

人工智能驱动的关键信息基础设施防御研究综述

廖方圆¹, 陈剑锋², 甘植旺³

(1. 中国电子科技集团有限公司, 北京 100846; 2. 中国电科网络空间安全技术重点实验室, 成都 610041;
3. 中国电子科技集团公司信息科学研究院, 北京 100086)

摘 要: 关键信息基础设施(CII)是经济社会运行的神经中枢与网络安全的重要保障,但也面临着复杂多变的网络攻击和威胁。基于人工智能的网络安全防护,能够为 CII 防御构建灵敏的异常识别机制、自动化的事件分析引擎和精确的全局运维能力。分析 CII 的攻击风险,研究已有安全防护体系的形态结构,并基于 SMCRC 环思想构建智能 CII 安全体系。针对人工智能驱动的态势感知、持续监控等 CII 防御要点以及信任机制、威胁情报等 CII 防御保障的发展趋势进行综述和分析。

关键词: 关键信息基础设施安全; 智能安全; SMCRC 环; 安全生态; 态势感知

开放科学(资源服务)标志码(OSID):



中文引用格式: 廖方圆, 陈剑锋, 甘植旺. 人工智能驱动的关键信息基础设施防御研究综述[J]. 计算机工程, 2019, 45(7): 181-187, 193.

英文引用格式: LIAO Fangyuan, CHEN Jianfeng, GAN Zhiwang. Review of artificial intelligence driven critical information infrastructure defense research[J]. Computer Engineering, 2019, 45(7): 181-187, 193.

Review of Artificial Intelligence Driven Critical Information Infrastructure Defense Research

LIAO Fangyuan¹, CHEN Jianfeng², GAN Zhiwang³

(1. China Electronics Technology Group Corporation, Beijing 100846, China;

2. Cyberspace Security Technology Laboratory of China Electronics Technology Group Corporation, Chengdu 610041, China;

3. Information Science Academy of China Electronics Technology Group Corporation, Beijing 100086, China)

【Abstract】 Critical Information Infrastructure(CII) is the nerve center of economic social operations for the operations of economic society, an important guarantee of network security, and also a target that may be subject to key attacks. The network security protection, which is based on artificial intelligence, can build a more sensitive anomaly identification mechanism, a more automated event analysis engine and more accurate global operations and maintenance capabilities for CII defense. This paper investigates and analyzes the attack risk of CII, studies the morphological structure of the existing security protection system, and builds the intelligent CII security system based on the SMCRC ring idea. On this basis, this paper reviews and analyzes the latest research development on CII defense key points of the situational awareness and continuous monitoring driven by artificial intelligence, and CII defense guarantee of the trust mechanisms and threat information.

【Key words】 Critical Information Infrastructure(CII) security; intelligence security; SMCRC ring; security ecosystem; situational awareness

DOI: 10.19678/j.issn.1000-3428.0055155

0 概述

关键基础设施是指对国家至关重要的资产,一旦遭受破坏,将对国家安全、经济命脉、公民的健康

安全等造成严重损害。关键信息基础设施是指对关键基础设施进行处理、接收、存储数据的信息系统。世界各国对关键信息基础设施的范围、边界以及保护的重点领域具有不同的理解和规定。如美国政府

基金项目: 国家重点研发计划(2017YFB0803201)。

作者简介: 廖方圆(1981—),男,高级工程师,主研方向为网络空间安全;陈剑锋,研究员、博士;甘植旺,博士。

收稿日期: 2018-12-21 **修回日期:** 2019-02-25 **E-mail:** atrix@163.com

规定了 16 类关键信息基础设施,而德国在政府层面划定了 9 类。我国在 2016 年 11 月 7 日发布的《中华人民共和国网络安全法》中指出关键信息基础设施可分为公共通信和信息服务、能源、交通、水利、金融、公共服务(水、电、食品、卫生)、电子政务 7 类。在 2017 年 7 月发布的关键信息基础设施安全保护条例(征求意见稿)中又追加了环境保护、国防军工、大型装备、化工、食品药品等领域的基础设施。关键信息基础设施覆盖了社会生产、生活的各个方面,是国家的重要战略资源,也是世界各国予以重点保护的关键领域。

随着信息技术的普及和广泛应用,关键基础设施和关键信息基础设施之间的界限日益模糊。作为高价值目标,关键信息基础设施面临复杂多变的持续性安全风险和挑战,成为网络攻击的重要目标。《全球关键信息基础设施网络安全状况分析报告》^[1]中显示,全球信息基础设施发生重大网络安全事件的类型主要有敏感信息泄露、系统破坏、金融资产盗窃等,2018 年披露的相关漏洞已达 3 万多个,并呈逐年高增长的态势。

