在本手册长达2年的使用周期里，所包含的战术、技术与程序将会不断完善。负责开源情报的国家情报总监助理建立了国家开源情报体系，这是一个看似分布式实则联合运作的部门，也是促进开源情报工作进一步完善的原因。

最终，美国情报界将对开源情报行动中的何人、何物、何地、何时、何事及为何等要素达成共识。这个共识将体现在未来的陆

军和联合情报条令文件中，以及在国家情报总监的指示——情报界第 301 号指令（国家开源情报中心发布）中，该指令将取代中央情报局主任第 1/7 号指令。

第二章 基本原则

开源情报行动是陆军情报行动必不可少的一部分，所有情报行动和情报产品都直接或间接地以公开可得信息为基础。公开可得信息的可获得性、深度和广度，可以让情报部门在无需动用特殊人力或技术的情况下，就能满足许多情报需求。开源情报通过提供经搜集和提炼的基础信息，能有效支援其他情报、监视与侦察（intelligence，surveillance，and reconnaissance，ISR）行动。作为综合情报的一部分，开源情报的运用和整合确保了决策者能够受益于所有可获得的信息。

一、定义

2006 财年《国防授权法案》（National Defense Authorization Act）中指出：“开源情报是指，为了响应特定的情报需求，通过搜集和利用公开可得信息而进行情报生产，并及时地分发给适当的受众群体”。在《陆军情报流程》中对开源情报进行如下描述：开源情报是为响应情报需求，对公开可得信息进行系统搜集、处理和分析而得出的有关信息。从这些补充定义中提到两个重要的术语：

• 公开来源（Open Source），是指提供信息的个人或群体，事先知道其提供的信息不涉及隐私，所包含的信息、关系是允许公开披露的。

• 公开可得信息（Publicly Available Information），是指用于公众消费的数据、事件、说明，或其他出版或广播的材料；普通公众成员可获得的；通过不经意的观察就能合法地看到或听到的；或者可以从一个向公众开放的会议中获得的。

二、开源情报门类

来源、信息和获取方式都无需特定的技术和人力资源，是开源情报区别于其他情报门类的主要特征（参见图 2 － 1）。公开来源广播、发行或以其他方式发布公共非保密信息，提供给公众使用。从这些媒介搜集公开可得信息的方式或技术是非侵入式的。其他情报门类则使用秘密来源或侵入式技术来获得私密信息。秘密来源和私密信息的定义如下：

• 秘密来源，是指提供信息的个人、群体或系统，事先知道其提供的信息、关系是禁止公开披露的。

• 私密信息，是指专门向特定的个人、群体或组织提供的数据、事件、说明，或其他材料。私密信息又包含两个子分类：保密信息和非保密受控信息。

• 保密信息只允许在被授权的范围内使用，而且在以文档或其他可阅读的形式传阅时，必须被标记其保密状态。

• 非保密受控信息是指因各种原因（比如敏感但非保密、仅限官方使用等）需要受控制或采取防护措施的信息，但不包括被列入密级的信息。

三、开源情报的特性

以下特性决定了公开可得信息与开源情报在陆军行动中扮演的角色。