

数智时代的国家安全学： 计算国家安全学的缘起、变革与进路

李明

[摘要] 国家安全学作为一门新兴交叉学科,亟须推动其研究范式的变革与创新。计算社会科学的发展与国家安全学建设的现实需要为计算国家安全学的提出提供了理论根基和现实基础。计算国家安全学的研究范畴包括相关理论基础、研究方法和实践应用,其研究范式实现了由小样本到大样本、片面认知向全面感知、因果关系向相关关系以及经验判断向循证分析的转变。当前,计算国家安全学在数据获取利用、研究方法创新和理论体系建设方面仍面临较大挑战。鉴于此,应兼顾理论与数据,打造特色鲜明的研究方法,推动学术共同体建设,不断推进国家安全学学科体系建设与研究范式的创新发展。

[关键词] 数智时代;国家安全学;计算国家安全学;范式变革;理论构建

[中图分类号] D631;D035.3;G203 **[文献标识码]** A **[文章编号]** 1007-5801(2025)02-0090-11

在百年变局加速演进的复杂背景下,国家安全学的设立对于践行总体国家安全观、推动国家安全工作的顺利开展具有重要现实意义。当前的国家安全学尚处在探索发展阶段,其在研究范式创新方面尚存在较大不足,而研究范式对于学科的建设和发展而言至关重要,因此探索国家安全学的研究范式创新是实现高水平学科建设目标的题中应有之义。与此同时,数智时代的到来使得旧的知识体系受到较大冲击^[1],为研究范式与研究方法的变革创新提供了有利条件,大数据资源的可获得性以及算法算力的巨大突破,使得数据与计算的赋能成为一种有效的研究手段。在此背景

下,本研究提出“计算国家安全学”的概念,并尝试对计算国家安全学的逻辑缘起、主要内容、范式变革、计算国家安全学发展面临的挑战以及未来进路进行深入探讨,以期对推动国家安全学的建设与发展有所助益。

一、逻辑缘起：数智时代计算国家安全学的提出依据

(一) 计算社会科学的发展与拓展

计算社会科学(Computational Social Science)是以数据为基础,采用计算的方式方法对社会系统中的复杂性与抽象化问题进行探究,以更好地

[收稿日期] 2025-01-07

[基金项目] 国家社会科学基金青年项目“数字智能时代网络舆情泛政治化风险的循证治理研究”(23CZZ045)。

[作者简介] 李明,吉林大学公共外交学院(国家发展与安全研究院)副教授。

帮助我们对其进行预测和应对^[2]。早在2006年,著名的计算机学家吉姆·格雷(Jim Gray)就已经提出人类将从实验科学、理论科学与计算机仿真科学三种研究范式,逐步走向第四种研究范式,即“数据密集型科学发现”范式,数据的挖掘与计算是该范式的鲜明特征^[3]。2009年,以拉泽尔(Lazer)为代表的15位美国学者在《科学》杂志上联合发文,正式提出计算社会科学的概念。该文章预言一个以计算机技术为基础,未来具有无限可能性的计算社会科学的产生将要成为现实,并指出在谷歌、雅虎等互联网企业已经出现了计算社会科学的相关研究^[4]。2012年,意大利学者R.康特(R.Conte)等人在《欧洲物理学刊—专刊》联名发表了《计算社会科学宣言》,在总结大数据计算方法对社会科学产生的影响及其发展前景的基础上,深入分析了计算社会科学的主要特征、鲜明优势及其应用场景。2014年,美国学者克劳迪奥·乔菲—雷维利亚(Claudio Cioffi—Revilla)出版了《计算社会科学概述:原理与应用》一书,该书对计算社会科学的概念、定义作出明确界定,并对计算社会科学的实践应用进行了分析与阐释。2016年,美国政治学教授R.迈克尔·阿尔瓦雷斯(R.Michael Alvarez)编著的《计算社会科学:探索与预测》对计算社会科学进行了全面的总结和回顾,并探讨了计算社会科学在社交媒体、政府治理、市场营销等领域的应用,进而对计算社会科学的未来前景进行了预测和展望^[5]。

伴随着计算社会科学的不断发展,相关研究迅速成为学界关注的焦点议题并对社会科学的诸多学科产生了重要影响,计算社会学、计算政治学、计算新闻学、计算传播学、计算教育学等学科范式得以迅速发展,相关研究不断深化,推动了各个学科体系的发展和完善^[6]。计算社会学是在传统的定量社会学研究基础上产生的一种具有理念新、数据新、分析手段新等优势特征的研究范式或研究工具。近年来,计算社会学的相关研究成果不断涌现,如基于谷歌关键词搜索的全球文化品位及其消费者偏好研究^[7],采用机器学

习法,通过主题建模的方式对海量文本内容进行挖掘与分析研究^[8]。计算政治学一般是指运用数学方法和模型构建对政治现象进行量化、实证性研究的社会科学学科^[9],计算政治学中常用的方法包括分类聚类、情感分析、主题模型等^[10],主要涉及在线政治博客挖掘^[11]、用户行为的社会网络分析^[12]等。计算传播学被认为是一种新的研究取向或研究方法^[13],它为传统传播学赋予了“计算性”,推动了学界对计算传播学的整体逻辑进行思考^[14]。计算传播学的发展为传播行为的实证检验、阐释与理解提供了新的机会^[15]。计算教育学是以教育学数据为研究对象,采用计算为主要研究方法的新兴学科^[16]。有的学者认为在计算教育时代,需要采取数据驱动的研究范式去解决复杂学习问题,并在此基础上倡导多模态学习分析,这为教育学研究提供了新方法^[17]。有的学者指出计算教育学或成为教育生态的关键基础,将在智能教育设计、教育演化研究、校园建设等教育领域产生重要效用^[18]。这些学科范式的发展经验给计算国家安全学的建立和探索提供了理论依据和实践基础。

