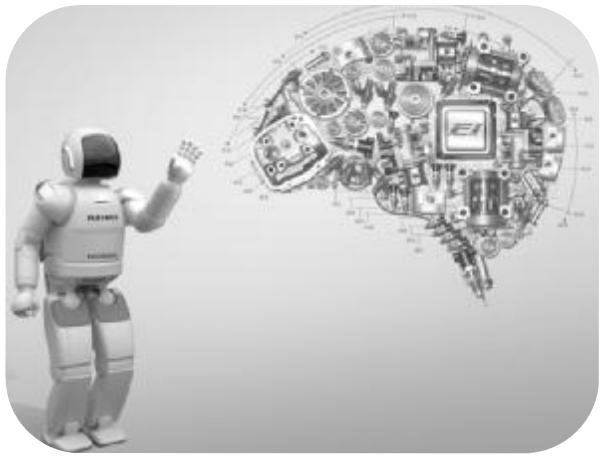
利用AI散布谣言、“杀猪盘”延伸黑链条……

网络安全防火墙如何筑得更牢？



2023年国家网络安全宣传周于9月11日至17日在全国范围内统一开展。当前，以大数据、人工智能等为代表的信息技术日新月异，但与此同时，网络攻击、网络窃密、网络诈骗等现象也不断出现，网络安全的风险正在被技术不断放大。网络安全风险对于个人、社会以及国家意味着什么？信息技术的更新换代又让现今的网络安全面临着哪些新情况、新问题和新挑战？如何严防网络攻击、网络窃密、网络诈骗，让网络安全防火墙筑得更牢呢？

我国网民规模超10亿人，网络安全事关你我

截至2023年6月，我国网民规模达10.79亿人，较2022年12月增长了1109万人，互联网普及率已经达到76.4%。当前，以大数据、人工智能等为代表的信息技术日新月异，给我们的生活带来了极大的便利，但与此同时，网络攻击、网络窃密、网络诈骗等现象也不断出现，一些不法分子利用快速迭代的信息技术不断放大网络安全的风险。

利用网络技术，“杀猪盘”延伸黑链条

近年来，各地各部门不断加大打击治理电信网络诈骗违法犯罪力度，有效遏制了案件快速上升势头。然而，仍有犯罪分子铤而走险，不断翻新手段实施诈骗。以“杀猪盘”为例，随着技术的更新换代，电信网络诈骗团伙在境外设立了多个电信网络诈骗窝点，并配备了电脑、手机、聊天软件账号等作案工具；在国内则组织洗钱人员、技术维护团队、推广引流团队、窝点主管、窝点作案人员搭建虚假投资理财返利APP，并利用国内公众号或网站进行推广引流，最终吸引潜在受害者下载指定的APP实施“杀猪盘”诈骗活动。

利用AI散布谣言，“有视频也未必有真相”

就个人而言，网络安全存在的风险让犯罪分子盯上了我们的“钱袋子”，而从社会层面来说，眼下就有不少人利用AI技术散播谣言，严重扰乱了社会秩序，造成了恶劣影响。

今年6月2日，浙江警方破获了一起利用AI技术制作虚假视频编造网络谣言非法牟利案。这则题为《绍兴上虞工业园区发生重大火灾》的视频就是通过AI技术进行深度合成的，看上去煞有其事的播报事件实际上子虚乌有，视频实为网上其他火灾画面通过剪辑拼接而成的。记者了解到，5月中旬以来，该团伙为吸粉引流、牟取利益，利用AI合成技术自动生成虚假视频，通过平台返利形式非法获利4万余元。截至案发时，该团伙已编造虚假视频1.8万余个，有20个视频造成了恶劣影响。

通过AI合成技术，不法分子大大降低了虚假视频的制作门槛，有的仅需1分钟就能制作完成，而当这种技术被应用于制造虚假文章时，则成了违法违规的重灾区。

今年6月，一则《绵阳大学生涉嫌卖淫800多次，赚120余万元，警方成功抓获》的配图文章引发网民围观，后经警方证实，此为AI软件自动生成的虚假文章。今年3月，山东警方破获了一起特大造谣引流网络水军案，某传媒公司利用群控软件和人工智能技术，大肆利用境内外短视频内容篡改编造敏感社会事件，并在网络平台上发布虚假信息，通过其运营的4万多个自媒体账号发布虚假帖子80多万篇。

