恶意软件检测技术课程思政教学案例

胡俊鹏 智能科学与工程学院

引言

随着信息技术的飞速发展，网络安全问题日益突出，恶意软件的威胁也愈发严峻。《恶意软件检测技术》作为信息安全专业的选修课程，不仅承载着传授专业知识与技能的任务，更肩负着培养学生网络安全意识、科技伦理观念以及社会责任感的重要使命。本课程通过深入挖掘恶意软件检测技术中的思政元素，将其有机融入教学全过程，旨在打造一门既有技术深度又有价值引领的专业课程，为培养德才兼备的信息安全专业人才贡献力量。

一、课程基本信息

《恶意软件检测技术》是一门面向信息安全专业三年级学生开设的专业选修课程，属于专业教育课程，课程学分为 2 学分。

二、课程教学整体设计思路

在课程教学中，将思政元素与专业知识有机结合，以实现知识传授、能力培养和价值引领的有机统一。例如在讲解恶意软件的工作原理时，强调其对个人隐私、社会安全乃至国家安全的危害，从而引导学生树立正确的网络安全观，增强学生对恶意软件的警惕性和防范意识。同时，通过介绍我国在网络安全领域的法律法规和政策举措，培养学生的法律意识和爱国情怀，使学生深刻认识到作为信息安全专业人员肩负的使命和责任。教学过程中，采用多样化的教学方法，如讲授法、案例分析法、小组讨论法、实践教学法等，充分调动学生的积极性和主动性，让学生在学习专业知识的同时，不断强化思政意识，提高自身的综合素养。

三、案例教学目标

知识目标 ：帮助学生深入理解恶意软件的检测原理、方法和技术，掌握恶意软件检测工具的使用，熟悉恶意软件检测技术的发展趋势和应用前景。

能力目标 ：培养学生运用所学知识和技能分析、解决实际恶意软件检测问题的能力，提高学生的实践操作能力和创新思维能力。引导学生学会自主学习和团队协作，提升学生的职业素养和综合竞争力。

素质目标 ：通过课程思政元素的融入，培养学生的网络安全意识、科技伦理观念、社会责任感和爱国情怀，引导学生树立正确的价值观和职业观，使学生成为德才兼备的信息安全专业人才。

四、案例教学实施过程

1. 课前准备

教师：精心备课，深入挖掘恶意软件检测技术中的思政元素，如网络安全的重要性、科技伦理的边界、法律法规的约束等，并将其合理融入教学内容。同时，选取相关的实际案例和新闻事件，制作成教学课件和资料，为课堂教学做好充分准备。

学生：提前预习课程内容，了解恶意软件检测的基本概念和相关知识点。通过查阅资料、观看在线课程等方式，对恶意软件的威胁和检测技术有一定的初步认识，并记录下自己在预习过程中遇到的问题和疑惑，以便在课堂上与教师和同学进行交流讨论。

2. 教学实施

导入案例：在课程开始时，教师通过展示一些近年来发生的重大恶意软件攻击事件的新闻报道和案例视频，如勒索病毒 “WannaCry” 爆发导致全球众多企业和机构的计算机系统瘫痪事件、黑客利用恶意软件窃取个人隐私信息引发的社会恐慌等，引发学生的思考和讨论，使学生深刻认识到恶意软件的危害性以及恶意软件检测技术的重要性和紧迫性。在讨论过程中，教师引导学生关注这些事件对个人、社会和国家造成的严重影响，从而引出本节课的主题 —— 恶意软件检测技术，同时也激发了学生的学习兴趣和求知欲。

知识讲解：结合教学内容，教师详细讲解恶意软件的定义、分类、传播途径以及常见的检测方法和技术，如特征码检测、行为检测、启发式检测等。在讲解过程中，教师注重将思政元素融入其中。例如，在介绍特征码检测技术时，强调其依赖于对已知恶意软件样本的分析和总结，这就要求研究人员具备严谨的科学态度和高度的责任感，及时更新恶意软件样本库，以确保检测的准确性和有效性；在讲解行为检测技术时，引导学生思考如何区分正常软件行为和恶意软件行为，从而培养学生的逻辑思维能力和判断力，同时也让学生明白在实际工作中要善于观察和分析事物的本质，做到心中有数，不被表面现象所迷惑。

