附件1

2025年首届“智安杯”

大学生国家安全案例大赛

竞赛手册

2025年4月

目 录

[2025年首届大学生“智安杯”国家安全案例](#_Toc191561435)[大赛竞赛通知 1](#_Toc191561436)

[“智安杯”大学生国家安全案例大赛](#_Toc191561437)[参赛案例选题指南（文科组） 6](#_Toc191561438)

[“智安杯”大学生国家安全案例大赛](#_Toc191561440)[参赛案例选题指南（工科组） 12](#_Toc191561441)

[“智安杯”大学生国家安全案例大赛](#_Toc191561442)[参赛案例提交模版 17](#_Toc191561443)

[“智安杯”大学生国家安全案例大赛](#_Toc191561444)[参赛报名信息表 20](#_Toc191561445)

[“智安杯”大学生国家安全案例大赛](#_Toc191561446)[案例编写格式要求 21](#_Toc191561447)

[“智安杯”大学生国家安全案例大赛](#_Toc191561448)[参赛团队知识产权原创性和法律责任声明 25](#_Toc191561449)

2025年首届“智安杯”大学生国家安全案例

大赛竞赛通知

为深入践行总体国家安全观，加快推进科技赋能国家安全战略，在第十个“4·15”全民国家安全教育日和《中华人民共和国国家安全法》修订颁布十周年之际，由国际关系学院等10所高校共同发起，组织开展2025年首届“智安杯”大学生国家安全案例大赛。本次大赛旨在通过实战案例设计促进国家安全学科与各领域的深度融合，遴选优秀案例，打造具有鲜明特色、多元参与的大学生国家安全教育品牌，提高大学生国家安全意识，筑牢国家安全屏障。

首届“智安杯”国家安全案例大赛报名通道正式开启，欢迎广大学子积极报名参加。现将有关事项通知如下：

一、竞赛主题

人工智能与国家安全

二、竞赛宣传口号

AI护航国家安全，创新引领安全未来

三、组织单位

指导单位：国务院学位委员会国家安全学学科评议组

中共北京市委国家安全委员会办公室

中共北京市委教育工作委员会

发起单位：国际关系学院、首都师范大学、华东政法大学 、

陕西师范大学、北京理工大学、北京交通大学、

上海交通大学、同济大学、中国人民公安大学、

河南大学 （发起单位排名不分先后）

本年度主办单位：国际关系学院、首都师范大学

承办单位：国际关系学院国家安全与发展研究院、国际关系学院网络空间安全学院和公共管理系、首都师范大学管理学院、华东政法大学国家安全研究院、陕西师范大学国家安全学院、北京理工大学网络空间安全学院、北京交通大学计算机与信息技术学院、上海交通大学国家安全研究院、同济大学法学院、中国人民公安大学国家安全学院、河南大学人工智能学院

协办单位：《中国信息安全》杂志社、北京市总体国家安全观研究中心、中国电子质量管理协会人工智能大模型工作委员会、高校思想政治工作创新发展中心（上海教育网研中心）、上海市人工智能社会治理协同创新中心、上海市大数据社会应用研究会青少年AI教育专业委员会

四、竞赛时间

案例作品网上报名和提交时间：2025年4月1日至5月31日24时。参赛人员需将本通知附件要求的《参赛团队信息表》和案例作品材料一并提交。

案例提交邮箱：zhianbeigongke@163.com（工科组）；zhianbeiwenke@163.com（文科组）。组委会将组织高校科研机构相关领域的专家分组别进行评审，并于6月中旬组织优秀案例现场汇报并正式公布评选结果。具体时间安排如下：

|  |  |
| --- | --- |
| **竞赛阶段** | **时间安排** |
| 大赛启动仪式 | 4月上旬 |
| 案例报名和提交 | 4月1日-5月31日 |
| 案例作品综合评审 | 6月1日-6月10日 |
| 优秀案例展示暨颁奖仪式 | 6月中下旬 |

五、竞赛形式

本次竞赛设置分为工科组和文科组，参赛团队须按照组别要求报名参赛。具体成果形式要求如下：

（一）工科组

参赛团队须提交案例说明（一般不超过3000字）和参赛案例实验过程视频（5-8分钟）。案例演示文稿（PPT）、参赛案例代码片段、系统截图等文件可作为附件一并提交，作为案例评选的重要参考。