人工智能(Artificial Intelligence, AI)是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学,具有重大社会经济意义,AI 正在持续改变着人们的生活、工作和学习的方式。人工智能为关键信息基础设施安全赋能是业界公认的研究领域和发展方向,国内外在具体的理论、体系、技术和工程方面均开展了多层次的研究和产品化实践,防御者运用人工智能技术构建灵敏的异常识别机制、自动化的事件分析引擎和精确的威胁检测方式。

本文介绍关键信息基础设施相关安全事件及风险,在此基础上提出基于 SMCRC 环的关键信息基础设施安全体系,并对其防御要点和防御保障的研究发展趋势进行综述和分析。

1 关键信息基础设施安全体系

1.1 针对关键信息基础设施的攻击风险

关键信息基础设施与国家和社会的紧密耦合使得一旦网络安全事故发生,则会影响重要行业的正常运行,可能对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

1) 针对电力等能源基础设施的攻击。2019 年 3 月 7 日,委内瑞拉全国 23 个州中的 18 个州发生了停电,原因是向全国提供 80% 电力的古里水电站遭到蓄意破坏,2 天后电子系统再次遭到“高科技手段”实施的电磁攻击,导致再次大范围的停电。

2) 针对经济运行和生产系统的攻击。2017 年, WannaCry 勒索病毒在全球范围内蔓延,多个行业领域成为重灾区,损失巨大。2018 年 8 月,全球最大的

半导体制造商台积电遭受 WannaCry 变种勒索病毒入侵,中国台湾北、中、南三处重要的生产基地全数停摆,订单大量延迟,受此影响市值蒸发超过 78 亿新台币。

3) 针对重大活动和重要事项的攻击。2018 年 2 月,韩国平昌冬季奥运会开幕式当天遭受黑客攻击,奥组委服务器宕机、网络中断,直播系统和奥运会官网均瘫痪较长时间,许多观众无法打印门票,最终未能正常入场。

4) 长期潜伏的窃密和破坏行为。从 2016 年起,多起针对我国重要信息系统实施的 APT 攻击活动被曝光。2018 年 3 月,美国司法部起诉了伊朗境内黑客组织马布那研究所 9 名黑客,其发起的 APT 攻击渗透至 100 多个美国目标,窃取了 31 TB 数据和估值 30 亿美元的知识产权信息。

关键信息基础设施作为一类应用在特殊领域的信息系统,同样遵循信息系统安全所追求的“CIA 三性”,即机密性、完整性和可用性特点。关键信息基础设施与网络空间相互依赖、相互关联、相互作用,因而网络空间面临的诸多安全问题也以摆渡、传导、转换等方式威胁着关键信息基础设施的安全。

在面对有组织的网络安全事件和威胁时,关键信息基础设施的运营和管理单位存在持续性监控和分析能力不足、内外协调联动力度不够的问题。传统以合规为主导的网络安全保障体系已不能抵御复杂多变的网络攻击威胁,难以有效应对国家级、有组织的高强度、针对性网络攻击。网络空间无固定边界、动态变化、立体多维度和虚实融合等特点为开展网络空间安全防护带来了空前的困难和挑战。

1.2 基于 AI 的关键信息基础设施安全防御体系

网络空间安全是人工智能应用最活跃的领域之一。尽管人工智能技术中符号主义、连接主义和行为主义的出发点不同,但各自思想和理念都能够运用至网络空间安全领域中,实现安全感知、认知、控制和协同能力的跃升。具体而言,深度学习、迁移学习等技术可以优化数据挖掘、行为识别和风险预测,提供更为自动化、智能化的安全感知和响应,驱动安全防御理念变革升级。目前,基于人工智能的网络安全防护已成为国内外网络安全产业发展的重点方向,其应用日益广泛。

基础设施的安全性是从底层开始设计数据中心的物理安全,进而设计基础设施的硬件和软件安全,最后是支持安全运维的技术规范和流程,具体技术包括物理边界安全、服务安全访问管理、统一认证和授权、数据容灾、加密和恢复、防 DoS 攻击、安全态势等^[2]。在通常情况下,层次化的安全防护体系是从空间结构角度出发,通过确认每一层的安全威胁风险和安全管理目标,至下而上地构建安全堆栈,确保

