IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

收到 2022 年 5 月 28 日，接受 2022 年 6 月 11 日，发布日期 2022 年 6 月 16 日，当前版本日期 2022 年 6 月 22 日。

数字对象标识符 10.1109/ACCESS.2022.3183642

面向国家安全的信息与人工智能比较分析

Mohammed nasser al-suqri 1 和 maryam gillani 2
1 苏丹卡布斯大学艺术与社会科学学院信息研究系，阿曼马斯喀特 123
2 都柏林大学学院计算机科学学院，都柏林 4,D04 VIW8 爱尔兰

通讯作者: Maryam Gillani (maryam.gillani@ucdconnect.ie)这项工作得到

了爱尔兰都柏林大学学院的支持。

涉及到国家安全，信息是不可避免的。信息革命似乎具有巨大的潜力，可以加强国家安全，抵御当前和未来的威胁和网络攻击。然而，信息可及性的进步给维护国家安全稳定带来了无数的复杂性。社交媒体是最重要的信息来源之一，它无疑增加了信息操纵因素，破坏了国家安全。为了更好地完成国家安全计划，信息技术可以帮助各国识别潜在威胁，安全地共享信息，并保护其中的机制。人工智能(AI)是智能领域之一，它强有力地促进安全信息处理，以避免威胁和网络攻击。它明智地审查通过社交媒体向公众提供的信息，并协助遏制对国家安全的负面影响。这篇研究文章广泛关注四个主要的分析里程碑;1)公众可获得的信息 2)影响国家安全的信息 3)网络攻击的风险 4)人工智能对国家安全至关重要，以发挥合格的信息作用。我们的主要目标是揭开信息可及性视角的神秘面纱，让读者了解与国家安全相关的信息可及性和不可及性的基本原理。为了支持和表明我们的里程碑和目标，系统文献综述(SLR)在方法上进行了调整，以得出合适的结论，并建立了一个有远见的模型和参考框架。本文总结了基于人工智能工具的分类、算法功能和基于区域的特定领域分析，以突出当前的需求。最重要的是，对于许多天真的社交媒体用户来说，这篇文章是一个发人深省的开始，他们通常会避开带有信息的元素，并成为网络攻击的受害者，随后会危及国家安全。

人工智能、网络攻击、信息角色、信息安全、国家安全、社交媒体信息。

I. 介绍

国家安全与信息传播密切相关。多年来已经开发了各种机制来解决信息处理问题[1]。然而，以社交媒体为基础的信息的快速和相对较新的传播，虽然带来了许多好处，但也表明迫切需要制定新的国家安全机制来应对不断恶化的环境。软件工程研究所(SEI)的计算机应急响应小组(CERT)[2]报告说，安全事件每年翻一番，随后增加自 2001 年以来的增长率。与这些数字相对应的是，有大量的安全事件从未被报道过。国家安全体系在很大程度上依赖于影响当前和未来变化的信息，而不考虑国家安全利益[3]。国家安全系统在很大程度上依赖于通过各种反国家渠道传播的信息。

国家安全可以定义为一种国家战略，以确保保护国家的基本和持久需求，同时以人员和社会价值观保护每个公民的基本安全需求[4]。利用国家安全利益操纵理想的安全领土参数，导致对国家价值观、利益和全球关系的诽谤[5]。社交媒体是由

协调审稿并批准发表的副主编是林俊伟。

这个拥有数十亿用户的庞大平台每秒匿名发布大量信息，这对维持国家安全的稳定构成了具体威胁[6]。网络虚假信息是一种持续存在的情况，目前毫无防御能力，这给监管违反言论自由原则的信息流动增加了担忧[7]。

通过各种途径传播的信息没有义务在安全参数内传播[8]。 例如，社交媒体上的信息也可能妨碍国家安全。社交媒体信息在信息战中的作用备受争议。它被黑客活动分子和犯罪分子用作网络开发、黑客攻击和敲诈勒索的便捷工具[9]。社交媒体账户和页面对国家安全至关重要，因为数百万用户在特定时间进行交互，为国家的脆弱性和声誉损害提供了巨大的风险。

在不付出额外努力的情况下，虚假信息在破坏国家安全措施方面发挥了巨大作用。它已经成为一个党派问题，可能使国家行动计划陷入瘫痪[10]。上网的最大代价是假新闻的传播，也被称为虚假信息或垃圾信息。然而，所有类别的信息(虚假信息、垃圾信息、虚假操纵信息、部分信息)都导致了一种恐惧和不作为的奇特混合[11]。信息也充斥着外国干涉，这取决于其他国家的敌意和破坏国家安全的意图。

为了防止面临威胁的情况，人工智能(AI)在数字发展和信息革命对社会的影响中发挥了作用[12]。人工智能支持的社交媒体信息监控工具可以作为社交倾听工具，帮助面对社交信息档案和受众。人工智能参与解释不同尺度的社会数据信息，可以促进调查其中所说的内容，并根据该信息提取罪魁祸首[13]。AI 在处理具有信息动作检查的内容生成机器人方面更智能，如图 1 所示，通过阶段及其子域和相关领域的层次结构。

这篇研究文章涵盖了信息在国家安全中的作用，涉及信息的可访问性和公众可获得性，同时批判性地审视网络空间共谋的影响和影响。更准确地说，本文的目标和里程碑如下

1. 在社交媒体平台上传播的信息对国家安全措施的有效性和效力的作用可能会得到强调、讨论和分析，以确定信息在国家安全中的作用。
2. 网络空间的竞争、网络攻击、网络盗窃、虚假信息活动以及网络相关因素的潜在风险被广泛讨论和探索，以提供一个更广泛和可理解的有远见的推断出实质性的推理，以衡量和防止国家的威胁和攻击。
3. 人工智能在国家安全救济和协助打击假情报者和各种网络分裂方面的立场和方面，即讨论人工智能对抗国家利益的数字信息战是本研究文章的另一个主要目标。
4. 另一个目标是揭示网络空间违法行为的信息圈，简要讨论并突出相互关联的可追溯性和跟踪性。
5. 设计并提出了一个限制/控制信息的模型，以及可能跟踪和停止针对和破坏国家安全的社交媒体信息的功能算法。
6. 此外，国家安全方面的挑战和信息缺口也被广泛覆盖，以描绘网络空间违反国家安全的行为。所提出的树形图展示了信息流和国家安全威胁的各种相关因素的更广泛的画面，以多样化读者的视野。

这篇文章概括了信息在国家安全措施中所起作用的精确观点。然而，本研究的意义和新颖性因素如下

1. 现有的调查既不全面，也不是基于系统文献综述。此外，据我们所知，现有的信息并没有涵盖社交媒体信息及其对国家安全的威胁的所有方面。
2. 现有的调查不是最新的[14]-[16]，也不包括人工智能在信息作用和国家安全措施领域的最新工作。
3. 另一个重要的方面是对人工智能方法的特定应用分析，这在早期文献中没有提供。
4. AI Tool 对社交媒体上信息流的分类和分析是这篇文章的另一个区别因素，这使得它与迄今为止其他可行的文献不同且重要。
5. 通过功能算法设计和支持信息身份验证和身份验证模型，并通过一系列步骤利用 AI 框架进行工具辅助。
6. 本文贡献知识的动机和主要意图是比较分析信息和人工智能对国家安全的影响，以启发与网络空间侵犯、社交媒体操纵者和虚假信息运动相关的威胁因素及其强化效果、措施和可能的预防措施。

研究文章[14]-[16]讨论的是狭窄的范围，而不是更广泛的领域。他们确定了弱点、优势和挑战以及威胁和风险

的机会。而我们的重点是设计一个模型和功能算法的潜在解决方案，以对抗国家威胁，网络空间违规和社会媒体操纵者。其次，这些文章对社交媒体信息流通的探讨较少，而我们在更详细的背景下考虑了社交媒体信息分析。

文章的其余部分组织如下: 第二部分为相关背景和文献综述;第三部分给出了系统文献综述参数的详细概述，作为一种方法，简要介绍了研究问题和排除/纳入标准。第四、五、六和七节分析地涵盖了提出的研究问题以及支持模型、算法和图形表示。第八部分对全文进行总结。

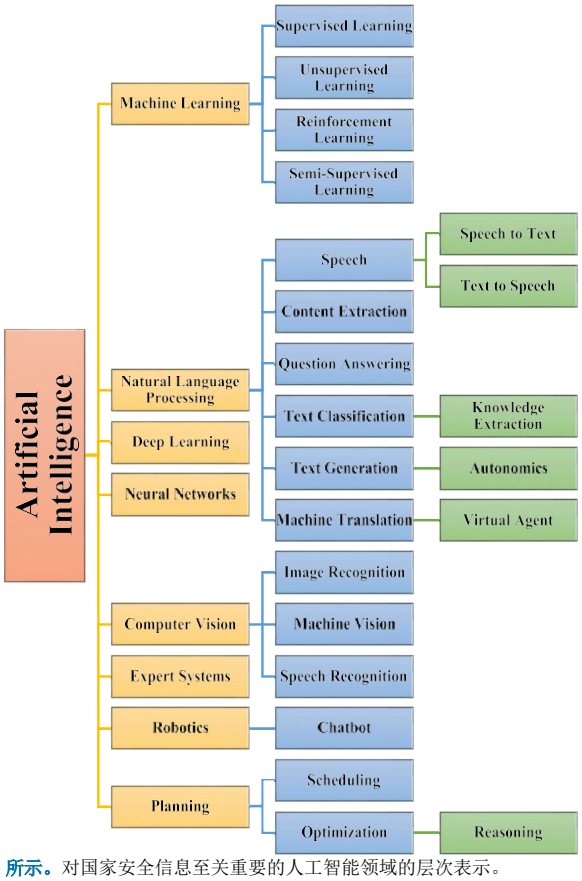

图 1 所示。对国家安全信息至关重要的人工智能领域的层次表示。

II. 文献综述

20 世纪见证了战争史和信息共享史上最致命和最活跃的战争[17]。然而，21 世纪的到来伴随着多重信息冲突，即将带来网络战争，破坏国家安全计划和特征[18]。使用人力和武器的物理战争现在被国家和非国家行为体取代，以控制网络空间的重要场所，对物理领域产生影响。网络空间为这些行为者提供了自由在没有任何物理障碍的情况下，以更大规模的社交媒体领域对应的信息操纵为基础扩展他们的权力。 这在早些时候被认为是不可能的。

