基于暗网的反恐情报分析研究*

李 超[1] 周 瑛[2] 魏 星[1,3]

(1. 蚌埠医学院卫生管理系 蚌埠 233000;2. 安徽大学管理学院 合肥 230039;
3. 中南大学信息安全与大数据研究院 长沙 410083)

摘 要 [**目的/意义**]对暗网概念、特征、暗网反恐情报的意义及分析方法进行论述,为反恐情报研究引入新的内容和方法。[**方法/过程**]通过文献调研、内容分析等方法,在对国内外暗网反恐情报分析相关研究进行系统梳理的基础上,提出暗网反恐情报分析的流程,并设计暗网反恐情报分析平台架构,对主要分析方法、关键技术、分析工具及未来研究重点进行详细论述。[**结果/结论**]暗网反恐情报对支持反恐预警、控制恐怖舆论传播、为涉恐案件侦查提供线索及证据、指导反恐行动资源优化配置等方面具有重要意义;暗网反恐情报分析流程包括:恐怖组织特征识别、数据获取与信息过滤、机器学习与智能分析、人工分析与情报研判、情报生成与成果传递五个环节;暗网反恐情报"深度"分析、暗网反恐情报共享、公民网络隐私权保护将成为未来的研究热点。

关键词 暗网 反恐情报 情报分析 恐怖主义

中图分类号 G353.1 **文献标识码** A **文章编号** 1002-1965(2018)06-0010-10

引用格式 李 超,周 瑛,魏 星.基于暗网的反恐情报分析研究[J].情报杂志,2018,37(6):10-19.

DOI 10.3969/j.issn.1002-1965.2018.06.003

Research on Analysis of Counter-terrorism Intelligence Based on Dark Web

Li Chao[1] Zhou Ying[2] Wei Xing[1,3]

(1. Department of Health Management, Bengbu Medical College, Bengbu 233000;
2. School of Management, Anhui University, Hefei 230039;
3. Institute of Information Security and Big Data, Central South University, Changsha 410083)

Abstract [**Purpose/Significance**] This paper primarily discusses the concept, characteristics, significance and analysis methods of dark net counter-terrorism information, and introduces new contents and methods for counter-terrorism intelligence research. [**Method/Process**] Through literature research and content analysis, this paper illustrates the research status of dark net counter-terrorism information analysis, analysis processes, important methods, technologies, analysis tools, analysis platform and explains the future research focus. [**Result/Conclusion**] Dark net counter terrorism intelligence is of great significance for supporting the early warning of terrorism, controlling the spread of terrorist public opinion, providing clues and evidence for investigating terrorism related cases, and providing guidance for optimizing the allocation of resources for counter-terrorism operations. The dark net intelligence analysis process mainly includes: terroristic organization feature recognition, data acquisition and information filtering, machine learning and intelligence analysis, artificial analysis and intelligence determine, intelligence generation and achievement transfer. The deep analysis of counter terrorist intelligence in dark web, the sharing of counter-terrorism intelligence in dark network and the protection of privacy in civil network will become the hot research topic in the future.

Key words dark web counter-terrorism intelligence intelligence analysis terrorism

收稿日期:2018-03-05 修回日期:2018-04-09

基金项目:国家社会科学基金项目"大数据环境下情报研究方法论体系研究"(编号:15BTQ045);安徽省教育厅人文社会科学重点项目(编号:SK2017A0187)基金支持。

作者简介:李 超(ORCID:0000-0003-2225-0388),男,1979年生,硕士,讲师,研究方向:情报分析、信息安全;周 瑛(ORCID:0000-0003-0023-7764),女,1968年生,博士,教授,博士生导师,研究方向:信息检索、情报分析;魏 星(ORCID:0000-0002-8432-2546),男,1980年生,博士研究生,副教授,研究方向:数据分析、信息安全。

0　引　言

近年来,传统恐怖主义与网络相结合产生了网络恐怖主义,正在成为威胁我国国家政治、经济安全和社会稳定的重大问题之一。“东突组织”等恐怖集团,通过网络发布各种涉恐音视频,策划了一系列暴恐袭击事件。我国“国信办”于 2014 年 6 月曾指出:“互联网已成为东突恐怖活动主要传播工具”[1]。在第三届世界互联网大会反恐主题论坛中,相关专家强调“加强国际合作,共同打击网络恐怖主义”是全人类的共同使命[2]。随着各国政府反恐决心的不断坚定,网络恐怖活动逐渐呈现出行为隐蔽化、形式多样化、地域全球化的特点。互联网络中存在的“暗网”因具有隐蔽性、匿名性的特点,已成为极端组织传播暴恐思想,传授暴恐技术,招募恐怖分子,筹集活动资金,筹划恐怖活动的重要工具,“暗网反恐”也随之成为国际反恐斗争的新前线。目前,国内针对“暗网反恐”的相关研究较为缺乏,且多侧重于暗网恐怖主义概念介绍和应对措施的探讨,缺少从情报分析视角对暗网涉恐信息进行分析研判的相关研究。本文主要意义在于:首先,对“暗网”的概念、特征、暗网情报的来源、意义等相关内容进行介绍,为反恐情报研究引入新的内容;其次,提出暗网反恐情报分析的主要流程,对网络反恐情报分析工作起到一定的指导作用;再次,对暗网情报分析技术和工具进行了归纳,并设计基于暗网反恐情报分析平台架构,有利于提高暗网反恐情报的分析的效率;最后,对暗网反恐情报分析未来研究热点进行了展望,以期为新形势下网络反恐情报分析相关研究提供有价值的参考。

1　研究概况

1.1　**数据来源**　为了解该主题研究现状,本文通过对“Web of Science”“Spinger Link”和 Google 学术数据库,以“dark web Mining”“dark web analysis”进行主题检索,年限不限,检索时间截至 2017 年 12 月 31 日。经过数据清洗、筛选、剔除重复及与主题弱相关的文献,最终得到英文相关文献 255 篇。中文数据库选择 CNKI 中国学术期刊网,进行主题、关键词检索,共获得 6 篇与暗网情报挖掘相关的中文文献。

1.2　**数量分布**

1.2.1　时间分布　暗网反恐情报分析的相关研究最早始于 2005 年(有 7 篇文献),此后该主题的研究成果呈逐年增加趋势。本文对 2005-2017 年国内外暗网反恐情报分析研究文献变动情况以曲线图进行展示,以反映该领域的研究水平和发展速度,如图 1 所示。可见,随着数据挖掘和情报分析技术的不断发展,国际暗网反恐情报分析研究已逐渐成为学术界关注的热点,并且已经取得显著进步。