整个关键信息基础设施安全的基底可信牢固、中部衔接可靠、上层灵活支撑。但在安全实践中攻击者的现实威胁呈现高度定向、长期潜伏与复杂多变,基于层次化设计关键信息基础设施安全体系的静态部署、功能固化特点越来越不能满足防御需求。因此,应从动态、持续、全局、协同的设计思维出发,构建能与风险演进相适应的、具有自主更新与进化能力的安全生态。

杨小牛院士提出“SMCRC”网络空间生态体系,针对关键信息基础设施空间即“K空间”的业务特点、威胁态势、安全需求和防护策略,构建基于人工智能的关键信息基础设施安全防御体系^[3]。该体系强调人工智能所带来的增强效应在态势感知、持续监控、协同防御、快速恢复和溯源反制等环节的耦合与赋能作用,打造面向关键信息基础设施的智能安全防御体系闭环,该防御体系设计如图1所示。



图1 基于AI的关键信息基础设施安全防御体系

人工智能与SMCRC环的5个关键环节和3个保障基础是横向增强、纵向贯穿的关系。一方面人工智能通过网络空间安全感知、认知、控制的协同方面的赋能作用,基于对网络空间各类要素信息进行基于数据和证据的分析和决策,显著增强SMCRC各环节面对不可预知、随机性强的网络空间安全事件时的应对能力;另一方面人工智能通过语义桥构建、知识图谱、动态适配、自动执行等方式实现验证评估、威胁情报和统一信任的保障作用与关键环节的衔接和支撑,使得信任的实现方式更加多样、情报的采集应用领域更加宽广、安全措施有效性验证更加实时、精确。

2 AI驱动的关键信息基础设施防御要点

2.1 态势感知

关键信息基础设施态势感知是对基础设施所在的内外网络环境中,对能够引起安全态势发生变化的要素进行获取、理解、评估、显示以及预测未来发展趋势的过程^[4]。态势能够使管理员掌控所辖网络域内某些关键因素或者参数,从而为科学决策提供

依据。

为了形成全局安全态势,首先需要对安全域内的资产和防护力量进行摸底和排查,其次要能够收集 and 汇聚多源异构数据,并对其进行清洗和分类,再次需要根据态势生成模型和指标体系,对安全风险和威胁进行量化,最后以人机友好的方式将分析结果转换为可视结构,辅助管理员进行有效决策。人工智能在此过程中能够加速数据的语义化处理、规范化映射、模型智能化生成,以及增强人机交互过程的体验^[5]。

为更好地应对复杂网络空间条件下的新型安全挑战,深度学习、模拟交互、行为异常识别等人工智能技术手段已经成为解决关键信息基础设施威胁的有效方法。在相关研究方面,文献[6-7]指出,网络空间测绘是对网络空间中的各类资源及其属性进行自动或手动探测、融合分析和绘制,还原网络空间结构/行为/特征,全面掌握网络空间特性及其资源分布的有效方法。文献[8]提出海量多元异构数据的汇聚融合技术,能够实现PB量级多元异构数据的采集汇聚、多维度深度融合、统一存储管理和安全共享。文献[9]提出的面向多类型的网络安全威胁评估技术,能够通过结合聚类分析、关联分析和序列模式分析等大数据分析方法来发现的恶意代码、域名信息等威胁项进行跟踪分析。文献[10]的态势决策支撑技术以网络安全事件监测为驱动,以安全威胁线索为牵引,对网络空间安全相关信息进行汇聚融合,实现对整体网络安全状况的判定。文献[11]提出的网络安全态势主动可视可提供交互式可视化工具,建立人与数据之间的图像通信,提升信息安全分析人员感知、分析和理解信息安全问题的能力。当前,受限于网络日志、设备状态、资产信息等安全态势来源数据的异构性、碎片化和分散性特点,态势信息存在时空不连续、语义不完整的问题,在形成可供管理员进行高精度顶层决策的支撑能力方面,还存在一定差距。

2.2 持续监控

从各种网络、主机监控设备获取的数据中了解关键信息基础设施安全的运行状态是识别威胁的最基本问题,也是异常检测、积极防御、预警通报和协同处置的前提。文献[12]建议持续监控以 7×24 h全面时间覆盖的方式运行,其监控范围广、对象多、层次深,例如流量突变、资源越权访问、可疑主机操作、数据非法回传等,试图从“正常状态”中快速地发现“异常情况”,同时实现定位异常位置,而不仅是只给出异常检测结果。

持续监控能力的来源是部署在关键信息基础设施云、网和端侧的多类型探针,通过大规模分布式部署、多设备联动、多区域协同、多技术融合的智能主

动监控感知机制,构建多维度复杂攻击模型,依据发现、识别、测量、验证手段确定攻击行为模式和事件发展过程,实现高猝发、高隐蔽度、高变化的复杂威胁和网络风险的实时捕获和跟踪。

