REPORTING

2023 WORK SUMMARY

网络信息安全与公共安全的协同防范

目录

CATALOGUE

PART 01

引言

背景与意义

背景

随着信息技术的快速发展，网络信息安全问题日益突出，对国家安全、社会稳定和公民个人权益产生重大影响。

意义

研究网络信息安全与公共安全的协同防范，有助于提高国家安全防护能力，维护社会稳定，保障公民合法权益。

研究现状与问题

研究现状

目前，国内外学者在网络安全领域取得了一定的研究成果，但针对网络信息安全与公共安全协同防范的研究尚不够深入。

问题

如何实现网络信息安全与公共安全的协同防范，提高防范效果，是当前亟待解决的问题。同时，需要解决不同部门之间的信息共享与协同作战问题，提高应急响应速度。

PART 02

网络信息安全概述

网络信息安全的定义与特点

定义

网络信息安全是指在网络环境中，通过采取一系列技术和管理措施，保障数据、系统和应用的安全性、完整性、可用性，防止未经授权的访问、使用、泄露、破坏、修改等行为。

特点

网络信息安全具有保密性、完整性、可用性、可控性和不可否认性的特点。

网络信息安全的主要威胁

黑客攻击

黑客利用漏洞、病毒、恶意软件等手段攻击网络系统，窃取、篡改或删除敏感信息，破坏网络正常运行。

内部威胁

内部人员滥用权限、非法访问敏感数据、恶意破坏系统等行为，可能导致数据泄露、系统瘫痪等严重后果。

社交工程攻击

攻击者通过伪装成可信的人或机构，利用人们的心理和行为弱点，获取敏感信息或诱导其执行恶意操作。

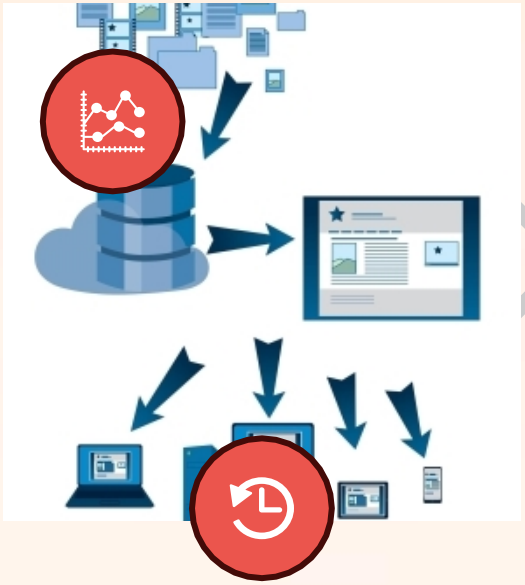
基础设施安全威胁

网络基础设施如路由器、交换机、服务器等可能遭受物理或逻辑攻击，导致网络服务中断或数据泄露。

网络信息安全的关键技术

加密技术

通过加密算法将敏感信息转换为不可读的密文，确保数据传输和存储的安全性。



安全审计技术

对网络系统进行安全审计，发现潜在的安全隐患和漏洞，及时采取措施进行防范和修复。

防火墙技术

通过设置访问控制策略，阻止未经授权的访问和恶意流量进入网络。

入侵检测与防御技术

实时监测网络流量和系统行为，发现异常行为和攻击行为，及时报警并采取相应的防御措施。

PART 03

公共安全概述

公共安全的定义与特点

01

公共安全是指公众所面临的危险和威胁，包括自然灾害、事故灾难、社会安全事件等。

02

公共安全具有突发性、不可预测性和紧迫性的特点，需要政府和社会各界采取及时有效的应对措施。

公共安全的主要威胁

自然灾害

如地震、洪水、台风等，具有不可抗力和难以预测的特点，对公众生命财产安全构成严重威胁。

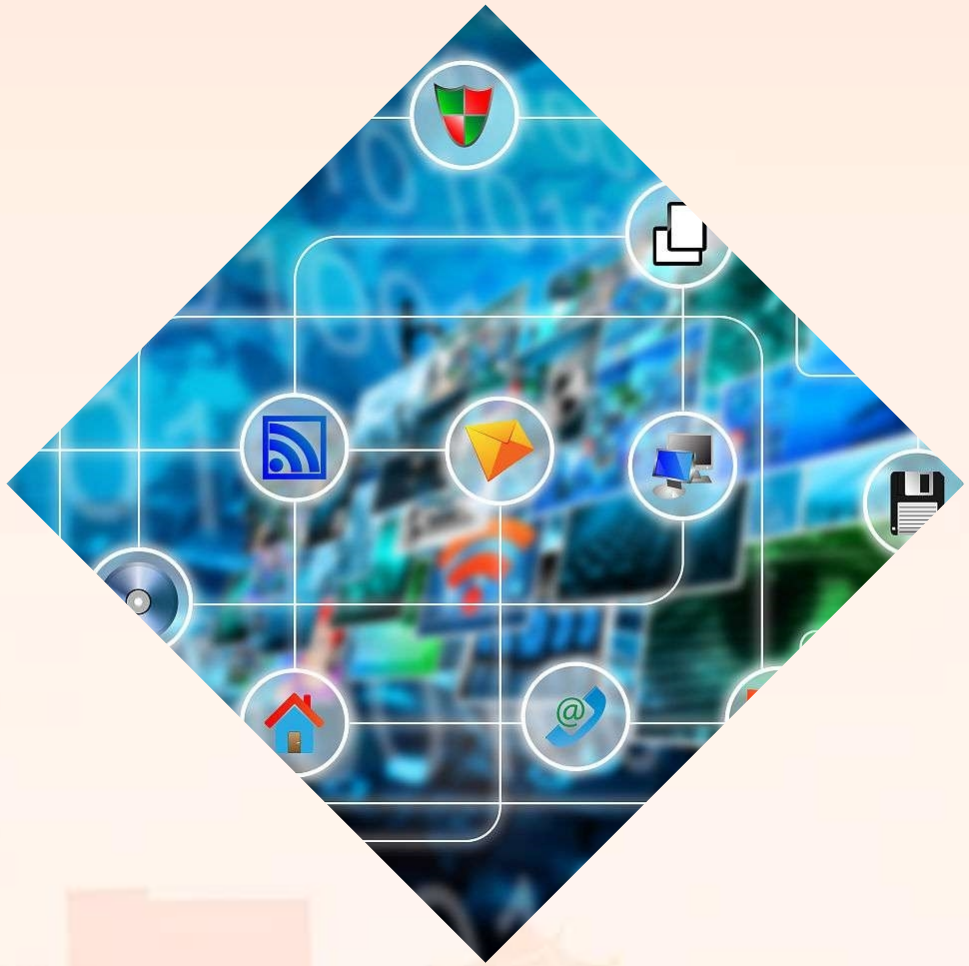
社会安全事件

如恐怖袭击、群体性事件等，具有政治、宗教或民族背景，对国家安全和社会稳定造成影响。

事故灾难

包括火灾、交通事故、建筑坍塌等，往往由于人为因素或设施设备故障导致，对公众安全造成直接危害。

公共安全的关键技术



预警监测技术

通过物联网、大数据等技术手段，实现对各类公共安全事件的实时监测和预警，提高应对效率。

应急救援技术

包括紧急救援装备、通讯设备、医疗救治等技术手段，提高应急救援能力，降低人员伤亡和财产损失。

公共安全信息管理技术

通过信息化手段，实现公共安全信息的收集、整理、分析和发布，提高信息共享和协同应对能力。