社交媒体不仅是连接、通知和共享数百万用户共同平台的技术生命力，而且具有强大的非存在性攻击能力，可以打击国家证券[19]。社交媒体在全球范围内帮助人们组织和策划侵略性骚乱，招募恐怖分子，策划袭击，美化民族战争，帮派汇编，传播暴力以应对小/大事件[20]。这些活动的功劳要归功于社交媒体上的信息流通，它以更大的速度影响着国家安全计划。这些强烈的过渡浪潮不仅放大了灾难性行动，而且协调了针对政府和执法部门的行动[21]。

为了控制信息交换，信息操纵控制是这个时代的迫切需要。 如果不及时正确地采取适当的措施，世界将濒临灭绝与和平。人工智能已经改变了范式，并有助于管理各种社交媒体平台上的信息需求[22]。人工智能通过社交媒体机器人进行工作，这些机器人通过内容更智能的算法进行监视[23]。这些算法比对立的机器人行动得更快，而学习、改变和改变速度则更加动态。实时自动屏蔽也是创作者更好的选择。它允许智能阻止以恶意攻击为目标的用户。第三节提出了一种这样的算法和模型。

网络空间允许入侵者以更快的速度和更轻松的方式在社交媒体领域扩展其权力，这在以前被认为是不可能的[24]。然而，人工智能完美地处理了国家和非国家行为体，以阻止在这个网络战争的数字战场上滥用思想和信仰的市场。美国社交媒体部门认为，媒体上的信息给国家安全带来了巨大的威胁，主要涉及社会工程、web 应用程序攻击和网络钓鱼威胁[25]。由于这些不可预见的后果，美国已经在政府机构正式禁止了 Twitter 和 Facebook。

信息破坏国家安全，造成巨大的经济损失。2013 年，一家知名媒体集团的社交媒体遭到黑客攻击，并发布了白宫发生两起爆炸导致总统受伤的消息。这一消息在两分钟内传到了美国股票交易者那里，它下跌了 143 点，即 1365 亿美元的估计损失。与检索和操纵信息有关的其他一些突出的网络攻击是入侵中央情报局局长约翰·布伦南和国家情报总监詹姆斯·克拉珀的电子邮件账户;2011 年 RSA SecureID 网络安全攻击;2016 年民主党全国委员会电子邮件泄露和 2014 年索尼影业神秘的黑客攻击，英国退欧运动，剑桥分析公司的美国大选[26]。

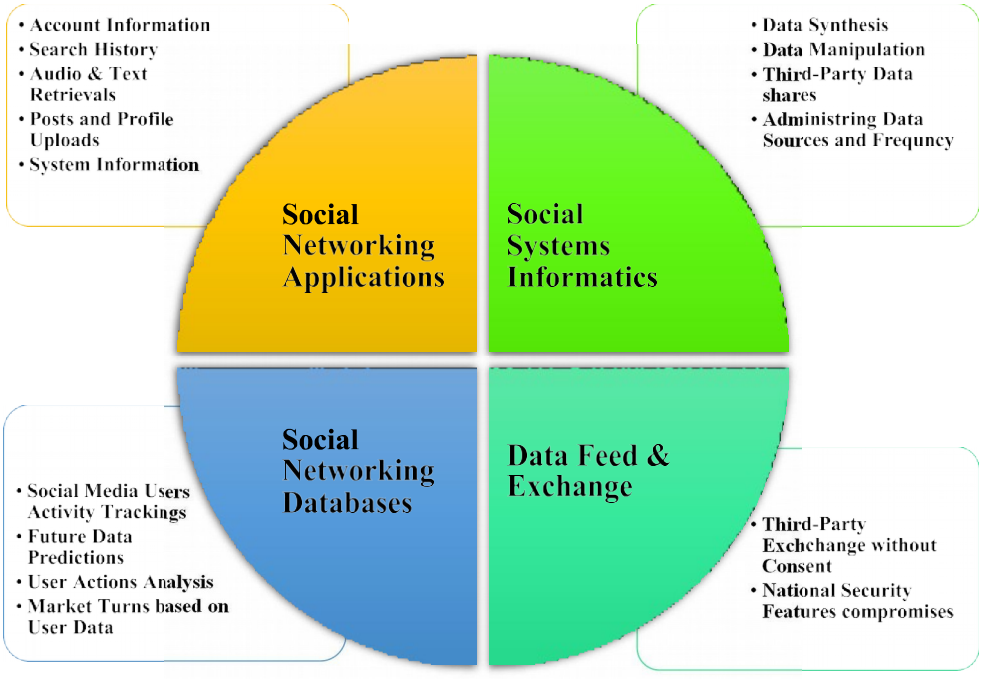

图 2。 网络空间的信息周期及其与社交媒体的融合。

另一个突出的、最近的网络违规行为是谷歌，它可能会干预国家安全。谷歌在 50 万谷歌用户数据安全受到威胁后+ + +
发了令人震惊的结果[27]。据报道，许多政府官员在这次事件报告后被勒索。

信息仅影响国家安全，关键信息如敌人的后勤、作战要素、训练时间表和机构、武器弹药细节、军队敏感行动以及敏感的国防目录等主要通过网络空间侵犯从社交媒体获取[28]。信息驱动的公司受到可疑的监视，信息可以迅速传播，同时带来相信有关国家安全的虚假信息的负面影响。国家安全在隐藏起来的反国家运动手中处于玩闹的边缘，这些运动实际上是针对想要的国家利益。

信息承载因素迫使决策者对国内和国际安全做出不同的反应，从而对国家计划产生不同的影响[29]。国家安全部门不应该禁止使用社交媒体，而是应该实施信息控制法律，限制和过滤社交媒体的信息共享能力。这一因素只有通过人工智能才能实现，我们将在下面的章节中详细讨论。

图 2 说明了网络空间中的信息周期，以及社交媒体作为其中一个组成部分是如何相关的。

社交网络应用程序和社交系统信息学是一个协调的纽带，以促进数据合成、数据操作和第三方数据共享。社会系统信息学管理与网络应用程序密切相关的数据源和频率。它更像是一个高度连接的特征，其中一个信息集触发其他信息集，循环继续，直到一个合适的受众被定位和告知。而社交网络应用程序方便并提供用户的帐户信息，他们的共享信息以及搜索和兴趣历史。

最重要的是，音频/视频和文本检索包含可用于国家安全的可信信息[30]。这组信息还有助于操纵用户进行欺诈、勒索，有时还可以利用一个人来损害国家利益[31]。如图 2 所示，另外两个主要因素是社交网络数据库和数据馈送与交换。有组织形式的信息创建了数据库。

社交网络数据库提供存在于数百万用户之间的完整链接集。例如，阿曼所有居民的数据库应该具有相同的数据链接，并且可以根据年龄、种族和族裔群体等因素在几秒钟内广播所需的信息[32]。任何意图操纵的信息都可能在这种联系的基础上传播，从而危及国家安全和国家行动计划。

图 2 还展示了社交网络数据库对未来数据预测、活动跟踪、市场趋势和用户响应任何国家威胁的响应率的贡献。数据馈送功能扩展了国家妥协。

表 1。摘要查询词和相关的搜索过滤器和结果。

S. No	Search term	IEEE		Elsevier		ACM		Taylor & Francis		Springer	
		Count	Filter	Count	Filter	Count	Filter	Count	Filter	Count	Filter
1	Role of information in national security	956	OR	1002	OR	180	AND	1	OR	9	OR
2	Tools for information synthesis	1138	OR	987	OR	682	AND	0	OR	13	OR
3	Artificial Intelligence for national security	3952	OR	4456	OR	559	AND	0	OR	11	OR
4	National security based parameters	1568	OR	1128	OR	462	AND	0	OR	10	OR
5	Artificial Intelligence social media tools	345	OR	246	OR	103	AND	0	OR	13	OR
6	Social media constraints for national security	3	OR	15	OR	4098	AND	0	OR	0	AND
7	Social media prevailing factors	3	OR	14	OR	3969	AND	0	OR	0	AND
8	Information and national security relatedness	2	OR	1	OR	558	OR	2	OR	5	OR
9	National security and social media	271	OR	35	OR	102	AND	3	OR	438	OR
10	Social media information threats	276	OR	1663	OR	3282	AND	65	OR	0	AND

即使一个国家的居民居住在该国以外的地方，数据馈送仍然会通过基于数据链接的手机发送，从而引发愤怒。这一因素也可以通过未经同意的第三方数据共享来实现[33]。社交媒体的力量已经发现了社会构建的信息炸弹，这些炸弹可以在几秒钟内成为国家安全的目标灾难，而无需付出任何代价。

III. 方法

本研究已作为系统文献综述(SLR)进行。这篇综述需要一个彻底的、透明的、可复制的文献检索和批判性分析过程。单反作为一种方法论，可以将研究问题的定量推理与有效的支持论据结合起来，以建立更好的研究对象。单反过程是由[34]的建议指导的。从[34]开始的审查过程如下:(a)范围界定(b)检索和分析(c)根据研究问题选择同行评议的论文。研究问题的设计是为了满足当前和最新的研究课题。研究问题如下。

本文所涉及的研究问题有:

1. **RQ1:** 通过社交媒体，公众可以获得哪些与国家安全相关的信息?
2. **RQ2:** 随着时间的推移，信息如何影响国家安全?
3. **RQ3:** 信息驱动媒体造成的网络攻击、网络空间操纵和网络战争的当前和未来风险是什么?
4. **RQ4:** 人工智能如何在国家安全中扮演至关重要的角色，完成称职的信息角色，成为国家安全的救世主?