（二）文科组

参赛团队须提交案例说明、调研报告等（一般不超过5000字），案例的演示文稿（PPT），涉及参赛案例调研问卷、访谈记录等亦可作为附录一并提交，作为案例评选的重要参考。案例中展示的视频自行选择制作。

六、参赛对象及要求

本届大赛以发起院校和北京地区高校学生报名为主，同时接受全国高校（含研究生、本科生）具有正式学籍的全日制在校生报名，具体要求如下：

（一）每支参赛队伍不超过5人（包含1名负责人），鼓励校内跨年级、跨专业组队，各高校参赛队伍数量不限，不允许跨校组队；

（二）每人只能参加1支队伍（即个人参赛后不可再与他人组队参赛，或个人参加一支队伍后不可再参加另一支队伍）；

（三）每支参赛团队可邀请1名指导教师，且须为参赛队伍所在高校教师，可以指导学生进行组队、实验演练、案例编写等；

（四）参赛提交的案例作品知识产权由大赛组委会和所在团队共同享有；

（五）各参赛队伍应严格遵守比赛规则，不得违反国家法律、法规、公序良俗，不得涉及国家秘密和工作秘密，同时严禁侵犯知识产权，一经发现违反，立即取消参赛资格，并按照国家相关法律法规处理。

七、奖项设置

一等奖：工科组、文科组各2名，颁发获奖证书，并奖励获奖团队5000元。

二等奖：工科组、文科组各3名，颁发获奖证书，并奖励获奖团队3000元。

三等奖：工科组、文科组各5名，颁发获奖证书，并奖励获奖团队2000元。

优秀奖：若干名，颁发获奖证书和大赛纪念品。

经专家评选出的优秀案例将汇编成案例库，供交流。若通过专家匿名评审并进行相应修改形成的学术论文，将优先在《国际安全研究》《中国信息安全》等发起单位学术期刊上发表；同时具有较强现实性和实践性的案例将向有关方面予以上报参考；参赛人员有机会被邀请作为成员参与相关专家学者在研科研项目。‌

八、其他事宜

本届大赛不收取包括报名费和其他任何费用。有关本届大赛的重要通知和说明事宜，由组委会通过《中国信息安全》杂志官方公众号、大赛各发起单位和支持单位的官方公众号统一公告和通知。涉及参赛报名和案例作品的有关要求，请参见附件。

九、联系信息

联系人：赵老师（工科组） 13126597355

电子邮箱：zhianbeigongke@163.com

杨老师（文科组） 18810378265

电子邮箱：zhianbeiwenke@163.com

刘老师（组委会） 13693239390

电子邮箱：zhianbei@163.com

附件：2025年首届“智安杯”大学生国家安全案例大赛竞赛手册

“智安杯”大学生国家安全案例大赛组委会

2025年4月1日

附件1：

2025年首届“智安杯”大学生国家安全案例大赛

参赛案例选题指南（文科组）

根据《大赛通知》要求,参赛团队（文科组）可结合人工智能技术，探索其在国家安全与社会科学领域的交叉应用,特别是在政治安全、经济安全、公共安全、国际安全格局、国家安全法治、前沿技术治理与社会伦理等领域。参赛者应从人工智能应用、安全格局影响和风险预测等角度，分析并提出创新性的解决方案，推动人工智能技术与国家安全深度融合。以下是针对本届大学生国家安全案例大赛参赛案例的选题指南和参赛案例提交参考模板，旨在帮助参赛选手系统性地完成从选题到案例撰写的全流程，确保作品具备技术深度、应用广度与现实价值。