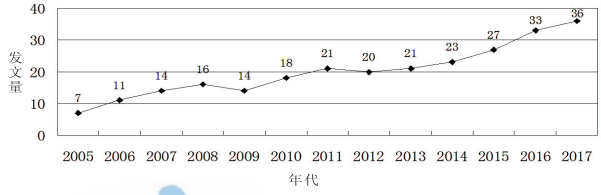

图 1　暗网反恐情报分析研究文献时间分布情况

1.2.2　国家地区分布　当前约有 25 个国家发表过暗网反恐情报分析相关论文,其中发文量超过 2 篇的国家或地区共 14 个:美国(105 篇)、英国(43 篇)、加拿大(22 篇)、中国(19 篇)、德国(12 篇)、印度(8 篇)、西班牙(8 篇)、以色列(8 篇)、爱尔兰(6 篇)、澳大利亚(6 篇)、瑞士(4 篇)、马来西亚(4 篇)、法国(3 篇)、意大利(2 篇)。可见暗网反恐情报分析研究已受到世界各国的普遍关注,但成果较为分散。其中美国发文量最多,远超过其他国家,亚利桑那大学的 Hsinchun Chen 博士研究团队中有多名成员是暗网反恐情报研究的核心作者。我国中国科学院自动化研究所的曾大军教授、国防科技大学的孙多勇教授和李国辉教授的团队也对暗网反恐情报挖掘进行了大量深入的研究。

1.3　**主题分类**　通过对题录数据进行统计分析,发现国内外暗网反恐情报分析领域研究热点主题包括:暗网的内涵(暗网概念、特点、原理、危害等)、暗网反恐情报收集途径(政府情报源、机构情报源、网络反恐数据库、内部情报源等);暗网反恐情报挖掘方法与分析技术(查询接口识别、链接发现、拓扑分析、情感分析、深度学习、社会网络分析、影响力分析、连通性分析、去匿名等);暗网反恐情报共享(情报共享的法律保障、共享模式、共享机制);暗网反恐的意义及策略等。

1.4　**重要文献**　随着暗网反恐情报研究的不断延伸和扩展,会形成学术影响力、创新性和价值均较高的高被引文献代表的核心文献集合,受到学术界普遍认同。本文列举国内外暗网反恐情报分析领域被引频次较高的 10 篇文献,以反映暗网反恐情报分析研究的基本动态,如表 1。

由表 1 可以看出,国外高被引文献均来自美国亚利桑那大学,排在首位的是 Ahmed Abbasi 于 2008 年发表的 *Sentiment Analysis in Multiple Languages: Feature Selection for Opinion Classification in Web Forums*, 共被引 793 次。作者采用情感分析方法通过文体和句法特征来对英语和阿拉伯语文本的情感表达进行分类。利用加权遗传算法并整合特征提取组件建立多国语言情感特征识别模型,并用美国及中东网络

论坛的文本数据和标准化的视频评价数据集进行了验证。

表1 国内外暗网反恐情报分析领域重要文献

序号	第一作者	所属机构	篇名	发表时间
1	Ahmed Abbasi	亚利桑那大学	*Sentiment analysis in multiple languages: Feature selection for opinion classification in web forums*[3]	2008
2	Hsinchun Chen	亚利桑那大学	*Crime data mining:A general framework and some examples*[4]	2004
3	Ahmed Abbasi	亚利桑那大学	*Applying authorship analysis to extremist group web forum messages*[5]	2005
4	Yilu Zhou	亚利桑那大学	*US domestic extremist groups on the Web: link and content analysis*[6]	2005
5	Hsinchun Chen	亚利桑那大学	*Uncovering the dark Web: A case study of Jihad on the Web*[7]	2008
6	曾大军	中国科学院	*Social Media Analytics and Intelligence*[8]	2010
7	李国辉	国防科技大学	一种基于颜色特征的图象检索方法[9]	1999
8	李国辉	国防科技大学	基于内容的音频检索:概念和方法[10]	2000
9	孙多勇	国防科技大学	*Study on covert networks of terroristic organizations based on text analysis*[11]	2011
10	孙多勇	国防科技大学	*Study on covert networks of terrorists based on interactive relationship hypothesis*[12]	2011

Hsinchun Chen是暗网反恐情报分析领域的核心作者,*Crime data mining:A general framework and some examples*是陈博士在2004年发表的一篇重要学术论文,被引用485次。作者对犯罪类型及其危害程度进行了详细划分,表明网络犯罪的危害性和影响力居于各种犯罪之首;之后,对犯罪数据挖掘技术的作用及其与犯罪类型之间的适用关系进行了详细论述;最后,建立了通用的犯罪数据挖掘框架,并通过案例进行了说明。

*Applying authorship analysis to extremist group web forum messages*是Ahmed Abbasi发表的另一篇高质量文献,将作者分析方法应用于极端主义团体网络论坛文本数据挖掘,被引用364次。作者在文中对写作风格分析、身份归属分析、阿拉伯语的特征识别等技术进行了介绍,建立阿拉伯语作者身份识别模型,并通过实证分析进行了验证。

Yilu Zhou在2005年发表的*US domestic extremist groups on the Web: link and content analysis*一文中,通过自动或半自动方法捕获美国国内极端组织网站数据,并应用链接分析和内容分析的方法,对恐怖组织网站结构、群体关系、组织结构进行了识别。

*Uncovering the dark Web: A case study of Jihad on the Web*是Hsinchun Chen于2008年发表的另一篇高被引文献,通过集成信息收集、分析和可视化技术,利用网络开源信息,对39个圣战网站的内容、关系和活动级别进行可视化分析,证明该方法能够为反恐决策提供有效的情报支持。

国内排名首位的重要文献是中国科学院自动化研究所的曾大军教授发表的*Social Media Analytics and Intelligence*一文,被引用279次。社交媒体分析作为暗网反恐情报研究的重要方法,已受到学术界的普遍关注。作者首先对社交媒体的概念、类型和作用进行了介绍,之后阐明了利用情报学方法和工具对社交媒体数据进行分析的目的,最后对社交媒体分析技术面临的挑战及社交媒体研究未来的发展方向进行了展望。

国防科技大学的李国辉教授,发表的《一种基于颜色特征的图象检索方法》和《基于内容的音频检索:概念和方法》两篇高被引论文,对多媒体数据的快速检索、获取和分析的关键技术进行了深入探讨。对涉恐图像、视频及声音数据快速检索数据库的建立、涉恐信息分析、恐怖分子行动追踪等方面有较高的指导意义。

此外,国防科技大学的孙多勇教授,通过文本分析法和关系分析法对恐怖组织隐藏网络进行研究并发表了两篇重要文献:*Study on covert networks of terroristic organizations based on text analysis*,*Study on covert networks of terrorists based on interactive relationship hypothesis*,为国内暗网反恐情报分析研究提供了新的方法。

