研究生选拔应更注重“泛”科研能力

□ 张军平

2023年研究生入学考试基本接近尾声。今年报考人数达到474万，比去年增加了17万。可以预见，未来几年考研人数仍然会继续维持上升趋势。在考研难度不断增加的形势下，考生会沿袭高考时的学习模式，通过刷题来固化对各种题型的记忆，提高得分的稳定性。然而，单纯通过分数来初筛学生，这与研究生的科研定位是背道而驰的。

因为唯分数，多数考研的学生可能会把绝大多数时间投入到对专业课的学习上。但事实上，现在的科研已经相当细化，即使在同一个学院，不同老师之间的研究方向也是千差万别。因此，研究生选拔不能仅依靠分数，还应该考察考生是否真正具备研究方向需要的科研能力。而目前的初试、面试等考研环节还难以满足考察考生科研能力的需求。要避免这一问题，在研究生考试中增加科研能力的筛选比重就显得尤其重要。

既然专业课的分数不等同于具体专业方向的科研能力，那较为合理的策略是通过考试来评估考生的“泛”科研能力，比如通过对科普文章和科技文献的阅读理解来评估。一方面，科研能力本身就应该是一种触类旁通的能力。这不仅是研究生期间需要掌握的，也应该是毕业后转换科研方向还能快速解决非本专业问题的能力。另一方面，科普文章、科技文献的阅读能力，也是研究生在解决科研问题中的必要手段。

事实上，从近两年的高考中已经能看到国家对学生科学素养提高的重视。比如，2022年高考语文乙卷的实用类文本阅读，就出现了3篇科普文章，分别为《对称与物理》（杨振宁著）以及《由雪引发的科学实验》和《冰的形态发生：雪晶中的物理学》。其目的是希望学生能从日常生活中发现科学问题，形成良好的科学观察习惯，并善用科学思维分析观察现象背后隐含的科学本质。无独有偶，2023年上海春季高考语文阅读理解中，也有16分的题目出自笔者的人工智能科普书《爱犯错的智能体》。该题是期望考生通过分析陆汝钤为该书撰写的序来推测书的结构，同时学会关注学术前沿，以利于培养考生的科学态度和创新精神。

将科研能力考察环节前置到研究生入学考试中，可以避免学生把大量时间花在专业课的刷题上，也能尽早地提升考生的科学素养。具体来说，可以在考研考试中单独设置与科普文章或科技文献的阅读相关的考试科目。一是通过科普文章或科技文献的阅读，来评测考生对科学知识了解的广度和平时知识积累的深度。二是通过科普文章，可以考察学生对文章的阅读理解能力，包括能否了解全文撰写的结构、中心思想，是否可以快速发现文章中存在的不足，以及可能探索的方向，等等。三是帮助考生形成适合科研的严密逻辑，因为多数科普文章或科技文献都有其内在的逻辑。除此以外，还可以引入短篇科技文献和短篇科普文章的写作，来提升考生的科技论文写作能力。

我相信，通过在考研中前置科研能力的考察，不仅可让考生在准备考研过程中间接地提升科研能力，而且能更好地筛选真正具备科研能力的考生，还能缩短考生进入相关科研方向的学习时间，更快地产生科研成果。

（作者系复旦大学计算机科学技术学院教授）

网络安全不是“打怪”升级

□ 杨义先 钮心忻

创作手记

编者按 4月15日是第八个全民国家安全教育日，今年的教育主题是“贯彻总体国家安全观，增强全民国家安全意识和素养，夯实以新安全格局保障新发展格局的社会基础”。为推动总体国家安全观深入人心、共筑国家安全防线，本报邀请《安全简史——从隐私保护到量子密码》一书作者讲述创作背后的故事，科普信息安全知识，增强读者安全意识。

以ChatGPT、脑机接口和自动驾驶为代表的人工智能（AI）取得新的突破，再次将AI安全推上了万众瞩目的新高峰。毕竟，过去的黑客主要是要钱，但今后攻击AI系统的黑客将会既要钱，又要命。因此，对付黑客将变得越发紧迫。