(二) 国家安全学发展的现实需要

国家安全学作为一门新兴学科,其学科交叉性十分明显,实现了大门类、大领域与大体系交叉。据统计,在我国学科体系中包含110多个一级学科,其中有46个一级学科与国家安全有关联^[19]。因此,国家安全学实质上属于跨学科门类、覆盖多学科群落的交叉学科,该学科还涉及诸多安全领域,包括政治安全、军事安全、国土安全、经济安全、社会安全、文化安全等众多传统安全领域和非传统安全领域,包括国家安全“本身”内容和“相关”内容^[20]。此外,国家安全学涉及物理空间和虚拟空间,物理空间是指我们生活的现实世界,虚拟空间则是一个“以实映虚”的“镜像”世界,尤其是元宇宙的兴起与发展,进一步拓展了国家安全学的研究场域和研究对象。正是在国家安全学大门类、大领域与大体系交叉的现实基础上,为更深层次地实现学科间横向与纵向的

交叉融合,有效地解决复杂巨系统中的国家安全问题,积极探究思维模式的转变与研究范式的变革则尤为必要。

与此同时,国家安全大数据资源有效地助推了新研究范式的发展与变革。数智时代,数据资源作为“新型石油”,已成为塑造国家竞争力和保障国家安全的新型生产要素和战略性资源^[21]。由于国家安全学的研究包含众多传统安全与非传统安全领域,因此涉及的海量数据具有交织性、复杂性和多维性。而伴随着新兴技术的发展,区块链、人工智能、云计算等计算的应用日益成熟,数据挖掘能力大大提升,能够从国家安全大数据中剥离出有效信息,尤其能够及时地捕捉和预测难以察觉的潜在风险,旋即进行预警和研判。传统的国家安全学研究多聚焦于基础理论,从研究范式而言,多为定性研究,而基于数据的定量研究相对缺乏,尤其是基于国家安全大数据的量化研究则几近空白,而要实现吉姆·格雷(Jim Gray)所说的“数据密集型科学发现”,则必须革新国家安全学的传统研究范式,积极探索科学适切的研究新范式,而得益于计算社会科学范式的影响和启迪,计算国家安全学的提出则正当其时,这也彰显了大数据时代国家安全学研究的总体发展趋向。

本文在借鉴计算社会科学^[22]、计算社会学^[23]、计算传播学^[24]等定义的基础上提出计算国家安全学的概念:计算国家安全学是国家安全学领域借助计算机、互联网和人工智能等新兴技术手

段,运用数据挖掘、机器学习等数据获取与分析工具,在跨学科视域下,解释和预测国家安全现象与国家安全行为的一种研究范式或思维方式。国家安全学本身被定义为一门交叉学科,因此计算国家安全学最大的特点也是跨学科性,它是横跨计算科学和社会科学,基于问题导向的一种研究范式(如图1)。

二、主要内容:数智时代计算国家安全学的研究范畴

计算国家安全学具备鲜明的跨学科特征,其研究范畴也非常广泛,相关研究可从理论层面、方法层面和实践层面展开,具体包括计算国家安全学基础理论、计算国家安全学研究方法以及计算国家安全学实践应用研究。计算国家安全学基础理论可对应关键构成要素、重点领域划分以及二级学科重塑,计算国家安全学研究方法可对应定性研究、定量研究和混合研究,计算国家安全学实践应用可对应风险评估、应急响应和政策优化,这些内容构成了计算国家安全学的主要范畴(如图2)。

(一)计算国家安全学理论研究

计算国家安全学的理论研究是国家安全学自主知识体系建构的重要内容,具体可从关键构成要素、重点领域划分、二级学科重塑等方面进行探索。首先,计算国家安全学的理论研究需要对其本质问题进行探讨,即从本体论角度确立计算国家安全学的研究对象,同时需从主体论角度探讨

