

## 基于跨域协同的网络空间威胁预警模式

熊钢, 葛雨玮, 褚衍杰, 曹卫权

(盲信号处理国家级重点实验室, 四川 成都 610041)

**摘要:** 网络空间威胁发展呈现出主动性、隐蔽性、泛在性的特点, 向传统被动式、局域性、孤立化的网络防御模式提出了严峻挑战。针对大数据、人工智能与网络安全融合的新趋势, 提出一种跨域协同的威胁预警模式, 为网络空间安全防护赋能增效。首先, 该模式从网络空间结构出发, 通过划分安全威胁域、解析系统功能、设计共享机制, 构建具有合纵连横作用的功能框架; 其次, 为提升威胁信息检测能力, 设计了分层司职的协同化技术体系, 阐述了威胁信息感知、处理、应用等关键技术; 最后, 借助应用场景, 定性化描述了所提预警模式的能力增量。

**关键词:** 网络防御; 人工智能; 流量大数据

**中图分类号:** TP393

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-109x.2020078

## Model of cyberspace threat early warning based on cross-domain and collaboration

XIONG Gang, GE Yuwei, CHU Yanjie, CAO Weiquan

National Key Laboratory of Science and Technology on Blind Signal Processing, Chengdu 610041, China

**Abstract:** The development of network threat shows the characteristics of initiative, concealment and ubiquity. It poses a severe challenge to the passive, local and isolated traditional network defense mode. In view of the new trend of integration of big data, artificial intelligence and network security, a cross-domain collaborative network threat early warning model was proposed, which could enable and increase efficiency for cyberspace security. Firstly, starting from the overall structure of the protected network space, the model constructs a cross-domain function framework with the vertical and horizontal conjunction by dividing the security threat domain, decomposing the system function, designing the information sharing mechanism. Secondly, to enhance the ability of threat information detection, the collaborative technology architecture is designed by the logic of hierarchical management, and the key technologies involved in threat information perception, processing and application, are systematically introduced. Finally, with the help of application scenarios, qualitatively the capability increment of the proposed threat early warning model was described.

**Key words:** Network defense, artificial intelligence, big traffic data

收稿日期: 2020-02-18; 修回日期: 2020-07-28

通信作者: 熊刚, xg1226@126.com

基金项目: 教育部重点基金项目 (6141A02011904)

**Foundation Item:** Key Foundation Project of Chinese Ministry of Education (6141A02011904)

论文引用格式: 熊钢, 葛雨玮, 褚衍杰, 等. 基于跨域协同的网络空间威胁预警模式[J]. 网络与信息安全学报, 2020, 6(6): 88-96.

XIONG G, GE Y W, CHU Y J, et al. Model of cyberspace threat early warning based on cross-domain and collaboration[J]. Chinese Journal of Network and Information Security, 2020, 6(6): 88-96.

## 1 引言

伴随网络空间战略地位的凸显，网络安全问题层出不穷，如病毒蠕虫、网络欺骗、拒绝服务攻击、数据泄露<sup>[1]</sup>。特别地，高级持续性攻击行为（APT 攻击）正成为网络威胁的重要来源，对此，业界一直在不懈努力和探索，已有研究成果可分为两类。

一类是以现有互联网体系为基础的“渐进式”方案，其主要进行安全“修补”“加固”“更新”等建设，以提高网络抗风险能力，如杀毒软件、防火墙等安全产品。该类技术侧重于解决局部性、单一性的安全问题，对整体网络空间威胁的缓解贡献仍不足。另一类是以未来新型网络体系设计为牵引的“革命式（clean slate）”方案<sup>[2]</sup>，其将安全性作为网络自身天然具备的基因，试图从根本上消除某些网络安全隐患，具体有软件定义网络<sup>[3]</sup>、拟态防御体系<sup>[4]</sup>等。该方案面临着建设成本高、时间周期长的压力。为此，面对大数据、人工智能发展的时代浪潮<sup>[5-6]</sup>，如何通过新技术实现对现有网络防御技术的赋能增效，成为网络空间安全领域亟待求证的命题<sup>[7]</sup>。

