DOI:10.12154/j.qbzlgz.2021.05.004

欺骗性信息:研究进展与展望

王海霞[1,2] （[1]中国人民公安大学国家安全学院 北京 100038； [2]福建警察学院 福州 350007）

摘 要:[目的/意义]欺骗性信息(disinformation)是信息制造者或传播者基于政治或经济动机,以欺骗、误导为目的,蓄意传播的虚假信息。国外围绕欺骗性信息做了大量理论研究,梳理欺骗性信息研究进展,了解、跟踪国际学术动态,有助于我国学术界掌握学术话语权,为把握复杂多变的信息安全局势提供参考和借鉴。**[方法/过程]**通过系统查阅文献及网络调研发现,欺骗性信息源于冷战时期的对敌情报实践;后逐步进入学术视野,融入多学科的研究方法和理论;近年来,受2016年美国大选风波和2019年新冠肺炎疫情的影响,在社交媒体环境中引起广泛讨论。**[结果/结论]**经过对研究进展的总结可以断言,欺骗性信息研究将成为学术研究的热点以及学术发展的方向。

关键词: 欺骗性信息 研究进展 研究趋势

Disinformation: Research Progress and Prospects

Wang Haixia[1,2] ([1] People's Public Security University of China, Beijing, 100038;
[2]Fujian Police College, Fuzhou, 350007)

Abstract: [Purpose/significance] Disinformation is a type of false information that information makers or disseminators intentionally spread based on political or economic motives with the purpose of deception and misleading. A great deal of theoretical research has been made on disinformation abroad. Sorting out the research progress of disinformation and tracking the international academic trends is helpful for domestic research community to master the academic discourse power and can provide reference for understanding the complex and changeable information security situation. **[Method/process]** Through systematic literature review and network survey, we found that disinformation is the result of enemy intelligence practice in the cold war. Then it goes into the academic horizon gradually, and integrated with multidisciplinary research methods and theories. In recent years, affected by the 2016 US election crisis and the COVID-19 epidemic, disinformation has been widely discussed in the social media environment. **[Result/conclusion]** By summarizing the research progress, it can be asserted that the research of disinformation will become a hot topic and trend of future research.

Keywords: disinformation research progress research trend

随着社交网络媒体的发展,信息过载、信息迷雾现象日益突出,人为制造的各种虚假信息在经济、政治利益的诱导下接踵而来。如何识别和应对网络环境中泛滥的虚假信息成为学者们争相探讨的热点话题。

目前,国外学术界已经不局限于假新闻、谣言等错误的、不真实的虚假信息的研究,提出了"disinformation"(本文译为欺骗性信息)的概念,并将它与虚假信息区分开来。欺骗性信息是信息制造者或传播者基于政治或经济动机,以欺骗、误导为目的,蓄意传播的虚假信息。欺骗性信息具有蓄意性、误导性、操纵性,以获取利益和制造损害为目的。在日常生活中,它是造成信息迷雾的最主要原因以及干扰决策者决策的信息噪音;在国家安全与国际竞争领域,它被视为信息战中的弹药[1],对敌斗争中的有力武器,战略欺骗中的有效

手段，隐蔽行动的重要组成部分以及推行外交政策的秘密工具。

国外政府部门和学术界将欺骗性信息视为干预国家政治和经济发展、影响国家安全和社会稳定的一个重要因素，因而围绕它开展实践探索和理论研究。例如，美国将包括欺骗性信息传播在内的信息失序状态归之为导致国家政治瘫痪的“真相崩塌”（truth decay）[2]，欧洲一些国家甚至把欺骗性信息列为混合战争中混合威胁（hybrid threats）的关键组成部分[3]。有学者提出欺骗性信息作为影响行动的核心要素，在改变目标国的公众认知和行为，制造社会愤怒感和对政府的不信任感，削弱社会凝聚力等方面将产生严重的安全威胁[4]。还有研究发现，在社交网络媒体环境中，由计算机脚本控制的社交媒体账户可以被蓄意、系统性地利用来传播政治欺骗性信息，进而操纵和改变公众舆论与认知[5]。牛津大学网络研究所公布的2020年欺骗性信息产业化研究报告指出，当前全球有组织的社交媒体操纵盛行，有81个国家使用社交媒体传播计算宣传和政治欺骗性信息，进而操纵公众认知和公共舆论方向[6]。目前，在我国政府和社会组织层面，对欺骗性信息的蓄意误导性、政治危害性等关注不多。在学术界，仅有少数研究成果也仅探讨了欺骗性信息对个体或组织层面的欺骗和影响，一些文献将欺骗性信息与谣言、舆情混为一谈，并未将它提升到国家安全、社会稳定、国际竞争与对抗的层面开展研究。据此，了解与跟踪国外欺骗性信息研究现状和发展脉络，有助于把握国外研究动态和趋势，拓展我国信息科学、国家安全学、情报学、国际关系学等相关学科的研究内容与学科视野，为政府和社会组织防范欺骗性信息提供参考与借鉴。

1 欺骗性信息的兴起：冷战时期对敌情报实践

欺骗性信息源于冷战时期苏联的对敌情报实践，后经信息哲学领域学者的研究，融入了多学科的研究方法和理论，逐步进入学术视野并确立起自己独立的研究对象和领域。欺骗性信息的大规模研究是近几年随着社交网络媒体的普及才逐步兴起的，受2016年美国大选风波和2019年新冠肺炎疫情的影响，引发了大量对欺骗性信息治理、应对、原因与传播规律等相关问题的研究成果。