A. 范围

审查的目的是只对特别使用“信息”和“国家安全”一词*的文件进行*审查。这种范围允许我们在信息对国家安全的作用以及在这种情况下的人工智能应用中更好地和有针对性地审查我们感兴趣的领域。根据[34]定义的SLR 建议，同义词和替代术语的识别如表 1 所示。搜索词是用来挖掘同行评议的研究文章的查询词。关于信息对国家安全的作用的工作缺乏明确系统的报道，但这一因素并不限制对调查结果的解释。另外，我们考虑了与我们提议的研究领域最接近的一般文献。

通过阅读摘要和文章的结论来检查相关性和清晰度。图 3 给出了入选和排除标准的完整覆盖范围，以及入选期刊上文章的统计数据。图 3 显示了基于标题的拒绝，基于摘要的拒绝，以及基于所选研究的一般和详细研究的选择的各种参数，以覆盖可信和更广泛的研究领域。

B. 搜索和分析

为了进行全面的搜索和分析，相关的同行评议文献是在可信的搜索引擎上搜索的

即 Google Scholar, Scopus[35] 和 Web of knowledge - edge[36]。就过滤的操作标准而言，我们已经排除了那些在国家证券中明确使用信息是最不受关注的论文。其次，对我们的查询词进行一般性讨论的文章也被排除在外。纳入时，考虑结合使用*“信息”和“国家*安全”并清楚说明我们的研究目的的论文。

C. 评审论文和参考文献概述

最早确定的关于信息在国家安全中的作用的研究文章是近 20 年前的。然而，大多数论文考虑的是 2010 年至 2021 年，主要针对最近的数字时代。表 1 给出了查询响应的完整覆盖范围和选定期刊上文章的统计数据。表 1 还说明了所选论文的出版年份及其会议和期刊类别差异。

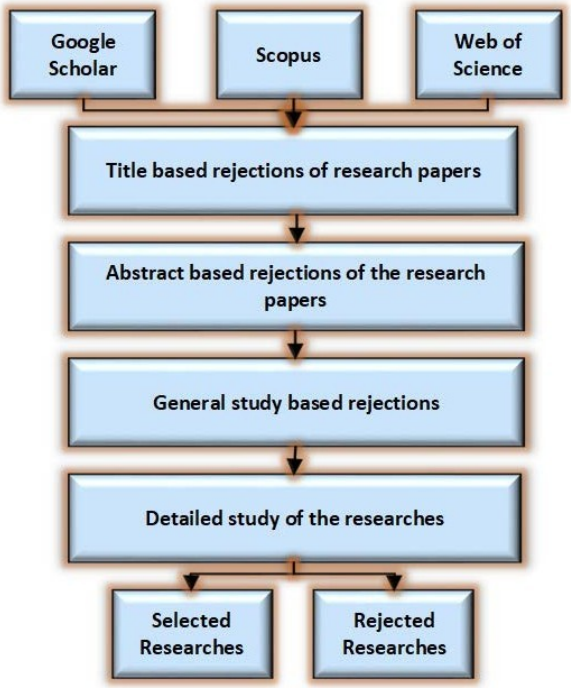

图 3。 排除和纳入标准。

IV. 信息及其对国家安全的影响

信息的意义可以通过

信息传播的速度和相信虚假信息对国家安全造成破坏的影响程度[37]。社交网络的巨大相关性及其可获得的信息是全球挫折，刺激了国家政策制定者对保持安全的兴趣[38]。Twitter 和 Facebook 等社交媒体平台的信息所带来的巨大影响和压力，可以想象会在短时间内破坏国内和国际关系[39]。

全球各国立法者认为，与其否认社交媒体信息的有效适用性，并将社交媒体作为对国家安全的威胁而被强调，不如确保信息的来源及其可信度，然后才能到达每个公民手中[40]。信息可以在发布之前被仔细审查和验证对整个国家开放，以更好地防止任何希望破坏国家安全的行为者[41]。我们需要确定通过社交媒体传播的信息是否值得信赖，从而找出其有效性和可信度。

通过传统方式和网络方式传播的信息具有不同的传播强度和后果[42]。网络战争使普通人的信息共享能力超越了控制能力[43]。受众和平台的变化现在成为国家反安全机构的首选武器。为每个使用者提供信息共享能力，应通过定义的过滤器，以保护任何负面和不可预见的情况[44]。人工智能有可能对信息进行过滤和审查，从而可能控制以下国家安全计划和措施。

A. 理解人工智能需要国家安全框架

在线社交网络一直呈现出爆炸性的年增长。在成为使用最广泛、适应性最强的信息源后，它极大地迎合了国家利益[45]。定向广告和病毒式营销被引入，在没有事先检查和审查的情况下利用社会信息[46]。由于媒体平台上的再分享功能，虚假信息往往传播得更快。 要删除虚假信息，需要将其从所有已经共享该信息的相关人员中删除。

移除威胁性信息是一项看似乏味的任务，但消除其对人们的影响更具威胁性和挑战性[47]。人们的日常生活越来越依赖于在线获取信息及其相关服务。通过网络空间对社交媒体用户的操纵既高效又方便[48]。有效区分授权和未经授权的信息源可以极大地帮助在第一时间阻止错误信息。

通过合并图 4 中建议的非常简单的检查，可以使信息变得可停止和可问责。在图 4 中，我们提出了一个简单的模型，它可以明智地采取行动，限制信息的传播，以限制国家的妥协。根据该模型，信息来源于两个来源:1)真实来源，如批准用户、国家组织和政府拥有的媒体渠道。2)非真实来源，如数百万社交媒体用户和私营信息广播集团。基于需求的非真实源有效地服从于 AI 框架。社交媒体信息不仅仅是基于文本的。它还源自图像、视频/视觉和语音/音频环境，这些环境可以通过提议模型中强调的人工智能框架进行显著监控。在经过广泛的过滤和检查后，信息要么被批准(允许潜在用户分享)，要么被不批准(抛弃)。详细的

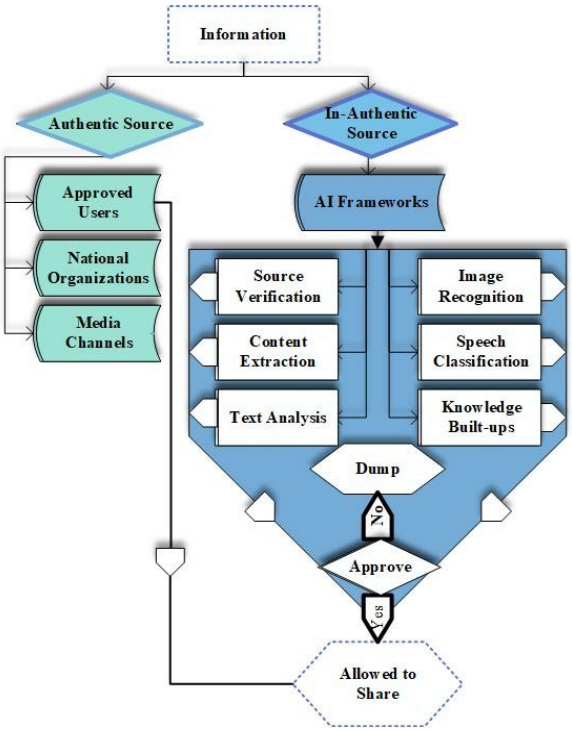

图 4。 限制信息模型。

算法 1 中描述了算法函数，它一步一步地解释了函数操作。

模型中提出的人工智能框架可以解决虚假信息传播、反国家用户、稳定威胁、信息过滤等问题。该模型封装了每个信息上下文，即来源验证，内容和文本分析，图像和语音分类以及知识构建，所有这些都由人工智能机制提供支持。此外，它还可以帮助定位信息来源。在不真实的源可以执行某种操作之前，应该始终检查它们。我们的模型中使用的人工智能机制将在下面的章节中讨论。

B. 基于人工智能的源识别机制

信息源识别和信息源定位是在潜在的错误信息源传播到数百万用户之前将其扼杀在萌芽状态的关键因素[49]。恶意参与网络空间违法行为的社交媒体账户持有人很难被追踪，从而继续其反国家使命，破坏行动计划的稳定[50]。在反击这些来源和追踪他们的后台支持机构时，担心被抓住和被追踪是至关重要的。

基于人工智能的源识别机制可以为跟踪和定位特征提供很大的支持[51]。人工智能机制有助于在几秒钟内更轻松地从更大的数据集中追踪数据源及其相对联系[52]。人工智能已经渗透到追踪社交媒体信息的根源，并提供了更好的来源树

算法 1 信息认证/内认证;
回收，拒绝，批准。

1. *功能信息_鉴权{*
2. *这是才∩经批准的信息*
3. *I(I,∩ I,/=*
4. *u(u,:= –*
5. *然后*
6. *批准 I(I)*
7. *声明我是真实的*
8. *Else If (θ)* then
9. *选择() ∩选择*

Σ10。 *如果 I,∩选择*

I，*那么* ∩

12. *恒真*
13. *如果*
14. *如果*
15. *结束时*

16. *}*

17. *函数 I_Rejection {*
18. *设置信息为 Sink，信息为*
19. *AI_Report_User*
20. *发送(information_message)*

21. *}*

22. *//接收来自 U 用户的 I 消息*
23. *函数 recv_users_Credentials (){*
24. *设置用户[n][o]为 UID*
25. *设置用户[L][1]为 ULOC*
26. *设置用户[IP][2]为 UIP*
27. *设置用户[A][3]为“不尝试”*
28. *设置用户[P][4]为 uid*

29. *}*

30. *recv_users_Credentials {*
31. *从 0 至=V*
32. *将用户分配到 Dump Seg [m]*
33. *UID,* ULoc, *UIP//d 是段的索引*
34. *转储*
35. *结束了*
36. *}*
37. *// AI 框架的真实过程--*
38. *函数 authenticate (){*
39. *如果(→U(υ)则*
40. *发送执行(P(ρ))(媒体，→*
41. *National_Organization,*
42. *(P，用户)(←*
43. *其他的*
44. *发送凭据(UID, ULoc, UIP) AI →*
45. *框架*
46. *如果*
47. *}*

可追溯性特性在几秒钟内。大量的用户曾经难以管理，现在 AI 引入了一种机制，可以通过高数据量带来更好的可追溯性[53]。

人工智能为准确的机制处理提供了可能的支持，这显示了信息来源/用户可以轻松地从数百万用户中定位的巨大潜力。很少有这样的机制:

