

# AI 技术增强网络空间安全防御能力

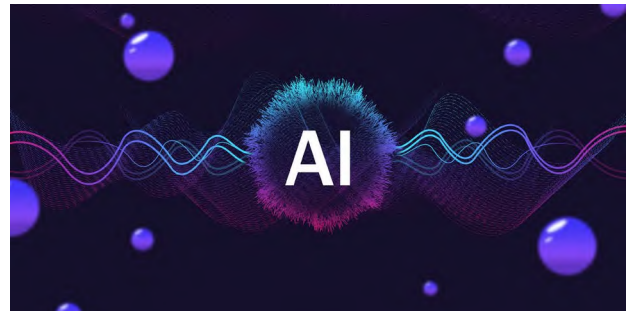
科技的突飞猛进促进了社会经济发展，使得互联网的大门越开越大。面对庞杂的互联网信息、潜在的信息安全风险，人工智能凭借强大的自我学习及数据分析运算能力，能够快速发现异常、风险和未来威胁，应用于网络安全防御大有可为。

文 | 刘飞

网络空间安全防御的主要目的，是营造一个稳定性优、安全性高的网络环境，提升网络空间的主动防御能力，最大程度地减少违法行为的出现。人工智能是基于计算机科学而建立、可实现语言与图像识别的高新技术，可以较好地对使用者需求进行信息模拟与分析，提高计算机网络空间安全性、有效缓解目前计算机网络空间安全防御发展面临的巨大压力。

随着科技水平不断提高，人工智能技术创造的应用极大方便了人们的工作与生活。目前，国内学者李德毅定义的人工智能是：探究人类智能活动的机理和规律，构造受人脑启发的人工智能体，研究

如何让智能体去完成以往需要人的智力才能胜任的工作，形成模拟人类智能行为的基本理论、方法和技术，所构建的机器人或者智能系统能够像人一样思考和行动，并进一步提升人的智能。



互联网发展日新月异，伴随海量信息的出现，互联网上同样产生了来源不明的信息链接，这些链接如果携带病毒，点击进去就有计算机中毒或者信息泄露的可能，这对计算机网络空间安全防御的要求进一步提升。近年来，我国印发《国家网络安全事件应急预案》，研究制定《关键信息基础设施安全保护条例》，不断健全国家网络安全应急工作机制，旨在提高网络安全事件预防能力和应对处置能力。

网络安全防御运用多种交叉融合技术，是一项至关重要的防御与保护。对于计算机网络空间来说，持续优化计算机网络可以实时、有效阻断网络病毒和不良程序入侵。就当前有关计算机网络空间安全防御的应用来看，使用较广泛的网络空间安全防御技术有主动诱惑欺骗技术、被动入侵检测技术与被动信息保障技术，保障网络空间安全已成为社会稳定发展的一项重要任务。

### 加速AI应用势在必行

网络空间安全与人们日常工作生活的联系日益加深，着力强化对网络空间的管控和引导既是社会不同层面形成的共识，又是加强网络安全的关键措施。现阶段网络上出现的海量信息，让人们工作生活更加便捷，但网络安全的把关作用越来越凸显，这种重视也进一步给网络安全防御领域带来更多的投入与更深入研究。尤其是网络犯罪形式变化多端，增加了破案难度，因而人们的计算机、手机等设备必须要有更强大的监测与防御系统，才有可能抵御外部有害信息侵袭，进而使数据信息得到更好保护。

人工智能技术的不断进步为加强网络空间安全

提供加持。人工智能技术应用于计算机网络安全空间防御，能够在网络信息的自动收集与分析判断中发现并解决不良入侵等问题，不仅能够较快速地推荐有效处理方法，而且能够提升网络运行速度。

除此之外，其重要性体现在以下三点：第一，可以稳定、精准地判断并识别来源不明的信息，对计算机网络信息数据进行实时、动态监测；第二，可以为用户提供个性化的网络数据信息保障等定制服务；第三，还拥有协作与整合能力，可有效提升计算机网络的可利用空间，提高计算机各类数据信息的管理效率。