总体来看,目前国内反恐研究领域对暗网情报分析的研究已取得一定的成果,但核心作者数量、技术先进性等方面与国外仍有差距。本文从理论角度对暗网反恐数据的研究热点、分析流程、重要方法、关键技术及相关工具等进行归纳和详细论述,以期促进我国暗网反恐情报分析工作更好的开展。

2 暗网的概念与特性

2.1 暗网的概念 “暗网”概念最早源于上世纪90年代,美国海军为保护船只通讯安全,启动了一项由代理服务器对数据加密传输的计划,旨在建立使用户在连接网络时身份信息不被泄露的系统。随后美国海军研究所的3位科学家在一篇题名为《隐藏路径信息》的论文中正式提出了“暗网”概念,指难以通过超链接方式进行访问,未被搜索引擎标引,只能采用动态请求方式获取信息的“不可见”网络。Tor官网对“暗网”的

定义是:无法通过公共网络访问,必须借助专用工具方能进入的网站[13]。Patrick Tucker[14]强调“暗网”是一种能够掩盖网络服务器地址和使用户匿名访问的方法。Raghavan[15]认为“暗网”是指无法利用超链接技术直接访问的各种网络数据库资源。维基百科[16]对“暗网”的定义是:仅能够通过特殊软件、配置或授权,并采用非标准的通信协议和端口才能访问的点对点或秘密网络。Bergman[17]认为,“暗网”是无法被普通搜索引擎索引的高质量数据集合,只能通过关键词查询方式进行访问。目前学术界普遍认为“暗网”可分为三种类型:以封包交换方式建立的 I2P 匿名网络,能实现网络浏览、交流、和文档的匿名传输;以分布式 P2P 技术为支持的 Tor 匿名网络,支持用户无痕迹访问;以自组织理论为基础的 firechat 网络,节点之间按照协同自组织方式完成特定任务,网络适应性较强。形成“暗网”的主要原因是,处于隐私保护原因人为设置访问限制,或技术人员未按照标准进行程序设计,造成部分网站无法被普通搜索引擎爬虫直接抓取。

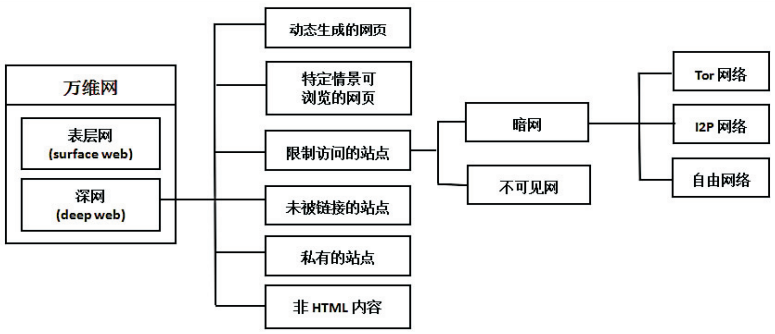

图 2　暗网与明网、深网、不可见网的关系

2.2　**暗网与相似概念辨析**　“暗网”与“明网”的区别。“明网”又称“表层网”(Surface Layers),是指能够通过公共计算机网络进行访问,利用普通浏览器或搜索引擎便可以检索并访问的网络站点或各种资源。明网数据量仅占互联网全部资源的 4% 左右,而暗网数据约占到 96% ,暗网体量较明网要大。

“暗网”与“深网”的区别。“深网”指不能用搜索引擎检索到的网络资源集合,主要分为以下几种:未被其它网页链接指向,从而无法被搜索引擎爬虫获取的孤岛网站;需人工注册才能访问的网络数据库;限制访问权限的站点;个人或公司的私有站点;特定情景下方可浏览的网页;由于搜索引擎的更新周期较长,造成无法同步实时更新的数据,如股票、飞机、天气等。即便是具有最强大搜索能力的 Google 和 Northern light 也只能检索到不超过所有网络信息的 0.03% 。暗网属于深网中“被限制访问站点”的一种,比深网的规模小。

“暗网”与“不可见网”的区别。“不可见网”由美国学者 Dr. JII Ellswath 于 1994 年提出,指网络中部分仅在被用户查询时才由服务器动态生成结果页面,从而难以被搜索引擎获取,无法直接索引和查询,但可被专用软件或人工方式搜索的网络数据库。不可见网虽与暗网同属于被限制访问的网站范畴,但其无论在范围还是数据体量上相比暗网都要小很多。“暗网”“明网”“深网”“不可见网”之间的关系如图 2 所示。

2.3　**暗网的主要特征**　a. 高度隐匿性。隐匿性作为暗网的核心特征之一,是指暗网通常难以被常规搜索引擎发现,用户需通过严格注册,以动态请求方式借助 Tor 浏览器等特定工具才能登录浏览。多节点、分布式的数据会在服务器构成的“保护层”进行加密,将客户端信息隐藏在“洋葱”路由的最深处,用户访问后不会留下完整的链接痕迹。网络服务提供商,执法部门都无法通过层层破解暗网加密体系,获取网络访问记录、服务器的具体位置、网站地址、用户身份、IP 地址等重要信息。因此,暗网常被军、商两界广泛使用作为数据保护、提升通信安全性、保护云服务使用者个人隐私的最佳方式。b. 交易便捷性。随着世界各国对现金和网络金融交易的管制日益严格,资金转移与积累受到金融体系的严密监管。暗网非法交易则采取以比特币(Bitcoin)、门罗币(Monero)、零币(Zcash)等虚拟货币作为匿名支付手段,并且支持与美元、欧元、人民币等主要货币进行兑换[18],资金收付双方信息均被加密隐藏,执法部门难以通过资金流向查询犯罪主体的个人信息[19]。c. 接入简便性。暗网接入虽有一定的技术要求但并不复杂,只需通过代理服务器进入外网,再简单安装“洋葱浏览器”,并经过设置便能够匿名访问网络资源。暗网开发小组甚至已在网络发布多款适用于手机终端的连接软件,以实现移动访问,且用户无需掌握任何网络基础知识[20]。d. 生态混乱性。据美国权威机构调查显示,暗网内容主要由:极端主义资讯、黑客资讯、非法色情、毒品贩卖、武器贩卖、人口拐卖、私人杀手、社交网络等不良信息组成,用户多为自由主义和无政府主义者,极端主义、拜金主义、自由主义思想严重。有学者[21]指出,暗网已成为犯罪和恐怖分子的“罪恶天堂”。

3　暗网反恐情报的意义

暗网反恐情报是以预防和打击网络恐怖主义活动为目的,而采集的特殊反恐信息资源,具有时效性、分散性、综合性、隐蔽性、弱关联性等特点[22]。暗网反恐情报的意义主要体现在下五个方面:a. 为反恐预警提