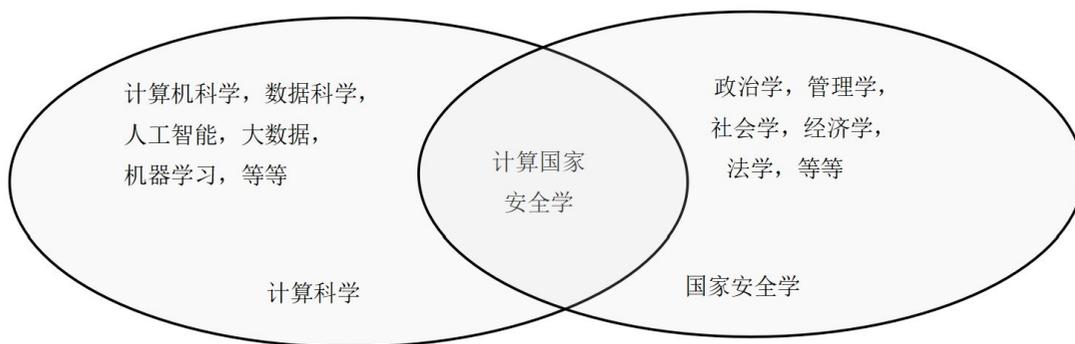


图1 计算国家安全学示意图

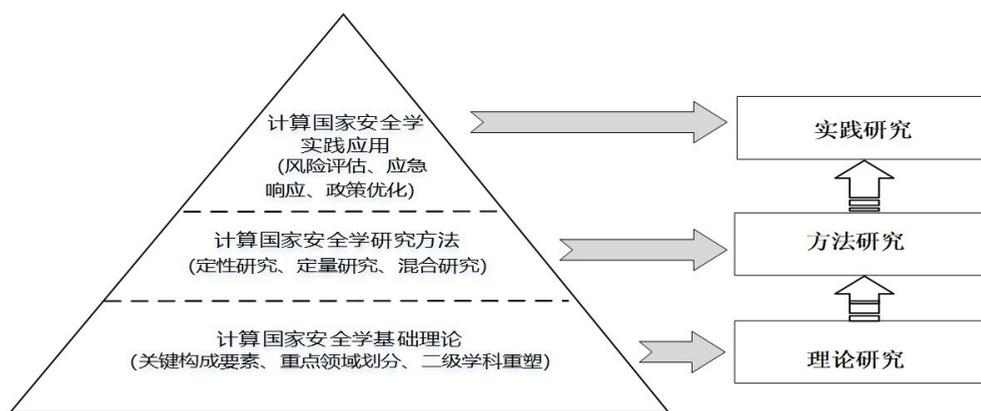


图2 计算国家安全学的研究范畴

计算国家安全的主体类型、主体特征、行为模式等,从客体论角度探寻引发国家安全风险的复杂因素,从价值论的角度衡量计算国家安全学在统筹发展与安全、推动社会进步与稳定所产生的重要作用,这些构成要素是计算国家安全学理论体系的重要内容。其次,计算国家安全学应明确其涵盖的重点安全领域,当前国家安全包含政治安全、军事安全、经济安全、社会安全、科技安全等诸多安全领域,在数智时代背景下应积极探索和推动这些重点安全领域的“计算”范式变革,不断对如计算政治安全、计算军事安全、计算经济安全、计算社会安全、计算科技安全等具体领域进行深入分析和探讨,以标志性概念创新积极推动计算国家安全学理论创新。此外,计算国家安全学应积极重塑国家安全学的二级学科划分。国家安全学当前设置了国家安全思想与理论、国家安全战略、国家安全治理和国家安全技术四个二级学科,这些二级学科实现了系统性、立体化的国家安全学学科体系构建与布局,而计算国家安全学的提出和建立需要在原有二级学科基础上,积极嵌入“计算”思维,实现计算国家安全思想与理论、计算国家安全战略、计算国家安全治理和计算国家安全技术的理论重塑与再造,推进计算国家安全学理论的创新与发展。

(二)计算国家安全学方法研究

计算国家安全学方法研究对于推动学科发展与范式变革的重要性不言而喻。从研究方法的类

型而言,计算国家安全学的研究方法包括定性研究、定量研究和混合研究。定性研究是科学研究中常用的研究范式,具体包括归纳、分类、比较等方法,侧重于对计算国家安全学相关问题进行深入理解和阐释,如对计算国家安全学的相关概念进行辨析,对现有理论进行分类,对相关案例进行比较分析等,以揭示计算国家安全学的内在逻辑和规律。定量研究是一种较为精确的语言,在计算国家安全学研究中可对相关问题进行客观的测量与分析。计算国家安全学涉及诸多重点安全领域,而这些领域会产生大量相关数据,通过收集和分析这些数据,能够较好地揭示计算国家安全领域问题的数量特征与趋势,为政策制定提供科学依据。混合研究是基于某个具体研究问题,将定性研究与定量研究两种方法综合起来使用,其突出的优点是既具备定性研究的深入性与灵活性,又具备定量研究的客观性与精确性。计算国家安全学的研究具有系统性和复杂性,因此需要综合问卷调查、深度访谈、模型构建、数据分析等多种定性定量方法,进而围绕计算国家安全学的重点问题开展有效研究,提供更加全面、深入的研究结果。值得关注的是,伴随着生成式人工智能、大数据技术的迅速发展,研究方法也实现了创新式发展,这为相关研究提供了良好的技术支撑与方法支持。因此,计算国家安全学需要积极推动与实现方法间的交叉融合,综合采用定性、定量与混合研究方法,更好地为推动计算国家安全学学科发

展和学术研究赋能增效。

(三) 计算国家安全学实践应用研究

实践应用是计算国家安全学研究的价值旨归。计算国家安全学实践应用研究可从风险评估与预警、应急响应与决策支持、政策效果评估与优化几个层面进行深入探讨。首先,重点领域风险防范是计算国家安全学实践应用的重要内容。在数智时代,算力、算法大大增强,积极采用先进的计算技术和模型,能够实现对国家安全潜在风险的全面评估,及时监测预警可能的风险点,这些研究有利于将风险“前移”,提前制定应对方案,实现国家安全风险的有效防范和化解。其次,当国家安全受到威胁时,需要能够迅速提供科学有效的应急响应,充分调动相关资源控制事态发展。而人工智能、大数据技术的发展与应用能够实现对海量数据的收集、挖掘和分析,并结合先进的算法工具和预测模型,从而为决策者提供精准全面、切实可行的应急方案,缩短应急响应和科学决策时间,从而提高决策效率和效果。同时,还可以针对国家安全重点领域建立决策支持系统,在数据挖掘的基础上结合专家的知识及经验,通过模拟仿真辅助决策者作出最优选择。此外,计算国家安全学实践应用研究中,对相关政策的效果评估与优化尤为重要,它直接影响国家安全治理现代化水平。政策效果评估与优化侧重于对国家安全政策实施后的成效及影响进行研究,具体可通过构建评估指标体系,对政策内容进行量化分析,