### AI技术关键应用

人工智能防火墙技术。传统的计算机网络空间安全防御中有不少防火墙，但实际上没有达到最好的防御效果，导致计算机网络空间仍然存在不少潜在安全问题。充分借助人工智能技术后，防火墙可以及时辨别及防御各类潜在安全风险，最大程度地保障计算机网络及设备的安全与稳定。

人工智能防火墙技术可更具针对性地对网络空间中潜在的安全问题进行综合分析并有效处理，对海量信息进行快速计算，及时、精确地发现并阻拦不良、高危网络病毒，依据网络空间环境消灭安全隐患，避免病毒入侵，同时可较早判断大概率会出现的不明攻击情况，显著提高计算机防火墙的网络安全防御水平。

在实际应用中，人工智能防火墙技术既有相对完整的应用功能，又有等级更高的防护能力，能够提升和强化计算机网络空间安全防御体系，更全面地展示人工智能技术的作用，为持续强化网络空间安全防御增添更多保障。



入侵动态检测技术。入侵检测是防火墙背后的第二道安全门，针对网络病毒与潜在的各类安全风险，需要引入动态、实时的入侵监测，多方面了解各类潜在的安全隐患对网络及系统造成的影响与破坏有多大，应在潜在安全风险被发现前就加以控制，最大程度地保障计算机系统与网络安全运行。

虽然惯常的做法是在网络安全防御中预置一定的安全监测方式，但根据实际的运行情况看，惯常的网络安全监测方式存在相关的安全隐患，并且还可能出现监测目标不全面等现象，无法对网络安全进行精准、有效的防御。

现在运用人工智能入侵检测技术，能够利用其智能化特征辨别各类网络信息，综合分析出潜在的安全隐患，然后依据检测出来的安全问题推荐相关的解决方案，减少因潜在的网络安全问题而引发更多问题，提升网络空间防御性。目前，有些公司以及对保密安全性要求较高的机构已大规模运用人工智能入侵检测技术，而且效果较为显著，避免了外部病毒入侵对网络空间造成破坏。

垃圾邮件安全防御技术。邮件已成为信息沟通的重要桥梁，运用人工智能技术识别垃圾邮件，可

进一步促使网络空间更安全稳定地运转。现阶段，很多未注明来源的垃圾邮件对系统的高效运行和网络空间安全防御造成干扰，除此之外，有些垃圾邮件中还携带网络病毒和木马程序，这类邮件一旦进入网络空间，如果没有得到精准处理，很容易造成木马病毒侵入。因此，持续强化针对垃圾邮件的判断与精准清除至关重要。

人工智能技术的应用可以进一步提升对垃圾邮件的判别和控制能力，从而最大程度减少垃圾邮件对网络空间的入侵。通过对网络空间的全面分析，应开发反垃圾邮件系统，持续优化网络空间。此外，人工智能技术可以自动分析垃圾邮件并生成相关数据表，为后期维护防御系统提供参考数据及依据。

专家系统防御技术。目前，专家系统的完善程度是较高的，在人工智能技术中处于非常重要的环节。专家系统主要是参考、借鉴专家在各自不同领域的经验进行网络安全防御保护工作，给使用者做出易于落地且有效的方案。根据当前网络安全防御中的突出问题，在接入专家系统阶段需要确保数据库的完整性，保障网络安全使用方法有序、稳定发展。

在专家系统的实际应用阶段，借助人性化、智能化人机交互界面，可以实现应用者信息与数据库信息最大程度地互相匹配，从而有效提升网络空间安全防御水平。现在普遍使用的专家系统开发工具，可以按照专家经验来处理网络空间安全中存在的问题，也为网络信息安全数据研究提供有益的借鉴。

目前，已有相当数量的人工智能技术应用在网络空间安全防御领域。未来应进一步加大对人工智能技术的开发与研究力度，更好地保障网络空间安全。🔗

(本文作者单位系长沙理工大学马克思主义学院)