供情报支持。随着互联网时代的到来,暗网已成为恐怖组织进行人员招募、技术培训、极端思想灌输、恐怖活动策划的重要平台和快速、廉价、匿名的交流工具。而隐藏在暗网中的极端组织网站和论坛数据,对于网络反恐预警工作有着重要的价值。通过暗网情报分析,能够对即将发生的恐怖袭击或更大范围内长期可能存在的恐怖主义风险进行评估和预警。b. 对恐怖舆论传播进行控制。对网络恐怖舆论的控制,是暗网反恐情报又一重要意义。恐怖主义舆论借助暗网快速传播,宣传复仇思想、影响社会稳定,利用冲突性话题激化网民情绪、制造恐怖心理,采用涉恐音、视频资料吸引不法分子加入,造成极端主义思想的迅速蔓延。利用暗网情报分析方法和技术,能够有效挖掘暗网涉恐信息,形成反恐情报,对于及早发现涉恐舆论事件、切断暴恐信息源头,实行线上线下全面监控,制定切实可行的预案,通过公众互动阻断恐怖舆论的大范围传播具有十分重要的意义。c. 为涉恐案件侦查和诉讼提供线索及证据。暗网反恐情报能够为恐怖事件的侦查提供线索和突破口,促进当前案件的解决,并通过深入挖掘恐怖组织的关系网络的情况,预见未来潜在的风险。在恐怖分子被审判过程中,经证实并符合法律程序规定的反恐情报,能够作为有力的证据进入诉讼过程。d. 指导反恐行动资源优化配置。反恐行动资源优化配置是指恐怖事件发生前后,将各种要素资源合理配置到最关键的节点,以避免人员、设备、资金等的浪费,防止因资源不足而错失预防和应对恐怖事件的最佳时机。充分运用暗网反恐情报,开展危机管理和风险分析,有助于对薄弱环节和各种风险发生的可能性进行评估,有的放矢地进行资源配置。e. 开拓反恐情报研究新领域,为反恐情报分析工作带来新的方法和技术。虽然机器学习在暗网情报的分析过程中发挥着重要作用,但情报分析研判是一项复杂而系统的工作,信息技术无法取代专家的智慧和经验。只有在领域专家的指导下,采用正确的情报研究方法、研究思路、研究技术对暗网反恐情报进行深入分析,才能充分发挥暗网反恐情报的真正价值。

4 暗网反恐情报的来源

暗网反恐情报的来源主要分为以下四类:政府及专业情报机构、高等教育机构的研究中心、网络恐怖主义数据库、安全部门内部反恐情报。(1)政府及专业情报机构是暗网反恐情报的主要来源,包括:①美国的兰德公司,作为非营利性研究机构,曾多次对涉及国际关系、政治暴力、恐怖主义事件进行过及时和完整的报道。②位于荷兹利亚的国际反恐研究所(ICT),定期提供有关中东事件的报告、评论及多媒体信息,每次年度会议约有400-800人参加。③中东媒体研究所(MEMRI),总部位于华盛顿,在欧洲、日本和以色列设有分公司,定期对阿拉伯语、波斯语和土耳其语的新闻、视频、网站内容及伊斯兰改革者的观点进行翻译。④恐怖主义预防研究所(MIPT),是由美国国土安全局资助的非营利组织。自1995年联邦大厦爆炸案后,该研究所一直从事恐怖主义信息库的建立工作。⑤西蒙·维森塔尔中心,以记录大屠杀和种族灭绝证据为目的而成立,统计了大量极端主义和恐怖主义网站的快照和相关信息。⑥网络恐怖组织搜索公司(SITE),于2002年成立,是以恐怖分子活动监控为目的,并向媒体、政府和公司提供恐怖组织文件和媒体信息的盈利性组织。⑦美国政府资助的达特默斯安全技术研究所(IST),主要专注于网络安全、信任和网络恐怖主义的研究,并提供IT基础设施攻击的图像和视频取证,可信数字证书,以及信息基础设施风险评估等服务。(2)高等教育机构的研究中心,是暗网反恐情报分析的中坚力量,主要包括:①马里兰大学的大学联盟,对恐怖组织的形成和招募、动态、以及社会对待恐怖威胁和攻击的反应进行了广泛的研究,并提供开源、可搜索的全球恐怖主义信息数据库(GTD),包含自1970年以来世界各地发生恐怖事件的时间、地点和方式。②西点军校的反恐中心(CTC),从2003年以来一直为五角大楼和美国政府提供反恐战略分析。③圣安德鲁斯大学的反恐研究中心(CSTVP),从政治学角度对恐怖活动进行了分析,并提供远程反恐培训资源。④新加坡南洋理工大学的国际政治暴力和恐怖主义研究中心(ICPVTR),旨在进行恐怖主义研究、反恐培训和反恐宣传,以减少全球暴力恐怖事件的发生。其建立的"全球探路者系统"能够对亚太地区和大洋洲当前及未来的恐怖主义和政治暴力事件进行记录和预测。(3)网络恐怖主义数据库,是反恐情报的辅助来源,主要是由组织和个人自发参与监测,以防御可能出现的恐怖袭击,向反恐机构和人员提供与恐怖组织相关的情报为目的而建立的网络反恐数据库。(4)安全部门内部网络反恐情报,是公共安全部门通过秘密途径,由线人、卧底、内部情报平台、技术侦查等方式,获取有关网络恐怖主义活动轨迹、通信方式等的重要情报。该类情报源较为权威、准确、质量高,但由于资金耗费较高、且具有一定的危险性,大量获取较为困难。

5 暗网反恐情报分析

5.1 暗网反恐情报分析流程 暗网反恐情报分析是在反恐领域专家的指导下,由专业情报分析人员借助自动化信息分析工具,对多种渠道获取的恐怖组织信息进行识别、整合、清洗,并经过人工分析和研判,最

终形成对恐怖事件检测、预防和响应具有较高价值情报的活动。本文在参考相关文献和专家咨询的基础上,提出暗网反恐情报分析的流程,主要包括:恐怖组织特征识别、数据获取与信息过滤、机器学习与智能分析、人工分析与情报研判、情报生成与成果传递五个环节,如图 3 所示。