1) 人工神经网络(ann)

因为所有不容易被跟踪的东西都可以通过神经网络很容易地分类。人工神经网络提出的工具允许人类处理架构决策，而优化和可追溯性特性由网络机制控制和执行。人工神经网络有助于在优化网络的同时建立关联链接[54]，[55]。

2) SCIKIT-LEARN

它支持无监督学习计算，以创建选择树和聚束组插图。它提供了一个经过精心计算和有针对性的顺序，并具有信息更改的附加特性。任何阶段的信息变化也可以通过特征确定和集成技术来跟踪，这些技术可以在几行代码和更少的时间内完成[56]。

3) THEANO

它使信息计数多达多次，以提供有关一条信息被共享多少次的计算数字。它简化了定位用户数量的复杂计算任务。这是发现信息传播严重性的一个非常重要的特征[57]。

4) MXNET

解决整套新的主机设备和新进入的设备以与社区开发的框架保持一致是有用的[58]。

5) KERAS

对于图像识别问题和选择合适的结构，KERAS 可以做出很好的贡献。社交媒体上的信息来源不仅以文本形式传播和共享。图像对网络空间违规行为同样具有威胁[59]。

6) 3

风险和欺诈分析是通过 H20 提供的一个急需的功能。它使用了预测分析、保险分析、广告应用以及客户情报。客户智能允许保持活动记录以产生所需的结果，而无需运行广泛的搜索活动[60]。

C. 国家安全和受控信息处理

社交媒体的主要优势之一是，它允许政府在危机中分享关键信息。一个这样的事件是政府在报道中受益2016 年的土耳其[61]。土耳其总统埃尔多安利用社交媒体通过强大的信息来源击败军事坦克，呼吁土耳其民族。成功地，土耳其人的叛乱企图被镇压，埃尔多安出面维持和平[62]。据报道，策划的反叛行为主要是通过社交媒体传播和传播的。

在这些事件浮出水面后，不同国家的国家安全措施开始采取不同的措施。在全球范围内，社交媒体防止国家安全的信息控制措施各不相同，有不同的选择和偏好。在这方面，有些国家似乎很死板，而另一些国家则有点放松。例如，中国和朝鲜是受控制的社交媒体和所有其他严格审查的信息寻求平台的首选国家[63]，[64]。所有的信息在到达其他受众之前都要经过严格的障碍。

此外，这些国家还会对违反国家安全计划的用户进行处罚。伊朗是另一个严格封锁所有社交媒体平台的著名国家，同时严格审查政治媒体以确保国家稳定。在朝鲜、中国和伊朗之后，还有白俄罗斯、卡塔尔、叙利亚、泰国和阿联酋等国家严格过滤传播的信息，以更好地应对国家安全问题[65]。欧洲也施加了适当的限制[66]。这些国家限制了社交媒体，并严格监控了通信应用障碍，限制了信息的快速和受控共享。最重要的是，大多数海湾国家已经停止了 wi-fi 呼叫，以加强对稳定国家安全的检查[67]。

D. 不同可能的攻击

社交媒体数据和信息并不是促成国家安全妥协的唯一因素。国家安全还可能受到其他不同的攻击。然而，不同可能的攻击因素主要是信息驱动的。例如:短信、语音通话、传真、电子邮件、宣传册、印刷信息以及其他各种印刷媒体资源。上述消息来源与社交媒体无关，但它们至关重要，足够强大，可以为攻击提供支持，破坏国家安全。无论是来自社交媒体的信息传播源，还是社交媒体之外的信息传播源，都同样扰乱着国家利益。然而，与其他手段相比，社交媒体的工作速度最快。图 6 中提到了具有广域覆盖范围的详细可能的攻击。

V. 信息随着时间的推移而进化

在不到一代人的时间里，信息交换平台
已经显著地从仅仅耗时的电子交换演变为虚拟实时高效的 21 世纪信息中心工具[68]。几年之内，社交媒体已经影响了数十亿人的生活。我们现在

生活在数字化转型的生活中，信息正在成为驱动生活方式的主要因素之一。

20 世纪 80 年代和 90 年代被认为是一个突出的时代，电子邮件和在线服务器，如美国在线[69]，Prodigy[70]和 CompuServe[71]，充当了网络平台，但不知怎的，鲜为人知，仅限于在线聊天。最早在 2000 年，Friendster[72]作为一个吸引数百万用户的平台出现，但仅限于基本的在线互动。2002 年是领英[73]推出的一年，有事业心的人在这一年被托管，现在已经增长到全球超过 6.75 亿用户。然而，该网站只针对求职者的利益，不提供违反国家关切的信息。

2008 年的 Facebook、2011 年的 Myspace 和 2012 年的+Google 成为信息交换媒介的关键媒介[74]。在短时间内，72%的美国成年人使用社交媒体平台，在没有任何检查和过滤的情况下分享信息。令人惊讶的是，每秒发送 6000 条 tweet，即每分钟发送 35 万条 tweet，每天发送 5 亿条 tweet，每年发送 2000 亿条 tweet[75]。

信息进化不仅局限于用户的个人资料平台，还将其维度扩大到流媒体视频平台、博客和博客，以提供真实和真实的感觉[76]。例如，由个人用户交换的信息可能不会像知名媒体机构拥有的博客那样迅速引发争议。各种基于视频的频道也可能不稳定。

图 5。信息时代的行动方针。

在前社会媒体时代，信息的传播是为了告知他人，而不是为了被操纵。大多数时候，报纸、杂志和期刊一天发一次，因此，任何细节和信息都应该在下班后到达。检查信息真实性需要一定的时间[45]。现在，情况不同了。信息的传播速度比否定先前信息的信息要快。

A.信息时代和行动方针

有两个信息时代，即初级信息时代和次级信息时代。初级信息时代是指互联网出现之前的时代，主要由报纸、广播和电视组成[77]。大多数情况下，信息部门是政府所有的，控制得很好，而且速度很慢。二次信息时代是互联网和卫星电视的时代。信息共享基于私有的快速平台，没有任何过滤、控制检查或政府干预[78]。

第三信息时代是指当前与移动设备相连的时代，数百万用户可以自由地共享信息，而无需事先审查。换句话说，病毒式广告和煽动性内容在很大程度上支持了破坏国家安全计划的行为[79]。第三信息时代对国家利益的潜在威胁和风险更大。为了与转变中的资讯时代竞争，图 5 展示了一个四步行动计划，以警惕地执行其行动，以应对以下第三次资讯时代:

1) 行动

第一步是 Action，它需要在实时响应的基础上发挥作用。定位用户并根据国家利益解释其社会活动的行动可以从一开始就根除反国家运动。定位和追踪可能充当共同罪犯的连接用户也可以降低网络空间违规行为的潜在来源。

2) 计划

第二步是在执行国家战略行动计划之前进行规划。这一步骤以国家目标和议程为基础。计划合适的行动方案有助于对未来通信进行预测分析。最重要的是，针对并根除攻击者的优势和劣势是通过完成这一步而获得的其他方面。

3) 策略

国家战略措施在维护安全和应对即将到来的变化方面是至关重要和保密的。确定战略，并使其保密，以攻击隐藏的行动计划。战略措施的健壮性有助于保持无缺陷的安全性。

4) AI 工具

模型中描述的基于人工智能的工具是正确的，正确使用可以帮助定位匿名活动[22]。监控活动并以适当的惩罚抓住罪犯可以降低未来遭受挫折的风险。最重要的是，人工智能工具还可以确保根据实施的国家安全计划衡量成功率。参见 IV (B)。