# 一、选题方向与案例设计

## （一）人工智能与国家政治安全

1.聚焦人工智能对国家政治安全及意识形态安全的现实挑战，分析信息失序及舆论操纵背景下的国家政治安全优化策略与治理体系。

2.聚焦人工智能操纵公共舆论的识别和应对，如疫情期间人工智能生成合成大量虚假新闻、虚假视频加剧印巴冲突等地区冲突情形。

## （二）人工智能与公共安全

1.聚焦数智时代人工智能技术在公共安全、风险治理、应急管理等领域的典型实践应用，提炼相应的赋能机制与路径，并分析其中的效度与限度。

2.聚焦人工智能公平性问题的来源，探究算法歧视、偏见等带来的社会公平正义问题，分析其中可能的阻力及实现人工智能公平性审计的多维策略。

3.聚焦人工智能技术部署与应用产生的社会排斥现象，分析社会公众态度与技术接纳心理，就可能衍生的就业替代、产业变革等社会稳定问题展开研究。

4.聚焦人工智能与社会风险，探究人工智能社会的风险形态及其表征、后果，分析智能社会风险的演化机理及应对策略。

## （三）人工智能与前沿技术治理

1.聚焦人工智能相关的数据、算法、算力等典型问题，分析芯片设计制造、软硬件系统设备、关键信息基础设施、网络连接传输、模型应用场景等层面的安全隐患及风险挑战，提出可行的治理策略。

2.聚焦人工智能与其他技术（如生物识别技术）的结合，分析应用过程中的安全问题与技术风险，并探究针对性优化路径。

3.聚焦人工智能发展带来的数据安全问题，探究隐私计算赋能多方互信数据安全治理；人工智能赋能跨境数据流动合规风险评估与管控；政务数据安全管理能力成熟度模型构建；公共数据开放共享模式与安全体系设计；公共数据授权运营的风险研判、模式构建与实践路径等问题。

4.聚焦数据主权与跨境传输，探究数据本地化合规框架；基于《数据安全法》，设计人工智能企业跨境数据传输的安全评估流程与法律应对方案。

## （四）人工智能与国际安全格局

1.聚焦分析开源背景下新型国际技术竞争格局，聚焦数据跨境流动、技术垄断与滥用、算力依赖等问题，提出削弱技术霸权，优化产业生态的治理策略。

2.聚焦人工智能军事化应用对国际安全格局与外交策略的重塑与变革，探讨人工智能驱动的致命性自主武器系统（LAWS）对战争伦理、国际人道法及战略稳定的影响，提出现实挑战与可能的控制方案。