除了一些“网络水军”通过编造传播虚假信息制造热点、牟取非法利益外，更有一些不法分子利用网络谣言实施敲诈勒索。

今年3月以来，山东的张某某等3人通过运营的多个超百万粉丝的“大V”账号，专门编造发布针对单位或个人的虚假信息，并利用多个账号相互转发、评论进行炒作，借机向受害单位及个人敲诈勒索，严重扰乱社会秩序，造成恶劣影响。

武汉市地震监测中心遭境外网络攻击事件

对于个人而言，网络诈骗让人深恶痛绝，但对于社会和国家来说，网络攻击、网络窃密又会构成哪些威胁呢？今年7月，武汉市公安局江汉分局发布了一份不同寻常的警情通报。该警情通报显示，武汉市地震监测中心部分地震速报数据前端台站采集点网络设备遭受网络攻击，相关地震烈度数据极有可能被窃取。

据地震领域的相关专家介绍，地震数据是目前探测地下空间的最有效手段。调查组获取的大量证据也显示，此次武汉地震监测中心遭遇网络攻击的幕后黑手来源于美国的情报机构。

360公司网络安全专家边亮说：“我们通过大数据发现了一个样本的编写复杂度，这种武器的缜密程度，包括攻击的单位的重要程度，是一个非常特殊的攻击事件。我们把这个事件进行分析和还原，发现它里边这种代码的编写习惯，包括武器的整体架构，都严格遵循着与CIA（美国中央情报局）相关的那种技术框架。”

据了解，近些年，美国的国家安全局、中央情报局等情报机构频繁对我国相关敏感机构发动网络攻击，他们的网络武器使用了极其严格的间谍技术规范，各种攻击手法前后呼应、环环相扣，如今已覆盖全球几乎所有互联网和物联网资产，可以随时随地控制别国网络，盗取别国重要、敏感数据。

国家计算机病毒应急处理中心高级工程师杜振华表示，目前，美国情报机构体系中的主要情报机构有18个，除了中央情报局和国家安全局外，隶属于美国国防部的国防情报局、国家地理空间情报局、国家侦察局等都具有很强的军事地理地质信息情报分析能力，此次攻击不排除多个情报机构合作的可能性。

网络安全领域面临着哪些新的挑战？

那么，随着信息技术的不断发展，我国网络安全领域目前面临着哪些新情况、新问题和新挑战？

广东省数字政府网络和数据安全应急响应专家组专家李新亮表示，我们面临的网络安全形势越来越严峻了，分布式拒绝服务攻击同期上升了200%，网站被篡改的数量同期增长了159%，被植入的后门同期增长的数据超过了250%。我们面临的一些问题尤其是在网络安全建设方面，因为在过往，我们更多的是基于合规原则去建设网站的安全能力，而这些面对高强度的网络攻击或者多样化的网络攻击是远远不够的。

全国信息安全标准化技术委员会委员李雪莹表示，生成式人工智能可能会被攻击者用来挖掘漏洞生成恶意代码，甚至自动地进行网络攻击，这就降低了网络犯罪的门槛，给网络安全带来了一个巨大的挑战。生成式人工智能也有可能被用来生成一些虚假的信息，这些信息在社会层面和国家层面可能会造成相应的安全危害。

网络安全领域的“四梁八柱”基本确立

今年是《中华人民共和国网络安全法》施行的第6年。这部我国网络安全领域的基础性法律对个人信息保护、治理网络诈骗、实施网络实名制等方面作出了明确规定，成为我国网络空间法治化建设的重要里程碑。近年来，我国加快推进网络安全领域顶层设计，网络安全的“四梁八柱”基本确立。那么，如何严防网络攻击、网络窃密、网络诈骗，让网络安全防火墙筑得更牢呢？

全国信息安全标准化技术委员会专家程度表示，近几年，国家在监管方面推出了很多关于网络安全方面的法律，从未来的预见来看，这种法律的推动力和执行力是在逐年加强的；第二，从整个信息化的转型来看，大部分的数据和信息系统，包括一些应用都在“云”上，未来对于“云”方面的安全保障也会投入越来越多的人力和物力；第三是对个人信息的保护，增强自身意识，包括对于自己敏感数据泄露的敏感性、警惕性以及不要随意下载一些恶意软件，公众要提高这方面的意识。

据新华网