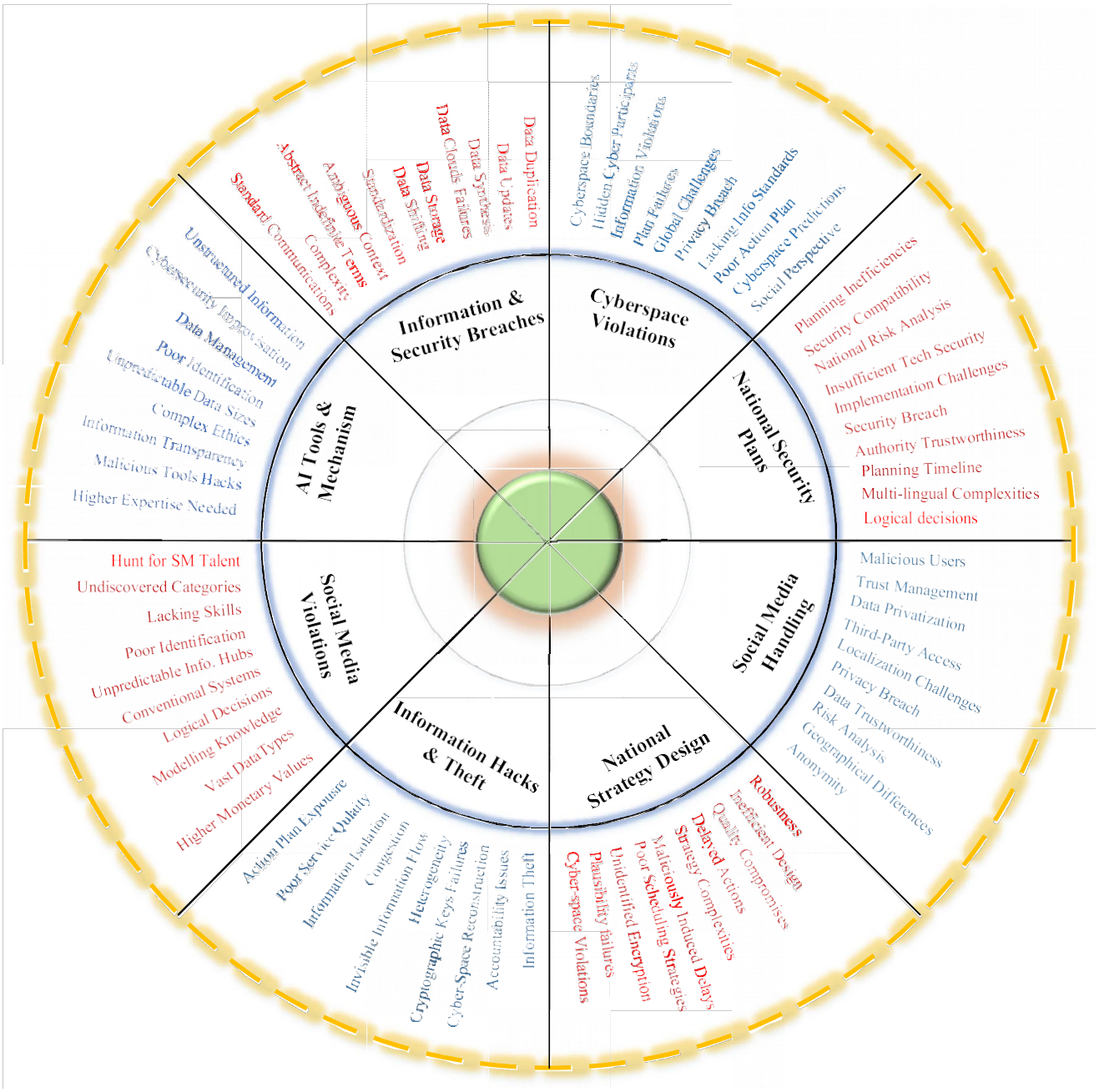

图 6。 国家安全的挑战和信息缺口树形图。

VI. 网络空间侵犯国家安全的当前和未来风险

目前和未来有许多网络攻击的风险，
网络空间操纵，以及信息驱动媒体引发的网络战争。由于严重的网络空间违规行为，事情不可避免地会失控[80]。受影响最大的领域是国家安全。实体战争现在已经转变为虚拟的网络战，在网络战中，贬低一个国家的国家进步和议程比使用更致命的武器和实际的军队要简单得多。

目前，社交媒体在全球的移动设备用户已经达到 50 亿[81]，社交网络已经深入扎根，可以在几分钟内满足用户的需求。这些信息泄漏设备由用户随时随地携带，从而保证了信息的最佳可访问性和网络攻击的最坏情况[82]。

具体而言，政府和军队官员是窃取敏感信息以瞄准国家证券的高目标[83]。目前的事实是，我们的数字生活似乎完全容易受到网络罪犯和间谍的影响。一大批网络攻击者就是如此

表 2。在社交媒体上提供信息协助的人工智能工具。

Tool	Purpose	Preferred Application Areas
DeepText [104]	To understand conversation better for information processing, Translation of different languages	Social Media applications specifically Facebook
FBLearner Flow platform [105]	To run thousands of user classifications along with content understanding	Primarily developed, used, and adapted by Facebook
MonkeyLearn [106]	To gain insight from social media Text data.	Natural language processing based social media applications
Aylien [107]	To deal with large volumes of real-time content from the new outlet and social media content	Academic publications, New reporting applications, entity extraction, and sentiment analysis platforms
IBM Watson [108]	To deal with information available on Clouds based on extracting keywords, categories, and entities.	Specifically designed by IBM to tailor industrial information needs and dive documents.
TextBlob [109]	For text classification, part-of-speech tagging	Excellent, easy, and user-friendly interface for easy and beginners applications.
GenSim [110]	Recognizing text similarities, text indexing, and navigating text documents.	For handling large volumes of data that needs a fast and scalable solution.
FAIR [111]	Facebook Artificial Intelligence Researchers tool to analyze and develop AI systems with the intelligence level of humans.	For AI-based research and innovation. Specifically, Facebook (a social media application) uses FAIR.
CRM[112]	AI-powered automation platform designed for scheduling a call and other audio-aided features.	Every social media application allows users for making/scheduling a call thus it is used by almost all current applications.
Chatbots [113]	Intelligent and self-supported auto answer generator (in response to user questions).	Specifically used for automated customer help, and widely used in online selling and buying websites.
rasa.io [114]	For one-to-one conversations for millions of contacts	Marketing, subscribing, and other broadcasting applications.

依附于最大的国家组织获取对国家尊严和安全最重要的敏感信息[84]。

在网络空间侵害的各种风险中，很少有风险能更容易地撼动证券参数。Ran- somware 天启是网络入侵的关键和流行现象之一[85]。恶意的全球攻击者要求一笔可观的赎金，并威胁说，如果条件不满足，他们将公开分享信息。在处理全球网络空间问题时，网络空间违规行为也构成了一定的风险。每个网络空间都遵循不同的标准和协议[86]。

最近的一个例子是美国情报机构“太阳风”(SolarWinds) 2021 年的黑客攻击[87]，黑客从美国政府和敏感部门收集了数不清的情报信息，进行勒索，以换取巨额赎金。根据网络安全和基础设施安全局(CISA)的报告[88]，SolarWinds 黑客攻击涉及三家重要的美国公司(SolarWinds，微软和 VMWare)以及 12 个联邦机构(NASA 和联邦航空管理局)。这次攻击的目的是破坏美国的声誉，并暴露对维护美国国家安全至关重要的秘密[89]。

图 6 显示了最近国家安全面临的深度挑战、人工智能和信息差距。有八个突出的因素。Social Media Violations 负责组建一支合适且技术娴熟的团队，能够有效应对任何可能的威胁[90]。 在谨慎应对社交媒体攻击的专业水平上存在适当的差距[91]。毫无疑问，利用社交媒体平台制造信息威胁的操纵者精通高科技。为了应对这样的专业水平，需要一个更高、更兼容的团队来消除威胁效应[80]。

信息黑客和盗窃是威胁国家安全的另一种方式。国家机构计划的行动过程受到盗窃的威胁，这使得黑客更有能力反击国家计划[92]。行动计划暴露是危险的，会导致无形的信息流。即使信息是通过适当的加解密功能存储的，被盗的加密密钥也会被修改以泄露信息[93]。

国家战略设计是促成信息操纵的另一个不可或缺的因素[94]。质量承诺和战略复杂性可能是主要原因。其次，恶意导致的战略行动延迟也允许信息传播，从而造成潜在危害并导致网络空间违规[95]。

处理社会媒体也有助于实现更好的国家安全。恶意和无法识别的用户;

第三方访问、本地化违规以及国际发达的社交媒体链接之间的信任管理，都增加了对国家安全的威胁因素[96]。地理差异(时区和语言障碍)也是确保国家安全稳定的重要因素[97]。

国家安全计划在应对全球威胁方面兼容性差，效率低下。执行已定义计划的实现挑战是允许恶意用户自由执行其操作的另一种方式[98]。时间自由本身就是一种非常乏味的行为，它直接为入侵者提供了便利。

网络空间违规行为包括跨越定义的边界、隐藏的参与者和网络空间预测的不相容的社会视角。网络空间预测对于预测下一个可能危及国家安全的操纵者行为是必要的[99]。缺乏信息标准来做这样的预测也增加了令人担忧的情况。

在数据重复、数据更新、数据云故障、数据存储和数据转移方面的信息和安全漏洞是非常关键的行为，在不知不觉中促进了安全漏洞。缺乏沟通标准也是导致信息和安全漏洞的一个因素。

VII. 用于国家安全的人工智能工具

人工智能对国家安全至关重要

完成称职的信息角色，成为国家安全的救星[100]。人工智能是一个鼓舞人心的技术平台，是几代人中最强大的工具，有利于国家安全[101]。人工智能并不局限于改善人类生活以解决自然问题。信息技术拓宽了人们探索看似不可能的奥秘的途径，如今已成为改变游戏规则的超级力量[102]。

人工智能已经扎根于基于社交媒体的平台，因为它拥有多样化的应用程序和便利设施。表 2 涵盖了各种工具及其用途和可能的应用程序，这些工具可以解决上面确定的许多问题。这些工具为当前许多网络空间问题提供了解决方案，并充当了防范反国家因素的卫士。所确定的每种工具在其性质、应用和目的方面都是独一无二的[103]。这些工具也会根据用户的选择进行所需的特征提取和编辑。

表 2 工具是基于人工智能的，有助于自动化图 6 中突出显示的许多繁琐的任务。这些工具使社交媒体管理变得可控，同时对社交媒体进行更大规模的监控。人工智能使社交媒体及其相关信息能够更好地理解国家偏好[103]。　人工智能有助于有效、便捷地定位和消除威胁因素。

VIII. 结论

人工智能正在通过其应用彻底改变信息角色，并帮助解决复杂的网络空间问题。人工智能可以根据社交媒体用户的意图和行为，为他们提供实时的信息个性化。它可以用来编辑、禁止和定位反国家运动，以满足国家安全需要。人工智能还可以帮助进行内容审查，以查找反国家特工、国家网络犯罪分子和安全计划破坏者的匹配。它可以用来处理日常任务，如性能分析、反政府竞选报告等等。

在我们的文章中，我们已经确定了可以帮助处理社交媒体信息以更好地保护国家安全的人工智能工具。我们已经确定了利用当前和最近旨在动摇国家安全参数和计划的攻击来操纵信息以破坏国家安全的初步方法。本文简要介绍了信息如何严重地参与敏感信息检索，传播虚假信息，创建垃圾邮件以错误地驱动用户的思想，以及为勒索目的可能的隐私盗窃，并举例说明当前功能领域的局限性。

本文所涵盖的所有内容都是通过系统文献综述(SLR)来演绎可信和真实的论点，以回应制定的研究问题，如信息对国家安全的影响，信息演变，网络空间侵犯对国家安全的当前和未来风险，特别强调人工智能是国家安全的救星。在最后一节中，列出了具有目的和应用领域的信息调查和分析的重要工具，以方便读者更好地使用信息和预防，以维护国家安全。

未来的发展方向

未来研究人员可能采取的行动是建立多功能的信息流信息处理工具，以帮助维持更好的国家安全措施。其次，未来的另一个方向是绘制可证明和可追溯的参数，以满足来自社交媒体平台的信息的安全标准。这些参数有助于建立负责任的措施，在国家威胁损害安全计划之前抓住它们。