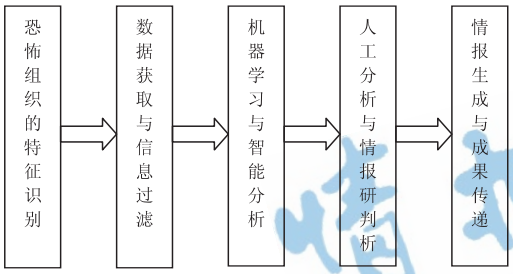

图 3　暗网反恐情报分析流程

a. 恐怖组织特征识别。作为暗网反恐情报采集的对象,恐怖组织特征识别是最为重要的环节之一。我国对恐怖组织认定标准[23]包括:采用暴力恐怖手段,从事危害国家、社会、人们群众生命财产安全的活动;有明确的领导和人员具体分工体系;从事恐怖活动基地建立、人员招募、恐怖分子培训;曾组织、策划或煽动过恐怖活动。有关恐怖分子特征识别的最新研究包括:2014 年美国国务院和美军中央总部发布的《反恐怖主义指南》中,从精神状态、视觉状态、身体动作等方面对恐怖分子识别特征进行了详细描述;以色列的 Faception 公司采用自动化人脸特征抽取方式成功实现对恐怖分子的精确识别;约旦 Mutah 大学的 Ahmad Hassanat 博士通过生物特征识别恐怖分子取得了较好的效果;英国《自然 · 人类行为》最新研究显示,恐怖分子的道德标准是“目的高于手段”等。首先,可参考政府机构、联合国安全理事会反恐委员会、恐怖主义研究中心等机构研究报告或中涉及的恐怖组织特征信息,以确定研究对象。由于近年来处于对恐怖活动侦破工作和防范打击等工作的需要,相关部门对涉恐数据的公开较为谨慎,此类数据的获得较为有限。因此,可将网络媒体披露的恐怖活动事件信息作为补充数据来源,通过文本挖掘等方式提取恐怖组织及其人物关系相关信息。其次,提取报告中记录的恐怖组织网址,或将恐怖组织名称、领导人名称、暗语、口号等作为关键词利用搜索引擎进行检索,通过出入链、反向链接分析等方法对涉恐网址进行扩充;最后,在反恐领域专家和语言专家的帮助下,进一步对结果进行增删,以获得较为全面的涉恐网站和论坛地址信息[24]。

b. 数据获取与信息过滤。涉恐网站常采用访问限制,动态验证等方式隐匿重要信息。因此,必须先申请极端主义网站或论坛的访问资格,以人工或自动方式填写表单,成为网站(论坛)注册会员;再将会员信息添加到本地 cookie 中,以利于爬虫软件读取并自动登录该网站[25];最后,设置网站或论坛登录参数,突破访问限制,实现选定内容的自动下载[26]。信息过滤是情报分析的基础,高质量的准确数据是情报质量的有效保障。应事先了解恐怖组织团体和支持者相关信息和当地术语、口号、符号及暗语,再通过半自动化方式对采集的信息进行筛选,并剔除无关的站点和内容(仅对恐怖主义活动进行报道而未涉及恐怖活动地点和时间的新闻、政府或宗教网站)。

c. 机器学习与智能分析。海量异构数据的处理以人工智能技术作为支持,能有效提高反恐情报分析的效率,为后续的人工分析、研判和最终结果的形成提供相应数据和决策支持。目前主流的暗网分析技术包括[27]:信息抽取、犯罪网络分析、链接内容分析、网络拓扑分析、情感分析、影响力分析、可视化分析、音视频分析、社会媒体分析、多维尺度分析、知识地图等。

d. 人工分析与情报研判。自动化分析工具仅能做到将海量数据缩小为有意义的集合,但无法真正实现对“反恐情报”本身的深度分析。因此,仍需邀请反恐领域专家,通过结构化问卷和规范化的程序,对机器学习的结果进行人工分析和评价,对恐怖组织能力、恐怖组织袭击动因、恐怖组织筹备迹象、恐怖组织活动环境、被侵害对象等重要内容再次进行鉴别和判断,以保证反恐情报的准确性和可靠性。分析与研判的具体过程包括:情报真伪分析、情报指向分析、情报转化分析、情报矫正分析等。

e. 情报生成与成果传递。是情报分析的结果和最终目标,主要包括:可视化的图像、统计分析报告、数据报表;用于取证、恐怖侦查、信息通报的共享情报;为政府、军队、武警和反恐研究机构提供用于反恐预警、恐怖舆论控制、应急响应的及时、准确、可靠的情报等。

5.2　暗网反恐情报分析方法和技术　暗网反恐情报分析工作的顺利开展离不开情报分析方法和技术的支持。引进和创新大数据环境下的情报分析方法和技术,并应用于暗网反恐情报分析,有利于提高新形势下反恐情报研究工作的质量和效率。本文通过文献调研和专家咨询方法,将适用于暗网反恐情报分析的主要方法和关键技术进行了归纳,如表 2 所示。

5.3　暗网反恐情报分析工具　暗网的隐蔽性和数据的庞大而复杂性,决定了其作为反恐情报的巨大价值却难以轻易获取的特性,功能强大的分析软件和“特殊”搜索引擎的开发便成为了各国反恐研究领域关注的焦点。①Analysis Notebook 是美国海湾战争中曾使用过的一款能够有效应用于反恐情报分析的软件。该软件能够集中各种复杂无序的数据并进行关联分析,通过对嫌疑人的通信记录、社会关系、网络邮箱、

表2 暗网反恐情报分析方法和技术

分析方法和技术	描述
信息抽取[28]	以结构化方式表示涉恐文本中选择的内容,并进行格式转化和存储
犯罪网络分析[29]	应用社会网络分析方法,研究犯罪组织网络的特征、结构及其运作模式
时空数据挖掘[30]	通过时空数据关联分析,对恐怖事件的属性特征、内在关联性及发展趋势进行预测
碰撞比对[31]	将需要关注的特定对象、事件的重要特征与数据库中的信息进行关联比对,以实现高危预警、动态监控等功能
身份识别[32]	利用多变量统计分析、神经网络、支持向量机、决策树等方法确认嫌疑人身份
网络拓扑分析[33]	对恐怖组织网络结构进行统计特性分析,以揭示其主要特性
情感分析[34]	通过识别和分析文本中包含的观点、情感、影响及偏见,以发现和预测极端分子的行为
跨语言检索[35]	搜索来自多种语言,与关键词有关的涉恐信息,解决反恐情报分析中语言障碍问题
可视化分析[36]	对抽象数据进行分析和提取,形成形象化的可视化结果,以发现恐怖活动的规律
社会媒体分析[37]	分析恐怖组织利用社交媒体开展暴恐活动的路径和行为模式,以遏制恐怖主义泛滥
深度挖掘[38]	利用语音识别、人脸识别、图像识别等技术,将嫌疑人信息与数据库进行比对,及时发现恐怖分子行踪
影响力分析[39]	分析极端主义活动和思想的宣传对人们认知和决策方面造成的影响程度
音、视频分析[40]	通过暴恐音视频内容解析以了解恐怖分子训练、宣传方式,以阻断暴恐视频的传播、追踪恐怖分子的行动
分词技术[41]	将非结构化情报数据,按照线索的属性特征分解为结构化数据
社会计算[42]	通过模拟恐怖分子的活动、对恐怖组织运行和发展的规律及其趋势进行预测
GIS 犯罪制图[43]	将恐怖分子犯罪数据与地理信息相结合,寻找犯罪热点,干预、预防和抑制恐怖主义活动
深网爬虫[44]	通过对深网数据进行收集和分析,获取普通搜索引擎无法访问的信息
人物画像[45]	通过嫌疑人作案手段、时间等特征来描述其心理、生理、行为特征以辅助锁定罪犯
活动热力图	以高亮点的形式显示恐怖活动高发及恐怖分子所在的地理区域,以利于反恐资源合理分配
人群分布图	对恐怖分子的数量和地区分布进行图示,以分析恐怖组织分布、密度和变化趋势
出行轨迹分析[46]	利用 GIS 技术和时空数据模型对恐怖分子出行位置信息进行实时分析,以利于对恐怖分子进行监控
活动规律分析	采用人工智能技术,对恐怖分子活动规律进行分析和预测,以利于恐怖事件预警
群体特征分析	通过分析恐怖组织的心理特征、情感特征、思维方式等,辅助对恐怖分子的识别
信息融合[47]	将不同来源、结构、特点的反恐数据进行逻辑集中,以利于反恐情报智能分析
内容分析[48]	通过对特定网站和论坛信息进行收集和检测,判断是否含有极端主义相关内容
多维分析[49]	通过对数据进行多角度、多侧面的深度观察及关联分析,提升情报研判的准确性
连通性分析[50]	分析恐怖组织关键节点,以减小恐怖组织耦合性、自组织性和重塑性
频率分析	对需要重点管控的某一要素特征出现的次数,进行排序、筛选,以发现可疑事件
去匿名技术[51]	利用暗网技术漏洞,采用主动或被动方式,获取匿名通信双方的真实信息