本文以网络空间纵深化防御思想为牵引，探索构建跨域联动、全局协同的网络威胁预警模式，以有效提升网络空间应对威胁风险的能力。

## 2 现状分析

### 2.1 威胁信息分析

网络威胁信息是指从多种渠道获取的用以描述网络资产安全状态的线索总和<sup>[8]</sup>。本文将所涉及的威胁信息划分为3类（如图1所示），具体内涵如下。

一是基础类威胁信息：诸如恶意文件 Hash 值、IP 黑名单、恶意域名、URL 列表、CVE 漏洞等较为普遍、容易获得的结构化基础数据。这类信息主要来源于网络安全设备（如防火墙）的观测度量和数据采集，或网络安全业务厂商（如赛门铁克、启明星辰）的专业分析与共享，用于安全分析的初始阶段。

二是攻击类威胁信息：与攻击事件相关联的网络或设备特征、攻击载荷、攻击源等结构化的属性信息和非结构化的文本信息。该类信息大多来源于安全分析人员或安全技术平台，对网络“黑市”或相关安全事件进行深入分析和定向挖掘，如卡巴斯基和安天公司先后发布的“方程式”组织分析报告<sup>[9]</sup>。

三是 APT 类威胁信息：以 APT 这类高级网络威胁为对象，可为政治、外交、经济等重大行动或国家战略制定提供支持的 TTP（Tactics（战术）、Techniques（技术）及 Procedures（过程））

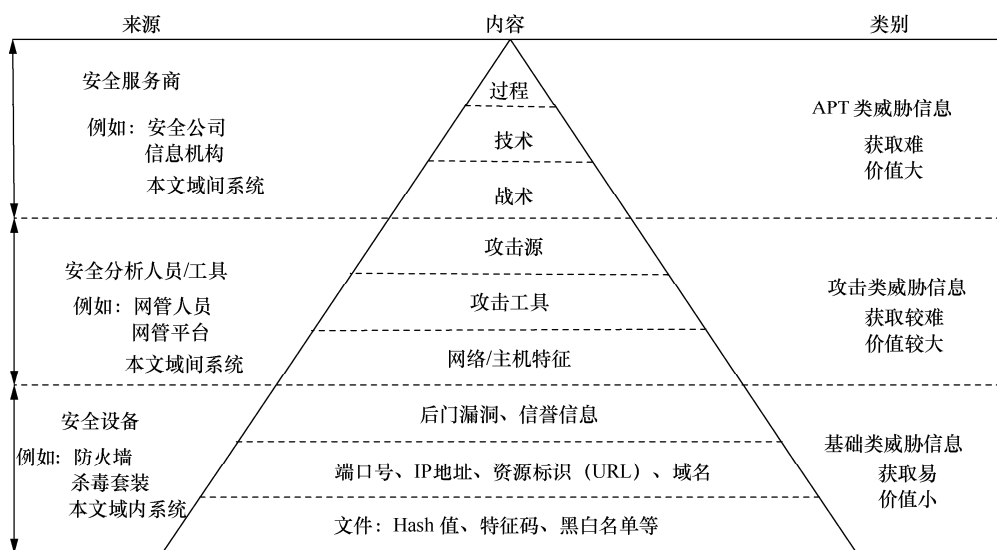


图1 威胁信息分类金字塔  
Figure 1 Pyramid of threat information classification

情报。该类信息包含丰富的知识内容和较强的逻辑关系，主要来源于具有专业能力的机构和人员长期、持续投入的分析，如火眼（FireEye）和 360 公司发布的 APT 报告。

