编者按

2024EDUCAUSE 十大教育议题中，把“将网络安全作为核心竞争力：平衡成本与风险”放在首位。可见，当前网络安全仍然是高校面临的主要风险。2024 年，高校如何保卫网络安全？为此，我们特别邀请北京外国语大学信息技术中心主任杨红波和厦门大学信息与网络中心副主任郑海山，对 2024 年高校网络安全发展趋势进行预测，以期指引新年度高校网络安全工作顺利开展。

2024 高校网络安全发展趋势分析

杨红波
北京外国语大学信息技术中心主任

“近年来，各式新技术层出不穷，网络安全边界变得复杂和模糊，大数据与人工智能（AI）的广泛应用，各类未知的安全威胁正在不断涌现。”杨红波表示，目前国内外各类网络攻击层出不穷且攻击方式越来越多，网络安全形势越来越严峻。他认为，在这样的环境下，2024 年高校网络安全发展趋势可以总结为人工智能下的数据安全、基础设施下的网络安全、全面监管下的供应链安全这三点。

趋势一：人工智能下的数据安全

人工智能（AI）技术是人类发展的新领域，以 ChatGPT 和 Sora 为代表的生成式人工智能技术带来了通用人工智能（AGI）的曙光。随着 AI 技术的深入应用，也会引发网络安全和数据安全隐患，犹如一个硬币的两面，需要我们关注并找到有效的应对方法。

目前，网络攻击的方式和手段在 AI 技术的推动下正在不断演变，呈现出分布式、智能化和自动化的特点。与此同时，AI 在训练和应用过程中，会处理包含敏感数据在内的大量数据，如用户的个人信息和生物识别数据，这些新颖的技术给网络安全防护带来了新的挑战。北京外国语大学是教育部“人工智能助推教师队伍建设行动”的第一批唯一试点高校，用技术创新了教学模式，加入了物联网和人工智能相关应用，这也对学校的网络安全防护提出了新的要求。

针对人工智能下的数据安全，高校首先要对个人信息的收集和使用加强监管。

第一，数据的采集要确保“一数一源”，这样既可以确保数据的一致性，又可针对数据源加强防护；第二，在数据建设阶段，要遵循数据设计规范，保证数据的保密性、权威性，这样可作为数据源向学校数据中心提供基础数据；第三，在使用数据时，要确保数据必须有合法来源，内部信息要脱敏使用，第三方系统调用时要确保“只使用不存储”的原则。

2023 年 5 月，国家网信办等七部门联合发布《生成式人工智能服务管理暂行办法》；2023 年 11 月，包括中国、美国与欧盟在内的 28 个国家代表，在全球首届 AI 安全峰会中签署了《布莱切利宣言》，一致同意加强国际合作，建立面向人工智能的监管框架。在这样的背景下，人工智能安全技术正在被全球监管机构、行业参与者和工业界持续关注和积极参与。未来，随着法律法规的逐步完善、公众意识的提高和技术的发展，个人信息保护的力度将持续加强。

趋势二：基础设施下的网络安全

当前，高校普遍都进入了智慧校园发展阶段，在国家政策引导、各部门协同推进下，新型智慧高校建设取得了显著成效，涌现出“一网通办”“OA 办公”“智能教室”等一批创新应用。物联网（IoT）、移动互联网、虚拟仿真等新技术应用的不断推动带来了新的安全问题，也进一步增加了网络空间和物理空间安全的相互依赖性。

网络是联接物理设施的纽带，既是智慧校园发展的关键基石，也是支撑学校数字化高效协同、校园服务的载体。服务中断、勒索软件攻击、信息泄露等问题的发生，将对智慧校园的日常运营造成巨大的损失。随着网络安全监管理念的创新和监管手段的进步，应统筹推进安全风险分析、协同监管机制、智能监管技术和安全应急处置等方面建设，为智慧校园发展保驾护航。

趋势三：全面监管下的供应链安全

信息技术的蓬勃发展离不开高新企业的力量，高校网络产品和服务的供应链已演变为复杂的组成结构。供应链安全问题已不仅限于产品范畴，而是波及整个供应链的各个环节。如今，供应链安全威胁和风险攻击日益凸显。比如，某关键软件产品被曝高危漏洞，其带来的影响是巨大的，很大程度上会涉及多个高校或多个业务系统。在攻防演练过程中，红队就研究 VPN 或者 OA 系统的漏洞，一旦得到 POC，便会波及多所高校。这时，产品在高校的通用性决定了其影响范围，其显著的特点就是“一点多面”，后果可想而知。所以，高校在供应链安全方面要严格把关，系统实施必须经过专家论证，系统上线必须经过源代码检查和安全检测，并经过一段时间的试运行，组织验收后才能正式上线。