参考文献

[1] 刘志强，“网络安全在信息技术教育中的作用”，《信息技术教育》第 1 期。*相依。正无穷。科技——nol。建造。(SIGITE)，美国纽约，纽约*，2011 年，第 113-122 页，doi: 10.1145/2047594.2047628。

[2] (2021)。s.e. 研究所。*CERT 协调中心*。(在线)。可用:https://sei.cmu.edu/about/divisions/cert/index.cfm

[3] 莫厄里，“国家安全和国家创新体系”，*j .抛光工艺。译本，第 34 卷*，第 6 号。5, p. 455, 2009。

[4] a . Dutta 和 K. mcrohan，“网络经济中管理在信息安全中的作用”，California Management。*Rev.，第 45 卷*，no。1，第 67-87 页，2002 年 10 月，doi: 10.2307 / 41166154。

[5] t.e.科普兰，“信息革命与国家安全”，陆军战争学院，卡莱尔兵营，战略研究中心。 美国理工学院代表,2000。(在线)。可获取:https://apps.dtic.mil/sti/ pdf /ADA382498.pdf

[6] S. L. Jarvenpaa 和 A. Majchrzak，“保护国家安全的专业人员之间的知识合作”；交互记忆在以自我为中心的知识网络中的作用[j]。*科学。*，第 19 卷，no。2，页 260-276,2008 年 4 月。

[7] 唐道克、林德明、林瑞麟:“虚假信息的传播:实证研究”社交媒体用户对假新闻的反应及其原因，《新闻》，第 21 卷，第 2 *期。3，第 381-398 页，2020* 年 3 月。

[8] S. J.施瓦茨斯坦和 W. *A.欧文斯:信息革命与国家安全: 尺寸和方向*。美国华盛顿特区: 战略与国际研究中心，1996 年。(在线)。可用: https://www.ojp.gov/ncjrs/virtual-library/abstracts/information-revolution-and-national-security-dimensions-and

[9] V. V. Novikov，“经济和教育的数字化: 通往商业领导和国家安全的道路，”巴士。伦理领导，第五 *卷，第 5 期。2，第 147-155 页，2021*。

[10] J. Der Derian，“全球事件、国家安全与虚拟理论”，《新世纪》(英文版)。钉。，第 30 卷，第 3 期。3, *pp. 669-690, Dec. 2001, doi:* 10.1177 / 03058298010300030301。

[11] K. A. Oluwadamilola，“信息技术在国家安全中的作用:“尼日利亚的案例研究”，Global J. Comput。 *科学。抛光工艺。，第 16 卷，*第 2 期。3, pp. 1-7, 2016。(在线)。可用:https://computerresearch.org/index.php/computer/article/view/1443

[12] “信息安全作为一个意识形态问题”，《思 *想科学》。Methodol。[J]，* 2020 年第 1 期。1, pp. 56-65, 2020。

[13] Z. D. Clopton，“领土、技术和国家安全”，university。*《芝加哥法律修订本》，第 83 卷，*第 2 号。1, p. 45, 2016。(在线)。可用:https://heinonline.org/HOL/P?h=hein.journals/uclr83&i=47

[14] “人工智能、前瞻性治理与安全的未来”，《瑞士政治科 *学》。Rev.， vol.* 27, no。1，第 170-179 页，2021 年 3 月。

[15] G. Mani，“国家安全情报的数据处理和分析:《数据 *管理、分析与创新》*。新加坡: Springer, 2022, pp. 293-315, doi: 10.1007 / 978-981-16-2937-2。

[16] A. Bratko, A. Datskov, D. Oleshko, V. Vychavka 和 O. Olytskyi，“国家安全领域中基于能力的规划的某些方面”，土耳其 J. Comput。*数学。建造。，第 12 卷，*no。6, pp. 2219-2225, april . 2021, doi: 10.17762 / turcomat.v12i6.4827。

[17] F. D. Kramer, S. H. Starr, L. K. Wentz，《网络力 *量与国家安全》*。美国华盛顿特区: 波托马克出版社，2009 年。

[18] D. S. Reveron，*网络空间与国家安全: 虚拟世界中的威胁、机会和权力*。美国华盛顿特区: 乔治敦大学。出版社,2012 年。

[19] C.惠 *兰，网络和国家安全: 动态，效率和组织*。美国伊利诺伊州埃文斯顿: 劳特利奇,2016 年。

[20] 罗根，“在信息技术中构建大学生信息安全重点”，J. Inf。 *系统。建造。，第 13 卷，*第 3 期。3，第 177-182 页，2002。

[21] R. von Solms 和 J. van Niekerk，“从信息安全到网络安全”，计算机。*安全内核。*，第 38 卷，第 97-102 页，2013 年 10 月。

[22] j·l·海耶斯，b·c·布里特，w·埃文斯，s·w·拉什，n·a·塔维利，以及 a.c. Adamson，“社交媒体监听平台的人工智能可信吗?”检验 crimson hexagon(现为 brandwatch 消费者研究公司)人工智能驱动分析的准确性，《J. Advertising》，第 50 卷，第 5 期。1，第 81-91 页，2021 年 1 月。

[23] A.蒙蒂和 R.瓦克斯:*《新世界秩序中的国家安全》；政府与信息技术，第 1 版*。印度: Routledge, 2021, doi: 10.4324 / 9780367809775。

[24] J. A. Lewis, J. S. Nye, E. Schlather，《计算机 *出口与国家安全》新世纪的新工具: 战略与国际研究中心 21 世纪技术安全委员会报告* 美国华盛顿特区: 战略与国际研究中心,2001 年。

[25] S. A.泰勒，“情报在国家安全中的作用”，当代。*安全内核。钉。，第 67-249* 页， 2007。(在线)。可用: http://people。柯林斯 exeter.ac.uk / mm394 /情报/ % 202007% 20 情报 % 20(泰勒). pdf

[26] J. Crawford，“计算机滥用行为和黑客: 对那些根据该法被定罪的人的审查。安全内核。罗伊。Holloway 大学。伦敦，埃格姆，英国，技术。代表,2021。(在线)。可用:https://regmedia.co.uk/2021/04/12/techreport-jamescrawford.pdf

[27] A. K. Franck 和 D. Vigneswaran，“入侵迁移控制: 重构和重新编程可移植性，“安全。*《对话》，2021 年 4 月，*艺术。不。0967010621996938, doi: 10.1177 / 0967010621996938。

[28] B. Charoenwong 和 M. Bernardi，“加密货币‘黑客’的十年: 2011-2021，“ssn 3944435，南京大学。新加坡，新加坡，科技。众议员，2021 年，doi: 10.2139 / ssrn.3944435。

[29] 蔡迪、罗斯，“资讯权利与国家安全”，《政府资 *讯》。夸脱。，第 22* 卷，第 2 期。4，第 663-684 页，2005 年 1 月。

[30] 宋,j·李,j .公园,C.-K。Kim，“社会关系的关键是: 安全的新范式。*系统。，* vol. 71, pp. 68-77, Nov. 2017, doi: 10.1016 / j.is.2017.07.003。

[31] C. Antonoudis，《利用社交网络进行执法》。 希腊的范例，“Int。希腊大学，Thermi, Greece, Tech 代表,2021。(在线)。可用地址:https://repository.ihu.edu.gr// xmlui/handle/11544/29722

[32] E. Elsawy，“数字平台及其在加强阿曼国家记录和档案当局的教育和媒体作用方面的重要性”，《国家档案和档案管理》，第 1 部分。*22 日 Int。阿拉伯相依。正无穷。抛光工艺。(ACIT)，十二月 2021,pp.* 1-8。

[33] G. Hitman 和 M. Zwilling，“与以色列的正常化: 社会网络话语在海湾国家的分析，”民族政治，第 1-27 页，*四月 2021,doi:* 10.1080 / 17449057.2021.1901380。

[34] B. A. Kitchenham，“执行系统评价的程序”，Keele university, Keele, Tech。代表,2004。(在线)。可用: https://www.inf.ufsc.br/aldo.vw / kitchenham.pdf

[35] P. Mongeon 和 A. Paul-Hus，“科学网络和 scopus 的期刊报道: 比较分析，《科学计量学》，第 106 卷，*第 6 期。1, pp.* 213-228, 2016 年 1 月。

[36] A. A. Chadegani, H. Salehi, M. M. Yunus, H. Farhadi, M. Fooladi, M. Farhadi 和 N. A. Ebrahim，“两种主要学术文献集的比较: 科学网络与 scopus 数据库，《亚洲社会科学》。，第 9 卷，*第 9 期。5, pp. 18-26, 2013* 年 4 月。

[37] F. Hernandez，“社交媒体对社会和国家安全的威胁: 社会媒体政策和立法的呼吁，”自由大学，林奇堡，弗吉尼亚州，美国，技术。代表,2021。

[38] 吕虹，袁思，“是什么促使人们在社交媒体上分享灾民的信息?”探索同情、悲伤、期望违反和享受的作用。[j] .防灾减灾，第 63 卷，*2021 年 9 月，第 1 期。不。102431.*

[39] L. Almadhoor，“社交媒体与网络犯罪”，土耳其 J.康普。 *数学。建造。，第* 12 卷，no。10, pp. 2972-2981, 2021。

[40] M. J. Baeth 和 M. S. Aktas，“使用大社会来源数据的自定义隐私策略 vio 检测问题的方法”，并发计算。, Pract。*擅长。，第 30* 卷，第 3 期。21, p. 469, 2018 年 11 月。

[41] C. C. Ashbrook 和 A. R. Zalba，“社交媒体对外交谈判的影响: 改变桌子的形状”，《谈判杂志》，第 37 卷，*第 7 期。1，第 83-96 页，2021* 年 1 月。

[42] C. L.文托拉，“社交媒体和医疗保健专业人员: 利益、风险和最佳实践”，《药学治疗学》，*第 39 卷，第 39 期。7, p.* 491, 2014。

[43] H. Okamoto，《解决担保-权利悖论: 如何在国家安全的范围内重新想象个人政治。芝加哥，芝加哥，伊利诺伊州，美国，技术。众议员，2021 年，doi: 10.6082 / uchicago.3275。

[44] 马德明，刘海华，宋德明，“词图网络: “理解社交媒体上的模糊句子以进行违规评论检测”。*CCF Int。相依。自然朗。的过程。下巴。 第一版。* 瑞士 Cham: Springer, 2020, pp. 738-750, doi: 10.1007 / 978 - 3 - 030-60450-9。

[45] T. Aichner, M. grnfelder, O. Maurer 和 D. Jegeni，《25 年的社交媒体: 《1994 年至 2019 年社交媒体应用和定义综述》，《网络心理学，行为学》。，社交网络。，第 24 卷，第 *2 期。4, pp. 215-222, april . 2021*。

[46] P. Harrigan, T. M. Daly, K. Coussement, J. A. Lee, G. N. southar, and U. Evers，“识别社交媒体上的影响者”，英。j . Inf。*管理。，vol. 56,* february 2021, Art。不。102246.