## 2.2 预警能力分析

当前，网络威胁动机正由个人兴趣、利益驱使（如窃取用户账号）向政治、国家意图（如 APT 攻击）转变，这向现有网络防御建设提出了新挑战，具体表现如下。

一是安全防御理念的被动性难以应对网络威胁的主动性。传统以防火墙、入侵检测为代表的防御理念，本质上是一种“先问题后补救”的被动式理念。然而，网络威胁天生具有主动属性，无论是漏洞挖掘，还是预留“后门”，都是攻击者的精心设计，使被动网络防御疲于应对。

二是安全检测技术的片面性难以应对网络威胁的隐蔽性。现有安全防护措施呈现局部性、“烟囱式”的布局，导致各自检测结果的片面性，如杀毒软件、流量分析、运营商监控等安全手段“泾渭分明”。相反地，攻击者利用零日漏洞、流量伪装、匿名网络等伪装手段，使网络威胁呈现出高隐蔽性。

三是安全告警信息的孤立性难以应对网络威胁的泛在性。现有网络安全机制对告警信息的处理原则是自我建设、自我响应。然而，网络威胁通常具有泛在性，其体现在具有同类安全缺陷的网络设备（或业务）可能遭受相似攻击。因此，告警信息的孤立使用与网络威胁的泛在影响之间

存在失衡。

## 3 基于合纵连横的跨域功能框架

基于网络空间结构分解，本文以数据在不同结构间的串行传输为“纵向”，以数据在同一结构上的并行传输为“横向”，提出具有“纵横解剖、关联融合”核心理念的威胁预警功能框架。

### 3.1 安全威胁域

借助“网络自治域（AS 域）”的概念，本文将数据在网络空间中的处理、传输、交换等流程所经历的信息资产划分为 3 个安全威胁子域，即防护目标域、汇聚传输域、网络关口域，如图 2 所示。

防护目标域是受防护网络空间内需要保护的重点目标，通常是指重要职能机构、关键基础设施、核心敏感信息所涉及的重要网络资产，包括用户终端、数据服务器、智能传感器、局域网网关等。防护目标域内的网络资产是数据产生与处理、信息功能承载的实体，通常也是网络攻击的“靶标”。

汇聚传输域是数据在防护目标域与网络关口域之间交换的通道，主要包括边界路由器、程控交换机、数据中心、网络链路等，如市、局级汇聚路由，运营商数据中心。汇聚传输域作为受防护网络空间内的数据汇聚与传输的“高速公路网”，可被网络攻击用于数据“导航”。

网络关口域位于受防护网络空间与全球网络空间链接的位置，主要包括网络数据的出入链路

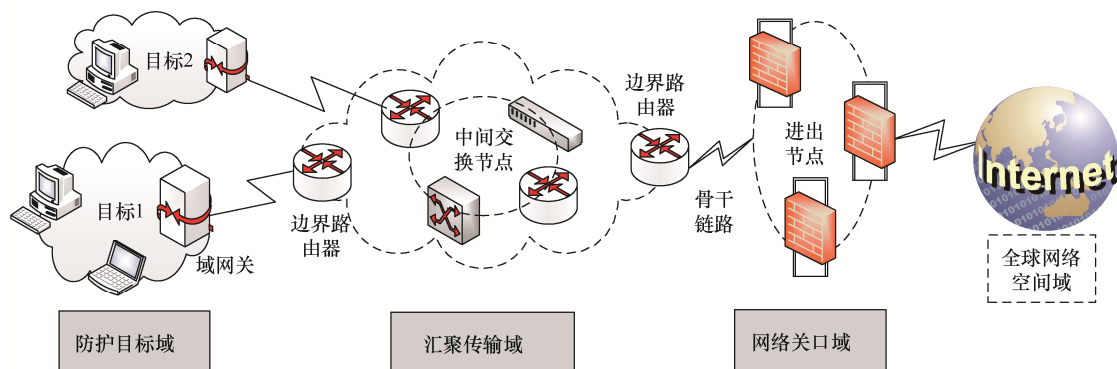


图 2 网络安全威胁域划分  
Figure 2 Division of network security threat domain

和节点，如 Internet 通信链路和主要节点。网络关口域主要用于实现全球网络空间的互联互通，是网络威胁数据的进出“门户”。

### 3.2 系统功能结构

基于安全威胁域划分，本节从“合纵连横”的思路出发，设计预警系统功能结构，如图3虚线框所示，包括域内威胁感知系统（简称“域内系统”）和域间信息协同管理系统（简称“域间系统”）。域间数据的串行传输为“纵向”，域内数据的并行传输为“横向”。

