新美国安全中心发布《人工智能与国家安全》报告

郭彦江

7月10日，继美国哈佛大学和国会研究处发布《人工智能和国家安全》报告之后，美国新安全中心（CNAS）智库发布2018年最新版《人工智能与国家安全》报告，报告全文共28页，分析了人工智能在网络安全、信息安全、经济和金融、国家防御、情报、国土安全等方面的应用，研究了人工智能变革对全球安全的不利影响。报告认为人工智能给未来世界发展带来前所未有的机遇，美国应制定国家战略，对人工智能产业发展进行引导，研究如何利用人工智能的优势，同时减轻人工智能带来的不利影响。

一、与国家安全相关的人工智能应用

在美国和其他许多国家，有许多与国家安全相关的人工智能应用的例子。报告研究了人工智能在网络安全、信息安全、经济和金融、国防、情报、国土安全、外交等方面的应用，这些领域并不全面，只是帮助从事国家安全研究的人员去思考人工智能对国家安全的影响。

网络安全

网络安全是人工智能一个突出的潜在应用领域。2016年8月，美国国防预先研究计划局（DARPA）举行第一次网络安全挑战赛，旨在实验性探索无人干预条件下的入侵、补丁、网络防御方面的软件程序。来自卡耐基梅隆大学ForAllSecure初创企业打造的Mayhem“自动攻击系统”在经历95轮的挑战后夺得冠军。美国国防部随后与ForAllSecure公司签署一份为期2年的“Voltron”实施计划，该计划旨在利用尖端人工智能（AI）技术发现美国军方操作系统和定制程序中存在的编码漏洞。2016年10月，美国国家安全局局长迈克尔·罗杰斯在讲话中指出“人工是能是未来网络安全的基础”。

信息安全

人工智能在不断变化的威胁形势中对信息安全产生重大影响，主要表现在人工智能通过信息时代的机器人和相关系统产生广泛影响。人工智能可以加剧或减轻不断变化的信息生态系统中虚假信息的影响。类似于人工智能在网络攻击中的作用，人工智能提供了一种机制，可以对目标用户进行片面的定制传播，或大规模扩大传播的效果和范围。采取的手段主要包括：

1. 开发行为数据。人工智能通过搜集特定行为数据，通过机器学习对数据进行分析，想特定用户推送符合消费者行为的信息。剑桥公司通过对Facebook中用户使用网络的数据进行个性化评估，为用户量身定制收到的信息和内容。

2. 模式识别和预测。当应用于人类行为分析时，人工智能通过模式识别来计算未来事件发生的概率。在社交平台上应用机器学习算法优先考虑用户期望支持的内容，自动生成相应的敏感信息。

3. 放大和议程设置。研究表明，机器人占2016年所有在线流量的50%以上。根据“人为推广的内容可以操纵”原则，人们看到某些内容的次数越多，人们往往认为这些内容很重要。人工智能通过学习和模仿真实的人的言论来影响人们对某些事情的判断。在选举中，政治候选人通过政治机器人，夸大候选人的真实追随者数量，从而引导广大选民的选票。

4. 针对目标情感的自然语言处理。人工智能在自然语言处理方面的进步使得人工智能可以针对不同政治倾向的人提供各自意识形态的信息。同样的，人工智能可以通过收集量化用户反应的方式最大限度影响用户。谷歌公司2016年开始针对不同政治倾向的用户提供相关意识形态的信息。

5. 深度欺骗。人工智能系统可以通过足够的语音训练合成逼真的人声。当前这项技术尚未取得突破，但相关人士推测，这项技术距离真正投入使用只有不到5年的时间。

经济和金融安全

通过分析和学习大量数据，人工智能可以完成以人为中心的反非法融资系统无法实现的任务。AI的异常检测和模式识别功能可以帮助系统从金融机构收集非结构化数据。即使缺乏大规模的模式分析，人工智能也可以改善反非法融资框架，确保持续关注非法融资威胁。人工智能还可以减轻金融机构的压力。银行将不再需要转移注意力来应对不断变化的政府优先事项。AI还可以帮助政府和金融机构解决数据隐私和保护问题。

国防

各军事强国正在研发自主系统和机器人。人工智能和机器学习将使这些系统能够在更广泛的环境中应对更具挑战性的任务。在作战行动中，机器人和自主系统有可能加快战斗速度。

1. 态势感知。小型机器人传感器可用于收集信息，采用人工智能技术的传感器和处理器可帮助作战人员更好地了解该信息。当前美国国防部已经将深度神经网络用于无人机视频输入的图像分类，以帮助作战人员处理收集的大量数据。