## （五）人工智能与社会伦理

1.聚焦技术伦理层面，探究人工智能技术应用对国家文化、价值观、伦理准则等的冲击，分析可能引发的伦理争议、价值观冲突以及人机关系的再思考。

2. 聚焦人工智能与社会发展，探究人工智能的社会效应，分析人工智能对社会运行的影响机制、现实挑战及应对策略。

3.聚焦人工智能与社会公平，探究研究人工智能在缩小收入差距、促进共同富裕方面的作用机制，分析存在的现实问题与挑战，提出人工智能维护社会公平的对策建议。

4.聚焦人工智能与社会治理，探究人工智能促进社会发展的机制，分析人工智能给社会治理带来的机遇与挑战，结合现实问题，探讨人工智能促进社会治理的路径与策略。

## （六）人工智能与国家安全风险预测

1.聚焦人工智能带来的国家安全风险，探究人工智能赋能网络安全态势感知。

2.人工智能与国家安全风险预警，人工智能与国家安全态势感知等问题。

## （七）人工智能与国家金融安全

1.聚焦人工智能社会工程攻击带来的金融挑战；算法互联造成金融闪崩的预测，如资本市场高频交易算法互联等。

2.聚焦研究人工智能金融犯罪监测与防控，如欺诈检测与反洗钱等。

（八）人工智能与国家安全法治

1.聚焦军用人工智能对人道主义法的挑战，包括自动化决策、面部识别炸弹、无差别攻击、比例原则、责任归属等。

2.聚焦人工智能伦理，探究人工智能伦理原则立法转化，结合《新一代人工智能伦理规范》，设计可行的人工智能透明、公平、可控性法律条款及处罚措施。

3.聚焦环境监测人工智能法律授权，探究污染预测算法的司法应用，基于《环境保护法》，论证人工智能环境监测数据在行政处罚中的证据效力认定规则及算法可解释性要求。

4.聚焦人工智能军事化法律约束，探究自主武器系统的国际法规制，参考《特定常规武器公约》，分析人工智能致命性自主武器研发部署的法律真空及国家责任体系构建路径。

5.聚焦算法偏见与反歧视法，研究算法公平性监管，结合《个人信息保护法》，探讨人工智能招聘系统性别偏见的法律规制及合规整改措施。

6.聚焦自动驾驶事故责任认定，探究智能驾驶的法律责任重构，依据《道路交通安全法》，分析L4级自动驾驶汽车事故中制造商、用户与保险公司的责任分配机制。

7.聚焦人脸识别与隐私保护，探究公共监控的合法性边界，基于《个人信息保护法》，评估人工智能人脸识别技术在治安管理中的法律授权范围及隐私风险防范。

8.聚焦深度伪造技术法律规制，探究合成媒体内容治理，根据《网络安全法》，设计针对人工智能深度伪造音视频传播的刑事定罪标准与平台审查义务框架。

9.聚焦无人机监管法律框架，探究城市空域管理的立法需求，基于《民用航空法》，提出人工智能无人机群体飞行监管的法律制度设计及空域冲突解决机制。

10.聚焦国家安全与人工智能监控授权，探究反恐监控的法定程序，依据《国家安全法》，论证人工智能大规模舆情分析技术在反间谍应用中授权范围与公民权利平衡方案。

11.聚焦金融人工智能安全合规风险，探究智能投资适当性义务，根据《证券法》，制定人工智能财富管理产品投资者适应性评估的法律标准及违规处罚细则。

12.聚焦人工智能漏洞的法定责任，根据《网络安全法》，分析人工智能系统漏洞导致数据泄露时开发者的法律责任划分。

（九）其他相关选题

二、评审标准

（一）案例的创新性

案例分析的创意性和创新性，特别是人工智能技术与国家安全相关领域社会科学应用的理念阐释、案例思路和实现路径。（40%）

（二）报告的实证性和规范性

案例运用国家安全交叉学科的理论和工具准确、合理；调研合理充实，有恰当的分析框架，描述清晰，文本规范，分析深刻，形成具有学术价值和实践价值的结论和建议。（30%）

（三）分析的可实践性与影响力

案例具有解决相关问题的适用性和实践价值，提出的对策建议和经验模式，能够为国家安全相关科技领域完善相关政策提供参考和潜在影响。（20%）

（四）案例的逻辑性与表达的说服力

提交案例描述的逻辑性强，包括演示文稿和其他案例材料等，以及现场展示具有的表述清晰度与说服力。（10%）

三、其他说明

所有参赛团队在案例选题和撰写过程中，应特别注意合规、保密，避免伦理风险。如一经发现违法违规行为，将按照国家相关法律法规执行。

（一）合法合规

提交的案例应使用可公开获取的合法合规数据和信息。

（二）保密原则

提交的案例不得涉及任何国家秘密和工作秘密。

（三）使用范围

提交的案例仅可用于高校科研和教学活动。

（四）伦理考量

提交的案例在研究和展示的过程中应纳入伦理考量，避免存在违反公序良俗等伦理风险。

附件2：

2025年首届“智安杯”大学生国家安全案例大赛

参赛案例选题指南（工科组）

根据《大赛通知》要求,参赛团队（工科组）可结合人工智能技术，探索其在国家安全领域的应用,特别是在网络安全、数据安全、人工智能硬件与软件安全等领域。参赛者应从技术实现、工程应用、系统架构等角度，分析并提出创新性的解决方案，推动人工智能技术与国家安全深度融合。以下是针对本届大学生国家安全案例大赛参赛案例的选题指南和参赛案例提交参考模板，旨在帮助参赛选手系统性地完成从选题到案例撰写的全流程，确保作品具备技术深度、应用广度与现实价值。