欺骗性信息是冷战时期苏联情报机构克格勃（KGB）经常使用的一个术语，原词为дезинформация（音译为“dezinformacija”），指通过编造谎言、捏造事实、散布混淆视听的信息等手段，攻击其他国家，干涉别国内政，从而塑造于己有利的战略态势[7]。它主要包括两种类型，一种是意图误导政府领导人和决策者的欺骗性信息；另一种是旨在影响公众舆论的欺骗性信息。前者可以影响后者，后者又反过来有助于执行“国家任务”[8]。美国中央情报局将欺骗性信息列为苏联对外采取的“积极措施”（active measures），也称“隐蔽行动”（covert action）或“影响活动”（influence activities）的重要组成部分。他们认为苏联的积极措施是一系列影响外国政府行为、事件和环境的实践活动，如书面和口头的欺骗性信息、伪造和虚假的谣言、灰色和黑色宣传等[9]，其中欺骗性信息是排在第一位的。可见，欺骗性信息源于冷战时期美苏两国对抗形势下所产生和使用的信息对抗手段，是政治斗争实践中的产物，是战略情报机构对外行动的主要职能。

冷战时期，欺骗性信息的研究刚刚起步，集中于一些新闻报道、简报和短文，主要对克格勃使用欺骗性信息作为冷战时期对付美国的一种斗争武器进行描述和讨论。例如，总结与回顾苏联针对美国的各种欺骗性信息运动[10]；梳理与描述苏联开展的一系列欺骗性信息活动内容和手段[11]；剖析与解读欺骗性信息手段作为战争武器使用的情况[7]。这一阶段的文献还不能称之为严格意义上的学术研究，主要描述或报道欺骗性信息相关事件、案件，学理性不强，且篇幅较短，未对欺骗性信息的概念、内涵及特征等理论问题开展系统、深入的研究。

冷战结束后相当一段时间，关于欺骗性信息的研究成为少有人关注的领域，这些文献多采用孤立的历史分析和案例研究的方法，讨论和概括冷战期间欺骗性信息的使用与发展情况。例如，从历史学角度对车臣共和国存在的欺骗性信息进行调查与解析[12]；披露克格勃使用艾滋病[13]、细菌战等欺骗性信息开展活动的案例[14]。此类研究成果较为分散，未形成一定的研究规模与固定的研究学者群，多数仅停留于欺骗性信息实施活动的现象描述，缺乏对这类实践活动的系统性总结、提炼与理论升华。

2 欺骗性信息研究对象的确立：21世纪前后信息哲学视角的学理性分析

在欺骗性信息进入社会科学研究者的视野之前，学界主要关注由认知心理学家提出来的，与欺骗性信

息相近的一个概念——“misinformation”(本文译为错误信息)。20世纪末,各国对国际安全的关注点逐步由传统安全转向非传统安全。欺骗性信息作为非传统安全中的一个要素,人们对它的关注也逐步从实践领域延伸至学术领域。信息哲学界的一些学者率先关注到了欺骗性信息这一特殊信息类型,并将其与错误信息区别开来,进行了单独、系统的学理性研究,形成了诸如Luciano Floridi、James H. Fetzer、Don Fallis等固定的研究学者群。他们主要集中于阐述欺骗性信息的概念、特征和范围,重点探讨欺骗性信息是什么这一本质性问题,从而奠定了欺骗性信息研究的理论基础。

著名的信息哲学家Floridi是较早开展这一研究的代表性学者。他曾于1996年提出“只要信息处理的过程有缺陷,就会产生欺骗性信息”[15]这一论断,描述了欺骗性信息的产生过程,但未对欺骗性信息的主体意识、目的、结果等进行限定。2005年,他对这一说法进行了修正,加入了欺骗性信息制造和传播者的主观意识的限定,提出“当信息的语义内容错误时它是错误信息,而当传播错误信息的人知道该信息的性质时则为欺骗性信息”[16]。这一定义弥补了之前表述的不足。相对于之前的定义有了一定的限缩,但仍未描述欺骗性信息的欺骗意图和目的。而且,即使信息传播者和信息接收者主观上认识到被传播的信息性质为错误信息,也并不一定是为了欺骗的目的,也并不一定造成欺骗的结果。因此,该定义依然较为宽泛。2011年,他再次提出新的概念界定,特别是将它与错误信息区别开来:“错误信息是结构良好、有意义的虚假数据(即语义内容),欺骗性信息是一种故意传递的错误信息,误导接收者相信它”[17]。至此,Floridi对欺骗性信息这一概念的认识经历了一个不断深化的过程,根据欺骗性信息的特征对其概念内涵进行不断限缩和提炼,逐渐将欺骗性信息与错误信息区别开来。

Fetzer[18]提出欺骗性信息“应该被或多或少地视为与说谎行为同等对待”,指明了欺骗性信息至少是信息主体认为是虚假的、旨在误导人的一种陈述。他认为欺骗性信息与谎言具有可比性,因为谎言是虚假的断言,是已知的虚假的断言,是带有误导、欺骗或混淆意图的断言[19]。与Floridi对欺骗性信息的定义相比,Fetzer的定义揭示了欺骗性信息的欺骗性、蓄意误导性。他认识到在政治、编辑和广告环境中,区分错误信息和欺骗性信息变得尤为重要,着重将缺乏意图和故意的错误信息与蓄意进行误导和欺骗的欺骗性信息进行区别,但他没有论及欺骗性信息产生的结果和政治危害性,也未认识到欺骗性信息是远比谎言概念内涵更为丰富的东西,即谎言并不一定会造成欺骗性信息所意图造成的有害后果。此外,Fetzer还列举了五种类型的欺骗性信息,包括:信息制造者制造的故意用来歪曲和误导目标的欺骗性信息、针对已有信息的筛选和诡辩形成的欺骗性信息、信息传播者基于与信息制造者所代表的立场无关或具有误导性的理由攻击信息制造者而使用的欺骗性信息、基于不理性信仰而产生的欺骗性信息、因不称职的评论而造成的欺骗性信息[18]。这一分类虽然具有一定的时代局限性,但是较早对欺骗性信息进行深入划分和区别的成果,为后期的欺骗性信息分类提供了可资借鉴的思考路径。