并提出针对性的优化建议,在这一过程中信息技术的发展与应用为政策效果评估与优化提供了新的手段。

三、范式变革：数智时代计算国家安全学的研究转变

计算国家安全学强调其“计算”属性,应将“计算”作为一种基本特征重新认识国家安全,并积极推动相关研究的范式重构。计算国家安全学不排斥传统国家安全学的研究方法和范式,只是对传统国家安全学研究范式的一种补充和完善,这种范式带来的变革主要体现在以下几点(如图3)。

(一) 由小样本向大数据转变

传统国家安全学的研究多基于学科定位、理论基础、建设路径等宏观视角的定性研究,相关领域的微观研究虽然也涉及定量研究,但其多采用小样本数据,小样本研究具有数据获取简单、成本低、效率高等显著优点,但也存在其自身难以克服的缺点。一方面,这些小样本数据的样本量较小,很难精准反映整体情况,往往是针对某一具体问题,数据的可利用范围和次数较为有限,而大数据动辄为数十万甚至上百万的海量数据,研究者不需要进行抽样分析,它包含的信息量大,数据的可利用范围较广。另一方面,传统小样本数据常用的问卷调查或访谈法获取的数据主观性较高而可信性较低,而大数据多为国家安全领域自动形成的自然数据,具有较强的真实性与客观性。Rubinfeld &

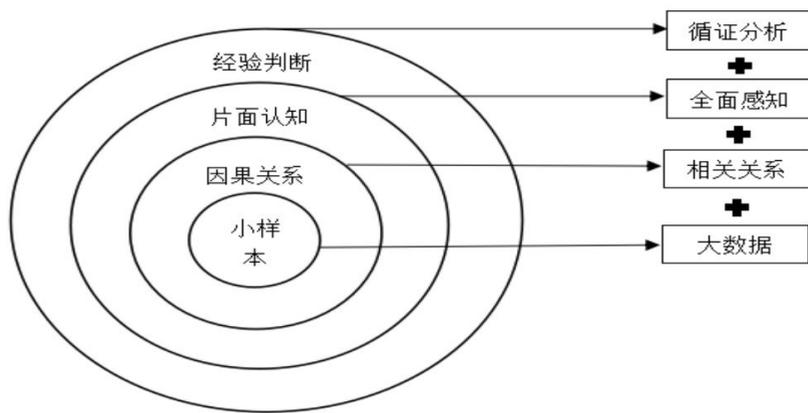


图3 计算国家安全学的范式变革

Gal将大数据总结为“4V”特征,即Volume(大量性)、Velocity(高速性)、Variety(多样性)、Value(价值性),强调其具有规模大、形式多、价值大等特点^[25]。大数据时代的来临为国家安全学的研究带来了新机遇,计算国家安全学以“数据”为核心,基于对大数据的挖掘与分析,实现了由小样本向大数据的转变。

(二)由因果关系向相关关系转变

在传统国家安全学研究范式下,不管是传统安全领域还是非传统安全领域,我们的研究取向往往是探寻威胁国家安全的影响因素,分析内在的因果关系,既有基于小样本的实证分析,也有基于理论和经验的学理分析,最终目的都是为了给出优化路径或对策建议,从效果上看具有一定的滞后性和局限性。人工智能、大数据、区块链等技术的发展与应用很大程度上消除了这种局限性,其为国家安全学的相关研究提供了新手段和新范式,也为弥补传统意义上因果关系存在的主观性、偏差性等不足提供了新途径。面对国家安全研究领域的复杂性、系统性以及相关数据的多元性与繁杂性,运用技术工具能够有效实现大数据的挖掘、存储、计算、预测,从海量的数据中重新整理和刻画全样本信息。在探索复杂因素间的逻辑关联时,不受传统基于因果关系的假设或推理的影响,而是在不预设前提假设的基础上,直接立足于大数据,捕捉复杂因素间的相关关系。对相关关系的挖掘和分析并不是简单地替代因果关系,而是为因果关系提供了更加科学的佐证与支持,以更高效、低成本、多维度的方式捕捉数据信息,为指导国家安全决策提供支持。

(三)由片面认知向全面感知转变

传统国家安全量化研究多基于抽样数据或随机样本的有限数据,这些数据往往还面临着有效信息缺失、无效信息泛滥等限制,在此情况下,相关主体难以捕捉关键信息。而大数据环境下,在信息技术的有效赋能下,国家安全研究得到的结果更加可靠,这使得国家安全的研究进一步深化,逐步由片面认知向全面感知阶段转变。此时,全