在持续监控相关研究方面,文献[13]提出的多智能学习范型的入侵检测模型融合了线性遗传规划、自适应神经模糊推理系统和随机森林学习算法,在分类前使用特征选择过程来约简特征,提升了入侵分类的性能。文献[14]通过持续对杀伤链进行监控和分析,对攻击事件、IP、时间戳属性进行模糊聚类,能够从安全日志中挖掘出场景,提升威胁事件识别的准确率。文献[15]将攻击图的自动构建问题转化为特殊的智能规划问题,分析企业或关键信息基础设施网络中各个脆弱点之间的相互作用关系以及由此产生的潜在威胁。文献[16]将机器学习、自然语言处理等人工智能技术应用于安全漏洞的研究与安全漏洞的自动化挖掘、自动化评估、自动化利用和自动化修补,能够实现对关键信息基础设施中面向漏洞的有效监控和风险管理。

2.3 协同防御

多样化、协同化、大规模是目前网络攻击的三大趋势。网络防御在理念角度包括纵深防御、积极防御、主动防御、动态防御、弹性防御等,在架构和协议栈角度关注链路、网络、操作系统、服务及应用软件、数据等方面,从网络互联结构角度关注网络边界、终端、飞地和业务域等方面和安全。关键信息基础设施防御机制的设计和实现是一个复杂的系统工程,受多个显式或隐含自变量、因变量的取值效果制约,应瞄准不同的安全目标、成本预期、领域特点、资产情况进行定制化设计,把分散的安全产品、技术、策略、管理规则、技术人员等能力进行协同化整合,形成有效、经济的防护能力。

人工智能驱动的协同防御通过大数据智能、群体智能、混合增强智能,基于阻断、隔离、分流、诱骗、过滤、混淆等机制来降低攻击面、增大攻击者利用的难度,从而在攻击未发起时威慑攻击者放弃、或在攻击发生时最小化攻击能够取得的效果,使安全投入发挥理想的防护价值^[17]。

文献[18]通过基于偏差和特征的防御检测、基于资源配置和校正控制的防御实施,实现对电力信息物理系统(电力 CPS)网络攻击的协同保护。文献[19]使用 Agent 的建模思想及输入-输出映射原理,建立包含自主行为和交互行为的实体行为概念模型,改进 Agent 行为形式化描述,为提升分布式拒绝服务(DDoS)协同防御能力提供实现方法。文献[20]以智能安全免疫为特征、以安全可控为目标,构建具备识别“自我”“非我”特征并进行安全控制的计算环境可信、应用行为可信、网络通信可信机

制。文献[21]通过系统特征主动变化的攻击面随机化技术,降低攻击成功的可能性,增加系统的动态性,缩短攻击的有效期,限制大规模攻击造成的安全损失。目前协同防御面临的问题是安全软硬件设备缺乏互联互通和互操作能力,只能接受安全管理中心的统一指挥和调度,在攻击导致安全管理中心功能离线条件下无法自治运作,降低了体系化防护效能。

2.4 快速恢复

在攻防对抗中,攻击者只需找到一个突破口,但防御者则必须精心构建防御体系,花费很大成本来抵御自所有方向、所有方式、针对所有目标的攻击。由于安全防御手段需引入成本,无法达到 100%“固守城池”的能力,而且经济上无法承受,因此更佳的选择是通过快速恢复来确保关键服务或资产的运行得到最低限度的连续性保证,降低关键信息基础设施安全事件对社会、政治、经济活动影响。

在掌握自身信息系统内潜在的风险和脆弱性特征基础上,通过引入人工智能驱动的先进计算和存储架构,能够基于资源配置、策略切换、路径重构和动作规避等方式减弱针对关键信息基础设施的攻击可能造成的破坏性效果,并在线对受影响的组件进行恢复,实现网络、计算和存储等层面的弹性、容灾和高可用^[22]。

文献[23]为达到释放云计算、大数据等新型服务平台潜力、降低准备时间、增强敏捷性的目的,采用云安全快速自主部署及高可用机制,使安全恢复能力在业务流程中自动嵌入、自动配置和实时接管。文献[24]讨论了构建实时应用程序自我保护(Real-time Application Self Protection, RASP)的新型应用安全保护技术,在程序运行的整个阶段实现有效的自我监控、资产采集和有害输入及行为的识别,使得真正的攻击临时能够调整策略以恢复防护能力。文献[25]在安全事件处置过程导致安全策略发生变更的情形下,可以通过全面分析所有网络安全设备的策略配置,按优先级排序以避免策略冲突和矛盾。

