# 课程思政案例集

**本课程思政案例集，将以各个融合点为索引组织各个案例。每个融合点将可以由多个案例来支撑。**

## 融合点1. 新型网络安全观

1.1 没有网络安全就没有国家安全。党的十八以来，习近平总书记高度重视网络安全和信息化工作，先后就网络安全和信息化工作发表了一系列重要讲话，提出了一系列治网新理念新思想新论断，形成了一系列网络空间治理的新思路新战略新要求，构成了习近平网络强国战略思想。在网络安全方面，习近平站在党和国家事业发展全局的高度，深刻分析了新形势下网络安全呈现的新特点、新趋势，提出了新的网络安全观。他将网络安全上升为国家战略，使其成为总体国家安全观的重要组成部分；将网络安全和信息化工作视为一个统一体，形成了一体两翼、驱动双轮的网络安全观；针对网络安全新形势、新特点，提出了整体、动态、开放、相对、共同的辩证网络安全观；针对全球互联网领域发展不平衡、规则不健全、秩序不合理等问题，提出了在相互尊重、相互信任基础上合作共赢的网络安全观；将以人民为中心的发展思想贯穿到网络安全领域，形成了“网络安全为人民，网络安全靠人民”的以人为本的网络安全观。

认真学习习近平总书记的新型网络安全观，对于维护国家网络安全，增强人民群众网络安全意识、推进网络强国建设具有重要意义。

<http://politics.people.com.cn/n1/2016/0420/c1001-28291543.html>

## 融合点2. 我国目前网络安全形势非常严峻。这一融合点旨在展示我们目前网络安全形势的方方面面，培养学生的家国情怀，鼓励广大青年学子努力学习技术，自觉维护国家网络安全利益与发展环境。

2.1国家互联网应急中心

国家互联网应急中心（CNCERT）：是中国的国家级互联网应急响应机构，负责协调处理互联网安全事件和应急漏洞，发布网络安全预警通报等工作。

实时动态更新数据 <https://www.cert.org.cn/>

近年来，中国的互联网安全形势呈现出以下几个趋势：

1.网络攻击事件频发：中国的互联网用户数量庞大，网络攻击事件屡屡发生，其中包括网络诈骗、网络钓鱼、恶意软件攻击等。

2.网络安全法规的不断完善：中国政府加强了对互联网安全的监管力度，发布了一系列相关法规和政策，包括《网络安全法》、《个人信息保护法》等。

3.网络安全技术的不断提升：中国的互联网企业和科研机构在网络安全技术方面投入不断增加，如人工智能、区块链等技术的应用，有助于提升网络安全防御能力。

4.网络安全意识的普及：中国政府和企业加强了网络安全宣传和教育，提高了人们的网络安全意识和防范能力。

2.2 我国是电信网络诈骗高发的国家

2022年上半年全国法院一审审结电信网络诈骗犯罪1.1万件

<https://www.bilibili.com/video/BV18d4y1X76R?spm_id_from=444.41.list.card_archive.click&vd_source=bb7d6a0a0a0e0e457b4b1dab9bd2b753>

2.3 西工大被攻击

西工大被NSA攻击

<https://mp.weixin.qq.com/s/LdcUVAHTDhHr3xAczhxsrA>

2.4 超级木马出现 专门攻击支付宝 2015年11月24日

<https://tv.cctv.com/2015/11/24/VIDE1448329323299592.shtml>

2.5 勒索病毒肆虐，我国广大网民损失巨大。

从2017年5月12日WannaCry蠕虫（“勒索病毒”）通过MS17-010漏洞在全球爆发，到2018年8月28日某酒店企业的数亿条用户入住信息在网上被公开售卖，以及2019年接连发生的他人高考志愿被恶意填报篡改的事件，让学生感受到“网络安全”竟然离我们这么近！

“人类社会已经进入信息时代，从日常生活到国家治理，信息与信息技术已经成为不可或缺的基础设施和重要资源。”周世杰指出，“社会发展对信息的依赖性越高，意味着网络安全的地位越重要。守护好网络安全，就是直接或间接地为国家社会做重要贡献！”

## **融合点3. 不断发展和完善我国网络安全法律法规体系，是建设网络强国的重要保证。近年来我国陆续出台了许多网络安全相关的法律法规。作为一名网络安全专业的学生，需要做到知法懂法。以实际行动遵守和执行国家《网络安全法》律法规。**

3.1 《网络安全法》的出台

3.2 个人数据保护法的出台

3.3 数据安全法的出台。

3.4 网络安全法修订

<https://new.qq.com/rain/a/20220920A01DKH00>

**融合点4. 漏洞是重要的战略资源。尤其在国际竞争日趋激烈的今天，如果安全人员发现了0day漏洞，需要首先上报国家互联网漏洞管理机构。**

**4.1 中国政府官方支持的两大漏洞库**

CNNVD：CNNVD是“中国国家信息安全漏洞共享平台”的缩写，由中国国家互联网应急中心（CNCERT）负责管理，也是中国政府官方的漏洞公告平台之一。CNNVD负责收集、整理和发布国内外的漏洞信息，并向相关厂商和用户提供漏洞修复建议和技术支持。CNNVD也负责协调处理各类漏洞事件，保障国家信息安全。

CNVD：CNVD是“中国国家信息安全漏洞库”的缩写。是中国政府官方的漏洞公告平台之一。CNVD负责收集、整理和发布国内外的漏洞信息，并向相关厂商和用户提供漏洞修复建议和技术支持。CNVD也负责协调处理各类漏洞事件，保障国家信息安全。

4.2 阿里云log4j漏洞未上报被处罚

2021年12月之后,Log4j漏洞曝光,存在大量互联网企业用户受到影响。阿里云作为云服务提供商,也存在该漏洞。但是阿里云没有及时向国家网信办等部门报告。2022年1月中,阿里云内部有员工向国家网信办实名举报此事。2022年1月底,国家网信办约谈阿里云高级副总裁,对阿里云未及时上报Log4j漏洞问题进行询问。2022年2月15日,国家网信办对阿里云作出行政处罚,决定给予警告并罚款50万元人民币。2月18日,阿里云公开回应并接受处罚。



<https://www.thepaper.cn/newsDetail_forward_15974734>

**融合点5：辩证法**

**从矛盾辩证的角度思考问题，反映了事物运动发展的一般规律，体现了事物本身的特性。网络安全攻防部分的学习，鼓励学生在学习攻防技术的同时，积极思考和反思攻防双方的博弈的本质是什么，一项技术是不是真正足够安全，是否可能存在漏洞和隐患，是否可能被滥用等等。引导学生具有批判性思维和辩证思考能力，不断探索和发现问题的本质和深层次原因。**

5.1 人工智能模型中对抗性样本的问题以及安全人工智能模型的问题

**融合点6：自我认同感与职业素养**

**6.1 耐心和细心**

**网络安全工作需要进行大量细致、耗时的代码审计、系统监测等工作。在一些网络安全相关工作，如代码审计、日志分析、漏洞修补、监控预警、数字取证**

**进行网络犯罪调查时,需要细致提取和分析数码证据,这需要极强的专注力。**

**6.2 良好的团队合作意识**

**安全防护需要各专业角色的通力合作。**

腾讯安全响应中心发现Linux系统新漏洞,与开源社区安全研究人员紧密合作,迅速修复漏洞。https://s.tencent.com/research/report/1179.html

**融合点7：科学精神与家国情怀**

7.1 王小云院士的事迹

7.2 艾伦图灵发明密码机，破解德国纳粹密码的事迹

融合点8：中国式现代化的道路自信