一、选题方向

参赛案例选题内容可以参考但不局限于以下方向。

（一）人工智能与网络攻防

1.智能防御体系：探索人工智能在网络攻防中的应用，提高系统对网络攻击的感知、预警与防御能力。

2.漏洞发现与安全加固：研究人工智能在网络、软件、硬件系统的漏洞检测、安全加固与威胁修复策略。

3.网络安全监测与应急响应：分析人工智能在网络安全监测、实时风险识别、自动化应急响应等方面的作用。

（二）人工智能与数据安全

1.数据安全防护：研究如何利用人工智能提升数据存储、传输和使用过程中的安全性，降低数据泄露风险。

2.个人隐私保护：探索人工智能在个人信息保护、匿名化处理、隐私计算等方面的应用，确保数据合规与安全。

3.数据共享与安全管理：研究如何在保障数据安全的前提下，实现数据的安全共享、访问控制与合规管理；探索大数据安全分析在风险检测、异常识别、数据治理方面的应用。

（三）人工智能及大模型的内生安全

1.人工智能及大模型安全防护：探索人工智能模型的隐私保护技术、模型版权保护技术、AIGC的检测与溯源技术等。

2.模型脆弱性的发现与安全提升：研究人工智能模型后门的检测、越狱攻击检测、对抗样本检测等脆弱性发现技术；研究模型后门的清除技术、剪枝或重训练等模型安全提升方法。

3.人工智能及大模型安全评估：通过技术的方法进行模型的对抗鲁棒性评估、投毒鲁棒性评估、后门鲁棒性评估、可信评估、能力评估、红方评估等，保障模型的内生安全。

（四）人工智能与经济金融安全

1.金融安全与风险管控：研究人工智能在金融市场预测、金融欺诈检测、智能风控等方面的应用。

2.智能交易与监管：探索人工智能在金融交易自动化、市场行为监测、合规监管中的作用。

3.经济数据分析与情报挖掘：研究人工智能在经济数据分析、产业安全评估、经济竞争情报方面的应用。

（五）人工智能与关键基础设施安全

1.基础设施安全防护：探索人工智能在能源、交通、通信等关键基础设施的安全监测与防护中的应用。

2.工业系统安全增强：研究人工智能在工业控制系统中的安全管理与异常检测。

3.关键系统智能调度：分析人工智能在优化关键基础设施调度、提升稳定性与安全性方面的作用。

（六）人工智能与社会稳定

1.舆情分析与信息安全：探索人工智能在社交媒体、新闻传播中的舆论监测、虚假信息识别与治理。

2.公共安全与应急管理：研究人工智能在社会治安、犯罪预防、突发事件响应中的应用。

3.社会治理与智能决策：分析人工智能在城市管理、人口监测、社会政策制定等方面的作用。

（七）人工智能与安全教育

1.智能化安全教育：探索人工智能在国家安全教育、培训系统、个性化教学中的应用。

2.仿真模拟与技能训练：研究人工智能在虚拟仿真演练、应急训练、对抗模拟中的作用。

3.智能安全意识培养与行为训练：研究人工智能如何在安全教育中帮助学员提升安全意识，通过智能化行为训练模拟安全威胁场景，强化学员的预防和应对能力，培养在现实中识别和处理安全风险的能力。

（八）人工智能与生物安全

1.疾病监测与预警系统：研究人工智能在生物安全领域如何通过大数据分析和机器学习模型进行疾病传播预测、早期检测和实时监控，帮助识别潜在的生物威胁并提供及时预警。

2.实验室安全管理：探索人工智能在实验室环境如何应用于安全监控、危险品管理以及突发事件应急响应，确保实验过程中的生物安全和设备安全。

3.生物威胁识别与响应：分析人工智能在生物威胁的识别、分析与响应中的作用，特别是在通过图像识别、基因序列分析等技术对新型病原体进行快速识别和分类，从而提供精准的防控策略。