2.5 溯源反制

网络溯源反制是基于采集、汇聚、分析和挖掘等手段,通过对攻击行为和攻击的中间介质(反射器、傀儡机或僵尸机、跳板)进行检测确认的过程,主要包括重构攻击路径、确定真正攻击者、攻击手段和过程信息、识别攻击目标和原因等,在条件和时机允许时进行防御反击,阻断攻击源头。

人工智能与溯源反制的结合点在于通过合作或非合作的方式对网络恶意行为或特定数据包进行定向追踪、对攻击时序和攻击路径进行重构、对攻击意图进行推断,并以此确定攻击者、攻击组织,避免受到更大的破坏。参与溯源和反制活动的关键信息基

基础设施单元通常具有独立的功能,能够与决策信息进行信息交互,实现汇聚碎片化攻击信息、关联攻击有关知识和执行反制动作等目的^[26]。

文献[27]结合动态概率对攻击中的数据包进行标记,对应用层 DDoS 进行检测和溯源的研究。文献[28]提出混淆攻击者对于目标资源的判断和认知,引导攻击者放弃目标或采用错误的方式攻击目标进而被捕获,增大攻击者和攻击手段的暴露概率。文献[29]构建智能蜜罐,嵌入集成多种工业网络协议模拟镜像,结合案例库和知识库对蜜罐提供的数据进行智能化分析和处理,追溯攻击源头。在当前溯源相关研究中,多数受限于数据采集位置和方式,仅具备溯源至跳板主机或真实主机的能力,通过关联域分析和画像技术等对攻击者、攻击组织的身份进行还原的研究还较少。

3 AI 驱动的关键信息基础设施防御保障

3.1 统一信任

信任是衡量可信程度的度量,与风险管理密切相关。关键信息基础设施中的信任是指以基于密码和非密码技术实现的,依托身份认证、权限判决、合规检测、责任认定等功能完成的实体与实体间在一定条件下的互信。关键信息基础设施管理者、维护者和用户通过身份认证、授权管理与应用系统建立可靠的信任关系,并在该关系上进行系统操作。一旦出现用户冒用身份或越权访问,这种信任链就会受到破坏,造成网络空间中信息的失窃密、不完整或不可用。

文献[30-31]指出,人工智能在信任的确立、维持和变更过程中将起到极为重要的检测、识别、告警和判决等作用。人工智能有助于对人、机器和程序的身份进行统一化综合,将关键信息基础设施中的身份活动进行映射和记录,在多个安全单元间建立信任和合作关系,提升攻击威胁的防护能力和处置效率。

在统一信任相关研究方面,文献[32]针对关键信息基础设施多应用协同工作的系统运行模式,基于安全声明标记语言(SAML)标准统一信任与授权平台可以构建安全、灵活的数据交换体系。文献[33]基于“零信任”模型,通过对使用者身份和行为的实时检测,实现网络层访问控制、强制加密、SSO 单点登录、访问控制引擎等机制,以对数据资源进行保护。文献[34]瞄准异构系统的安全可验证,从拓扑结构角度设计基于信任节点二阶智能体的控制策略,实现全局安全一致性。

3.2 威胁情报

情报及情报学在网络空间论域中具有其崭新的特点和属性,能够有效指导和解决关键信息基础设

施防御实践中新涌现的难点性问题,安全威胁情报是包含漏洞、威胁、特征、名单、属性、解决建议等多种内容的动态更新的知识载体,是一种基于证据的判断和预告。在系统内、系统间公认并遵循准则化、模块化协议、配置或共识条件下,威胁情报能够共享,防御者进行有效处置,那么关键信息基础设施目标能够免疫未来发起的相关攻击,避免可能遭受的破坏损失。此外,情报中关于威胁细节的披露也能使关键信息基础设施更快地从故障中恢复^[35-36]。

人工智能对关键信息基础设施中威胁情报生态的核心意义在于赋予其获取知识、传递知识、应用知识的能力,能够从大量的、不完全的、含噪声的、模糊的、随机的安全数据中,提取潜在可理解、有价值的信息和知识,将这一过程蕴含的概念、技术、工具、方法应用于感知和防御,通过“知识互联”颠覆性地改变传统日志情报机器处理、动向情报人工解读、异构信息融合关联困难的局面,提升数据驱动安全的技术能力水平。