交易信息等关键数据与数据库进行比对,形成数据关系网和可视化分析图表,为情报分析人员提供决策支持。②Memex 源于美国国防部高级研究项目局(DARPA)于2015年4月正式宣布开发的 MEMEX 项目。该软件是一款以打击恐怖主义犯罪为目的而研发的暗网搜索引擎,基于开源数字可视化搜索和分析技术,能够按照用户的要求对相关内容进行抓取,并进行复杂的计算和数据分析,从而有效识别在线数据中的模式和关系,捕获隐藏在暗网中的网站。通过时空数据构建数据图和可视化分析,以及图像模糊匹配定位技术,能够辅助执法人员跟踪非法活动,并迅速对嫌犯实施抓捕。③美国联邦调查局于2015年2月开发的网络监测工具(NIT),能够单次搜索到1300个暗网地址,成功识别和破解"洋葱路由"的加密机制,并找到真实的暗网用户信息。④我国百度公司于2008年12月启动的"阿拉丁计划",旨在开发一款能够自动对暗网数据进行深度检索的搜索引擎,目前已取得重大突破。⑤沃民高新科技(北京)公司自主研发的暗网数据实时监测与智能分析系统,采用态势感知、情绪分析、节点分析等技术,具有自动建立网络隧道方式获取暗网数据,对恐怖事件进行跟踪溯源、分析和预警,并提供热词排名和查询等功能。⑥Matchlight 是 Terbium 实验室发布的暗网分析软件,能够实现在数据泄露的第一时间向用户发送预警报告。IBM、LifeLock 等知名大型公司均在使用该系统,以减少数据失窃带来的损失。⑦ONION. CITY 搜索引擎,是一款面向普通网络用户的暗网深度挖掘工具,采用 Tor2web 代理技术和 Google 的 API 接口,无需 Tor 类软件的支持便能够实现对暗网数据进行搜索和访问,目前大约能检索到超过35万个暗网网页。⑧Pipl 是专为搜索特定人物信息而开发的暗网搜索引擎,能从搜索到的数据库中提取联系方式、成员目录、法院记录、用户名、邮箱地址、电话号码等个人信息,并通过高级语言分析和排名对最匹配的结果进行展示。⑨Yippy 是一款多搜索引擎信息集成平台,能够将不同搜索引擎获取的数据进行融合并统计分析。⑩Not Evil(Tor Search)是一款非营利性暗网信息专用搜索引擎,被誉为暗网中的谷歌。开发小组通过长期对搜索算法持续更新,使搜索效果一直处于领先地位。⑪计算机和互联网协议地址验证器(CIPAV)是美国联邦调查局与2002年开发的代理服务器识别工具,通过定位网络罪犯、黑客的位置,识别隐藏的嫌疑人。

5.4　**暗网反恐情报分析平台**　暗网反恐情报分析平台是基于大数据技术的集成分析系统,主要由数据层、平台层、分析层和应用层组成。本文在参考国外相关资料的基础上,结合专家咨询方式,绘制暗网反恐情报分析平台架构,主要包括:资源层、平台层、分析层和应用层,如图4所示。

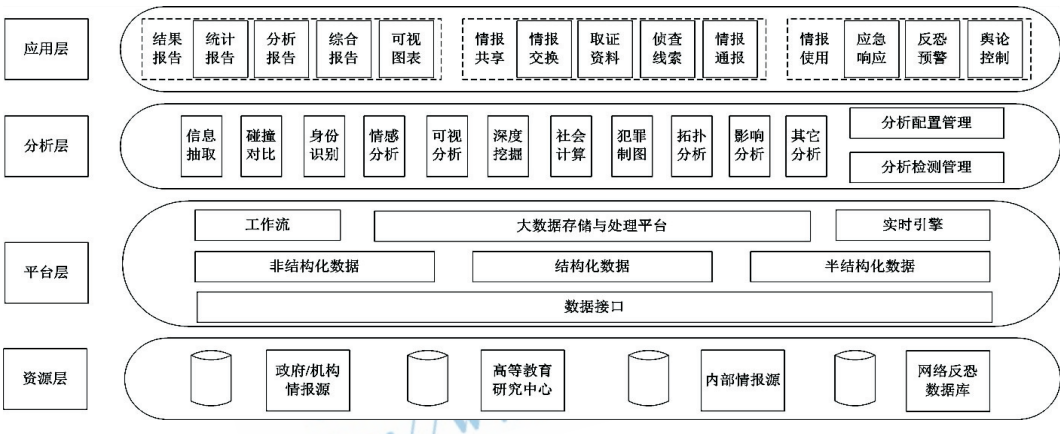

图4　暗网反恐情报分析平台架构

a.资源层。是暗网反恐情报分析平台的最底层,为系统运行提供必须的硬件设备、操作系统、应用软件等基础设施和通过政府及专业情报机构、高等教育机构的研究中心、网络恐怖主义数据库及安全部门内部渠道获取的数据资源,是暗网反恐情报分析的重要保障。只有来源广泛,准确、及时、全面的数据,才能对暗网反恐情报的分析、研判、预测及监控起到重要的支撑作用。b.平台层。主要功能是:为系统的构建和运行提供支撑,通过面向数据源的数据接口,实现多源异构数据的融合、清洗、支持大数据的高可扩展存储,为反恐情报的半自动分析提供精准而有效的数据。大数据环境下海量、低价值密度且结构复杂的数据,只有经过格式转换,归并整理后,才能汇聚成面向多种应用的统一数据集合。c.分析层。采用自动化工具对数据进行初步分类和分析,结合反恐领域专家人工判别方式对反恐情报的真实性、准确性和有效性进行判断,并剔除错误和冗余信息,形成有价值的网络反恐情报。d.应用层。情报产品是情报分析人员智慧和经验的结晶,而反恐情报最终能够服务于警务活动才是反恐情报分析的目的所在。应用层的作用是以具体业务实现为目的,为人机交互提供支持。包括:以可视化方式自动产生与恐怖组织网络特征、活动规律等相关的反恐情报统计报告、分析报告、综合报告;实现与公安、军队、武警等国家安全保障和反恐部门的情报共享,为恐怖案件的侦查、取证和情报通报提供支持,为网络反恐预警工作和恐怖主义舆论的发现和控制及时提供重要情报。