面感知主要依赖于“量”的提升,大数据的开放性、多源异构性等特征,使得从整体上全景式认识国家安全现象,进而科学有效地解决国家安全问题成为可能。同时,由片面认知向全面感知转变还体现在“质”的跃升,借助于机器学习、文本挖掘与复杂网络分析等技术工具,可以有效地识别影响国家安全的“苗头”与“风向”,全面感知问题的走势、成因,进而通过及时预警和研判,为解决相应的国家安全问题提供针对性的对策建议。因此,技术赋能下的大数据分析能够迅速挖掘出相关问题存在的“痛点”与“堵点”,探究国家安全问题与数据间的内在逻辑关系及耦合机制,最终实现由数据的片面认知向全面感知转变。

(四)由经验判断向循证分析转变

传统国家安全的很多领域都是基于理论推演和经验判断,如在政治安全、领土安全等传统安全领域,多采用因果分析法、比较分析法等方法对影响安全的因素、原因进行分析,如从主权、制度、政权等维度对国家政治安全的不安全状态及其成因进行探究^[26]。通过比较中俄两国在政治安全秩序观之间的异同,进一步分析两国在对多极化的理解、维护政治安全的手段以及对国际安全制度的遵守程度等方面存在的差异,最终得出中国在维护国际政治安全秩序方面贡献更为突出^[27]。而在非传统安全领域,多采用专家咨询、头脑风暴等途径获取相关信息,研判和评估具体状况,进而根据经验形成对策建议,如在食品安全领域,采用专家咨询法构建食品安全风险预警指标体系,为政府食品安全监管提供决策依据^[28]。在公共卫生安全领域,通过专家咨询和小组讨论等方式设计问卷和收集数据,进而对影响公共卫生安全的关键因素进行分析^[29]。而信息技术突破了传统经验判断的局限,基于大数据的国家安全研究可以在数据收集、数据分析及数据相关性研究的基础上,为相关领域提供对策建议,还可通过自动模拟和仿真预测提供最优的决策方案。因此,当前国家安全研究在技术赋能下能够深挖数据蕴藏的内在关联与规律,为相关领域的安全决策提供科学支撑,国

家安全研究实现了由经验判断向循证研究的转变。

四、现实挑战：数智时代计算国家安全学面临的多维困境

计算国家安全学在发展和推进过程中主要会受到数据、方法与理论三大要素的限制,因此其面临的现实挑战主要包括数据获取与利用的挑战、研究方法创新的挑战与理论体系建设的挑战,如图4所示。

(一)数据获取与利用的挑战

计算国家安全学研究范式的基础和前提便是数据,从大数据当中能够挖掘客观有效的内在关联与规律,而当前的国家安全学领域虽产生了大量的相关数据,但实际上现阶段的研究仍是以基于理论的学理阐释为主,涉及的定量研究也多是以“小数据”和零散数据为基础的研究。而这些研究反映的是样本的具体情况,并不是总体数据的全貌,因此容易造成“碎片化”和“片面性”的认知局限,而造成该状况的一个重要原因在于数据获取的可及性限制。当前国家安全领域产生的海量数据往往被相关机构或相关平台所掌握,且这些数据源中绝大部分属于非结构化的离散型数据,

应用者和研究者难以获取和使用。因此,在数据方面形成的霸权与垄断造成了“数据烟囱”,这不仅强化了数据获取难度,也会很大程度上弱化数据的联通价值^[30]。此外,数据隐私及数据伦理一直是数据获取与使用过程中需要关注的问题。国家安全学的相关领域也会涉及数据利用的隐私忧患,这也是大数据时代大数据利用方面无法回避的一大问题。相对而言,数据隐私问题很大程度上可以依赖于技术规避,但伦理问题却往往被视为一种较为严重的危机。国家安全学作为一门新兴学科,其相关领域研究所面临的问题仍不断出现,相关的探讨与实践也正在进行中,而伴随着新兴技术对大数据的有效赋能,伴随着计算国家安全学的探索与发展,传统研究范式的各种制约与边界不断被突破,计算国家安全学范式下国家安全研究的全新图景即将到来。

(二)研究方法创新的挑战

国家安全学作为一门新兴的交叉学科,其兼具“社会系统”与“自然科学”的双重性格,在研究方法上呈现出定性与定量之争问题较为突出。事实上,定性与定量方法各具优缺点,但有的研究者为了强调所用方法的优越性而批评其他方法存在的局限性。从研究者角度而言,只有根据具体