在威胁情报相关研究方面,文献[37]针对网络攻击向高隐蔽性、高持久性和高扩散性发展,将画像分析思路引入攻击识别建模过程,构建准确、完整和丰富的攻击识别模型。文献[38]利用对威胁情报进行各种汇聚关联并进行综合分析,覆盖网络攻击链的所有阶段,实现基于综合保障主动防御与及时响应。文献[39]通过监督性的深度学习模型,对威胁情报的实体和实体关系进行自动化抽取,基于图数据库进行知识图谱的可视化展示以提升安全感知能力。文献[40]根据安全威胁情报的生命周期,提出包含静态体系、动力学特征和威胁情报生态,设计了面向情报的服务框架来确保诸多领域中威胁情报标准化和统一化的实现。

3.3 验证评估

随着关键信息基础设施复杂度的提升和面临网络空间威胁的加剧,安全性测试与评估难度大幅增加,对测试与评估人员、技术和设施的要求更高。有效的、持续的验证评估机制应从关键信息基础设施安全体系的组成结构出发,建立验证评估基准尺度规范,针对攻击与防御活动和影响规律,设计有效的关键信息基础设施风险评估模型,在运行前和运行时对生产环境的资产、脆弱性、威胁等进行全局性检测与监测,最大程度降低安全事件的发生概率。

从客观、普适、可操作角度,在对网络安全验证评估科学理论及方法进行探索的基础上,进一步结合人工智能技术,对网络空间的各种复杂协议、软硬件信息系统中存在的漏洞、后门、脆弱性进行纵向、横向深入分析,能够为安全应对机制、攻防技术演练、人才队伍培养、基础设施建设提供测试与评估保障,达到信息力和安全力的进化。

在验证评估相关研究方面,文献[41]通过组件风险和攻击损失2个方面指标,结合组件资产价值和关联影响等因素,实现基于攻击图的智能制造系统安全风险量化。文献[42]采用多层次模糊综合评定法,科学准确地评定出信息的安全风险级别以及风险程度,有利于在减少风险、控制风险以及转变风险的过程中做出正确及时的措施。文献[43]基于大数据技术和模块化设计的智能网络安全分析平台,

实现安全分析场景及模型的快速模块化扩展,保障全方位立体式安全分析、防护及态势预测能力。

4 效能对比与热点趋势

在对人工智能驱动的关键信息基础设施安全防护要点和防御保障等领域研究基础上,对传统安全防护效能和智能化安全防护效能在各个维度进行比较,结果如表1所示。

表1 关键信息基础设施防御效能比较

领域	传统安全体系	智能安全体系	适用场景	相关文献	有益效果	存在问题
安全感知	物理层、网络层感知为主,关键要素监控	拓展认知层行为和语义感知,持续全景监控	合作式感知	文献[6-7]	感知效率高、属性多、能力强	特定情况下无法取得资源控制权
			非合作感知	文献[12]	只需存在连通关系,无需资源控制权	感知范围和能力受限,容易被安全机制拦截
			人机联合感知	文献[39]	可视化感知利用人的经验,结果更精确	难以实现海量数据条件下完整精确的态势可视化
安全认知	区域性、局部安全态势,已知威胁识别能力	全局性、跨区域安全态势,未知威胁识别能力	时间维度威胁认知	文献[14-16]	从攻击链入手,可还原整个攻击过程	难以发现不同场景中攻击的相似性和关联关系
			空间维度威胁认知	文献[37-38]	从攻击特征入手,可归纳攻击类别谱系	碎片化场景中攻击的先后顺序与因果关系难以确定
			时空联合综合认知	文献[18-19,13,33]	综合威胁的时间和空间特征,准确度高	需要的原始数据质量高,模型复杂,计算效率低
安全防御	基于规则匹配的阻断、拦截和流量清洗	基于启发式关联和自主学习的容侵防御	基于遏制的防御	文献[17,19-20]	以杜绝风险为目标,达到威胁有效拦截	需构建完整的体系防线,成本高、代价大
			基于保护的防御	文献[18,21-22,24]	以降低攻击效果为目标,保护重要资产	难以在动态环境下精确掌握和评估待保护资源情况
安全协同	面向安全策略和预置规则的设备间协同	面向安全目标和设备能力的非预期自主协同	面向处置的协同	文献[26-27]	有效发挥各安全机制的优势,集约资源	需要具备各安全机制的先验知识以制订策略
			面向防御的协同	文献[28-29]	有效发挥各安全机制的优势,集约资源	需要合理安排各防御机制的顺序和优先级
			面向共享的协同	文献[32,35-36,40]	有效发挥信息的赋能作用,传递知识	需要在各使用主体间达成协同内容的共识
安全运维	以人工处置和运维为主的事件预警和响应	以自动化为主、人工确认为辅的高效管理运维	“机主人辅”的运维	文献[23,25,34,41-43]	以机为主,最大限度减轻运维人员负担	难以在虚警、漏警之间取得最佳平衡
			“人在环路”的运维	文献[11,43]	利用专家丰富的运维知识指导机器工作	难以将专家的经验形式化、规则化应用