Fallis教授是继Floridi之后,在信息哲学领域对欺骗性信息研究取得较多持续性研究成果的学者,并对欺骗性信息的范畴和类型做出了新的阐释。他于2009年使用概念分析法解析了欺骗性信息的概念,提出欺骗性信息是“有意(或至少被预见)会误导人的错误信息”,它非常接近于谎言,必须具有误导性,但不一定就是错误信息的子集[20]。但是他认为谎言又不足以解释欺骗性信息的主观“害性”,2014年,他再次指出欺骗性信息的危害性在于,人们被误导绝非偶然,它来自那些积极从事误导行为的人,是比谎言概念范围更广、危害性更大的一种故意误导的信息,包括非语言的假动作和图片、视频等[21]。2015年,他概括了欺骗性信息的三个特征,即:欺骗性信息是一种信息,具备信息的基本特征;它是一种具有误导性的信息;它的这种误导不是偶然的、无意的[22]。Fallis教授对欺骗性信息的定义是较为广泛、系统和概念性的一个分析,综合了欺骗性信息的谎言、主动误导和欺骗的特征,对欺骗性信息是否一定是错误信息的问题提出了与其他学者不同的见解。他对欺骗性信息的分类也采取了与Fetzer不同的方案,从有意误导的类型维度进行划分,包括:关于信息内容准确性的误导、关于信息内容来源可信度的误导、关于信息来源身份的误导、关于信息内容准确含义的误导[22],是基于信息误导性质本身进行的更加细致的划分方法。

Skyrms参照生物的欺骗信号来解释欺骗性信息这一社会现象,“如果错误信息被系统地发送,并且以接收者的损失为代价使发送者受益,我们将毫不畏缩地

遵循生物学文献将其称之为欺骗”[23]。与前人的研究相比，他首次提出欺骗性信息是一种有系统地使信息源受益而损害接收者利益的错误信息，但忽视了欺骗性信息有时损害的并不是或不仅是信息接收者的利益，而可能是其所在集体、国家或第三方的利益。

Søe综合了Fetzer、Fallis等人的前期研究成果，使用格赖斯的合作原则和意义理论，构建了一个统一的概念来描述信息、错误信息和欺骗性信息之间的关系，并指出，信息内容的真假不是区别错误信息和欺骗性信息的主要特征，信息的意图才是两者区别的本质所在[24]。他将欺骗性信息与错误信息归结为信息的阴暗面，认为信息是追求真善美、减少不确定性的东西，而欺骗性信息和错误信息则正好相反。与Fetzer和Fallis对欺骗性信息的分类不同，Søe首先将信息分成自然信息与非自然信息，然后将有意图的非误导性信息、无意图的误导性信息（即错误信息）、有意图的误导性信息（即欺骗性信息）都列入为非自然信息的行列。与前人的分类方法相比，这一划分方法的优势在于能够将关注的焦点从信息内容的真值转移到内容的意图性和误导性上来，为真实内容的潜在误导(如真实的欺骗性信息)，虚假内容的潜在非误导(如讽刺)，以及介于两者之间的其他类型欺骗性信息腾出了概念空间[25]。

信息哲学家们关于欺骗性信息是什么，即欺骗性信息本质的研究，经历了一个不断完善的过程：“信息处理不当造成的信息错误——信息制造者主观认识到信息内容本身的错误——信息制造者或传播者故意误导或欺骗——通过损害信息接收者的利益而获利”。在这一层层递进、逐步深化的研究过程中，将欺骗性信息（disinformation）从错误信息（misinformation）中剥离出来，最终形成了清晰、明确的欺骗性信息概念和独立的研究对象。概念的界定和研究对象的确立是欺骗性信息研究的起点和基础。

根据冷战时期的对敌实践以及20世纪前后信息哲学家们的解析，欺骗性信息的概念至少包含以下几层含义：第一，从性质上看，欺骗性信息首先是一种信息，是信息的一种类型，是信息的子集，而不是除信息以外的物质、能量或者其他东西，即欺骗性信息的信息本质；第二，从内容上看，欺骗性信息一般是虚假、不属实的信息，而不是真实、准确的信息，即欺骗性信息的虚假性；第三，从传播者主观意图上看，欺骗性信息是信息生产者或传播者故意、有目的地进行传播或操纵的信息，而不是因无心之过或者因传播主体的知识能力所不能理解、辨识才无意识传播的错误信息，即欺骗性信息的蓄意性；第四，从传播目的上看，欺骗性信息是为了误导和欺骗信息接收者，改变信息接收者的政见、意见和信念，从而影响其决策和行为，即欺骗性信息的误导性和欺骗性；第五，从欺骗性信息的起源上看，欺骗性信息往往带有浓厚的政治色彩，与战略情报手段中的欺敌情报、战略欺骗、隐蔽行动等相对应，即欺骗性信息的政治性；第六，从欺骗性信息的传播结果上看，欺骗性信息以损害或影响信息接收者或其所在组织、国家的利益为目标，影响目标国国家安全、社会稳定和政治民主，干涉目标国内政，制造恐慌与混乱，引发政府信任危机，从而形成有利于自己的信息局势，具有强烈的对抗性质，即欺骗性信息的危害性。

因此，欺骗性信息可以认为是信息制造者或传播者基于政治或经济动机，以欺骗、误导为目的，蓄意传播的虚假信息。它通过影响、干预信息接收者的认知和决策，进而损害信息接收者的生命和财产安全或其所在组织、国家的政治、经济和社会利益，塑造于己有利的态势，具有虚假性、蓄意性、操纵性、误导性、欺骗性、政治性、对抗性和危害性。基于此，欺骗性信息的概念范围逐步从错误信息中独立出来，成为具有特定意义的独立概念，形成了具有明确的研究对象和独立的研究领域，为欺骗性信息研究向纵深推进奠定了坚实的理论基础。

3 欺骗性信息研究的新发展：社交网络环境及国际关系新形势提出新的研究课题

随着现代科学技术的发展和网络多媒体传播手段的普及，欺骗性信息这一社会现象从实体空间转移至网络虚拟空间，并在网络空间中找到了迅猛发展的立足点，进一步肆虐和发酵成一种新的信息操纵和对抗的竞争手段，进而在一定程度上影响了国际关系和国家信息安全。2016年，世界经济论坛将网络战争和欺骗性信息列为全球十大风险之一[26]，欺骗性信息成为影响国家信息安全的一个重要部分。欺骗性信息是实施影响活动的一种武器，尤其是专门利用民族主义、种族和宗教紧张局势制造民众对政府的不信任和社会混乱，开展欺骗性信息运动，将它与信息战、心理战相结合，成为威胁国家信息安全的具有超强破坏力的斗争武器。