4.人工智能在生物医学安全方面的应用与设计。

（九）其他相关选题

二、案例类型

参赛选手可以考虑（但不局限于）提交以下案例类型。

（一）工程原型型案例

开发一个基于人工智能的技术原型，展示解决方案的实际可行性（如人工智能驱动的网络安全防护系统）。

（二）技术优化型案例

针对某一技术瓶颈或安全问题提出优化方案（如基于深度学习的网络入侵检测系统优化）。

（三）跨学科整合型案例

结合人工智能技术与其他学科知识（如大数据、云计算等），提出复合型的创新性解决方案（如基于人工智能大数据安全分析平台）。

三、评审标准

（一）案例的创新性

案例分析的创意性和创新性，特别是人工智能技术应用于国家安全的理念阐释、案例思路和实现路径。（40%）

（二）技术的先进性

解决方案的技术深度和先进性，运用的人工智能方法与理论的可行性，以及方案执行的可操作性。（30%）

（三）方案的实用性与影响力

解决方案的实际应用价值，解决相关问题的适用性，以及对国家安全领域的潜在影响力。（20%）

（四）案例的逻辑性与表达的说服力

提交案例描述的逻辑性，包括演示文稿和其他案例材料等，以及现场展示的表述清晰度与说服力。（10%）

四、其他说明

所有参赛团队在案例选题和撰写过程中，应特别注意合规、保密，避免伦理风险。如一经发现违法违规行为，将按照国家相关法律法规执行。

（一）合法合规

提交的案例应使用可公开获取的合法合规数据和信息。

（二）保密原则

提交的案例不得涉及任何国家秘密和工作秘密。

（三）使用范围

提交的案例仅可用于高校科研和教学活动。

（四）伦理考量

提交的案例在研究和展示的过程中应纳入伦理考量，避免存在违反公序良俗等伦理风险。

附件3：

2025年首届“智安杯”大学生国家安全案例大赛

参赛案例提交模版

根据《大赛通知》要求，参赛团队须按照以下参考模版提交参赛评选相关材料。

一、案例提交内容

（一）工科组

参赛团队须提交报名信息表（附件4）、案例说明（一般不超过5000字）、案例演示文稿（PPT）、涉及参赛案例实验过程视频（5-10min）、代码片段、系统截图等文件，作为案例评选的重要参考。

（二）文科组

参赛团队须提交报名信息表（附件4）、案例说明（一般不超过5000字），案例演示文稿（PPT），涉及参赛案例的调研报告、调查问卷、访谈记录等亦可作为附录一并提交，作为案例评选的重要参考。案例中展示的视频自行选择制作。

二、案例说明的主要内容

1.案例标题

标题要求：简明扼要，体现人工智能与国家安全不同领域的关联（例：《对抗深度伪造：多模态检测模型在舆情安全中的应用》）。

2.案例摘要（300字以内）

主要阐述本案例拟说明和研究的核心问题、技术（工科组）或政策方案（文科组）、创新点和预期影响等。

3.案例研究的背景与问题（500字以内）

（1）案例的国家安全场景：说明选题背景（如人工智能伪造领导人讲话视频可能引发外交危机）。

（2）主要存在的问题分析：现有技术工具或政策手段不足（如传统检测工具误报率高）。

4.案例的分析框架

（1）案例研究方法和工具：技术路线（如深度学习模型等）或政策分析工具（如SWOT分析等）。

（2）案例数据或信息来源：注明数据集类型与获取方式（如公开的Deepfake数据集）。

5.案例提出的解决方案与论证情况

（1）技术类（工科组）：算法设计、系统架构、实验验证结果（附准确率/效率对比）。

（2）政策类（文科组）：政策法规模型、国际合作机制、风险评估矩阵、工作方案建议。

各竞赛小组应对提出的方案进行较全面的论证说明。

6.方案的执行实施计划

实施计划可参考包括：如短期（1年内）技术原型开发或试点应用的具体内容；中长期（3-5年）涉及的技术迭代、政策法律、合作机制、风险预警等的推广路径；资源需求涉及的预算、硬件支持、跨部门协作等支撑保障条件。