在人工智能的助力下,网络空间防御的空间广度、层次深度和时间跨度都有较大拓展,未来关键信

息基础设施的研究将向全局化、动态化、精细化、联动化发展。热点趋势包括:

1) 防御模式由设备堆砌向云服务保障模式转变。关键信息基础设施的安全交付手段、方式和目标逐步发生变化,通过智能安全服务的按需使用,做到“关口前移,后端赋能”。

2) 防御理念由外挂式、嵌入式防护向内生式防御转变,建设由底至上、包含安全“基因”的智能关键信息基础设施,实现安全能力的可信生长。

3) 防御效果由单行业、单领域的关键信息基础设施向全行业、全生命周期的整体保障转变。基于采集、汇聚的大量不同节点监测、决策和响应数据进行智能分析,实现“全天候全方位感知网络安全态势”的能力,服务于整体网络安全保障体系建设。

5 结束语

关键信息基础设施是经济社会运行的神经中枢和网络安全的重要保障,但其较为薄弱的安全防控能力难以有效应对国家级、有组织的高强度网络攻击。本文着眼于改变当前分散、分领域的独立安全部署模式,强化面向任务和安全目标的一体化策略集成管控能力、协同保障能力和全局综合态势感知能力,为关键信息基础设施运维和管理设计并实现全系统智能、科学、高效的安全机制,在安全和智能共同演化的发展趋势下,为维护国家安全提供可靠的技术保障。

参考文献

- [1] 360 威胁情报中心. 全球关键信息基础设施网络安全状况分析报告(2018年)[EB/OL]. [2018-11-12]. <http://zt.360.cn/1101061855.php?dtid=1101062514&did=491171819>.
- [2] 罗强,吴少欢,曾梦岐. 关键信息基础设施安全架构研究[J]. 通信技术,2017,50(8):1816-1821.
- [3] YANG Xiaoni, WANG Wei, XU Xiaofeng, et al. Research on the construction of a novel cyberspace security ecosystem[J]. Engineering, 2018, 4(1):47-52.
- [4] 谭小彬,张勇,钟力. 基于多层次多角度分析的网络安全态势感知[J]. 信息网络安全,2008(11):47-50.
- [5] 陶源,黄涛,张墨涵,等. 网络安全态势感知关键技术研究及发展趋势分析[J]. 信息网络安全,2018(8):79-85.
- [6] JIANG Bin, ORMELING F J. Cybermap: the map for cyberspace[J]. Cartographic Journal, 2013, 34(2):111-116.
- [7] 赵帆,罗向阳,刘粉林. 网络空间测绘技术研究[J]. 网络与信息安全学报,2016,2(9):1-11.
- [8] 刘效武,王慧强,赖积保,等. 基于多源异质融合的网络态势生成与评价[J]. 系统仿真学报,2010,22(6):1411-1415.
- [9] 席荣荣,云晓春,张永峥,等. 一种改进的网络安全态势量化评估方法[J]. 计算机学报,2015,8(4):749-758.
- [10] 陈兴蜀,曾雪梅,王文贤,等. 基于大数据的网络安全与情报分析[J]. 工程科学与技术,2017,49(3):1-12.
- [11] 陈成. 网络安全态势感知可视化平台的设计与实现[D]. 北京:北京邮电大学,2017.
- [12] BEJTILICH R. The practice of network security monitoring[J]. Network Security, 2014(10):4.
- [13] 兰远东,高蕾. 融合多智能技术的网络入侵检测模型[J]. 信息安全与技术,2014,5(4):31-37.
- [14] 霍彦宇. 基于杀伤链和模糊聚类的APT攻击场景生成方法的研究与设计[D]. 北京:北京邮电大学,2018.
- [15] 陈锋,苏金树,韩文报. 一种基于智能规划的攻击图快速构建方法[J]. 解放军理工大学学报(自然科学版),2008,9(5):460-465.
- [16] 孙鸿宇,何远,王基策,等. 人工智能技术在安全漏洞领域的应用[J]. 通信学报,2018,39(8):1-17.
- [17] YOON C, LEE S, KANG H, et al. Flow wars: systemizing the attack surface and defenses in software-defined networks[J]. IEEE/ACM Transactions on Networking, 2017(99):1-17.
- [18] 汤奕,李梦雅,王琦,等. 电力信息物理系统网络攻击与防御研究综述[J]. 电力系统自动化,2019,43(10):1-9,18.
- [19] 揣迎才,张明清,唐俊,等. 基于Agent的DDoS协同防御实体行为建模[J]. 计算机工程,2013,39(6):158-161.
- [20] 高昆仑,辛耀中,李钊,等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化,2015,39(1):48-52.
- [21] 许书彬,贾哲,张海峰. 基于SDN的网络特征动态隐藏技术[J]. 通信学报,2018,39(2):28-34.
- [22] LAM H Y. A hybrid security architecture for datacenters[C]//Proceedings of IEEE International Conference on Communications. Washington D. C., USA: IEEE Press, 2014:211-220.
- [23] MONTESINO R, FENZ S, BALUJA W. SIEM-based framework for security controls automation[J]. Information Management and Computer Security, 2012, 20(4):248-263.
- [24] 吴天雄,陈兴蜀,罗永刚. 大数据平台下应用程序保护机制的研究与实现[J]. 信息网络安全,2019(1):68-75.
- [25] 胡义香,李先义. 网络安全策略冲突分类及自动检测与恢复[J]. 微计算机信息,2007,23(21):54-56,78.
- [26] 陈周国,蒲石,郝尧,等. 网络攻击追踪溯源层次分析[J]. 计算机系统应用,2014,23(1):1-7.
- [27] 孙守鑫. DDoS攻击溯源与检测方法的研究[D]. 沈阳:辽宁大学,2016.
- [28] 贾召鹏. 面向防御的网络欺骗技术研究[D]. 北京:北京邮电大学,2018.
- [29] 孟祥君. 基于软件定义安全的智能蜜网技术研究[D]. 杭州:浙江大学,2019.
- [30] DANGELO G, RAMPONE S, PALMIERI F. An artificial intelligence-based trust model for pervasive computing[C]//Proceedings of IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. Washington D. C., USA: IEEE Press, 2016:154-164.
- [31] BEDI P, KAUR H, GUPTA B. Trust-based access control for collaborative systems[J]. Journal of Experimental and Theoretical Artificial Intelligence, 2014, 26(1):109-126.