经美国参议院情报特别委员会调查，在2016年美

国总统大选期间，俄罗斯政府下属的情报机构和代理人机构有计划地在网络社交媒体上散布欺骗性新闻，公开抹黑民主党总统候选人希拉里，制造有利于共和党总统候选人特朗普的舆论从而影响美国选民政治情绪，刺激选情，干预和操纵选举[27]。该事件及其余波引发了包括传播学、政治学和信息学在内的多个学科对欺骗性信息这一话题的兴趣，掀起了欺骗性信息研究的学术热潮。这一部分研究文献认为，欺骗性信息植根于党派和国家斗争之中[28]，党派或国外敌对势力通过散播欺骗性信息、操纵社交媒体平台来影响选举结果、干预民主进程[29]。对于欺骗性信息到底是否会影响选举结果的研究，不同的学者采用不同的研究对象和研究方法，得出了不同的结论。例如，Allcott 和 Gentzkow [30]对美国2016年大选期间，欺骗性信息的传播进行了研究，发现此类欺骗性信息对选举结果的影响有限；政治意识形态是人们感知欺骗性信息真实性的最重要预测因素。Zimmermann 和 Kohring[31]认为，Allcott 的研究没有对这种有限影响的假设进行实证检验。他们采用样本量为989人的小组调查，研究了2017年德国议会选举中的欺骗性信息对选民投票的影响，发现欺骗性信息与人们的选举行为具有密切的相关性，导致人们相信欺骗性信息的因素是对媒体和政治体制的信任。

还有一些学者认为欺骗性信息不仅会影响选举结果，甚至会进一步加速民主制度的崩塌。例如，Bennett 和 Livingston[32]提出了由欺骗性信息引发的“欺骗性信息秩序”（disinformation order）的概念，认为政治代表核心进程的破坏，以及政府机构和公职人员权威的下降，说明人们对民主制度的信任已经崩溃，这使国家信息系统在混合信息战中向来自本国和外国行为者传播的欺骗性信息直接开放。于是欺骗性信息干扰选举、破坏民主进程的威胁论席卷全球，各国学者纷纷开始研究欺骗性信息如何干扰选举，例如基于复杂动力系统建模模拟选举动态，通过选举过程的信息流管理研究欺骗性信息的传播如何影响竞选结果[33]。

一些学者还评估了各国选举管理中的欺骗性信息抗干扰能力，并提出可行的应对之策。例如，Bossetta[34]采用实验法测试美国2018年中期选举前公众在Twitter上被欺骗性信息网络钓鱼的脆弱性，结果发现通过钓鱼被泄露的账户可能被操纵以散布欺骗性信息从而干预选举，社交媒体可能会武器化。Tan[35]提出选举管理数字准备度（Electoral Management Digital Readiness，EMDR）指数，比较评估了东亚和东南亚十个选举管理机构（EMBs）应对欺骗性信息干扰的准备度，并提出改善选举治理应该采取动员各利益相关者多管齐下的监管方式而不是单纯依靠国家主导。在不确定的时代和信息超载的情况下，要“综合运用技术、经济、法律和社会干预手段”，从自决、代表负责和公众审议三个角度防止欺骗性信息侵蚀民主[36]。

还有一些学者调查了不同国家抵御欺骗性信息风险的能力及其社会抗逆力。例如，Humprecht 等[37]采用跨国比较的方式对西方民主国家的网上欺骗新信息的战略抗逆力进行量化的评估与调研，发现调查的18个国家中，北欧具有较高的战略抗逆力而南欧和美国战略抗逆力较差。至于如何提高欺骗性信息的战略抗逆力，Kolotaev 等[38]总结了欧盟国家的一些实践经验，包括认可公民信息权，提升公民的批判性思维和信息素养；及时披露和曝光欺骗性信息；家长式引导和自我平衡等策略。

国际关系中的战略宣传、公共外交、安全困境以及软实力、巧实力和锐实力等理论和概念可以为了解国际关系中欺骗性信息的运作方式提供独特的解读，包括欺骗性信息的促进因素、欺骗性信息的利用和欺骗性信息的应对[39]。在混合战争背景下，学者们认为有必要采取相应的措施应对欺骗性信息运动[40]，有必要重新审视在人工智能和全球化网络社交媒体环境中的欺骗性信息对国际关系和国家信息安全的威胁、影响，并强化对欺骗性信息的治理，以及应对由此产生的伦理问题[41]。互联网和社交媒体平台是施加影响活动的主战场，同时也是欺骗性信息传播的温床。欺骗性信息的武器化、工具化一方面成为影响他国内政外交的重要因素，成为国际关系处理中的不能忽视的一个部分，另一方面也引导学者们积极地从国际关系理论中去探寻欺骗性信息的应对与治理之路，进一步推动了欺骗性信息理论与实践的交叉与融合发展。

社交网络环境下，欺骗性信息的泛滥对国家信息安全与国际关系平衡提出了新的课题。该阶段的研究主要基于各国对欺骗性信息干扰、渗透、操纵其选举过程，影响其民主进程的一些实验与调查研究，进一步拓展了欺骗性信息的研究领域，出现了一些综合性、实践性和创新性的研究成果，集中体现了欺骗性信息从实践领域走向学术研究领域并与实践形成良性互动的状

态。同时，该部分研究也提升了欺骗性信息的研究层次、研究范围和现实感，为深入剖析欺骗性信息在网络环境中对国家安全、国际关系与国际战略格局的威胁与挑战，以及网络欺骗性信息的治理与应对提供了更为全面的理论框架。