高校业务系统数量较多，网络安全防护工作任重而道远。目前，北京外国语大学设有信息化建设与管理办公室，统筹学校信息化建设和网络安全管理工作，通过管理加技术多方位的手段，严格把关，对学校信息化系统掌握主动权，形成信息化系统资产台账，形成全生命周期的监管体系，形成高校环境下的网络安全防护体系。

此外，网络安全制度体系化、网络安全责任制同样发挥着非常重要的作用。高校加强网络安全责任体制落实、各部门主管责任落实、技术部门运维工作落实，外加高新公司的专业产品和安全服务，是目前网络安全工作运行与年度考核的机制。随着相关法律法规的制定和施行，高校未来的整体防护能力将会越来越强。

AI 让网络物理攻击成为可能

AI 的广泛普及，让网络物理攻击成为可能。美国麻省理工学院工程系统教授、斯隆管理学院网络安全系联合创始人斯图尔特·马德尼克（Stuart Madnick）表示，随着生成式 AI 的广泛普及，网络犯罪者在下一阶段发动物理攻击的概率正在增长。马德尼克认为，传统网络攻击只是让系统暂时离线，而网络物理攻击带来的后果远甚于此。他说：“如果通过传统网络攻击让发电厂停止运行，它很快就会恢复并重新上线。但是，如果黑客让发电厂爆炸或烧毁，就无法在一两天后恢复在线状态，因为这些专用系统中许多零件是定制的。借助 AI 技术，网络攻击技术已经能对物理系统造成严重破坏。”

美国叶史瓦大学卡茨科学与健康学院项目主任兼教授、网络安全管理平台 Onyxia 首席执行官西万·特希拉（Sivan Tehila）也担心网络物理攻击的潜在上升。特希拉说：“AI 支持的网络攻击可能很快就会发生，它们极为复杂、难以检测和缓解。”同时，她表示，AI 也在帮助防守方，AI 可以分析大量数据并实时识别恶意活动，在增强网络防御方面发挥着关键作用。

郑海山
厦门大学信息与网络中心副主任

“数字化时代，网络安全问题日益凸显，高校网络安全已引起社会各界的广泛关注。”郑海山表示，结合当前现状，2024 年高校网络安全应着重关注攻击面管理、软件供应链安全管理、生成式人工智能应用这三个方面。

趋势一：攻击面管理

Gartner（美国高德纳咨询公司）将攻击面管理分为外部攻击面管理（External Attack Surface Management，EASM）、网络资产攻击面管理（Cyber Asset Attack Surface Management，CAASM）和数字风险保护服务（Digital Risk Protection Services，DRPS）三类。

EASM 是指对组织在互联网上可见的所有数字资产和脆弱性进行管理。然而，目前部分高校的攻击面管理仅仅局限于 EASM 的范畴。甚至，高校大量师生各类终端以及各种教学、科研和管理等庞杂数字资产所形成的校园网环境也未被纳入“外部”统一进行考虑。这使得攻击面管理流于表“面”。

未来，在攻击面管理方面，高校应以“攻击者一定会进入校园网”为底线思维，比照共享数据治理，做好数字资产各类数据的整合，通过与现有工具、各类业务系统和网络管理系统进行集成，获取数字资产属性，形成类似师生画像的数字资产画像，并基于资产梳理结果进行暴露面收缩和脆弱性管理。

趋势二：软件供应链安全管理

近年来，在高校开展攻防演练或日常网络安全运营过程中，越来越多的软件供应链问题开始显露。其中，包括由于各种原因导致的供应链中断，对软件的供应和更新产生影响；新的软件开发模式所引起的特有的第三方库和组件之间复杂的依赖关系，使得管理依赖和更新成为一项技术难度和工作量较大的任务；供应链企业遭受攻击可能导致敏感运维信息泄露，恶意代码被部署到生产环境等问题。

面对这些软件供应链层面的安全风险，高校往往表现得较为被动。因为许多高校是采用外包开发或者购买成熟产品的方式进行信息化建设，并且相关运维工作也高度依赖第三方服务，这使得软件供应链安全管理变得更加困难。

高校无法直接参与具体的软件开发过程，因此也无法采用较为先进的软件供应链管理和脆弱性发现工具来提升软件代码质量。高校即使可以从终端安全软件收集到第三方库和组件的使用情况，但由于各种因素的影响，比如组件是否被使用、使用程度以及是否已经采用缓解措施等原因，导致依赖脆弱性误报率较高，管理收效甚微。因此，更多的高校只能对软件供应商的运维服务提出要求，而无法直接干预和管理软件开发过程中的供应链安全问题。