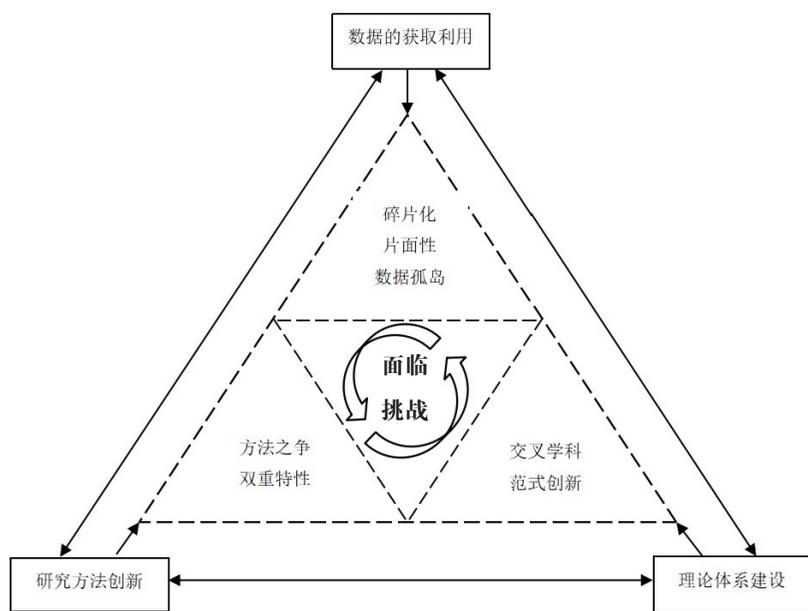


图4 计算国家安全学面临的现实挑战

问题选择恰当的研究方法才能较好地实现研究目的,同时可进一步探索定性方法与定量方法的有机融合,从而避免各自方法的自身劣势,实现方法上的优势互补。当前国家安全学的相关研究多聚焦于基础理论的定性研究,相关的定量研究较为薄弱。而计算国家安全学囿于其“计算”属性,容易卷入研究方法之争,计算国家安全学往往建立在数据挖掘的大数据分析基础之上,它很大程度上引发了数据观念、研究范式、模型选择等方面的变革。从计算国家安全学的研究方法来看,其主要涉及数据计算、科学实验、仿真模拟等,而数据计算方面往往会出现数据缺失、代表性较差、质量不均衡等问题,科学实验容易受到条件控制力、样本代表性、结果可重复性等问题影响,仿真模拟则在环境仿真度、影响因素关联度、内外部效度等方面容易存在偏差,因此,需要进一步完善和创新数据计算、科学实验与仿真模拟等方法体系。此外,当前许多新的计算方法尚未形成规范的流程与标准,这容易降低相关研究结果的可信度与说服力,与此同时,在探索和使用研究新方法的过程中需要研究者思考如何将理论分析与“计算”方法有机融合,实现相关研究领域的发展与突破。

(三)理论体系建设的挑战

计算国家安全学需要同时完成“计算”与“国家安全学”两条进路的理论建设。一方面,计算国家安全学不应该仅仅局限于算法基础上的实用主义,而应仔细考量在国家安全学的理论框架中如何有效构建以计算为研究范式的理论体系。而这需要积极探索计算国家安全学自有的计算模型体系,同时要深刻理解国家安全学作为一门新兴交叉学科,其本身具有的跨学科特征,需要以开放包容的姿态展开深入思考,同时对于涉及的一系列计算国家安全学的理论问题,包括哪些是计算国家安全学的研究领域,计算国家安全学如何实现理论创新与理论体系建设等需要给予特别关注。伴随着国家与学界对国家安全学的日益重视,近年来相关研究成果不断增加,但总体而言,相关领域的基础理论研究仍需进一步细化,只有国家安

全学的理论体系有所发展,计算国家安全学才能在此基础上发展和形成自身的理论体系,二者密不可分,前者是后者的母体,后者是前者的分支。当前国家安全学迅速发展,但与此同时未能形成对相关理论的深入研究,距形成较为成熟的理论体系仍任重道远,且从事国家安全学理论研究的学者相对偏少,未能形成学术共同体。此外,国家安全学的重点研究领域具有动态性和时代性,在百年大变局背景下影响国家安全的因素也愈加多样,相关研究内容不断丰富和拓展,这使得构建具有中国特色的国家安全理论体系的任务更加艰巨,而在此基础上构建计算国家安全学的理论体系则更是当前需要面临的一大挑战。

五、未来进路：数智时代计算国家安全学的推进策略

(一)兼顾理论与数据,推进研究范式创新

理论与数据是计算国家安全学的“道”与“术”。数智时代背景下,计算国家安全学的相关研究应注重理论与数据的双轮驱动,从国家安全学的理论脉络中汲取养分,同时重视数据的可获取性与代表性,致力于通过理论与数据的结合回应现实问题与创造新知,这是计算国家安全学的要旨所在。首先,计算国家安全学需要通过计算深度和开阔思路来改变传统意义上对从事定量研究的学者轻视或忽略理论的刻板印象。计算国家安全学研究者应努力学习和把握国家安全的基础理论,包括国家安全学的基本概念、研究对象、研究边界、内在逻辑等内容,在此基础上,根据国家安全的具体研究领域提炼出定量分析对象,并可运用大数据技术对学者提出的相关理论进行检验和修正。同时,计算国家安全学研究者还可运用计算方法对国家安全现象或国家安全问题进行深入分析、解释和预测,提出新的概念或构建新的理论。其次,计算国家安全学的研究应通过计算工具获取国家安全研究的海量数据,进而全景展现中国国家安全的现实情形,为推进国家安全实践提供理论支撑。一方面,我国面临着日益复杂的

内外环境,这使得国家安全领域产生的数据量大大增加;另一方面,人工智能、大数据技术的兴起与应用使得数据挖掘与分析的技术手段更加高明。对于同一研究对象,我们可以运用不同的工具,借助不同的方法,收集和处理不同来源、不同类型的相关数据,从而进行多重数据的挖掘分析与交互验证,尽量减少主观性误差,以较好地实现计算国家安全学研究目标,推动计算国家安全学研究范式创新。