7.案例创新点

案例提出的问题解决方案与现有技术模式或政策手段比较，重点突出技术、策略或视角上的创新（如“首次将强化学习用于反恐路径预测”）。

8.案例实施可能带来的预期影响

（1）对维护国家安全的技术绩效或政策贡献（如“将虚假信息识别速度提升40%”）。

（2）仍然存在的潜在风险、局限性与应对措施（如技术模型被攻击的防御方案，政策方案实施的漏洞或短板）。

9.参考文献与知识产权原创性责任与声明

案例参考使用的学术论文、政策文件、技术报告等，按标准格式（附件5）列出；并由团队全部成员电子签署知识产权原创性责任与声明（附件6）

|  |  |
| --- | --- |
| 案例编号 |  |

附件4：

2025年首届“智安杯”大学生国家安全案例大赛

参赛报名信息表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 学校名称 | |  | | | 参赛组别 | | | 工科组□ 文科组□ | | | |
| 参赛案例名称 | | |  | | | | | | | | |
| 负责人  （联系人） | | 姓名 |  | | | | 联系方式 | | |  | |
| Email |  | | | | | | | | |
| 通讯地址 |  | | | | | | | | |
| 参  赛  团队人员信息 | 序号 | 姓名 | 性别 | 学号 | | 年级专业 | | | 任务分工 | | 签名 |
| 1 |  |  |  | |  | | | 负责人 | |  |
| 2 |  |  |  | |  | | |  | |  |
| 3 |  |  |  | |  | | |  | |  |
| 4 |  |  |  | |  | | |  | |  |
| 5 |  |  |  | |  | | |  | |  |
| 指导教师 | | 姓名 | 性别 | 职称 | | Email | | | | 签名 | |
|  |  |  | |  | | | |  | |
| 案例摘要（限300字以内） | |  | | | | | | | | | |
| 院系报名  推荐意见 | | 单位盖章：（公章）  2025年 月 日 | | | | | | | | | |

**填写说明：**1.案例编号由组委会统一填写； 2.联系人为项目负责人，负责比赛期间与学校或组织单位的沟通；3.每个案例作品参赛者不超过5人，指导教师不超过1人，所有参赛队员和指导老师均须本人签名确认（可电子签名，如相关成果出现知识产权等法律责任由参赛团队和指导教师共同承担）；4.单位意见栏盖章处需加盖项目负责人所在高校院系公章；5.本表务必打印在一张 A4 纸上，否则视为形式审查不合格。

形状

AI 生成的内容可能不正确。附件5：

2025年首届“智安杯”大学生国家安全案例大赛

案例编写格式要求

**一、文字、标点符号和数字**

一般用中文书写，除特殊需要外，不得使用已废除的繁体字、异体字等不规范汉字。

文字、标点符号和数字的使用应严格执行《中华人民共和国国家通用语言文字法》和国家语言文字工作委员会制定的有关规定。

**二、中英文摘要**

摘要的字数限300字。居中打印“摘要”二字（小三号黑体），摘要内容（小四号宋体，1.5倍行间距），每段开头空二格。摘要内容后空一行后顶格编排“关键词：”三字（小四号黑体），其后为关键词（小四号宋体）。每篇案例应选取3-5个关键词，每一关键词之间用分号分开，最后一个关键词后不加标点。

英文摘要应与中文摘要内容相对应, 居中编排“Abstract”,（小三号Times New Roman字体，加黑）。摘要内容每段开头留四个字符空格，用小四号Times New Roman字体，1.5倍行间距。摘要内容后空一行顶格编排“Keywords：”（小四号Times New Roman字体，加黑），每个关键词之间用逗号分开，各英文关键词的第一个字母应大写。

**三、目录**

“目录”二字使用小三号黑体字，目录内容使用小四号宋体字，字间距为标准，行间距为1.5倍行间距。

目录中章、节的编号和绪论、附录等均顶格编排。章、节的标题及附录等的标题与前面的内容之间空一个字的间隙。章、节等与页码之间用“…………”连接，页码不用括号。具体格式见下表：

|  |  |
| --- | --- |
| **示 例** | **字体及排版要求** |
| 目 录 | 小三号黑体字，二字间空两格，居中排，下空一行 |
| 摘要..........................................I | 论文前置部分，罗马数字单独编连续码（封面除外），小四号宋体字，左侧0缩进，页码右对齐 |
| Abstract.....................................II |
| 绪论..........................................1 | 论文正文部分，阿拉伯数字连续码编排，小四号宋体字，左侧0缩进，页码右对齐 |
| 第一章 XXXXXX................................5 | 一级章标题目录，小3号黑体字，左侧0缩进，页码右对齐 |
| 第一节 XXXXXX..............................5 | 二级节标题目录，4号宋体字加黑，左侧缩进一个字符位置，页码右对齐 |
| 一、XXXXXXXXXXXX..........................6 | 三级标题目录，小4号宋体字，左侧缩进两个字符位置，页码右对齐 |
| …… …… |  |
| 结语.........................................43 | 小四号宋体字，左侧0缩进，页码右对齐 |
| 参考文献.....................................45 |
| 附录.........................................47 |

