一、人工智能安全是指什么

1、ETSI发布了有关AI安全的报告。ETSISAI主席AlexLeadbeater在记者采访中指出，该报告描述了基于机器学习的基于AI的系统和解决方案的安全保护问题，以及在AI生命周期的每个阶段与机密性，完整性和可用性相关的挑战。人工智能面临许多挑战，包括偏见，道德规范和在规则内部署的能力，许多应用对于自动化网络的安全性而言已变得至关重要。

2、人工智能（AI）在社会的数字化转型中起着关键作用。很难想象，没有一个在各种商品和服务上都没有人工智能的世界，在工作，金融，医疗保健，安全和农业领域已经发生了许多变化。人工智能对于欧洲的绿色交易和疫情后的经济复苏至关重要。

3、作为一门科学学科，人工智能包括多种方法和技术，例如机器学习，机器推理和机器人技术。因此，涵盖人工智能，机器人技术和相关技术的道德方面的法规是关键目标。

4、欧洲议会也对此发出了声音，欧洲议会已经宣布，在2021年的头几个月中，将以规制的形式对算法进行规范。它成立了一个特别的临时议会委员会（AIDA），以分析AI对欧盟经济的影响。

5、ETSI将人工智能定义为系统处理显式和隐式表示的能力，以及执行由人类执行的被认为是智能的任务的程序。在机器学习和深度学习技术的发展以及数据分析技术的广泛应用的推动下，一系列技术正在继续朝着完全适用性的方向发展。

6、“AI显而易见的一件事是，大多数历史安全模型都不太适合。因此，AI本质上是高度并行，高度分布式的。它既是威胁自身，也威胁其他AI。”Leadbeater说。

7、人工智能可以促进新一代产品和服务的开发，包括在欧洲公司已经占据优势地位的行业中，例如循环经济，农业，医疗保健，时尚和旅游业。实际上，它可以提供更平滑，更优化的销售路径，改善机械维护，提高产量和质量，改善客户服务并节省能源。

8、人工智能已成为社会变革的最强大动力之一：它正在改变经济，影响政治并重塑公民的生活和互动。与人工智能相关的许多具体的道德和法律问题已经出现在各个领域，例如责任，保险，数据保护，安全，合同和犯罪。数据保护在AI与法律之间的关系中起着重要作用，因为许多AI应用程序涉及对个人数据的大量处理，包括基于该数据对人进行针对性和个性化处理。

9、基于人工智能的系统正在以多种形式淡化人类和社会世界：工厂中的工业机器人，家庭和医疗设施中的服务机器人，交通中的自动驾驶汽车和无人飞机，电子商务和金融中的自动电子代理，将军事和智能通信设备集成到每个环境中。

10、当然，并非所有算法都涉及AI，但是每个AI系统（如每个计算机系统）都包含算法，其中一些算法处理直接影响AI功能的任务。尽管AI系统包含许多算法，但也可以将其视为单个复杂算法，将执行其各种功能的算法与通过触发相关的较低级算法来协调系统功能的高级算法结合起来。

11、人工智能，区块链和大数据技术在全球数据处理基础架构中的相互作用可以带来许多好处：改善信息访问；全球知识的产生和传播；节省成本，提高生产率和创造价值；以及新的高薪创意工作。

二、人工智能与信息安全哪个方向好

信息安全好就业。主要学习通信、编码、信息网络与系统、信息与安全保密、信息对抗等基本理论、基本原理和技术，学习在信息、信息过程和信息系统等方面进行信息安全与保密的关键技术的研究方法，典型设备、部件的分析、设计、研究、开发的方法和能力。

三、人工智能与网络安全哪个更有发展前途

1、我建议都学习，因为在编程领域，技多不压身，以后人工智能肯定是发展的必然趋势，但网络安全是根基之本，在过去十年左右的时间里，出现了数百起身份盗用、资金损失和数据泄露案件。自然界中的网络攻击非常普遍，并影响到每个人、企业和政府机构。我们正在走向一个网络犯罪分子可以随时在世界任何地方达到目标的时代，对网络安全的需求从未像现在这样重要。