6　未来研究重点

6.1　**暗网反恐情报"深度"分析**　随着"暗网"逐渐成为恐怖组织和极端分子宣传仇恨、暴力思想的工具和快速、匿名的交流方式,暗网恐怖主义已成为国家政治稳定、经济安全、社会安定的重大威胁。随着大数据时代的到来,海量异构数据的处理,使得传统的情报分析方法和技术已难以应对新形势下暗网反恐情报分析的需求。而既精通反恐情报分析相关理论,又熟悉宗教和多国语言知识,并且能够熟练运用大数据环境下反恐情报分析工具的高端综合型人才严重不足,也对暗网反恐情报分析工作造成了不利影响。因此,如何引进和创新大数据环境下暗网反恐情报分析方法和技术,加强网络反恐情报分析人才的培养,在紧紧依托信息技术的基础上,充分发挥人的经验和智慧,"深度"挖掘暗网反恐情报的真正价值,将成为暗网反恐情报分析未来的研究重点。

6.2　**暗网反恐情报国际共享**　当前暗网恐怖主义活动已呈现国际化发展趋势,单个国家或部门难以拥有足够的信息以防范和打击恐怖分子,暗网恐怖主义的国际协同治理是新形势下网络反恐工作的主流趋势。然而"棱镜门"事件的曝光加剧了世界各国对数据跨境流动的限制,各国政府都在不同程度地加强对本国反恐数据主权的保护。如美国在《网络信息安全共享法案》中明确要求美国公民数据归美国政府管辖;俄罗斯和巴西政府同样也提出本国公民信息不得在境外存储的规定。各反恐机构之间,由于运行平台、数据标准、信息传输格式等不尽一致,也同样造成了数据共享和交换的困难。此外,激励机制、协调机制的缺乏,也是限制暗网反恐情报共享的重要原因。因此,如何完善反恐情报共享的标准规范,建立情报共享的长效激励机制,强化情报共享的技术支撑条件,通过政策、法律手段,促进暗网反恐情报的国际共享,将成为未来关注的重要内容。

6.3　**公民网络隐私权保护**　随着公民权利意识的增强,网络隐私权作为自然人在网络上拥有个人隐私、私人活动、私密空间不受非法侵犯、知悉、利用的人格

权逐渐受到重视。采用暗网分析工具虽然能够实现大量网络信息的采集和分析,但难免会涉及到公民的个人隐私。2009 年美国国土安全局提出的“爱因斯坦计划”(EINSTEIN),引起了美国国内隐私保护机构和民权主义者的反对。2013 年 11 月联合国人权理事会通过一项由巴西和德国联合发起的保护公民网络隐私权的决议,旨在要求各国政府结束大规模监控行为。2017 年 3 月美国国会众议院以投票方式,将 2016 年 10 月由美国联邦通信委员会提出,旨在保护公民“健康信息”“准确定位”“浏览记录”“社会安全号码”等隐私信息的《互联网隐私法案》进行废除,允许网络服务商任意收集用户敏感信息,再次引发网络权益倡导者的声讨。我国目前尚无专门针对公民网络隐私权保护的法律规定,也未形成完备、周全的网络隐私权保护方案[52]。因此,如何加强暗网情报的管控和公民网络隐私权保护也将是未来研究的热点。

7 结论与展望

暗网反恐情报在有效预测恐怖组织活动的动向,控制恐怖舆论的传播,为涉恐案件的侦查提供重要线索和突破口,指导反恐行动资源优化配置等方面起到至关重要的作用;同时也开拓了反恐情报研究的新领域,为反恐情报分析工作带来了新的方法和技术。本文通过文献调研、专家咨询等方法,提出暗网反恐情报分析的流程,设计暗网反恐情报分析平台的架构,在详细论述暗网情报分析主要技术和相关工具的基础上,对暗网反恐情报未来的研究重点进行了展望。本研究不足之处在于,仅对暗网反恐情报分析平台架构进行了理论研究,并未对系统具体功能模块进行详细设计和实现,该内容将在后续研究中进一步探讨。

参 考 文 献

[1] 国信办:互联网已成恐怖势力活动主要工具须坚决打击[EB/OL].[2014-06-24].http://news.cri.cn/gb/42071/2014/06/24/7551s45890 63.htm.

[2] 网络反恐论坛举行加强国际交流合作打击网络恐怖主义[EB/OL].[2016-11-18].http://www.cac.gov.cn /2016-11/18/c_1119943188.htm.

[3] Ahmed Abbasi. Sentiment analysis in multiple languages: Feature selection for opinion classification in web forums[J]. ACM Transactions on Information Systems,2008,26(3):45-50.

[4] Chen H,Chung W,Xu J J,et al. Crime data mining:A general framework and some examples[J]. Computer,2004,37(4):50-56.

[5] Abbasi A,Chen H. Applying authorship analysis to extremist group web forum messages[J]. IEEE Intelligent Systems,2005,20(5):67-75.

[6] Zhou Y,Reid E,Qin J,et al. US domestic extremist groups on the Web: link and content analysis[J]. IEEE Intelligent Systems,2005,20(5):44-51.

[7] Chen H,Chung W, Qin J,et al. Uncovering the dark web: A case study of Jihad on the web[J]. Journal of The Association for Information Science and technology,2008,59(8):1347-1359.

[8] Zeng D,Chen H C,Lusch R,et al. Social media analytics and intelligence[J]. IEEE Intelligent Systems,2010,25(6):13-16.

[9] 李国辉,柳伟曹,莉 华. 一种基于颜色特征的图象检索方法[J]. 中国图象图形学报, 1999(3):248-251.

[10] 李国辉,李恒峰. 基于内容的音频检索:概念和方法[J]. 小型微型计算机系统,2000(11):1173-1177.

[11] S Duo-Yong, G Shu-Quan, Z Hai. Study on covert networks of terroristic organizations based on text analysis[J]. Intelligence and Security Informatics,2011(7):373-378.