4 欺骗性信息研究的新视角：基于信息行为学的受众个体特征和行为研究

国际关系学和国家安全学领域将欺骗性信息运动纳入信息战的范畴，即为实现政治和军事目标而战略性地使用欺骗性信息，在这一视角下欺骗性信息成为战争武器，而公众的思想则是主战场，因此一般认为欺骗性信息是由国家主体间制造和传播的，公众则被视为信息操纵的目标和对象。但是，有研究表明，在欺骗性信息的传播中公众也可能是欺骗性信息的制造者、受害者和试图对抗欺骗性信息的最活跃的驱动者[42]。一些信息行为学的学者从信息接收者也就是从受众的角度来研究欺骗性信息的影响、传播规律，了解受众的个体特征和行为特征等，能够更全面地了解欺骗性信息的性质特征，识别出欺骗性信息的脆弱性群体，进一步拓展欺骗性信息的研究范围。

基于信息行为学的视角，学者们认为欺骗性信息是信息的一种形式，它扩展了信息的概念内涵；而信息欺骗行为是信息行为的一种类型，是信息行为的重要组成部分[43]，将追求真实信息的主动信息搜寻行为、被动信息偶遇行为延展为基于虚假信息、采用欺骗手段进行的信息欺骗行为。也就是说，从信息行为学的角度来解读欺骗性信息的传播其实就是一种信息行为，信息属性(来源的权威性、共识指标)、信息接收者特征(信息素养、个性和人口统计学变量)及其交互作用(信息与接收者信念之间的一致性)对传播欺骗性信息的可能性都会产生一定的影响[44]。已有文献的相关研究也主要从欺骗性信息、欺骗性信息用户和欺骗性信息行为的视角对欺骗性信息受众开展调查研究。例如，Zerback 等[45]让2353名受试者接触亲俄罗斯的欺骗性信息，测试这些信息对其政治观点的影响，结果发现欺骗性信息确实可以改变受试者的政治观点。Schaewitz 等[46]进行了一项样本量为294人的实验，研究了信息自身因素和用户个体差异是否会在一定程度上影响个体对欺骗性信息的信任度、感知度和分享意愿，发现信息来源、不一致性、主观性、轰动效应或图片操纵等信息自身因素对用户个体评价欺骗性信息的影响似乎不如用户自身个体差异产生的影响大。

尽管欺骗性信息在社会中普遍存在，但人们对使一些用户比其他人更容易接受欺骗性信息的个体特征知之甚少，根据用户的这种“抵抗力”差距可以将受众划分为：容易接受欺骗性信息的群体和能够抵抗欺骗性信息的群体[47]。关于哪些个性特征的群体更容易接受欺骗性信息以及为什么有些群体对欺骗性信息具有更强的抵抗力的研究有助于识别受众群体中的脆弱性因素和风险性因素。例如，Wolverton 和 Stevens[48]使用五因素模型，量化研究性格特征对识别和检测欺骗性信息的影响，发现具有不谙世事、谨慎、内向、不友善或没有爱心、没有责任感或没有目标、情绪稳定等性格特征的个体更能识别欺骗性信息。Tandoc 等[49]对2501名新加坡受访者进行调查并对20名参与者进行了深度访谈，试图通过研究社交媒体用户对待欺骗性信息的反应及原因来了解欺骗性信息的传播，发现新加坡的大多数社交媒体用户对欺骗性信息通常采取忽略的态度，只有在欺骗性信息涉及自己及其密切相关人的利益时才会去纠正。

欺骗性信息受众传播欺骗性信息的驱动因素、对欺骗性信息的抵抗力差距、接收者个体特征与脆弱性因素的研究是一个漫长、动态和复杂的过程，需要相关研究者于不同的地域、时间和环境背景下进行进一步的调查研究，这也是值得相关学者进行进一步探索的研究议题。

5 欺骗性信息研究的突发增长点：新冠肺炎疫情引发“信息疫情”热议

2019年，新型冠状病毒性肺炎疫情(COVID-19)的暴发使得欺骗性信息再次成为全球热议的话题。世界卫生组织指出“人们不仅要抗击新冠疫情，更要抗击‘信息疫情’(infodemic)”[50]。信息疫情所引发的次生灾害在一定程度上可以超过疫情本身所带来的危害。所谓的“信息疫情”，即在信息过载的情况下，人们已经无法判断哪些是真实信息，哪些是欺骗性信息[51]。欺骗性信息并不是一个新鲜的概念，但在疫情期间其杀伤力暴露得比以往的任何时候都更加淋漓尽致，抗击欺骗性信息已经成为抗击疫情的一个重要部分。疫情与谣言相伴而生虽是常态，但由新冠病毒引发的“信息疫情”在当今的社交媒体环境下被放大了，远超过先前规

模，造成了新的社会风险[52]。在自媒体时代，欺骗性信息的传播可能会引起公众的恐慌、夺走人们的生命、扰乱社会的秩序、损害公众信任、操纵信息话语、破坏国家的安定，甚至威胁国内和国际安全。

人们对疫情信息的不确定性会促发其信息查寻行为，而在查寻的过程中却发现自己被那些欺骗性信息所包围，而且对于一些没有正确搜索技能和识别能力的人来说很难立即区分欺骗性信息与事实[53]。在新冠肺炎疫情期间，英国通信管理局对2000多人进行的一项调查发现，在采取居家隔离措施的第一周内，46%的人遇到了欺骗性信息或错误信息，66%的人每天至少看到一次关于COVID-19欺骗性信息[54]。欺骗性信息泛滥，甚至引发了一些犯罪行为，犯罪分子利用公众对疫情信息的不确定性进行欺诈。英国有公民收到过声称来自英国政府的网络诈骗短信，通知他们因为违反疫情期间规定的社交距离而必须支付35英镑罚款[55]。人们对COVID-19的起源、治疗和预防方法产生了极大的不确定性和恐慌，加之能够为临床实践提供支持的信息紧缺，使得疫情期间的欺骗性信息在网络空间肆虐，极易被一些别有用心的行为者趁机散布阴谋论[56]。还有学者担心近几年反疫苗接种运动所提倡的阴谋论在社交媒体上广为流传，可能阻碍人们最终接种COVID-19疫苗[57]。