未来，高校的软件供应链安全管理应当从供应商的评估和选择出发，要求供应商持有适当的网络安全资质证明，要求开发者获得相关的安全认证，督促供应商提高软件供应链透明度，在合同管理方面加入适当的安全条款和责任，加强运维安全，做好应急响应，实施纵深防御，加强行业内威胁情报共享等。

趋势三：生成式人工智能应用

生成式人工智能技术在网络安全领域可发挥较大作用，它能够分析大量的网络流量、恶意软件样本和网络安全日志数据，同时也可以对软件开发代码和系统配置进

行分析。此外，它还能够归纳总结应急响应措施。这些能力使得越来越多的网络安全厂商和服务提供商开始将生成式人工智能技术引入其产品或安全服务中。

然而，生成式人工智能技术尽管对产品功能的提升和服务人员工作量的减轻起到了积极作用，但在高校网络安全中的显示度并不高，其更多的是对厂商和服务提供商自身的提升。

对于高校网络安全运营如何结合生成式人工智能而言，可以从简单的聊天开始，例如咨询常规的网络安全相关问题，或提交单位的网络拓扑结构和安全需求，由系统自动生成相应的安全策略，又或者结合单位的各类流量和日志数据，对一次攻击行为进行深入的分析和解读。期待未来能有更多结合生成式人工智能的场景出现，以提高高校网络安全运营的效率。

总体来看，对于 2024 年高校网络安全发展趋势，两位高校信息化管理者在“人工智能”和“供应链”两个关键词上达成共识。本刊通过这次预测，以期为 2024 年高校网络安全建设与发展树立方向。CEN（责编：陈永杰）

CCF 2024 年网络安全十大发展趋势

近期，中国计算机学会（CCF）计算机安全专业委员会来自国家网络安全主管部门、高校、科研院所、国有企业及民营企业界的专家学者，投票评选出了 2024 年网络安全十大发展趋势。

1 人工智能安全技术成为研究焦点。人工智能技术是当前科学与工程研究的一大热点。随着人工智能技术在众多领域的深入应用，网络安全和数据安全的问题也日益突出。

2 网络安全基础设施和公共安全服务属性将得到加强。在数字技术不断重塑经济和社会的背景下，网络安全的公共安全属性、非排他性和外部性不断凸显。面对迅速蔓延的网络安全威胁，借鉴公共安全治理模式以推进网络安全公共安全服务机制的形成变得极为重要。

3 生成式人工智能在网络安全领域应用效果初显。随着大语言模型与多模态技术的日益融合加速，预计生成式人工智能将在威胁检测与响应、自动化安全防护与修复、实时威胁情报与预测，以及自适应安全策略与防御、人机协同防御等多个方面发挥更大的作用。

4 供应链安全管理的重要性日益凸显。如今，供应链安全问题已不仅限于产品范畴，而是波及整个供应链的各个环节。可以预见，随着安全技术的不断完善和发展，供应链安全管理的战略地位将日渐上升，其重要性也将更加凸显。

5 隐私计算成为学术和产业界共同关注的焦点。在数据要素加速开放共享的新形势下，隐私计算正成为支撑数据要素流通的核心技术基础设施。据预测，隐私计算将在 2024 年获得学术界与产业界更广泛的关注，并在相关技术研究中占据重要地位。

6 勒索软件攻击依然是最普遍的网络威胁形式。据 2023 年数据显示，全球共发生了 4832 起勒索软件攻击事件，较前一年增加了 83%，且呈现出全球迅速扩散的趋势。展望 2024 年，网络安全将面临着严峻的挑战，随着黑客组织不断更新和改进攻击策略和技术，如智能化、多重勒索常态化等，新一代的勒索软件攻击会变得更加难以预防和处置。

7 高级持续性威胁（APT）攻击成为网络空间突出风险源。近年来，高级持续性威胁（APT）攻击已演化为集各种社会工程学攻击与零日漏洞利用的综合体，成为了最严峻的网络空间安全威胁之一。未来，APT 攻防较量更趋复杂。

8 国产密码技术广泛应用。随着国家“十四五”规划及其他一系列促进数字化发展战略的深入实施，我们预计国产密码技术将在基础信息网络、关乎国计民生的重要信息系统、重要工业控制系统以及面向社会服务的政务信息系统中实现更为广泛的推广与应用。

9 关键信息基础设施保护成为行业新的增长点。据预测，到 2024 年，我国对关键信息基础设施保护的需求将保持增长趋势，尤其在网络安全建设方面，国家重要行业及关键领域的资金投入预计将显著提升。

10 个人信息保护力度将持续加强。个人信息保护不只关乎个人隐私权益，也事关国家安全层面，成为全球普遍关注的议题。未来，随着法律法规的逐步完善、公众意识的提高和技术的发展，个人信息保护的力度预计将持续加强。