对付黑客最重要的是安全科普

对付黑客四两拨千斤的手段是什么呢？不是任何一种高精尖的信息安全技术，也不是对违法活动的打击，而是对信息安全的科普。因为，群众的科普水平每提高1分，黑客的攻击难度就会增加10分，整个网络空间的安全强度就会增加100分。

但是，信息安全的科普谈何容易！首先，信息安全的高科技含量很大，且非常抽象，即使是信息安全专家，许多人也只懂自己所在领域的内容；其次，即使有些专家明白相关的信息安全技术，但是要把这些内容用通俗易懂的语言描述出来，也是一个极大的挑战；而且，人们对信息安全问题都怀有很强的侥幸心理，很少有人仅仅是为了获取知识来阅读信息安全科普书籍。因此，必须动用所有合理、有效的手段来牢牢抓住读者的心。比如，优美的文字、风趣的语言、精彩的故事、巧妙的类比、耳目一新的风格、举一反三的启发，等等。

为了写出一本“外行不觉深，内行不觉浅”的安全科普，我们做了近10年的准备：一方面，要努力提升自己的文字表述能力和幽默系数，这对我们这些只会写程序、推数学公式呆板的理工科人员来说无异于脱胎换骨；另一方面，我们还要登上技术和学术顶峰，鸟瞰整个网络空间安全的几乎所有领域，把过去“只见树木”的眼光，提升到“能见森林”的高度。

三大特色成就《安全简史》

在这样的背景和努力下，我们创作的《安全简史——从隐私保护到量子密码》（以下简称《安全简史》）出版不久即入围“中国好书”。本书的最大特色体现在3个方面。

其一，文学理念完全不同。我们认为，用“字”写成的文章最精确，用“词”写成的文章最实用，用“意境”写成的文章最美妙！因此，《安全简史》一书就是努力用“意境”来写成的。把高深莫测的信息安全核心技术，用身边喜闻乐见的趣事来解释，使得读者处于一种非常熟悉的“意境”之中，去类比抽象难懂的虚拟技术。比如，用垃圾回收与处理，去类比大数据挖掘技术；用“家谱”来解释区块链等。

其二，创作方式完全不同。本书其实是用“赛博”方式写成的。更形象地说，为了“引玉”，先由我们“抛砖”，把本书初稿的相关章节公布在网上，然后由读者来进行全方位的修改、批评和版本更新。

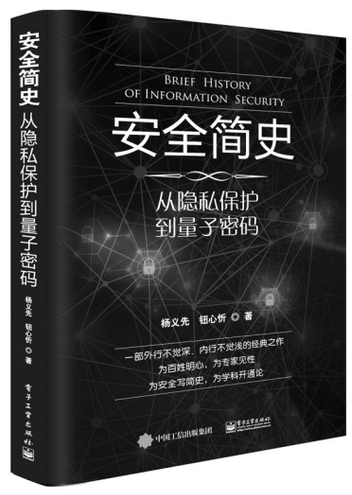
其三，外在形式完全不同。比如，每章的小结，我们都恰如其分地套用了一首耳熟能详的著名诗篇，来重新简洁地归纳该章的内容，既让普通读者感到“不可思议”，又让安全专家觉得“还真是这么回事”。又比如，书中的内容其实不是“硬写出来的”，而是“设计出来”的，每章的文字创作工作，都被当成一个软件工程项目，经过规划、组织、实现和控制等过程，最终完成相关初稿，然后再不断改进。

让网络安全不再被牵着鼻子走

《安全简史》一书在内容和形式等方面也有超越和创新。本书不是对高精尖技术进行简单、机械、堆砌性解释，而是抓住了它们的本质规律，前后呼应，浑然一体，甚至弥补了全球信息安全界过去忽略掉的若干关键。比如，作为画龙点睛的信息安全度量指标“安全熵”，就是本书的独创和首创；信息安全对抗的核心是“人”，而人的核心是“心理”，但从来没有人认真研究过“黑客心理学”，这又是本书所开的先河。此外，本书还首次深入探讨了信息安全管理学。