2. 电磁频谱的优势。人工智能产品可以通过与另一个人工智能产品进行电磁对抗来进行学习和提高。例如，一个AI系统可以尝试通过一个有复杂的电磁环境进行通信，而另一个系统试图堵塞发送电磁信号。通过这些对抗方法，两个系统都可以学习和改进。DARPA于2014年开始举行频谱挑战赛。DARPA现在正在使用机器学习来辅助完成无线电频谱分配。

3. 诱饵和伪装。人工智能可通过生成对抗性网络来制造与军事相关的伪装和诱饵，小型机器人系统可用作消耗性诱饵。随着军队将更多的AI传感器用于数据分类，针对此类系统的欺骗攻击也将越来越重要。

4. 策略。进化和强化学习方法可用于在模拟环境中生成新策略，从而在其他环境中提供专门的解决方案。

5. 指挥与控制。随着信息数量和处理速度超过作战人员的能力，人工智能对指挥和控制将变得越来越重要。已被授权执行某些操作的自主系统可以在战场边缘以机器速度做出反应，而无需等待人工批准。AI还可以帮助指挥官更快地处理信息，使他们能够更好地理解快速变化的战场空间。通过自动化，指挥官可以更快，更精确地将他们的命令传递给他们的武装力量。

情报

AI在情报收集和分析方面有很多用途。AI工具可以帮助分析智能设备、物联网和人类互联网活动数据之间的联系，标记可疑活动，融合不同的数据元素，映射网络以及预测未来行为。人工智能在情报分析方面也具有巨大的潜在价值。人工智能系统可用于大规模跟踪和分析大量数据（包括开源数据），寻找可疑活动的迹象和警告。通过异常检测可以帮助找到恐怖分子，秘密特工，或潜在的敌人军事活动的迹象和警告。

国土安全

AI还可以用于国土安全和国土安全应用。基于人工智能的数据感知，处理和分析可以更好地为人类决策提供信息。美国国土安全部（DHS）已经开始采用并实施一些人工智能相关技术，包括：

1. 语音识别算法。美国海岸警卫队使用人工智能分析语音，这有助于在法律上解决虚假遇险信号。

2. 用于机器学习的开源数据。与Alphabet公司的Kaggle平台合作开发更好的算法来评估非法和存有危险物品的乘客行李。

3. 理解数据。由DHS和NASA喷气推进实验室开发的AI平台集成了实时数据，为消防员提供了如何最好地发挥团队作用的建议。

AI还广泛适用于各种国土安全功能，如边境安全。与无人机和地面机器人相结合的人工智能系统可通过自动监视和异常检测技术帮助对美国边境进行监测。

外交和人道主义行动

人工智能的进步也可以重塑外交的实践。图像识别和信息分类中的AI技术可以通过监控人员和识别潜在漏洞来提高外交能力。此外，语言处理算法将降低国家之间的语言障碍，允许他们更容易地与外国政府和公众沟通。国际人道主义行动也可以从人工智能技术中获益。人工智能技术可以帮助监督选举，协助维和行动。人工智能还可以通过提高生产力，帮助直接改善欠发达国家的生活质量。

二、人工智能对全球安全的不利影响

除了直接的国家安全影响外，人工智能如何产生与国际安全环境相关的政治和社会变革？鉴于经济和军事力量之间的整体联系，特别是在中长期，理解人工智能创新将如何影响全球经济，信息环境和世界各地的社会至关重要。

经济和未来工作

人工智能将影响劳动力市场的方式有很多预测，而这些预测存在很大程度的不确定性。例如，麦肯锡全球研究所最近的一份报告表明，目前几乎所有行业的工作任务都是自动化的，根据麦肯锡的数据，到2030年全球失业人数中值估计为4亿，最高可达8亿。Forrester研究报告认为，到2027年，将有2470万个就业岗位将被取代。

在人工智能革命开始时，当今尖端公司创造的就业岗位数量已远远小于数十年前尖端公司创造的就业岗位数量。在这种情况下，执行重复身体和认知劳动的工人变得不那么重视。

政治和社会混乱

经济混乱也可能助长社会和政治动荡。维持稳定需要一定程度的政治灵活性。在最坏的情况下，政治冲突可能导致国内动乱，叛乱，内战，民族主义，仇外心理和转向威权主义。

人工智能产生的不稳定性已经成为全球民粹主义民族主义运动兴起的潜在推动力。

信息环境

随着计算机越来越能够针对特定用户定位信息，放大消息，过滤信息，甚至生成虚假的音频，图像和视频，AI将继续改变信息环境。这种转变会带来深远的影响。人工智能技术可能会削弱（如果不是结束）记录证据作为证据的能力。