域间系统是整体预警系统的功能中枢，其主要用于实现“合纵”功能，即对纵向各域威胁信息的关联分析和预警信息管理。该系统以域内系统的上传数据信息为输入，并对其进行汇聚与融合，以大数据技术为支撑展开关联分析，形成对攻击行为的检测预警结果，以及产生新的检测规则信息下发到各域内系统。“合纵”功能模式的优势在于：一是充分利用各域子系统所感知到的

攻击行为的不同侧面信息，对同一攻击行为或事件进行更为清晰完整的刻画；二是信息融合后的集中管理与控制，可提高预警响应的效率。

域内系统是威胁数据采集站，其主要用于实现“连横”功能，即对域内网络资产的信息进行采集与汇聚，从而实现域内攻击信息的有效放大。域内威胁感知系统分为3个子系统：防护目标域威胁感知系统、传输汇聚域威胁感知系统、网络关口域威胁感知系统。“连横”功能模式的优势在于：一是各子系统的功能可以基于现有技术能力进行升级改造，避免建设上的重复；二是对域内威胁线索进行并行化检测，有利于细微或者隐蔽特征的挖掘。

### 3.3 信息共享机制

为有效解决威胁信息共享过程中的描述、传输、关联等问题，本节基于 OASIS 标准规范<sup>[10]</sup>，设计跨域威胁信息共享机制，如图4所示，主要包括3个信息共享的操作环节，分别是：域内威