小组讨论：将学生分成若干小组，每组围绕教师提出的问题进行讨论。例如，“在恶意软件检测过程中，如果发现某款软件存在潜在的安全风险，但又无法确定其是否为恶意软件，作为信息安全专业人员，应该如何处理？” 各小组成员充分发挥自己的见解，结合所学知识和实际情况进行深入探讨。在讨论过程中，教师巡视各小组，适时给予指导和启发。小组讨论结束后，每个小组选派代表进行发言，分享本小组的讨论成果。教师对各小组的发言进行总结和点评，进一步强调在面对不确定的安全问题时，要遵循谨慎、科学的原则，既要保障系统的安全稳定运行，又要避免过度反应造成不必要的损失，同时也要考虑到软件开发者和使用者的利益，秉持公平、公正的态度，这体现了一种职业操守和社会责任感。

案例分析：教师选取一个实际的恶意软件检测案例进行详细分析。例如，分析一款名为 “X” 的恶意软件，首先介绍该恶意软件的传播途径、感染症状以及对计算机系统和用户数据造成的危害，然后引导学生运用所学的检测方法和技术对该恶意软件进行检测和分析。在案例分析过程中，教师让学生亲身体验恶意软件检测的全过程，包括样本采集、环境搭建、检测工具的使用、检测结果的分析等环节。同时，教师引导学生思考如何将检测结果及时准确地反馈给相关部门和用户，以及如何协助用户进行恶意软件的清除和系统恢复工作。通过案例分析，不仅加深了学生对恶意软件检测技术的理解和掌握，还让学生深刻认识到作为信息安全专业人员，在面对网络安全威胁时，要有担当和作为，积极运用自己的专业知识和技能为维护网络安全贡献力量。

课堂总结：教师对本节课的教学内容进行总结回顾，重点强调恶意软件检测技术的关键知识点和思政元素。再次强调网络安全意识的重要性，提醒学生在今后的学习和工作中要时刻保持警惕，规范自己的网络行为，遵守法律法规和道德规范，不参与任何制作、传播恶意软件等违法活动，做一个合格的信息安全专业人员和守法公民。

3. 教学评估

平时表现评估：教师根据学生在课堂上的出勤情况、参与讨论的积极性、回答问题的准确性以及小组作业的完成质量等方面进行综合评估，了解学生对课程知识的掌握程度和思政意识的培养情况，占总成绩的 10%。

实验项目评估：通过布置恶意软件检测相关的实验项目，让学生在实践中运用所学知识和技能，检测和分析恶意软件。教师根据学生的实验报告、实验结果以及实验过程中的表现进行评估，重点考察学生的实践操作能力、问题解决能力和团队协作能力，占总成绩的 30%。

期末考试评估：期末考试采用闭卷考试的形式，涵盖课程的全部知识点，包括恶意软件检测理论、方法、技术以及思政相关内容，重点考察学生对知识的系统掌握程度和综合运用能力，占总成绩的 60%。

五、教学效果及反思

1. 教学效果

学生的学习兴趣和积极性显著提高。通过实际案例的引入和多样化的教学方法，学生们对恶意软件检测技术产生了浓厚的兴趣，课堂参与度明显提升，课后主动查阅资料、深入思考问题的积极性也大大提高。

学生的专业知识和技能得到了有效掌握。通过理论学习、案例分析和实践操作，学生们深入理解了恶意软件检测的原理、方法和技术，能够熟练运用检测工具对恶意软件进行检测和分析，并且具备了一定的解决实际问题的能力。

学生的思政意识得到了明显增强。在课程思政元素的潜移默化影响下，学生们树立了正确的网络安全观、科技伦理观和社会责任感。在学习和生活中，学生们更

加注重遵守法律法规和道德规范，积极参与网络安全宣传活动，主动向身边的人宣传网络安全知识，提高大家的网络安全意识。

2. 反思

在教学过程中，虽然注重了思政元素的融入，但在某些知识点的讲解中，思政元素的融入还不够自然流畅，存在生硬拼接的现象。在今后的教学中，需要进一步优化教学设计，深入挖掘思政元素与专业知识的契合点，使二者更加有机地融合在一起。

实践教学环节的时间安排相对紧张，部分学生的实验操作不够熟练，导致实验结果不够理想。在后续教学中，应适当增加实践教学的学时，为学生提供更多的实践机会，同时加强对学生的实验指导，提高学生的实践操作能力和解决问题的能力。

对于学生的个体差异关注不够。在教学过程中，发现部分学生在学习能力和思政意识方面存在差异，但在教学方法和评价方式上没有充分考虑这些差异，导致个别学生的学习效果不够理想。今后应更加注重因材施教，根据学生的不同特点和需求，采取个性化的教学方法和评价体系，使每个学生都能在课程学习中有所收获，得到充分的发展。