政治权力

人工智能可能影响民主进程和集权政权的力量，同时也影响全球公共舆论。通过应用人工智能技术实现的高度细化的选民分析可以通过选举过程影响民主规范。

人工智能带来的技术机遇塑造了未来，但并未确定它。国家、组织和个人可以选择如何使用和响应人工智能的各种用途。他们的政策可以指导，限制或鼓励人工智能的某些用途。为了应对未来的挑战，美国需要采取国家战略，以便如何利用人工智能的优势，同时减轻其破坏性影响。

F-35与防空压制

随着势均力敌的对手的出现，西方国家空军已不可能在没有对抗的空域作战。事实上，一些国家正在实施“反介入/区域拒止”战略，加大防空能力建设，使美国空中力量很难进入这些受保护的空域。

因此，对于攻击方来说，对敌防空压制（SEAD）再次成为先决条件，以保证后续的空中打击不至于遭受难以接受的损失。所谓SEAD指的是，通过物理和/或电子手段摧毁敌方的防空系统或使其暂时失效。

与过去SEAD作战只包括第四代非隐身飞机不同，未来的SEAD任务将把F-35等第五代飞机和传统平台结合在一起，以形成互补效果。

在执行SEAD任务时，F-35的隐身特性能够发挥无与伦比的能力。F-35将多种高科技传感器收集的数据进行融合，形成可供作战使用的情报，发送给其他F-35飞机以及第四代战斗机，为空中编队提供一幅通用图像。

F-35将作为一种“情报、监视、目标捕获与侦察”（ISTAR）平台，深入敌后飞行，识别和定位敌方交战雷达及相关的地对空导弹，从而为己方传统战斗机发射的导弹提供末段制导，这些传统战斗机将在远离敌方A2/AD系统的安全距离上巡航。

目标定位雷达（或交战雷达）设计用于制导那些对付来袭飞机的导弹，这些雷达工作在较高的波段。由于可以形成窄波束，较高的波段能够产生更好的雷达分辨率，提高了雷达对目标的定位精度，从而可以锁定目标，为武器提供制导信息。

第四代战斗机不具备隐身设计，会反射目标定位雷达发射的高频雷达波，从而很容易在远距离上就被探测和锁定。不过，这种情况不会发生在第五代飞机上，因为它们的隐身设计使其不会反射地基目标定位雷达发射的高频雷达波。

不过，隐身并不是说完全不可见。当F-35距离交战雷达太近时，它仍可以被高频火控雷达探测和锁定。这就是所谓的延迟探测。但是，因为F-35配备了机载有源相控阵雷达，使其能够在更远的距离上探测目标，而且比传统雷达具有更高的精度，因此，F-35不需要飞抵敌方防空系统太近去收集情报。此外，由于不需要抵近执行ISTAR任务，F-35也可以避免被点防御红外制导防空系统探测到。隐身技术在这些红外系统面前无效，因为它们是通过热信号进行探测的。实际上，尽管一直在改进，但与雷达相比，红外传感器固有的特性还是限制了其探测距离。

虽然传统飞机依赖F-35的隐身特性为其提供导弹的末段制导，而F-35同样也依赖第四代飞机优越的载荷能力。由于采用了隐身设计，F-35只能在机舱内携载武器，这就使其有效载荷非常有限，而不像传统战斗机可以作为防区外武器库使用。

但是，隐身战斗机在A2/AD环境中也可能变得像老式飞机那样易损，因为它们可以被低频雷达（或搜索雷达）探测到。这种类型的雷达设计用于监视和预警，它们能够引导高频交战雷达指向F-35的位置。也就是说，低频监视雷达具有较宽的波束，可以搜索较大的区域，但其雷达分辨率比高频目标定位雷达要低。因此，它们的任务仅仅是把来袭飞机的大概位置发送给地基交战雷达，后者的窄波束使其无法有效搜索较大的区域。与采用机械旋转抛物面天线的传统搜索雷达相比，新型地基低频有源相控阵搜索雷达能够在更远的距离上探测到第五代飞机，而且更重要的是，它们能够提供更高的精度，从而引导高频交战雷达指向隐身平台。

因此，在执行ISTAR任务之前，F-35必须先摧毁那些低频有源相控阵雷达，以阻止它们引导高频的火控雷达。为了执行这样的任务，F-35就要依赖电子战平台。电子战平台与隐身飞机截然不同，具有诸多手段，包括搜集射频辐射的雷达告警接收机（RWR）以及机翼下的干扰吊舱。电子战飞机将从安全的距离干扰搜索雷达，使其无法探测隐身飞机和引导火控雷达，从而允许F-35安全地潜入敌方空域，摧毁敌方的搜索雷达。一旦这些搜索雷达被摧毁，交战雷达对F-35构成的威胁就会大大降低，从而使F-35能安全地执行ISTAR任务，为携载了大量武器的第四代战斗机保驾护航。

总的来说，未来SEAD任务的成功，将依赖于第四代和第五代战斗机的混合编队，它们能够实现优势互补。（EW）