[47] A.蒙蒂和 R.瓦克斯:*《新世界秩序中的国家安全》；政府与信息技术*。美国伊利诺伊州埃文斯顿: 劳特利奇,2021 年。

[48] K. Patel 和 D. Chudasama，“网络空间中的国家安全威胁”，*Nat. J.网络安全。法律，*第 4 卷，第 2 号。1, pp. 12 - 20,2021。

[49] M. Kryshtanovych, L. Antonova, B. Pohrishchuk, Y. Mironova, and

“国家安全背景下的反危机管理信息系统”，国际信息技术研究所。j .*第一版。科学。Netw。安全内核。，第*21 卷，第 1 期。12spc, pp. 719-725, 2021。

[50] O. M. Rieznik, N. S. Andriichenko 和 I. V. Zvozdetska，“作为国家安全部门一部分的警务结果和观点”，《语言学文化》，2021。(在线)。可用:https://essuir.sumdu.edu.ua/handle/123456789/86772

[51] B. Babic, D. L. Chen, T. Evgeniou, a . L.。Fayard，“一种更好的搭载人工智能的方式”，哈佛巴士。Rev.， vol. 98, no。4, pp. 56-65, 2021。

[52] C. Collins, D. Dennehy, K. Conboy, P. Mikalef，“信息系统研究中的人工智能：一个系统的文献综述和研究议程，“国际。j . *Inf*。*管理*。， *vol.* 60, october 2021, Art。不。102383.

[53] E. Schmidt, B. Work, S. Catz, S. Chien, C. Darby, K. Ford, J.-M。格里菲思,
E. Horvitz, A. Jassy, W. Mark 和 J. Matheny，“国家安全委员会对人工智能(AI)的任务”，《国家安全》。委员会 Artif。智能。，华盛顿特区，美国，科技代表,2021 。(在线)。可用:https://apps.dtic.mil/sti/pdfs/AD1124333.pdf

[54] I. A. Akour, R. S. Al-Maroof, R. Alfaisal 和 S. A. Salloum，“海湾地区高等院校中确定元生态采用的概念框架: 一项使用混合 SEM-ANN 方法的实证研究。*建造*。, *Artif*。*智能*。， *vol.* 3, january 2022, Art。不。100052.

[55] R. Amalraj 和 M. Dharmalingam，“基于反向传播的工作点计数系统求解双假桥问题”，《神经计算》，vol. 168, pp. 160-178, Nov. 2015, doi:10.1016 / j.neucom.2015.06.001。

[56] M. Khorrami, M. Khorrami 和 F. Farhangi，“基于社交媒体照片预测五大人格特征的树型集成算法的评估: 来自伊朗样本的证据，《个性个体*差异*》，*第 188 卷，2022 年 4 月，第 1 页*。*不*。111479.

[57] A. Kumar 和 N. Sachdeva，“基于注意力和 CapsNet 的 bi-GRU 混合模型在社交媒体上的网络欺凌检测”，《万维网》，第 1-14 页，2021 年 7 月，doi:10.1007 / s11280 - 021 - 00920 - 4。

[58] 张欣，“基于神经网络数学模型的艺术设计色彩匹配研究”，《数学》。*Eng 问题*。， *2022 年* 3 月，第 1-8 页。

[59] D. Sumathi 和 K. Alluri，“使用 keras 为各种实时应用部署深度学习模型”，《面向工程师和科学家的高级深度学习》。瑞士 Cham: Springer, 2021, pp. 113-143, doi: 10.1007 / 978-3-030-66519-7。

[60] g.z. Savaci, b.k. Bayraktar 和 Ç。 Özen，“行为因素对社交媒体成瘾的影响”， J. Comput。*建造*。*Res.*， *vol.* 9, pp. 1059-1083, december 2021。

[61] M. Savci 和 M. D. Griffiths，“土耳其社交媒体渴望量表(SMCS)的发展: 一项验证性研究，“Int。J.心理健康成*瘾，第 19 卷，第 19 期*。*2, pp. 359-373, april* . 2021。

[62] 奥兹先生和亚尼克的《对监视的恐惧: 调查土耳其社交媒体用户对监控的看法以及在社交媒体上表达意见的意*愿*。《*政治*》，*第 1-25* 页，2022 年 3 月。

[63] 吴 x .和 R.菲茨杰拉德，《隐藏在视线之中》在中国社交媒体上表达政治批评，“话语 Stud”。，第 23 卷，第 2 期。3, pp. *365-385, june . 2021*。

[64] S. Park, L. M. Bier 和 H. W. Park，“使用混合文本挖掘的信息娱乐对公众对朝鲜反应的影响: 内容分析、基于机器学习的情感分析和共词分析，”El professional de la Información，第 30 卷，第 3 期。2021 年 5 月 3 日。

[65] P. S. Motahar, R. Tavakoli, P. Mura，“社交媒体影响者在 Youtube 上对伊朗的视觉框架”，《旅游娱乐研究》，第 1-13 页，2021 年 12 月，doi:10.1080 / 02508281.2021.2014252。

[66] V. Van Roy, F. Rossetti, K. Perset 和 L. Galindo-Romero，《人工智能观察:国家人工智能战略》“欧洲视角”，联合研究中心(塞维利亚站点)，塞维利亚，西班牙，Tech。 代表,2021。(在线)。可用:https://ideas.repec.org/p/ipt/iptwpa/jrc122684。超文本标记语言

[67] N. I. Alnaghaimshi 和 E. Pearson，《在 21 世纪赋予阿拉伯部落文化权力》; 社交媒体在海湾国家的使用，“Inf, Com- mun。*Soc*。，*pp.* 1-19, Nov. 2021, doi: 10.1080 / 1369118 x.2021.1993956。

[68] T. Ngoensuk 和 C. Viriyavejakul，“孟库特国王理工学院研究生使用社交媒体的隐私侵犯行为预防系统”， Medit。 *J.社会科学，第 10 卷*，第 1 期。4, p. 102, 2019。

[69] H. Postigo，“美国在线志愿者: 从早期的合作制作社区的经验教训，“Int。J.文化研究。，第 12 卷，no。5，第 *451-469 页，2009 年 9 月*。

[70] J.科塞夫，＜2＞。《创造互联网的 *26 个单词》中的“奇才例外”*。美国纽约州伊萨卡: 康奈尔大学。 出版社，2019，第 36-56 页。

[71] s·e·班尼特，《罐头垃圾邮件: CompuServe,”大学。 *《里士满法律修订版》，第 32 卷*，第 2 号。1998 年，第 545 页。(在线)。可用:https://heinonline.org/HOL/P?h=hein.journals/urich32&i=563

[72] D. M. Boyd，“Friendster 和公开的社交网络”，Proc。*Abstr 延长*。*嗡嗡声*。*第一版的因素*。 *系统*。 *(中国)，2004,pp.* 1279-1282。

[73] j·范·迪克，"你只有一个身份"在脸上表演自我书和领英，“媒体，文化社会”。，*第 35 卷，第 35 期*。*2，第 199-215* 页，2013 年 3 月。

[74] P. Kaur, N. Islam, A. Tandon 和 A. Dhir，《社交媒体用户》在线主观幸福感与疲劳: 从网络异质性的角度看，《技术》。《*预测社会变迁*》，*第 172 卷，2021 年 11 月*，第 1 期。不。121039.

[75] J. M. Banda, R. Tekumalla, G. Wang, J. Yu, T. Liu, Y. Ding, E. Artemova E. Tutubalina 和 G. Chowell，“面向开放科学研究的 COVID-19 大规模 Twitter 聊天数据集——国际合作”，《流行病学》第 2 卷，第 2 期。3, pp. 315-324, august 2021。

[76] E. Kross, P. Verduyn, G. Sheppes, C. K. Costello, J. Jonides, and O. Ybarra，“社交媒体与幸福感: 陷阱，进展和下一步，“*趋势认知*”。*科学*。，*第* 25 卷，第 25 号。1, pp. 55-66, january 2021。

[77] 希拉里和奥巴马。Dumebi，“社交媒体是传播错误信息的工具《语言与文化》，第 5 卷，第 5 期。*S1, pp. 496-505, Aug. 2021*。

[78] S. Sanasi, D. Trabucchi, E. Pellizzoni 和 T. Buganza，《进化的含义: 对社交媒体行业的实证分析，“Eur。*j .创新*。*管理*。，*第 25 卷*，第 25 号。6，第 97-121 页，2021 年 3 月。

[79] L.-V。大众媒体、社交媒体和技术进化今天: 一个理论的方法，”J.媒体研究，第 14 *卷，第 2 号*。*3* pp. 95-105，十一月 2021。

[80] S. Lebovitz, N. Levina 和 H. Lifshitz-Assaf，“人工智能真的是真实的吗
“真正的”？基于专家的“专业知识”来培训和评估人工智能工具的*危险*。*正无穷*。*系统*。*夸脱*。，*第 45 卷*，no。3，第 1501-1525 页，2021 年 5 月。

[81] O. D. Apuke 和 B. Omar，“假新闻和 COVID-19: 造型的社交媒体用户中假新闻分享的预测者，“Telematics information”。，第 56 卷，2021 年 1 月，Art。不。101475.

