**第一次课 学科定义和课程概述**

网络攻击趋势变化

为什么要进行态势感知

网络安全态势感知的问题与挑战

**第二次课 态势感知概念和内涵**

态势感知与网络安全态势感知的定义

网络安全态势感知定义、目的、与实体区别、研究目标

网络安全态势感知主要技术研究方向

网络安全态势感知相关标准、实践演进

模型：JDL、OODA、Endsley、Tim\_Bass

性能和有效度量

**第三次课 态势感知技术代系**

网络安全态势感知挑战

网络安全态势感知三代对比

一二三代系统

**第四次课 态势感知技术体系**

网络通信的三个层次：承载层、应用层、行为层

态势感知三个阶段：信息提取、识别、评估和预测

态势理解、预测的方法

正向计算和逆向解析

深度包检测、实际应用

网络安全态势感知现有系统

**第五次课 态势要素获取技术**

攻击方、防御方、攻防环境态势要素

态势要素获取方法

态势要素获取关键技术

态势要素表示方法

态势要素典型系统和框架

**第六次课 语义与本体表示技术**

语义网络概念与内涵、RDF

本体概念与内涵

语义网与本体的应用

**第七次课 态势要素分类方法**

分类的作用和意义

分类标准规范

结构性、对象性、类型性分类方法

**第八次课 新兴领域网络安全态势技术**

面向新兴领域的态势感知

利用新兴技术的态势感知

新兴领域案例、未来挑战

**第八次课 深度包分析技术**

深度包检测概念与内涵

关键技术

系统与工具、爱因斯坦计划

DPI面临的挑战

**第九次课 数据质量评价方法**

数据质量评价的概念和内涵、面临的问题、好处

面向数据的评价模型

面向过程的评价模型

数据质量评价案例

**第十次课 网络安全态势评估技术**

态势评估概述、典型的态势评估技术

面向攻击的态势评估方法

面向防守的态势评估技术

态势评估实例、未来挑战

**第十一次课 传统态势识别技术**

入侵检测、入侵防御系统

安全信息和事件管理SIEM

安全管理中心SOC

相关系统和工具

**第十一次课 态势要素融合和归一化技术**

意义

主要技术、数据层、特征层、决策层

未来挑战

**第十二次课 攻击威胁识别分析技术**

定义

特征已知的攻击威胁识别

特征未知的攻击威胁识别、技术分类

态势感知系统实例、启明星辰

机器学习在安全方面的应用

**第十三次课 安全态势可视化**

定义、研究现状

可视化分析流程分类

可视化开发工具

可视化分析在网络安全态势中的作用

应用实例

**第十四次课 威胁情报**

意义、kill chain

威胁情报概念、类别

关键技术方向、感知采集、分析处理、共享与应用

代表性系统

应用场景

**第十六次课 面向态势感知的知识图谱**

为什么需要知识图谱

知识图谱技术概述

网络安全态势感知本体模型

知识图谱的应用

总结与未来方向

**第十七次课 评估和预测方法**

态势评估和预测的方法

态势评估、数学模型、层次分析法、贝叶斯方法、DS方法

态势预测、时间序列预测、马尔科夫、ARIMA、机器学习预测

态势预测典型方法比较

**第十八次课 国家级态势感知实践**

美国发展态势感知目的和现状

藏宝图计划

X计划

爱因斯坦计划