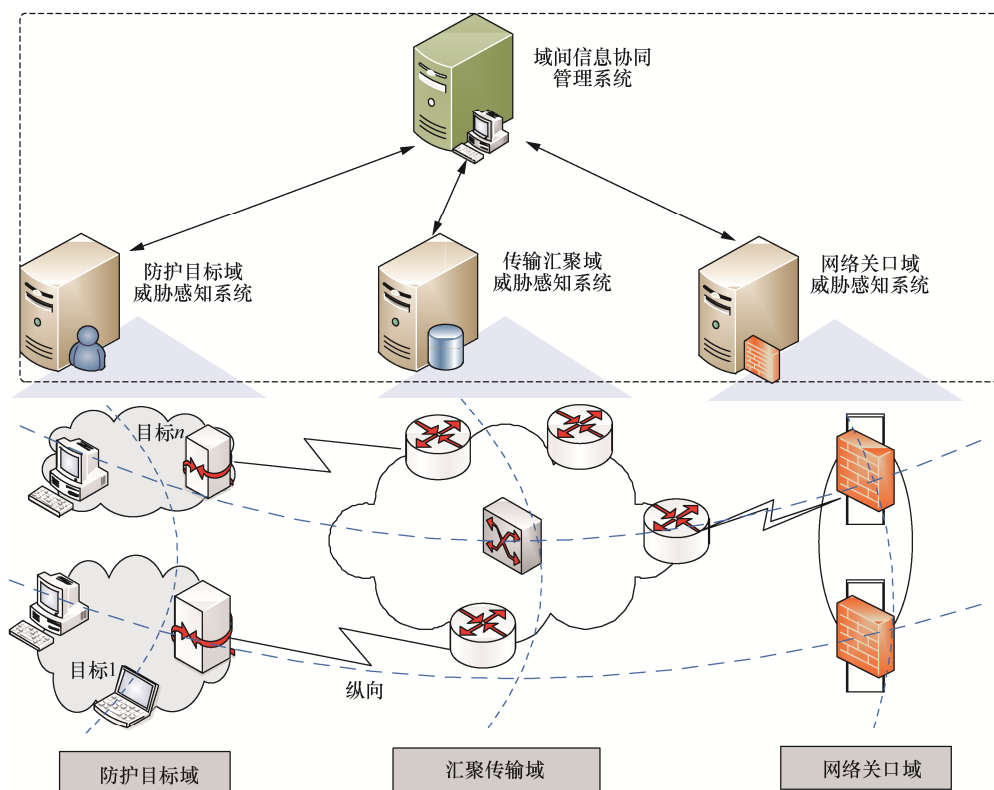


图3 跨域威胁预警的功能结构

Figure 3 Functional structure of cross domain threat early warning

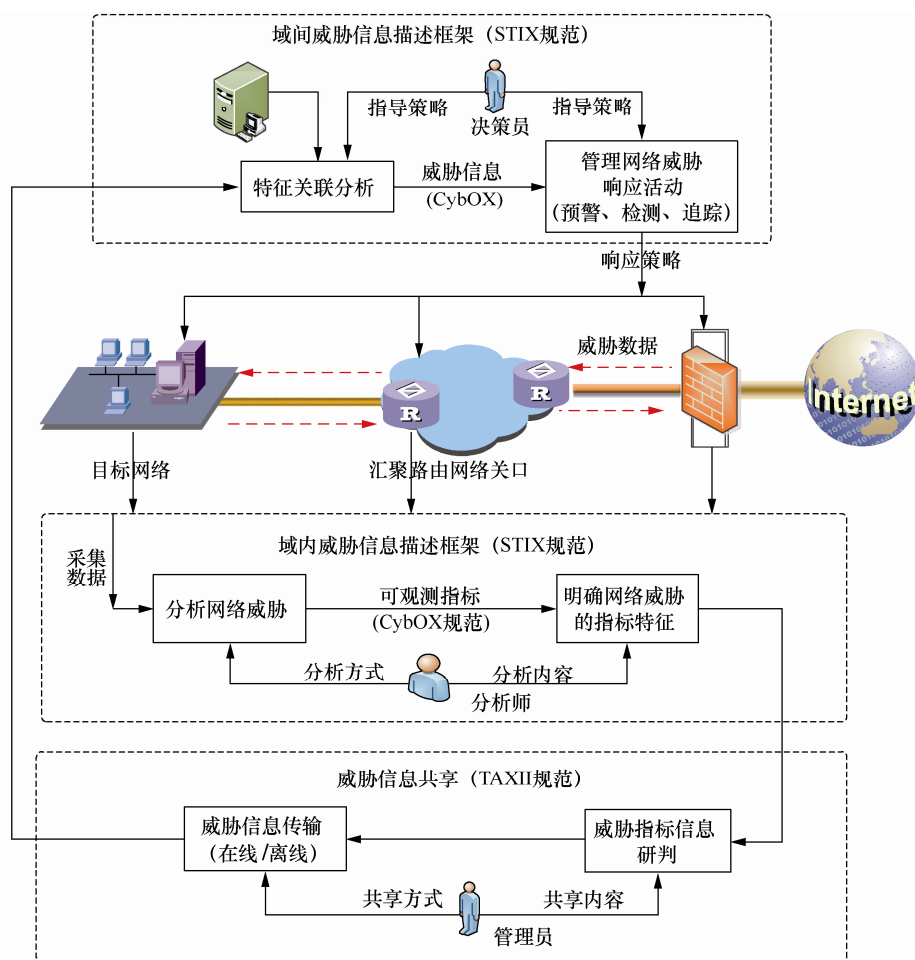


图 4 威胁信息共享机制流程  
Figure 4 Flow of threat information sharing mechanism

胁信息描述、威胁信息共享、域间威胁信息描述。

域内威胁信息描述是指将各安全威胁域的采集数据转换为威胁信息的过程，基于 STIX (structured threat information eXpression) 和 CybOX (cyber observable eXpression) 规范进行描述。其中，网络威胁分析是指分析师对采集到的数据进行识别、评估和分类。明确威胁指标特征是指对威胁情境及其相关数据的可观测度量，建立威胁描述指标特征，如恶意邮件的源 / 目的 IP。