[82] S. Wagenpfeil, F. Engel, P. M. Kevitt 和 M. Hemmje，“基于人工智能的seman”
为智能手机上的社交媒体提供多媒体索引和检索。”《*情报*》，*第 12 卷*，第 7 号。1, p. 43, 2021 年 1 月。

[83] A. Dafoe, Y. Bachrach, G. Hadfield, E. Horvitz, K. Larson 等 T. Graepel，“合作型人工智能: 机器必须学会找到共同点，”《自然》，第 593 卷，第 593 期。7857, pp. *33-36, May* 2021。

[84] P. van Esch 和 J. Stewart Black，“人工智能(AI): 的数字化营销”，澳大*利亚*。 *市场营销杂志，第 29 卷*，第 29 期。3, pp. 199-203, august 2021。

[85] J. A. Kroll, J. B. Michael, D. B. Thaw，“加强网络安全。通过人工智能: 风险、回报和框架”，《计算机》，第 54 卷，第 5 *期*。*6, pp.* 64-71, june . 2021。

[86] R. Montasari, F. Carroll, S. Macdonald, H. Jahankhani A. Hosseinian-Far 和 A. Daneshkhah，“人工智能和机器学习在产生可操作的网络威胁情报中的应用”，发表于物联网(IoT)设备的数字取证调查。瑞士 Cham: Springer, 2021，第 47-64 页，doi: 10.1007 / 978-3-030-60425-7。

[87] M.威利特，“太阳风黑客的教训”，《生存》，第 63 卷，第 *2 期*。*2*，
第 7-26 页，2021 年 3 月。

[88] O. Analytica，“Solarwinds 黑客攻击将改变我们的网络战略”，专家简报，Oxford Analytica, Oxford, Tech。众议员，2021 年，doi: 10.1108 / OXAN-DB259151。

[89] O. Analytica，“太阳风公司的大胆黑客攻击将使西方政策更加强硬，”
Emerald Expert briefing, Oxford Analytica, Oxford, uk, Tech。众议员，2020 年，doi: 10.1108 / OXAN-ES258311。

[90] P. Ranade, A. Piplai, S. Mittal, A. Joshi 和 T. Finin，“生成假”使用基于变压器的模型的网络威胁情报，”在程序。*Int*。*联合会议*。*神经*。*(IJCNN)*， *2021 年 7 月*，第 1-9 页。

[91] U. Reisach，“在社会动荡时期，社交媒体的责任政治操纵，”欧元。*j .打开*。*Res.*，*第 291 卷*，第 291 号。3, pp. 906-917, june . 2021。

[92] B. Alhayani, H. J. Mohammed, i.z. Chaloob 和 J. S. Ahmed,

“人工智能技术对抗网络安全风险的有效性——IT 行业的应用，”马特。今天，*2021 年 3 月*，doi: 10.1016 / j.matpr.2021.02.531。

[93] W. Steingartner, D. Galinec 和 A. Kozina，“威胁防御: 网络混合威胁模型中的欺骗方法和适应力教育。”*《对称》，第 13 卷*，第 2 期。4, p. 597，四月 2021。

[94] S. Rodgers，《主题问题介绍》:《人工智能与广告的承诺与危险》，《广告杂志》，第 50 卷，第 5 期。1, *pp. 1* - 10, 2021 年 1 月。
[95] A. Tursunbayeva, C. Pagliari, S. Di Lauro, G. Antonelli，《伦理学》关于人员分析: 风险、机会与建议>，《人事导报》，第 51 卷，第 1 期。*3，第 900-921 页，2022 年 4* 月。
[96] I. Anica-Popa, L. Anica-Popa, C. Ra - dulescu, M. vrncianu，“人工智能在零售业的整合: 利益、挑战和专门的概念框架”，《amfitatru 经济》，第 23 卷，第 2 期。56, pp. 120-136, *2021*。
[97] V. Galaz, M. A. Centeno, P. W. Callahan, A. Causevic, T. Patterson, I. Brass, S. Baum, D. Farber, J. Fischer, D. Garcia, T. mcpherson，李建平，李建平，“人工智能、系统风险和可持续性”，《科学技术》。*Soc*。， *vol.* 67, Nov. 2021, Art。不。101741.
[98] R. Eitel-Porter，《超越承诺: 实施道德人工智能(AI)*《伦理学》，第* 1 卷，第 2 期。1，第 73-80 页，2021 年 2 月。
[99] Z. Stanley-Lockman，“军事人工智能合作工具箱”，安全中心。紧急情况。 抛光工艺。，华盛顿特区，美国，科技 众议员，2021 年 8 月。(在线)。下载地址 :https://cset.georgetown.edu/wp-content/ uploads/CSET-Military-AI-Cooperation-Toolbox.pdf
[100] M. Imran, F. Ofli, D. Caragea 和 A. Torralba，“使用人工智能和社交灾害应对与管理媒体多式联运内容: 机遇、挑战和未来方向。*的过程。管理。，第 57 卷*，no。2020 年 9 月 5 日不。102261.
[101] A. Capatina, M. Kachour, J. Lichy, A. Micu, a - e。Micu, F. Codignola，“将基于人工智能的社交媒体营销软件的未来能力与潜在用户的期望相匹配”，《科技》杂志。*《预测社会变迁》，第 151 卷，2020 年 2 月*，第 1 期。不。119794.
[102] T. Gillespie，“内容审核、人工智能和规模问题”，Big *Soc 的数据。，第 7 卷*，第 7 期。2020 年 8 月 2 日不。2053951720943234.
[103] R. Radu，“指导人工智能的治理: 展望国家战略，“政策 Soc”。，第 40 卷，no。2，第 178-193 页，四*月 2021*。
[104] 钟忠，金亮，黄 s .，“深度文本: 文本的新方法自然图像中的提案生成和文本检测”，在 Proc。 *IEEE Int*。*相依。Acoust*。*语音信号处理。(ICASSP)， 2017 年 3 月，pp.* 1208-1212。
[105] A. Mackenzie，《从 API 到 AI: 平台和它们的不透明性，” *Commun*。*Soc*。，*第 22 卷*，第 2 期。13, pp. 1989-2006, Nov. 2019。
[106] 庄毅，“基于机器学习的句子情感分析”，《科学进展》。*Int*。*相依。大数据肛门。Cyber-Physical-Syst*。新加坡: Springer, 2019, pp. 813-820, doi: 10.1007 / 978-981-15-2568-1。
[107] K. S. Kumar, D. E. Geetha 和 P. R. Sahoo，《处理的方法》在线社交网络生成的异构数据[j]。*定理。Nanosci*。，*第 17 卷 no*。*9，第 4098-4102 页*，2020 年 7 月。
[108] K. Khalil, U. Asgher, Y. Ayaz, R. Ahmad, J. A. Ruiz, N. Oka, S. Ali，和 M. Sajid，“人机交互的认知计算; IBM 沃森实现”，见《程序》。*Int*。*相依。达成。嗡嗡声。factors Ergonom*。瑞士 Cham: Springer, 2020, pp. 400-406, doi: 10.1007 / 978-3-030-51041-1。
[109] J. P. Gujjar 和 P. K. HR，“情感分析: 文本 blob 的决定、“Int。j .科学。*Res*。*Eng*。*《趋势》，第 7 卷，第 7* 期。2，第 1097-1099 页，2021。
[110] M. M. Haider, M. A. Hossin, H. R. Mahi 和 H. Arif，“使用 gensim Word2Vec 和 K-means 聚类算法的自动文本摘要”，《科学进展》。*IEEE 第 10 届会议(TENSYMP)， 2020 年 6 月，第* 283-286 页。
[111] z 曾庆红,r .伊斯兰教,k . n .凯亚•j .福尔兹 y 的歌,和美国锅,“公平异构信息网络的表征学习”，2021，*arXiv: 2104.08769*。
[112] “客户关系管理(CRM)作为一种商业知识和智能管理工具的评估”，中国工商管理大学学报。，第 3 卷，第 3 期。2, pp. 171-184, september 2021。
[113] N. Zierau, K. Flock, A. Janson, M. Söllner 和 J. M. Leimeister，“基于人工智能的聊天机器人及其设计对在线贷款申请中用户信任和信息共享的影响，”Proc。*夏威夷 Int*。*相依。系统。科学。(HICSS)， Koloa, HI, USA,* 2021。
[114] D. S. Mishra, A. Agarwal, B. P. Swathi 和 K. C. Akshay， < Nat-自然语言查询形式化到 SPARQL，使用 rasa 查询知识库。*Artif*。*智能。， pp. 1-14,* december 2021, doi: 10.1007 / s13748 - 021 - 00271 - 1。

MOHAMMED NASSER AL-SUQRI，阿曼苏丹卡布斯大学图书馆与信息科学系图书馆与信息科学学士学位，美国纽约普拉特学院信息与图书馆科学学院图书馆与信息科学硕士学位，美国恩波里亚州立大学图书馆与信息管理学院图书馆与信息管理博士学位。大学的副教授和研究生院院长。他是《艺术与社的总编辑，也是多本杂志的副主编，包括《信息科学》杂志《证据》、*《应用信息科学》杂志(尼日利亚)*、《社会信息学》杂志和《社会与人文科学评论》*(阿尔及*利亚)。他还是几个期刊和研究组织的审稿人，包括图书馆与信*息科学杂志(阿尔及利亚)*、*研*究委员会(阿曼)和卡塔尔国家研究基金会(卡塔尔)。他在 ISI 和 SCOPUS 上发表了几篇文章，编辑了由知名国际出版社出版的书籍和章节，以及会议论文集。他的研究兴趣包括用户研究、知识管理和共享、技术采用理论和模型、研究方法、信息产业以及新技术对大学图书馆的影响。他于 2014 年获得最佳研究员奖，并于 2018 年获得最佳学术奖。

MARYAM GILLANI 毕业于拉合尔福尔曼基督教学院(FCCU)的软件工程和计算机科学学士学位，以及巴基斯坦伊斯兰堡 NUST 机电工程学院(cme)的计算机软件工程硕士学位。她目前在都柏林大学学院攻读机器学习和人工神经网络博士学位。
爱尔兰。她的其他研究兴趣包括 VANETs 的数据收集和通信协议、智能交通系统、快速软件开发和信息处理与安全。