实际上，至今全球信息安全界，其实是没魂的，形象地说，大家都在“打怪”，哪里有安全问题或哪里有捣蛋的“怪物”出现，大家就一哄而上冲向哪里，完全被“怪物们”牵着鼻子走，而本书作者的另外一部著作《安全通论》则分别从“立地”和“顶天”的角度，为网络空间安全找到了“魂”。

本书还从“赛博”的角度，重新审视了网络空间安全，指出了网络空间安全的攻防过程其实都是“反馈+微调+迭代”的“赛博”过程。强调信息安全是整体的，不是割裂的；是动态的，不是静态的；是开放的，不是封闭的；是相对的，不是绝对的；是共同的，不是孤立的。



《安全简史——从隐私保护到量子密码》，杨义先、钮心忻著，电子工业出版社出版。

我们创作本书的目的和目标是为百姓明心，为专家见性；为安全写简史，为学科开通论。期望普通读者通过“看热闹”，在愉悦的阅读中体会安全的精髓，增强自己的安全意识，从而整体上提高我国网络空间安全的防卫实力；业内专家通过“看门道”，在深思中体会安全的实质，把握今后的学术趋势。

（作者系北京邮电大学信息安全中心教授）

科技采编人员科普能力提升培训班在京举办

科普时报讯（记者**张英贤**）4月12日，由中国科协科普部、中国记协新闻培训中心共同组织的科技采编人员科普能力提升培训班正式开班，来自中央主要新闻单位、全国性行业类媒体及北京市属媒体的50余名科技采编人员参加。

中国科协科普部副部长庞晓东作开班致辞。他指出，随着传统媒体与新媒体不断融合，海量信息能更直接、快速地触达受众。如何让内容更加有趣有用，把优质内容传递给公众，让公众从纷繁复杂的信息中明辨真伪，这些成为摆在所有科技编辑、记者面前的重要课题。在全党全国深入学习贯彻党的二十大精神和全国两会精神之际，组织此次培训就是为了帮助科技采编人员进一步创新科普方式、提升科普能力，发挥媒体作用、贡献新闻力量，在全社会营造热爱科学、崇尚创新的良好氛围。

中国科普研究所研究员朱洪启对《全民科学素质行动规划纲要（2021—2035年）》进行了解读，并指出要注重科学传播的特点，一是善用图像、视频等可视化的表达方式，二是从公共视角出发提炼科普内容，三是贴近老百姓生活，科普内容不脱离生活状态。

此次培训班为期4天，邀请中国科学技术发展战略研究院研究员丁明磊等作政策解读，人民日报、科技日报等中央媒体相关领域专家学者作专题报告。培训还开展两场现场教学，组织科技采编人员前往中国科技馆、百度、快手参观、学习，近期还将组织部分地方媒体科技编辑、记者以线上方式观看课程视频。

跨越分界点的省思

□ 尹传红

不知不觉中，我们已然身处一个像是被科幻所演绎、大大迥异于以往的时代。一切都变得如此之快，以致我们很难用诸如智能社会、信息时代之类的宽略语词来概括了。

特别是，ChatGPT（聊天生成预训练转换器）划时代的应用及其产生的爆发性效应，将人工智能（AI）领域的发展和竞争加速推入了新阶段，甚而引发了国际科技巨头的“军备竞赛”，诸多相关问题也被提了出来。

让我们将视线转向中国。4月11日，国家互联网信息办公室就《生成式人工智能服务管理办法（征求意见稿）》向社会公开征求意见。征求意见稿提出，服务提供者禁止非法披露个人信息，不得根据用户输入信息和使用情况进行画像。

征求意见稿所提到的生成式人工智能（Generative AI），是指基于算法、模型、规则生成文本、图片、声音、视频、代码等内容的技术。它具有很强的的自然语言理解能力和高效的文本生成能力，能够更高效地处理和分析大量数据，更快速准确地回答复杂的问题。总之，过去认为只能做好判别性工作的AI，眼下正在跨越一个分界点：从“判别式领域”迈入“生成式领域”。我们或许可以这样说：新的交互革命开始，AI新纪元来临。