2、现在典型的网络攻击是攻击者或网络犯罪分子企图以未经授权的方式访问，更改或损坏目标计算机系统或网络的企图，影响了计算机网络和系统，去破坏依赖它们的组织和运营。

3、不过鉴于人工智能未来发展，黑客肯定也会学习人工智能技术去攻击计算机系统，绕过简单防火墙和人为攻防，利用AI进行大规模自动化网络攻击。人工智能也可以比人类更快更好地入侵系统的漏洞。AI可以用来有效地伪装攻击，以至于人们可能永远不会知道他们的网络或设备受到了影响。

4、我觉得有一门可以兼容机器学习和网络安全的技术——网络威胁检测，机器要能够提前检测到网络攻击，以便能够阻止攻击者试图实现的任何目标。机器学习是

人工智能的一部分，在利用信息系统中利用漏洞之前，基于分析数据和识别威胁来检测网络威胁时，这已被证明非常有用。

5、机器学习使计算机能够根据收到的数据使用和调整算法，从中学习，并了解所需的后续改进。在网络安全环境中，这将意味着机器学习使计算机能够预测威胁并观察任何异常情况，并且比任何人都更准确。

6、传统技术过于依赖过去的数据，无法以AI的方式即兴发挥。传统技术无法像AI那样跟上黑客的新机制和伎俩。此外，人们每天必须处理的网络威胁数量对人类来说太多了，最好由人工智能处理，所以能多学习一门技术就多学习，人工智能与网络安全都是未来的科技发展必不可少的方向之一。

四、人工智能用在工作上的应用

1、传统的工业机器人仅是以机器人代替部分繁琐的人工劳动，成为人类体力的延伸，但机器人的智能程度还不够，无法完成一些比较精细的工作。但随着科学技术的发展和工业生产的需要，人们也开始研究如何让机器人去代替部分脑力劳动，使其具有更高的智慧与能力，而AI技术的发展则弥补了这一短板。

2、AI技术的加入，使得工业机器人能以与人类智能相似的方式做出反应，赋予了机器人新的活力，让它不仅能代替人类大部分的体力劳动，也可以在程序设定的基础上代替部分的脑力劳动，提高生产效率，降低工厂生产成本。

3、由于人眼无法看清快速移动的目标，对微小目标分辨能力弱，而且人眼疲劳后漏检率会提高，这些都使得人工检测费时费力。而智能缺陷检测机器人则克服了这些困难，高速工业相机能够在动态检测的情况下极大降低误报率，还可根据产品检测需求调整检测精度，提高检测效率。同时可配合自动化生产线，实现自动检测、自动处理，降低次品率，减少人工成本，使得生产效率显著提升。

4、对于工厂来说，分拣速度慢意味着生产出的产品会在产线上积压，造成生产线流转不顺畅，拉低生产效率。目前人工分拣速度慢，尤其是体积小、颜色形状多的产品更是分拣难度大，很容易造成分拣失误，但如果使用智能分拣机器人则可以大大提高分拣速度。

5、智能分拣机器人可以通过摄像头对分拣物品进行识别，再通过分析得出该物品应放置的区域，最后通过机械臂或产线配合将产品送至相应的位置。该机器人的在线识别速度一般都高于生产速度，分拣失误率低，不易造成产品在产线上积压。

6、传统的产品尺寸检测由于人员使用量具熟练程度的不同，量具使用不熟练或是

人员疲劳会造成检测速度变慢，延缓生产进度，而且人工测量误差较大。但智能尺寸检测机器人可以24小时持续检测，检测速度快，测量误差小。

7、视觉机器人想要成功接收各项指令并完成相应的动作，也像人一样需要大脑的调配。智能装备研发的视觉引导系统就是这样一个“大脑”，它通过自主软件控制系统来下达指令，工业相机进行目标产品信息捕捉，再通过多轴机械臂进行操作，整个过程流畅自然。

8、01管桩自动领域：管桩自动装配机器人

9、该设备用于水泥管桩行业的头尾板自动装配

10、采用视觉获取笼筋墩头的空间角度位置，配合四轴矫正专机完成墩头的自动撑开，最后通过机械臂实现头尾板的装配

11、02检测领域：检测中心检测机器人

12、检测系统由六轴机器人、自动上料装置、自动扫码装置、测径仪、测宽仪、三点测弯机构、拉力机、安全防护系统等组成。

13、机器人系统实现样品检测自动化、无人化、数据自动上传与处理功能，提了检测准确性、真实性，降低人工成本、提高检测效率。