(二) 凸显跨学科特征,打造特色鲜明的研究方法

国家安全学作为一门交叉学科,具有非常鲜明的跨学科特征,尤其和政治学、管理学、社会学、经济学、情报学等学科紧密相关,同时在计算工具、算法算力的加持下,其跨学科特征尤为显著。计算社会科学范式下的多学科交叉融合观念由来已久,但实施起来并不容易,大数据时代带来的思维方式、研究范式与技术手段的变化为跨学科交叉融合研究带来了新机遇。国家安全学作为一门“大学科”,其研究范畴覆盖了经济安全、政治安全、社会安全、文化安全、生态安全等传统安全与非传统安全的诸多领域,不同学科可从不同视角、不同维度对国家安全内容展开研究,如经济学、政治学、社会学学科可基于国家战略的重大需求对经济安全、政治安全、社会安全面临的紧迫难题进行深入研究,充分发挥自身的学科优势。与此同时,计算国家安全学的跨学科、多视角研究必然呈现研究方法上的“百花齐放”,这些研究方法既包括定性的,又包括定量的,因而多元方法的融入为计算国家安全学的研究提供了一个“方法池”,相关研究应基于问题导向,选择适切的研究方法,同时注意避免单一方法带来的系统偏差,推动研究方法间的融合创新。而打造具有特色的研究方法是一门学科区别于另一门学科,或一种范式区别于另一种范式的重要标志,对于计算国家安全学而言,需要在多元方法的基础上形成颇具特色的国家安全学方法体系,而研究方法的创新诞生于具体的研究实践,因此,在计算导向下,可将数据

计算、科学实验、仿真模拟等新方法与传统方法相结合,努力构建特色鲜明的计算国家安全学方法体系。

(三) 强化协作共享,推动学术共同体建设

学术共同体建设对于推进计算国家安全学的发展至关重要,基于国家安全学的跨学科特征,当前从事相关研究的学者来自各个学科,因此需要推动学者间的协作共享,打破学科壁垒,促进不同理论与方法的碰撞,建立有效的合作机制。首先,要“兼容并包”,广泛吸纳不同学科的研究人员加入国家安全学的研究队伍,解决研究队伍数量不足的问题。国家安全学是一个新兴领域,尚处于发展初期,相关研究还没有大规模地展开,当前具有国家安全学硕士点、博士点的高校数量较少,全国总体上尚未形成较为浓厚的国家安全学研究氛围,而计算国家安全学作为国家安全学的“计算范式”,其相关的深入研究需要引起更多学者的关注。同时,计算国家安全学的相关研究应实现跨领域、跨地域合作。积极鼓励和推动不同领域的研究者从不同视角出发开展国家安全研究,可定期召开相关学术会议,将理论研究者、实证研究者、智库人员等汇聚在一起,加强学术交流与合作。同时,不同院校的研究团队应建立起长期、深入的合作关系,共同补齐计算国家安全学在理论、方法等方面存在的短板。此外,鉴于国家安全学是一门服务于国家安全理论与实践需求的综合性学科,而“计算”技术又和一些信息技术企业密切相关,因此应强化高校与政府、企业间的合作,政府部门在相关研究中主要起到政策引导作用,企业部门主要为相关研究提供技术支撑,而高校专家学者主要提供智力支持,从而建立起高效的跨场域合作团队,有力地推动学术共同体建设。

结 语

计算社会科学的发展带来了新的研究范式革命,计算社会学、计算政治学、计算传播学、计算教育学等相继被提出并得以迅速发展,它们反过来

又推动了计算社会科学研究范式的丰富与发展,彰显了其强大的生命力。数智时代背景下,计算国家安全学的提出既丰富了国家安全学的时代内涵,又为国家安全学的相关研究插上了“计算”的翅膀,为其提供了新的研究范式。本研究首先从不同层面对计算国家安全学的逻辑缘起及主要内容进行介绍,廓清计算国家安全学提出的依据及其研究范畴,进而对计算国家安全学带来的范式变革进行阐述,与传统国家安全学研究相比,其具有大数据取向,重视对国家安全问题痛点的全面感知,致力于解决相关性问题的全面感知,并据此为因果关系提供佐证,且实现了由经验判断向循证研究的转变。在此基础上,从数据获取、研究方法应用、理论体系等方面对计算国家安全学面临的现实挑战进行分析,进一步针对性地提出计算国家安全学的未来进路。

中国的计算科学时代已经来临,国家安全学应与时俱进,以开放包容的态度主动拥抱新范式、新方法、新数据、新思维,确保在世界百年未有之

大变局下能够更好地促进国家安全研究,推动国家安全学科的发展和建设,同时国家安全学科还要以宏大的视野和包容的胸襟,努力为中国国家安全实践服务,积极为全球贡献中国智慧,推动全球安全倡议的实施。一种新兴研究范式的兴起是多种条件共同促进的结果,就计算国家安全学而言,其是国家安全知识、现实国家安全重大问题、数据挖掘与分析技术、网络基础设施与算法模型等方面共同促成的产物。数智时代的到来使得国家安全学研究者能够借助新兴技术或手段采用“计算”范式研究国家安全问题,这是计算科学发展的必然趋势。然而,数据获取与处理的挑战、研究方法的突破、计算思维的应用与理论体系的构建在国家安全研究中尚处在萌芽阶段,观念的滞后、方向的模糊、原有学科框架知识的制约都会阻碍计算国家安全学的发展。因此,计算国家安全学的建设与发展,计算国家安全学研究的推进与深化需要多方力量、更多学者共同努力。

[参考文献]