以ChatGPT为代表的生成式AI，最直观的应用场景或许就是可以像人类一样进行聊天交流，以及由此衍生的客服及专业咨询。在成为历史上用户增长速度最快的消费者应用程序的同时，这类新型工具也引发了人们的伦理焦虑。上月底，意大利因一起严重的数据泄露事件而宣布在其境内禁用ChatGPT；包括业界领袖埃隆·马斯克在内的上千名人工智能专家和行业高管签署了一份公开信，呼吁立即停止训练智能水平可与人类竞争的AI系统，称它们可能对社会和人类构成深远风险。

《纽约时报》最近载文指出，AI浪潮席卷硅谷，立法者却困于不懂技术。目前还没有任何法案被提出来，用以保护个人或抑制AI在潜在危险方面的发展。近年来针对限制脸部识别等AI应用的立法，在国会中未能获得成功。而美国国会中唯一拥有AI硕士学位的议员杰伊·奥伯诺尔特抱怨说：“在实施监管前，需要先就AI的危险是什么达成一致，而这需要对该技术有深刻的理解。你会惊讶于我花了多少时间向同僚们解释，AI的主要危险不会来自眼睛里冒着红色激光的邪恶机器人。”

因推出ChatGPT而闻名的硅谷初创公司OpenAI首席执行官萨姆·奥特曼（这名字瞧着就很科幻），今年1月拜访了数位国会议员，当面展示了全新的AI模型GPT-4。它可以完成撰写论文、解决复杂的编程问题等任务，令议员们大开眼界。奥特曼同时表示支持监管，声称GPT-4将比过往的AI模型有着更强大的安全控制机制。

其后在谈到AI的潜在风险时，奥特曼提出，还是需要保持谨慎，整个社会应在短期内抓紧弄清楚如何应对AI带来的变化，要在代价还不会很大的时候试错。他说，现在他特别担心那些模型可能会被用于虚假信息宣传——现在它们写代码越来越熟练，很可能被用来开展网络攻击。他提议全球主要国家应该一起制定一份文件，来规范关于AI的应用哪些可为哪些不可为，对于危险的领域应该永不触及。这样就能让语言模型开发者有个参照标准。

事实上，一家专注人工智能安全研究的非营利机构对齐研究中心（ARC），已于2021年在美国加州湾区成立。作为第三方评估者，ARC主要与领先的人工智能实验室合作，评估他们研发的最先进的机器学习模型是否具备潜在的危险能力。从大的方面看，是否会偏离人类设定的目标自主行动，造成严重的后果，譬如操纵股票价格、设计合成DNA等。这都是通过具体的行动来介入新技术可能带来的社会风险问题。不过，据估算，目前全世界全职从事人工智能安全研究的技术人员只有300名左右，且很难找到“科班出身”的技术人员。

而经济合作与发展组织则在今年2月发布了《推进AI问责制：围绕可信赖AI生命周期的治理和管理风险》报告，介绍了如何整合风险管理框架和AI系统生命周期，探索了有助于实施“基于价值观的可信赖AI原则”的流程和技术属性，确定了围绕AI系统生命周期定义、评估、处理和管理风险的工具和机制。

该报告所涉AI系统的背景，包括其社会经济、物理环境及其对人类和地球的潜在影响。确保AI问责制的一个步骤，是要把AI伦理原则和特定的过程和技术特征联系起来。AI风险可以从两个层面来评估，一个是基于价值观的AI原则层面的风险，另一个是技术层面的风险。确保AI问责制需要将AI原则与特定的过程和技术属性一一对应起来。

生成式AI如何看待当下人们的忧虑呢？它对关涉它的一个提问——“对于那些已经或即将被你取代工作的人，你有什么建议？”——作出了这样的回答：

对于那些工作可能受到自动化影响的人，我的建议是专注于发展难以自动化的技能，例如人际交往能力、创造力、批判性思维和适应能力。此外，跟上技术进步的步伐并学习可以补充自动化的新技能也很有价值。重要的是要对新机会保持开放态度且愿意适应就业市场的变化，因为自动化也有可能创造新的就业机会。