如何应对突发公共卫生事件中的欺骗性信息，成为法学、传播学、情报学和网络安全学等相关学科共同关注的学术问题。有学者从法律视角总结了近年各国从法律层面规制欺骗性信息传播行为的立法情况，指出一些国家通过扩展现有法律条款把疫情期间恶意传播欺骗性信息的行为规定为刑事犯罪行为，为应对COVID-19欺骗性信息制定了相应的法律框架[58]。也有传播学的学者提出，新冠肺炎疫情引发的信息疫情只是数字媒体空间长期积累的欺骗性信息泛滥弊病的一个引爆点，是第一次真正的社交媒体疫情也是酝酿已久的信息危机，仅仅依靠事实核查和纠正信息是远远不够的，需要置身于当代社会文化背景下深入地理解数字媒体如何促进或阻碍理性事实、知识与情感、价值观和信念之间的互动，积极探索欺骗性信息在数字媒体环境中的产生传播机制、限制其传播的技术和策略、多方力量参与打击欺骗性信息的潜在合作机制[59]。还有学者认为，提高科学素养和新闻素养，特别是为社交媒体用户提供识别、消费和分享高质量信息的工具，是抗击Covid-19欺骗性信息的基石[60]。医生应该以简单和直接的方式向公众提供和共享基于证据的疫情信息，以避免误读和误解，需要加强医学界、政府和大众媒体之间的协调，以避免疫情欺骗性信息通过不同渠道传播和扩散[53]。在当前的COVID-19危机中，迫切需要为普通民众(特别是那些最容易患病的人)提供可执行的自我保护信息，包括症状的识别和如何寻求和接受正当治疗的明确的指导性信息[61]。当今的网络社交媒体环境在促进疫情相关欺骗性信息传播的过程中起到了极大的促进和助长作用，如何解决公共传播中的阴暗面并促进其光明的一面需要社会各界的共同努力。

此外，还有一些学者开展了关于各国在新冠肺炎疫情期间应对欺骗性信息的实证调研。例如一项关于巴西的社交网络上疫情欺骗性信息传播情况的调查表明，巴西传播欺骗性信息频率最高的平台依次是WhatsApp、Instagram和Facebook，且认为与Covid-19相关的恶意内容的传播会导致全球科学和卫生机构的信誉下降，而解决此问题的方法是提高巴西社会获取充足、正确信息的水平[62]。另外，一项关于个体对COVID-19欺骗性信息的态度的实证研究发现，对其他社会群体的信任、对疫情新闻的兴趣和帮助病人的意愿，是个体愿意采取行动保护自己和社会不受欺骗性信息侵害的先决条件[63]。

疫情期间传播的欺骗性信息引发了社会的混乱、对政府部门信任的丧失和公众的不安全感，也触发了学者们对欺骗性信息危害、识别和应对的研究，国外的此类相关成果不胜枚举。可以预期，随着疫情的进一步发展，这一方面的研究成果将持续增加。

6 总结与展望

欺骗性信息是一个极具争议性、话题性和学理性的学术议题。国外的欺骗性信息研究先是从冷战时期苏联的对敌情报实践中总结经验和规律，再从信息哲学视角确立起自己独立的研究对象和研究领域，因2016年美国大选风波掀起研究热潮，顺应社交网络媒体的发展和复杂的国际形势变化，融入了多学科的研究方法和理论，形成了丰硕的研究成果。2019年突发的全球性新冠肺炎疫情引发的信息疫情使得欺骗性信息又一次引起了学术界的广泛关注，成为当下各国学者争相热议的话题。纵观欺骗性信息研究的发展历程，它的每一次发展都离不开现实世界实践活动的助

推。现实世界的变化与需求一次次地推动着欺骗性信息从实践上升到理论，由理论指导实践，再到实践与理论相互融合与促进的发展过程。可以说，欺骗性信息的研究从实践中来，形成了一定的理论基础，又在实践过程中产生了理论指导实践的需求，最终促进理论与实践融合、交互与协同发展。欺骗性信息的研究拓展了信息科学、国家安全学、情报学、国际关系学、政治学、网络安全学等相关学科的研究内容与学科视野，随着社交网络媒体的普及以及国际关系的日益复杂化，它将是未来学术界不可回避、不可忽视的重要研究课题。

在国外学者积极开展欺骗性信息研究的情况下，我国学术界也应该加大对这一问题的关注。诚然，国外对欺骗性信息理论层面的解读以及实证角度的论证，其政治观点有待探讨和商榷，但其呈现的丰硕研究成果体现了学术界对欺骗性信息的研究探索，为更高、更广泛层次的欺骗性信息研究提供了理论引领。在开展欺骗性信息相关研究的过程中，我们应该认识到国外对欺骗性信息研究也仍然处于初级和探索阶段，且一些研究成果往往夹杂和代表着其所在国的政治观点和政治立场，我国在开展相关研究的过程中既不能直接追随西方国家的研究话语，完全听从国外研究的指挥棒，但也不能漠视其研究进展与成果，需要科学评估欺骗性信息产生的影响进而寻求我们在欺骗性信息研究中的可行路径，以应对复杂多变的信息安全局势，在总体国家安全观的指导下牢牢掌握国际学术话语权。

笔者认为，我国学术界应该及时跟进、参与欺骗性信息研究，客观评估欺骗性信息对国家安全的威胁，在总体国家安全观的指导下结合我国的实际情况提出欺骗性信息的应对方案。具体来说，可以从以下几个方面展开进一步研究：

一是欺骗性信息的历史及其与相关概念间的关系。欺骗性信息起源于对敌情报实践，具有一定的历史渊源，且与隐蔽行动、政治宣传、秘密行动和反情报等相关概念都有一定的关联，欺骗性信息与错误信息、假新闻、虚假信息等概念之间也存在一定的交叉。梳理欺骗性信息的相关历史、明晰相关概念间的关系是深化欺骗性信息研究的重要基础，能够为我国的欺骗性信息基础理论研究奠定基础，也是值得我们继续研究和探讨的方向。