(下转第193页)

(上接第 187 页)

- [32] 罗昌行,胡立勇,欧阳晋,等. 基于信任与授权的多方数据安全交换体系[J]. 计算机工程,2005,31(23):138-140.
- [33] 薛朝晖,向敏. 零信任安全模型下的数据中心安全防护研究[J]. 通信技术,2017,50(6):1290-1294.
- [34] 黄锦波,伍益明,常丽萍,等. 信任节点机制下的异构多智能体系统安全一致性控制[J]. 中国科学:信息科学,2019,49(5):599-612.
- [35] QAMAR S, ANWARZ, RAHMAN M A, et al. Data-driven analytics for cyber-threat intelligence and information sharing[J]. Computers and Security,2017,67:35-58.
- [36] ONWUBIKO C. Security operations centre: situation awareness, threat intelligence and cybercrime[C]//Proceedings of IEEE International Conference on Cyber Security and Protection of Digital Services. Washington D. C., USA: IEEE Press,2017:122-131.
- [37] 杨沛安,刘宝旭,杜翔宇. 面向攻击识别的威胁情报画像分析[J/OL]. 计算机工程:1-8 [2018-12-21]. <http://www.ecice06.com/CN/10.19678j.issn.1000-3428.0051157>.
- [38] 荣晓燕,宋丹娃. 基于大数据和威胁情报的网络攻击防御体系研究[J]. 信息安全研究,2019,5(5):383-387.
- [39] 王通,艾中良,张先国. 基于深度学习的威胁情报知识图谱构建技术[J]. 计算机与现代化,2018(12):21-26.
- [40] 徐锐,陈剑锋,刘方. 网络空间安全威胁情报及应用研究[J]. 通信技术,2016,49(6):758-763.
- [41] 李建春,谢瑞云,张旭博. 基于攻击图的智能制造系统安全风险量化分析方法[J]. 信息技术,2018,42(12):47-51,56.
- [42] 吴元立,司光亚,罗批. 人工智能技术在网络空间安全防御中的应用[J]. 计算机应用研究,2015,32(8):2241-2244.
- [43] 刘博,范渊,聂桂兵. 基于大数据技术的智能网络安全分析平台[J]. 信息技术与标准化,2018(9):73-76.

编辑 索书志