一、人工智能应用基础

1、知识是人类智能的基础，人类在从事阶级斗争、生产斗争和科学试验等社会实践活动中，其智能活动过程主要是一个获取知识并运用知识的过程。

2、人工智能是一门研究用计算机来模仿和执行人脑的某些智力功能的交叉学科，所以人工智能问题的求解也是以知识为基础的。

3、如何从现实世界中获取知识、如何将已获得的知识以计算机内部代码的形式加以合理的表示以便于存储，以及如何运用这些知识进行推理以解决实际的问题，即知识的获取、知识的表示和运用知识进行推理是人工智能学科要研究的3个主要问题。

4、在人们的日常生活及社会活动中，“知识”是常用的一个术语。例如，人们常说“我们要掌握现代科学知识”，“掌握的知识越多，你的机会就越多”等。人们所涉及的知识也是十分广泛的，例如，有的知识是多数人所熟悉的普通知识，而有的知识只是有关专家才掌握的专门领域知识。那么，到底什么是知识？知识有哪些特性？它与通常所说的信息有什么区别和联系？

5、现实世界中每时每刻都产生着大量的信息，但信息是需要用一定的形式表示出来才能被记载和传递的。尤其是使用计算机来进行信息的存储及处理时，更需要用一组符号及其组合进行表示。像这样用一组符号及其组合表示的信息称为数据。

6、数据与信息是两个密切相关的概念。数据是记录信息的符号，是信息的载体和表示。信息是对数据的解释，是数据在特定场合下的具体含义。只有把两者密切地结合起来，才能实现对现实世界中某一具体事物的描述。

7、另外，数据和信息又是两个不同的概念，相同的数据在不同的环境下表示不同的含义，蕴涵不同的信息。比如，“100”是一个数据，它可能表示“100元钱”，也可表示“100个人”，若对于学生的考试成绩来说，可能表示“100分”。同样，相同的信息也可以用不同的数据表示出来。比如，地下工作者为了传达情报信息，可以用一首诗词的每一句的第一个字组成一句话，或诗的斜对角线上的字组成的一句话来传达信息，也可能会用一个代码或数字来表示同一信息。

8、正如上述，现实生活中，信息是要以数据的形式来表达和传递的，数据中蕴涵着信息，然而，并不是所有的数据中都蕴涵着信息，而是只有那些有格式的数据才有意义。对数据中的信息的理解也是主观的、因人而异的，是以增加知识为目的的。

9、对于人工智能，很多人并不了解，我也如此。关于这个问题，我与我的朋友人工智能工程师张

二、人工智能的最大技术工具集

1、它是计算网络工具包(ComputationalNetworkToolkit)的缩写，CNTK是一个微软的开源人工智能工具。不论是在单个CPU、单个GPU、多个GPU或是拥有多个GPU的多台机器上它都有优异的表现。

2、微软主要用它做语音识别的研究，但是它在机器翻译、图像识别、图像字幕、文本处理、语言理解和语言建模方面都有着良好的应用。

三、人工智能的安全评估和测评包括

1、人工智能数据安全风险评估平台包括风险评估、数据集管理、知识库管理、威胁情报等功能，用于对特定人工智能应用场景中的数据安全风险进行总体评估和评级，以及数据集管理和知识库建设。

2、该平台设定了安全基线，开发用于敏感数据探测、数据质量检测、数据差异检测、漏洞检测以及脆弱性检测的工具。基于检测工具汇集的数据实现数据安全风险信息实时收集、自动推送、智能分析、量化评估与诊断分级。针对人工智能应用场景中的数据安全实现多层级、多维度风险评估，为企业对人工智能系统开展自评以及第三方测评机构针对人工智能项目开展风险评估和产品认证提供技术、工具和平台。

四、为何说人工智能将改变战争形态

1、据报道，近年来，随着科学技术的发展，无人作战系统已开始应用实战。美国国家科学委员会曾预言：“21世纪的核心武器是无人作战系统”，目前这一预言正逐渐成为现实。

2、随着AI技术的突破性发展，这项技术已开始广泛应用可各武器平台。如美俄等军事发达国家凭借其先进技术，早就开始计算机及智能技术应用于军用无人机、军用机器人、无人战车、无人作战潜艇等多种作战武器平台。从而使无人作战系统的智能化程度不断提高，并在实战中获得显著效果。

3、评论称在2015年底，俄罗斯在支援叙利亚政府军强攻伊斯兰极端势力据点的战斗中，首次以战斗机器人为主进行攻坚作战，战斗持续了20分钟，一边倒的精准打击令极端势力武装分子毫无还手之力，约70名武装分子被击毙，而参战的叙利亚政

府军只有4人受伤。这次战斗充分显示了战斗机器人的巨大优势。对此，俄罗斯媒体宣称，这是世界上第一场以机器人为主的攻坚战。

4、专家则表示2016年AlphaGo人机大战的胜利，标志着人工智能有了质的飞跃，也使人们由此联想到AI与未来战争。如果将AI成果应用到无人作战系统，必将对未来战争形态及作战规则产生颠覆性影响。

五、人工智能应用不当会产生哪些风险

所谓的“数据投毒”指人工智能训练数据污染导致人工智能决策错误。通过在训练数据里加入伪装数据、恶意样本等，破坏数据的完整性，进而导致训练的算法模型决策出现偏差。

一方面逆向攻击可导致算法模型内部的数据泄露;

另一方面，人工智能技术可加强数据挖掘分析能力，加大隐私泄露风险。比如各类智能设备（如智能手环、智能音箱）和智能系统（如生物特征识别系统、智能医疗系统），人工智能设备和系统对个人信息采集更加直接与全面。人工智能应用采集的信息包括了人脸、指纹、声纹、虹膜、心跳、基因等，具有很强的个人属性。这些信息具有唯一性和不变性，一旦泄露或者滥用将产生严重后果。

运行阶段的数据异常可导致智能系统运行错误，同时模型窃取攻击可对算法模型的数据进行逆向还原。此外，开源学习框架存在安全风险，也可导致人工智能系统数据泄露。

图像识别、图像欺骗等会导致算法出问题，比如自动驾驶，谷歌也做了一些研究，如果模型文件被黑客控制恶意修改，并且给它学习，会产生完全不一样的结果;

算法设计或实施有误可产生与预期不符甚至伤害性结果;

算法潜藏偏见和歧视，导致决策结果可能存在不公;

算法黑箱导致人工智能决策不可解释，引发监督审查困境;

含有噪声或偏差的训练数据可影响算法模型准确性。

人工智能不可避免的会引入网络连接，网络本身的安全风险也会将AI带入风险的深坑;

人工智能技术本身也能够提升网络攻击的智能化水平，进而进行数据智能窃取;

人工智能可用来自动锁定目标，进行数据勒索攻击。人工智能技术通过对特征库学习自动查找系统漏洞和识别关键目标，提高攻击效率;

人工智能可自动生成大量虚假威胁情报，对分析系统实施攻击。人工智能通过使用机器学习、数据挖掘和自然语言处理等技术处理安全大数据，能自动生产威胁性情报，攻击者也可利用相关技术生成大量错误情报以混淆判断;

人工智能可自动识别图像验证码，窃取系统数据。图像验证码是一种防止机器人账户滥用网站或服务的常用验证措施，但人工智能通过学习可以让这一验证措施失效。

第三方组件问题也会存在问题，包括对文件、网络协议、各种外部输入协议的处理都会出问题。被黑客利用，带来的是灾难性的毁灭。