**四、案例页码编排**

案例的页码，前置部分用罗马数字单独编连续码（封面和题名页除外），正文和后置部分用阿拉伯数字编连续码，封底不要页码。每一章的首页都要另起一页，页码居中。

**五、字体及字号**

除特殊要求外，一级标题（即章标题）一律采用小3号黑体字，二级标题（即节标题）采用4号宋体字加黑，三级标题（即小节标题）采用小4号宋体字，四级标题采用小4号宋体字。字体一律采用小4号宋体字，1.5倍行间距。章的标题占2行，正文另起行，空2个字起排。

**六、正文章节标题序号**

章节的序号按层次划分，层次的划分应科学合理，清晰分明。相同级别层次划分使用的序列号要采用同一系列的序号或字符。

**七、图、表、公式等**

案例中的图、表、公式等，均按论文章节的划分，用阿拉伯数字依序连续编号，章节号和序列号之间用“.”隔开。

图的位置应该在相关文字说明之后，随文排。图号和图题排于图的下方，以图所占位置为限，居中排列。图号和图题之间空一个汉字的位置。

表的位置依次放置在相关文字说明之后,随文排。表号和表题排于表的上方，以表格所占位置为限居中排。表号和表题之间空一个汉字的位置。如表格太大需转页时，需在续表左上方与表格左边线对齐位置注明“续表”，表头也应重复排出。

图题和表题均采用五号黑体字，表格内容为五号宋体字。

公式应另起一行居中排，较长的公式尽可能在等号处回行，或者在“+”“－”等符号处回行。公式中分数线的横线，长短要分清，主要的横线应与等号取平。

公式的编号右端对齐，公式与编号之间用“…………”连接。

**八、名词和术语的使用**

案例中所使用的名词和术语，应采用国家标准或部颁标准中规定的名词或术语。标准中未列出的术语应采用行业通用术语或名称。在整篇论文中，名词和术语必须统一。对于特殊名词或术语应在适当位置加以说明或注解。

采用英语缩写词时，除本行业广泛应用的通用缩写词外，文中第一次出现的缩写词应该用括号注明英文原词。

**九、量和单位及符号**

量和单位要采用国际标准符号和单位。由作者本人拟定的符号、制图规范等均应在第一次出现时加以说明。

**十、参考文献**

参考文献的要件顺序与注释相同。按时间顺序排列，古籍也可按经史子集四部分类排列；同一作者的不同著作按出版时间先后顺序排列，其著作一律排在论文前。

不同资料类别分别排序，按中文专（编、译）著、论文、报刊文章；外文专（编、译）著、论文、报刊文章；互联网资料；其他参考资料等顺序分类，用阿拉伯数字编排。

参考文献应另起一页，“参考文献”四字采用小三号黑体字，居中。空一行左起按顺序依次列出参考文献，将序号置于方括号内，用小四号宋体字。

附件6：

2025年首届“智安杯”大学生国家安全案例大赛

参赛团队知识产权原创性和法律责任声明

本参赛团队郑重声明：本团队在2025年首届“智安杯”大学生国家安全案例大赛所提交的案例作品：\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_，是团队同学在指导老师的指导下，

1. 独立进行研究工作所取得的真实成果，从创意到实现均为原创，使用现有人工智能工具进行内容生成或辅助创作，已在案例说明中明确注明涉及使用内容和比例。

2. 除案例报告中已经标注引用或使用的内容外，本团队参赛作品不包含任何其他个人或集体已经发表或撰写过的研究成果。对本作品的研究做出贡献的个人和集体，均已在报告中以明确方式标明。

3. 本团队及作品严格遵守案例大赛组委会的参赛各项规定，并且无侵害他人合法权益行为和违反相关法律法规行为。若因本次参赛作品涉及人工智能工具辅助内容而引发任何知识产权纠纷或法律责任，本团队愿意承担全部责任。

4. 本团队同意由大赛组委会和本团队共同拥有完整、合法的知识产权及其他相关权益，双方均可将案例用于科学研究和教学培养工作。

5.本团队严格遵守比赛规则，提交参赛案例不涉及国家秘密和工作秘密，如有违反一经发现立即取消参赛资格，涉及违法行为将由相关国家机关依法处理。

6. 本声明的法律责任由本参赛团队和指导教师承担。

案例作品参赛团队全体成员（签名）：

案例作品参赛团队指导教师（签名）：

年 月 日