二是国外的欺骗性信息治理实践与经验。国外在治理和应对欺骗性信息方面具有较长的历史和实践经验，尤其是欧盟、北约、英国、美国，都从专门的职能机构、法律制度规范、技术和标准等方面构建了欺骗性信息综合治理体系，其中一些具有普适性和推广价值的做法、理论和实践指南，值得我们进一步调研和批判性地借鉴与吸收。

三是受众的欺骗性信息抗逆力与个体特征。不同国家、不同地区的受众对欺骗性信息具有不同的社会抗逆力。评估我国社会欺骗性信息抗逆力是进一步制定和实施治理策略的基础。此外，哪些受众的哪些个体特征容易接受和传播欺骗性信息、为什么有些国家对欺骗性信息的战略抗逆力较强而有些国家则较弱、影响欺骗性信息传播的脆弱性因素和风险性因素等问题都是深入研究欺骗性信息值得考虑的话题。

四是应对欺骗性信息的中国方案。欺骗性信息的应对是一个复杂的系统工程，需要在总体国家安全目标的指导下，从欺骗性信息应对机制的构成要素、应对方式入手，从应对欺骗性信息的战略规划、相关政策、应对模式、涉及主体、协同方案等多角度考虑，以及从国际交流、责任机构、法律制度、识别技术、受众教育等多元约束与保障的维度来探寻应对欺骗性信息的中国方案。

（致谢：中国人民公安大学博士生导师彭知辉教授对该文进行了指导和修改，特此感谢！）

参考文献

[1] Freelon Wells. Disinformation as political communication[J]. Political Communication,2020,37(2):145-156.

[2] Rand Corporation. Truth Decay: An initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life [EB/OL]. [2018-01-15]. https://www.rand.org/pubs/research_reports/RR2314.html.

[3] North Atlantic Treaty Organization. NATO's Approach to Countering Disinformation: A Focus on COVID-19 [EB/OL]. [2020-05-19]. https://www.nato.int/cps/en/natohq/115204.htm.

[4] Sarts J. Disinformation as a Threat to National Security[M]// Jayakumar S, Ang B, Anwar N D. Disinformation and Fake News. Singapore: Palgrave Macmillan,2020:23-33.

[5] Ferrara E. Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election[J]. First Monday, 2017, 22(8):1-33.

[6] Bradshaw S, Bailey H, Howard P N. Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation [EB/OL]. [2021-01-13]. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report20

-FINALv.3.pdf.

[7] Martin L J. Disinformation: an instrumentality in the propaganda arsenal[J]. Political Communication,1982,2(1):47-64.

[8] Barron J, Conquest R. KGB: The secret work of Soviet secret agents[J]. Russian Review,1974,33(4):437.

[9] House Select Committee on Intelligence. Soviet Covert Action (the Forgery Offensive): Hearings before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence [R/OL]. [1980-02-06]. http://cryptome.info/cia-FM30-31B.htm.

[10] Meiselman W, Pilon J G, Lenczowski J, et al. Soviet disinformation and the news[J]. Political Communication,1987,4(1):29-64.

[11] Kux D. Soviet active measures and disinformation: overview and assessment[J]. Journal of the US Army War College,1985,15(4):19-28.

[12] Clogg R. Disinformation in Chechnya: an anatomy of a deception[J]. Central Asian Survey,1997,16(3):425-430.

[13] Boghardt T. Soviet Bloc intelligence and its AIDS disinformation campaign[J]. Studies in Intelligence,2009,53(4):1-24.

[14] Romerstein H. Disinformation as a KGB weapon in the Cold War[J]. Journal of Intelligence History,2001,1(1):54-67.

[15] Floridi L Brave.Net.World: the Internet as a disinformation superhighway?[J]. Social Science Electronic Publishing,1996,14(6):509-514.

[16] Floridi L. Semantic Conceptions of Information in the Stanford Encyclopedia of Philosophy [EB/OL].[2005-10-05]. https://stanford.library.sydney.edu.au/archives/sum2007/entries/information-semantic/.

[17] Floridi L. The Philosophy of Information[M]. New York: Oxford University Press,2011:260.

[18] Fetzer J H. Disinformation: the use of false information[J]. Minds and Machines,2004,14(2):231-240.

[19] Fetzer J H. Information: does it have to be true? [J]. Minds & Machines, 2004,14(2):223-229.

[20] Fallis D. A Conceptual Analysis of Disinformation [EB/OL]. [2009-02-28]. http://hdl.handle.net/2142/15205.

[21] Fallis D. The Varieties of Disinformation[M]// Floridi L, Illari P. The Philosophy of Information Quality.Switzerland: Springer International Publishing ,2014:135-161.

[22] Fallis D. What is disinformation? [J]. Library Trends,2015,63(3):401-426.

[23] Skyrms B. Signals: Evolution, Learning, and Information[M]. Oxford: Oxford University Press,2010:80.

[24] Søe S O. A unified account of information, misinformation, and disinformation[J]. Synthese,2019,198(11):5929-5949.

[25] Søe S O. The urge to detect, the need to clarify Gricean perspectives on information, misinformation, and disinformation[D]. Faculty of Humanities, University of Copenhagen, 2016.

[26] World Economic Forum. The Global Risks Report 2016 [EB/OL]. [2016-01-14]. https://www.weforum.org/reports/the-global-risks-report-2016.

[27] Select Committee on Intelligence United States Senate. Russian Active Measures Campaigns and Interference in the 2016 U.S Election [EB/OL].[2018-01-29].https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume4.pdf.

[28] Faris R, Roberts H, Etling B, et al. Partisanship, propaganda, and disinformation: Online media and the 2016 U.S. presidential election[R/OL]. Social Ence Electronic Publishing.[2017-08-24]. https://dash.harvard.edu/bitstream/handle/1/33759251/2017-08_electionReport_0.pdf.

[29] Marwick A, Lewis R. Media Manipulation and Disinformation Online[EB/OL]. [2017-05-15]. https://datasociety.net/output/media-manipulation-and-disinfo-online/.

[30] Allcott H, Gentzkow M. Social media and fake news in the 2016 election[J]. Journal of Economic Perspectives,2017,31(2):211-236.

