

## 第15讲

# 第15讲：未来展望与伦理思考

牛温佳 教授

北京交通大学·网络空间安全学院

# 本讲内容

---

1

15.1 技术发展趋势

---

2

15.2 融合趋势：量子+类脑+自动驾驶

---

3

15.3 伦理与社会思考

---

4

15.4 我们必须回答的问题

---

5

思考题与小结

## 🎯 学习目标

了解量子类脑计算与智能汽车安全的发展趋势

思考AI技术发展带来的伦理和社会问题

培养对技术发展的批判性思维和社会责任意识

# 15.1 技术发展趋势

Section 15.1 技术发展趋势

---

# 15.1 技术发展趋势

## 15.1.1 量子计算的下一个十年

**短期 (1-5年)**：NISQ设备持续改进，量子比特数量达到数千，错误率进一步降低；量子-经典混合计算成为主流范式；在特定优化问题上展示实用价值。

**中期 (5-10年)**：容错量子计算初步实现；量子纠错技术取得突破；量子计算机开始在药物研发、材料科学等领域产生实际影响。

**长期 (10年以上)**：大规模通用量子计算机有望实现；量子机器学习算法在AI领域产生深远影响。

## 15.1.2 类脑计算的产业化路径

- **当前阶段**：类脑芯片从实验室走向工业场景的渗透期

## 15.1 技术发展趋势（续）

- **近期**：在特定垂直领域（自动驾驶、医疗、IoT）率先落地
- **中期**：类脑-传统混合架构成为边缘计算的标配
- **长期**：神经形态计算与量子计算的异构融合

### 15.1.3 自动驾驶安全的演进

- **当前**：对抗攻击的学术研究与实践探索并行

## 15.1 技术发展趋势（续）

- **近期**：多传感器融合成为安全标配，对抗防御机制逐步成熟
- **中期**：AI安全评测标准建立，安全认证体系完善
- **长期**：实现从防御到免疫的范式转变

## 15.2 融合趋势：量子+类脑+自动驾驶

Section 15.2 融合趋势：量子+类脑+自动驾驶

---

## 15.2 融合趋势：量子+类脑+自动驾驶

### 15.2.1 三层融合架构

未来的智能汽车安全系统可能采用以下三层融合架构：

- **感知层**：类脑芯片驱动的低功耗实时感知，脉冲神经网络处理传感器数据
- **决策层**：量子增强的路径规划和决策优化
- **安全层**：量子-脉冲混合网络提供对抗防御

### 15.2.2 关键挑战

## 15.2 融合趋势：量子+类脑+自动驾驶（续）

1. **硬件融合**：如何在单一平台上集成量子、类脑和传统计算？
2. **算法协同**：如何让三种不同范式的算法高效协同工作？
3. **工程落地**：如何在满足车规级要求的前提下实现量产？

# 15.3 伦理与社会思考

Section 15.3 伦理与社会思考

---

## 15.3 伦理与社会思考

### 15.3.1 自动驾驶的伦理困境

**著名的"电车难题"在自动驾驶中的体现：**当碰撞不可避免时，自动驾驶系统应该如何选择？是保护乘客还是保护行人？是撞向一个人还是撞向一群人？

这类问题没有绝对正确的答案，不同文化背景和社会价值观可能有不同的选择。关键是要让公众参与讨论，形成社会共识，并通过法规和政策来规范。

### 15.3.2 AI安全研究的双刃剑

对抗攻击的研究具有两面性：

- **防御角度：**通过研究攻击方法，更好地理解模型的脆弱性，设计更鲁棒的防御

## 15.3 伦理与社会思考 (续)

- **风险角度**: 攻击方法的研究成果也可能被恶意利用

如何在开放研究与风险控制之间找到平衡, 是学术界和产业界共同面临的挑战。

### 15.3.3 技术公平与社会责任

- **技术鸿沟**: 高端智能汽车的安全技术是否会加剧数字鸿沟?

- **数据隐私**: 自动驾驶车辆收集的大量数据如何保护隐私?

## 15.3 伦理与社会思考 (续)

- **责任归属**: 自动驾驶事故的责任在车主、制造商还是算法开发者?

# 15.4 我们必须回答的问题

Section 15.4 我们必须回答的问题

---

## 15.4 我们必须回答的问题

1. **安全性**: 我们如何确保AI系统的安全性不落后于其智能化程度?
2. **可控性**: 人类如何保持对越来越智能的系统的有效控制?
3. **包容性**: 如何让安全技术惠及更多人, 而不是少数人?
4. **可持续性**: 技术发展如何与环境保护和可持续发展目标协调?

## 延伸阅读

---

- 📖 《人工智能安全》（方滨兴 著）
- 📖 IEEE Ethically Aligned Design guidelines
- 📖 世界各国自动驾驶法规与政策

1. 你认为自动驾驶汽车面临紧急情况时，应该优先保护谁？为什么？
2. 对抗攻击的研究应该公开还是保密？公开的好处和风险是什么？
3. 当你乘坐L4级自动驾驶汽车时，你对安全性有什么期待？你会完全信任AI吗？

## 本讲小结

---

- ✓ 15.1 技术发展趋势
- ✓ 15.2 融合趋势：量子+类脑+自动驾驶
- ✓ 15.3 伦理与社会思考
- ✓ 15.4 我们必须回答的问题
- ✓ 思考与讨论

# 感谢聆听

第15讲·未来展望与伦理思考