[12] S Duo-Yong, G Shu-Quan, L Ben-Xian. Study on covert networks of terrorists based on interactive relationship hypothesis[J]. Intelligence and Security Informatics,2011(7):26-30.

[13] How big is the dark web[EB/OL].[2016-04-02]. https://trac.torproject.org/ projects/tor/ wiki/doc/How Big Is The Dark Web.

[14] Tucker P. How the military will fight ISIS on the dark web[EB/OL].[2016-04-02]. http://www.defenseone.com/technology/2015/02/how-military-will-fight-isis-dark-web/105948/.

[15] Raghavan S, Garcia-molina H. Crawling the hidden Web[EB/OL].[2015-08-12]. http://ilpubs.stanford.edu:8090/456/1/2000-36.pdf.

[16] https://en.wikipedia.org/wiki/Dark_web.

[17] BergM K. The dark web:Surfacing hidden value[J]. Journal of Electronic Publishing, 2005,7(1):8912-8914.

[18] Kirkpatrick,Keith. Financing the dark web[J]. Communications of the ACM, 2017,60(3): 21-22.

[19] Daniel Moore,Thomas Rid. Cryptopolitik and the darknet[J]. Survival Global Politics&Strategy,2016,58(1) : 7-38.

[20] Weimann, Gabriel. Going dark:Terrorism on the dark web[J]. Studies in Conflict and Terrorism,2016,39(3):195-206.

[21] 罪恶的天堂? 带你了解搜索不到的暗网[EB/OL].[2014-12-31]. http://oa.zol.com.cn /494 /4945765_ all. html.

[22] 章小童,阮建海. 国内反恐情报研究结构特征与研究热点分析[J]. 情报杂志, 2016,35(8):31-34.

[23] “东突”犯下累累罪行 反恐,我们别无选择[EB/OL]. http://news.163.com /2003w12/12401 /2003w12_1071526170835.html.

[24] Li Yang, Feiqiong Liu. Discovering topics from dark websites. In Computational Intelligence in Cyber Security[C]. CICS ´09 IEEE Conference,2009(9):175-179.

[25] Zhou Y,Reid E,Qin J,et al. US domestic extremist groups on the web:Link and content analysis[J]. IEEE Intelligent Systems, 2005, 20(5): 44-51.

[26] Fu A Abbasi,Chen H. A focused crawler for dark web forums[J]. Journal of the American Society for Information Science and Technology,2010, 61:1213-1231.

[27] Bergholz A, Chidlovskii B. Crawling for domain-specific hidden web resources[J]. Conference on Web Information Systems Engineering,2003:125-133.

[28] 孟　玺,周西平,吴绍忠. 语义分析在反恐研究领域的应用研究[J]. 情报杂志,2017,36(3):12-17.

[29] Xu J,Chen H. Criminal network analysis and visualization[J]. Communications of the ACM,2005,48(6):100-107.

[30] Chung W, Chen H, Chaboya L G,et al. Evaluating event visualization:A usability study of COPLINK spatio-temporal visualizer [J]. International Journal of Human-Computer Studies,2005,62(1):127-157.

[31] 努尔麦麦提·尤鲁瓦斯,等. 跨语言声学模型在维吾尔语语音识别中的应用[J]. 清华大学学报(自然科学版),2018(2):1-5.

[32] Zheng R, Qin Y, Huang Z, et al. Authorship analysis in cybercrime investigation[C]. In Proceedings of the first NSF/NIJ Symposium, ISI 2003, Tucson, AZ, USA.

[33] Steve Ressler. Social network analysis as an approach to combat terrorism:Past,present, and future research[J]. Homeland Security Affairs,2006,2(2):529-535

[34] Daniel Graziotin, Miikka Kuutila. The evolution of sentiment analysis-A review of research topics, venues, and top cited papers[J]. Computer Science Review,2018, 27: 16-32.

[35] Gina-Anne Levow. Dictionary-based techniques for cross-language information retrieval[J]. Information Processing & Management,2005,41(3):523-547.

[36] Zhu B,Chen H. Chapter 4: Information visualization[J]. In B. Cronin (Ed.), Annual Review of Information Science and Technology,2005,39: 139-177.

[37] Wu He,Shenghua Zha,Ling Li. Social media competitive analysis and text mining: A case study in the pizza industry[J]. International Journal of Information Management. 2013,33(3): 464-472.

[38] Popp R, Armour T, Senator T, et al. Countering terrorism through information technology[J]. Communications of the ACM,2004,47(3):36-43.

[39] Bunt G R. Islam in the digital age: E-jihad, online fatwas and cyber islamic environments[M]. Pluto Press,London,2003.

[40] Fischer S, Lienhart R, Effelsberg W. Automatic recognition of film genres[J]. Proceedings of the 3rd ACM International Conference on Multimedia,1995:295-304.

[41] Nabila Shahid,Muhammad U. Word cloud segmentation for simplified exploration of trending topics on Twitter[C]. London:Institution of Engineering and Technology Press,2017:214-220.

[42] Zeng, Daniel,et al. Social computing[J]. IEEE Intelligent Systems,2007,22(5):20-22.

[43] Ourania Kounadi. Crime mapping on-line: Public perception of privacy issues[J]. European Journal on Criminal Policy and Research,2015,21(1):167-190.

[44] Pant, P Srinivasan. Learning to crawl:Comparing classification schemes[J]. ACM Transactions on Information Systems ,2005, 23(4), 430-462.

[45] Dianne Cyr, Milena Head. Exploring human images in website design: A multi-method approach[J]. MIS Quarterly,2009,33(3):539-566.

[46] 张治华. 基于 GPS 轨迹的出行信息提取研究[D]. 上海:华东师范大学,2010.

[47] Shanchieh J. Yang. High level information fusion for tracking and projection of multistage cyber attacks[J]. Information Fusion, 2009,10(1):107-121.

[48] Zhou Y,Reid E,Qin J,et al. U. S. Domestic extremist groups on the web: Link and content analysis, IEEE intelligent systems [J]. Special Issue on Artificial Intelligence for National and Homeland Security, 2005,9:44-51.

[49] Zhang Yong-chao. The research on the critical technology of darknet resource mining[D]. Xi'an:Xidian University,2013.

[50] Chen H. Interaction coherence analysis for dark web forums[C]. In Proceedings of the 2007 IEEE Intelligence and Security Informatics Conference[A]. New Brunswick, NJ, 2007:342-349.

[51] Marc-Olivier Killijian. De-anonymization attack on geolocated data[J]. Journal of Computer and System Sciences, 2014, 80(8):1597-1614.

[52] 韩学志,孙义清. 论网络隐私权的法律保护[J]. 情报杂志,2002(12):19-21.

(责编:贺小利;校对:王平军)