[31] Zimmermann F, Kohring M. Mistrust, disinforming news, and vote choice: a panel survey on the origins and consequences of believing disinformation in the 2017 German parliamentary election[J]. Political Communication,2020,37(2):215-237.

[32] Bennett W L, Livingston S. The disinformation order: disruptive communication and the decline of democratic institutions [J]. European Journal of Communication,2018,33(2):122-139.

[33] Brody D C. Modelling election dynamics and the impact of disinformation[J]. Information Geometry,2019,2(2):209-230.

[34] Bossetta M. A simulated cyberattack on twitter: assessing partisan vulnerability to spear phishing and disinformation ahead of the 2018 U.S. midterm elections[J]. First Monday,2018,23(12):1-23.

[35] Tan N. Electoral management of digital campaigns and disinformation in East and Southeast Asia[J]. Election Law Journal, 2020,19(2):214-239.

[36] Tenove C. Protecting democracy from disinformation: normative threats and policy responses[J]. The International Journal of Press/Politics,2020,25(3):517-537.

[37] Humprecht E, Esser F, Aelst P V. Resilience to online disinformation: a framework for cross-national comparative research [J]. The International Journal of Press/Politics,2020,25(3):493-516.

[38] Kolotaev Y, Romanova T A, Sokolov N I. Disinformation (fake news, propaganda) as a threat to resilience: approaches used in

the EU and its member state Lithuanian[J]. Baltic Region, 2020,12(1):53-67.

[39] Cour C L. Theorising digital disinformation in international relations[J]. International Politics,2020,57(11):1-20.

[40] Giannetti M W. A duty to warn: how to help America fight back against Russian disinformation[J]. Air & Space Power Journal, 2017,31(3):95-104.

[41] Landon-Murray M, Mujkic E, Nussbaum B. Disinformation in contemporary U.S. foreign policy: impacts and ethics in an era of fake news, social media, and artificial intelligence[J]. Public Integrity,2019,21(4):1-11.

[42] Yevgeniy G, Mareike H, Rebecca A N. State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation[J]. International Affairs,2018,94 (5):975-994.

[43] Karlova N A, Fisher K E. A social diffusion model of misinformation and disinformation for understanding human information behaviour[J]. Information Research,2013,18(1):573.

[44] Buchanan T. Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation[J]. Plos One,2020,15(10):1-33.

[45] Zerback T,Töpfl F, Knöpfle M. The disconcerting potential of online disinformation: persuasive effects of astroturfing comments and three strategies for inoculation against them[J].New Media and Society,2020,23(1):2-40.

[46] Schaewitz L, Kluck J P, Lukas K, et al. When is disinformation (in)credible? Experimental findings on message characteristics and individual differences[J]. Mass Communication & Society,2020,23(4):484-509.

[47] Amazeen M A, Bucy E P. Conferring resistance to digital disinformation: the inoculating influence of procedural news knowledge[J]. Journal of Broadcasting & Electronic Media,2019,63 (3):415-432.

[48] Wolverton C, Stevens D. The impact of personality in recognizing disinformation[J]. Online Information Review,2019,44(1): 181-191.

[49] Tandoc E C, Lim D, Ling R. Diffusion of disinformation: how social media users respond to fake news and why[J]. Journalism, 2020, 21(3):381-398.

[50] Word Health Organization. Munich Security Conference [EB/OL]. [2020- 02- 15]. https://www.who.int/dg/speeches/detail/munich-security-conference.

[51] Word Health Organization. Providing Timely and Accurate Information to Dispel the 'Infodemic' [EB/OL]. [2020-04-15]. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200415-sitrep-86-covid-19.pdf?sfvrsn=c615ea20_4.

[52] Zarocostas J. How to Fight an Infodemic[J]. Lancet,2020,395: 676.

[53] Tagliabue F, Galassi L, Mariani P. The "Pandemic" of disinformation in COVID-19[J]. SN Comprehensive Clinical Medicine, 2020, 2(9):1-4.

[54] Ofcom. Covid-19 News and Information: Consumption and Attitudes [EB/OL]. [2020- 04- 09]. https://www.ofcom.org.uk/_data/assets/pdf_file/0031/193747/covid-19-news-consumption-week-one-findings.pdf.

[55] Ofcom. Advice for Consumers: Coronavirus Scam Calls and Texts [EB/OL]. [2020- 04- 09]. https://www.ofcom.org.uk/about- ofcom/latest/features- and- news/coronavirus- scam-calls-and-texts#.

[56] Jaiswal J, Loschiavo C, Perlman D C. Disinformation, misinformation and inequality-driven mistrust in the time of COVID-19: lessons unlearned from aids denialism[J]. AIDS and Behavior,2020,24(2):2-6.

[57] Pereira P S, Silveira A D S, Pereira A. Disinformation and conspiracy theories in the age of COVID-19[J]. Frontiers in Sociology,2020,5(12):96.

[58] Radu R. Fighting the 'Infodemic': legal responses to COVID-19 disinformation[J]. Social Media + Society,2020,6(3):1-4.

[59] Nguyen A, Daniel C. Digital mis/disinformation and public engagment with health and science controversies: fresh perspectives from Covid-19[J]. Media and Communication,2020,8(2): 323-328.

[60] Vraga E K, Tully M, Bode L. Empowering users to respond to misinformation about Covid-19[J]. Media and Communication, 2020,8(2):475-479.

[61] Heymann D L, Shindo N. COVID-19: what is next for public health? [J]. The Lancet, 2020, 395(10224):542-545.

[62] Galhardi C P, Freire N P, Minayo M, et al. Fact or Fake? An analysis of disinformation regarding the Covid- 19 pandemic in Brazil[J]. Ciência & Saúde Coletiva,2020,25:4201-4210.

[63] Михеев Е А,Нестик Т А. Psychological Mechanisms of Infodemic and Personal Attitudes to Disinformation about Covid-19 in Social Media[EB/OL]. [2021-02-15].http://www.researcsearchgate.net/publication/350822436.

[作者简介]王海霞,女,1988年生,中国人民公安大学国家安全学院博士生,福建警察学院图书馆馆员。

收稿日期:2021年02月19日