研究生课程思政案例

案例二、网络武器攻击实体：震网病毒

研究生课程：计算机网络与信息安全

讲授章节：计算机病毒

切入点：讲授网计算机病毒，自然会介绍危害网络安全的各类病毒，从而引出“震网病毒”案例。“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”在2018年4月20日召开的全国网络安全和信息化工作会议上，习近平总书记着重强调树立网络安全意识，就做好国家网络安全工作提出明确要求，为筑牢国家网络安全屏障、推进网络强国建设提供了根本遵循。

讲授目的及效果：通过讲述震网病毒案例，引导学生树立网络安全意识，引导学生理解“网络安全和信息化是一体之两翼、驱动之双轮”。在我国信息化的建设过程的同时，要树立网络安全意识，确保我国信息实体的安全有效运行。

震网病毒于2010年6月首次被发现，2012年6月1号纽约时报正式公布。有证据表明，该病毒是由美国和以色列联合开发的，用以定向攻击真实世界中基础（能源）设施的“蠕虫”病毒。只要电脑操作员将被病毒感染的U盘插入USB接口，这种病毒就会在神不知鬼不觉的情况下(不会有任何其他操作要求或者提示出现)取得工业用电脑系统的控制权。该病毒已经针对伊朗核设施进行了网络攻击，取得部分工业用电脑系统的控制权，并影响了其能源系统中工业电脑的正常使用。伊朗政府发布公告确认该

国的布什尔核电站遭到了 Stuxnet 蠕虫的攻击，导致了伊朗方面核计划的推迟。

2010 年 9 月，瑞星公司监测到这个席卷全球工业界的病毒已经入侵中国。瑞星反病毒专家警告说，我国许多大型重要企业在安全制度上存在缺失，可能促进 Stuxnet 病毒在企业中的大规模传播。

由此可见，网络病毒及网络蠕虫，不但可以干扰信息数据，而且可以对实体设备进行破坏。各位同学以后会工作在信息化相关的各个岗位，一定要树立安全意识，注意进行病毒防护。信息化建设和网络安全是密不可分的，必须树立网络安全意识，遵守相关制度， 才能确保信息实体的有效运行。