- [1]郭一宁.数智协商民主:全过程人民民主的新形态[J].探索,2023(1).
- [2]阙天舒,方彪.治理中的计算与计算式治理——国家治理现代化的治理技术和艺术[J].理论与改革,2022(5).
- [3]曾琼.突破与重构:大数据时代的计算广告学研究[J].湖南师范大学社会科学学报,2019(5).
- [4]Lazer D, Pentland A, Adamic L, et al. Computational Social Science[J]. Science, 2009(4).
- [5]Alvarez R M. Computational Social Science: Discovery and Prediction, Cambridge: Cambridge University Press, 2016: 199.
- [6]范晓光,刘金龙.计算社会学的基础问题及未来挑战[J].西安交通大学学报(社会科学版),2022(1).
- [7]Bail C A, Brown T W, Wimmer A. Prestige, Proximity, and Prejudice: How Google Search Terms Diffuse Across the World[J]. American Journal of Sociology, 2019(5).
- [8]Mohr J W, Bogdanov P. Introduction-topic Models: What They Are and Why They Matter[J]. Poetics, 2013(6).
- [9]王国成.计算社会科学引论:从微观行为到宏观涌现[M].中国社会科学出版社,2015:248.
- [10]Monroe B L. Fightin' Words: Lexical Feature Selection and Evaluation for Identifying the Content of Political Conflict[J]. Political Analysis, 2008(4).
- [11]Bolsover G, Howard P. Chinese Computational Propaganda: Automation, Algorithms and the Manipulation of Information about Chinese Politics on Twitter and Weibo[J]. Information Communication & Society, 2019(14).
- [12]Koger G, Masket S, Noel H. Partisan Webs: Information Exchange and Party Networks[J]. British Journal of Political Science, 2009(3).
- [13]祝建华,彭泰权,梁海,等.计算社会科学在新闻传播研究中的应用[J].科研信息化技术与应用,2014(2).
- [14]徐翔,王雨晨.社会回音室:网络传播中的信息趋同及其媒介逻辑——基于“今日头条”样本的计算传播学分析[J].国际新闻界,2021(7).

- [15]塔娜,赵倩誉.计算传播学:数据与计算驱动的传播学研究[J].青年记者,2022(20).
- [16]郑永和,严晓梅,王晶莹,等.计算教育学论纲:立场、范式与体系[J].华东师范大学学报(教育科学版),2020(6).
- [17]张琪,李福华,孙基男.多模态学习分析:走向计算教育时代的学习分析学[J].中国电化教育,2020(9).
- [18]孙仕亮.计算教育学与十大研究主题[J].中国人工智能学会通讯,2015(9).
- [19]邹江兴,邹宏,张帆.对国家安全学学科建设范式创新的若干思考[J].国家安全研究,2022(3).
- [20]刘跃进,刘黎明.国家安全“本身”与“相关”——“国家安全包括什么不包括什么”辨析[J].中共中央党校(国家行政学院)学报,2024(4).
- [21]李阳,孙建军.国家安全数据管理的兴起及图情档学科的角色[J].图书与情报,2021(5).
- [22]丁波涛.计算社会科学相关概念的比较与辨析[J].情报资料工作,2018(6).
- [23]陈云松.中国计算社会学的发展:特征、优势与展望[J].湖南师范大学社会科学学报,2020(5).
- [24]塔娜.“计算传播学”的发展路径:概念、数据及研究领域[J].新闻与写作,2020(5).
- [25]Rubinfeld D L, Gal M. Access Barriers to Big Data[J]. Arizona Law Review, 2017(2).
- [26]王丹彤,何增科.国家政治安全的新维度:不安全状态及其原因探析[J].河南社会科学,2021(9).
- [27]雷建锋.中俄国际政治安全秩序观:基于实证分析的比较研究[J].国际安全研究,2021(1).
- [28]郭添荣,韩世鹤,罗季阳,等.风险治理视阈下食品安全风险预警指标体系的构建[J].食品安全质量检测学报,2022(5).
- [29]程晨,刘保华,席亚伟,等.基于因子分析公共卫生安全战略目标与策略优选[J].中国公共卫生,2020(5).
- [30]陈新明,高小平.地方政府首席数据官制度运行的现实审视与优化路径[J].探索,2023(6).

(责任编辑 吕红娟)

National Security Studies in the Digital Age: The Origin, Transformation, and Path of Computational National Security Studies

Li Ming

Abstract: As an emerging interdisciplinary subject, national security studies urgently requires the promotion of transformation and innovation in its research paradigm. The advancement of computational social sciences and the practical demands of national security studies have provided a theoretical foundation and practical basis for the proposal of computational national security studies. The research purview of computational national security studies includes relevant theoretical foundations, research methodologies and practical applications. Its research paradigm has accomplished a transformation from small samples to large samples, from partial cognition to comprehensive perception, from causal relationships to correlative relationships, and from empirical judgment to evidence-based analysis. Currently, computational national security studies still confronts substantial challenges in data acquisition and utilization, research methods innovation, and theoretical system construction. In light of this, it is imperative to strike a balance between theory and data, devise distinctive research methods, facilitate the establishment of academic communities, and continuously promote the innovative development of the national security studies discipline system and research paradigms.

Keywords: The Era of Digital Intelligence, National Security Studies, Computational National Security Studies, Paradigm Shift, Theoretical Construction