看起来措辞讲究、逻辑严密、无懈可击，似乎还闪现了些许“人性的光辉”。不知读者诸君意下如何？

时代呼唤更多战略科学家

□ 科普时报记者 陈杰

“为加快实现高水平科技自立自强，需要一批战略科学家从国家发展的战略高度出发，深刻理解科技、政治、经济、社会、文化等方面的发展规律和特点，把握世界科技发展大势，探索新的方向，开辟新的疆域。”近日，在“中国战略科学家与科技自立自强”院士专家研讨会上，国际欧亚科学院院士、中国科学院原党组副书记郭传杰呼吁，战略科学家的成长之路曲折漫长，发现和培养更是一项系统工程，我们需要不断完善其发现、培养、激励和使用机制，培养更多的科技领军人才，为实现科技自立自强提供支撑。

大科学家不一定是战略科学家

俗话说“千军易得，一将难求”。作为科技帅才存在的战略科学家，一直是国家战略人才力量中的“关键少数”，在推动科技自立自强和现代化进程中发挥着至关重要的作用。

当前，我国战略科学家缺口大，是全球科技人才竞争日趋激烈的态势下所必须面对的现实问题。中国科学院自然科学史研究所联合科学出版社主办“中国战略科学家与科技自立自强”院士专家研讨会，旨在通过研讨中国战略科学家这一主题，为实现中国式现代化和科技高水平自立自强提供历史借鉴和现实启示。

近年来，我国日渐重视对战略科学家群体的培养和支持。2021年9月的中央人才工作会议上，“大力培养使用战略科学家”就成为重要议题之一。这个群体被定义为专门研究和解决战略性问题的科学家，能为政府和各种组织提供战略性的思考、分析和建议，以帮助他们制定更有效的政策和计划。

与会院士和专家普遍认为，战略科学家的工作与科学家以及科技人才的工作有所不同，他们更加注重战略性问题的分析和解决，关注的是整体性和长远性的问题，而不仅仅是技术问题。

郭传杰表示，战略科学家是一个多类型、多层次的高级科学家群体，在不同的分类中，战略科学家素质结构不尽相同。“大科学家可能名声会很大，但并不一定都是战略科学家。”

国家国防科工局直属机关党委巡视员袁和平说：“战略科学家的使命就是抢占科技发展战略制高点，他们身上体现了强烈的科学家精神。”

培养战略科学家是系统工程

不同于科技人才和科学家，战略科学家该具备什么样的特质？

郭传杰表示，战略科学家要拥有家国情怀和一种使命感，为人公道正派并具有团队合作精神，能够以大局为重，既要善于倾听不同的意见，又有独立的主见。在知识结构上，他们往往有很深的专业造诣，但同时也应该对国际国内的科学技术、经济、社会的发展，有一定的了解和认识。在能力结构上，应该重点考虑科学家是否具有创新成就、战略头脑以及跨界组织协调能力。“钱学森就是我国历史上最著名的战略科学家之一。”

中国科学院院士、中国科学院力学研究所研究员李家春指出，战略科学家应知识渊博、视野开阔、高瞻远瞩，具备长远规划经验和团队组织能力。

在谈到如何培养战略科学家时，他认为，培养战略科学家，需要建立科学合理的人才评价制度，也要努力创造有利于战略科学家涌现的学术环境。“在人才评价方面，要破除‘唯论文、唯职称、唯学历、唯奖项’倾向，评价科研成就要把关注点放在能否真正解决问题上，尤其是一些关键技术问题。”

郭传杰介绍，战略科学家的成长对应着3种不同的路径，分别是从有宏观思维的一线创新科学家到战略科学家，从有科学素养的企业管理者到科技战略家，以及从有宏观战略思维的科技管理者到科技战略家。“培养战略科学家，除了积极参与国家战略规划，还需要构建重大项目平台，改革科研体制机制，建设良好生态文化，疏通建言献策渠道，这是一项系统工程。”

郭传杰强调：“在科学技术发展处在范式变革的当下，也是最缺战略科学家之时，我们急切地需要像钱学森这样的战略科学家出现。”