威胁信息共享是指实现各域内威胁描述信息研判与传输的过程，基于 TAXII (trusted automated eXchange of indicator information) 规范实现。信息研判是指网络管理员通过共享决策机制，决定威胁信息的共享范围、途径、方式等内容，如共享恶意附件等信息。信息传输是指域内信息向域

间系统进行信息汇集的过程，包括离线传输和在线传输。

域间威胁信息描述是指将各域内威胁信息转化为预警响应决策的过程，基于 STIX 规范和 CybOX 规范进行描述。其中，威胁信息关联分析是对接收到的域内威胁信息进行关联分析，形成高价值的威胁预警分析结果。威胁响应管理是指根据预警结果制定检测规则、漏洞修复、配置更新等威胁响应决策，如分析恶意邮件威胁态势等响应。

#### 4 基于分层司职的协同技术体系

本节以高效获取网络威胁信息为目标，对关键技术进行层次化编排，提出“分层司职”的协同技术体系，如图 5 所示。其中，基础技术层位于域内系统，协同技术层和应用技术层位于域间系统。

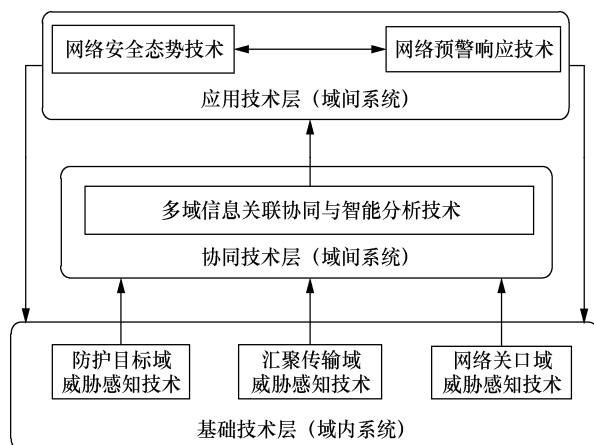


图5 协同技术体系分层结构

Figure 5 Hierarchical structure of collaborative technology architecture

#### 4.1 面向威胁感知的基础技术层

基础技术层主要是对各安全威胁域进行数据采集与分析,以获得基础类威胁信息。根据各域职能划分,基础技术层涉及的技术分为3类,如图6所示。

##### (1) 网络关口域威胁感知技术

网络关口域主要面对大规模流量数据,其威胁感知依赖于网络异常流量检测技术,具体挑战如下。一是海量高速流量建模。网络关口流量速率通常为百 Gbit/s 甚至 Tbit/s 数量级,以全流量采集或单一业务类型为主的传统局域网流量模型难以适用,需要发展抽样统计模型、信号分析(如小波变换)等复杂环境下的流量建模方法。二是流量特征工程。传统流量特征提取主要依赖于研究者的精心设计和长期经验积累,而深度学习等人工智能分析方法的发展能够促进特征提取的智

能化和自动化。三是未知/隐蔽的流量检测。网络威胁利用加密、协议伪装等手段,使流量数据的内容分析更为困难。

##### (2) 汇聚传输域威胁感知技术

汇聚传输域内的网络设备(如路由器)具有较好的连通性和汇聚性,主要技术手段在于识别恶意网络目标,具体如下。一是恶意样本捕获技术。为了获取网络攻击所采用的攻击手段、攻击载荷、攻击武器等威胁线索,可利用汇聚传输域的数据优势,构建蜜罐、蜜网等高仿真诱捕环境,捕获恶意样本信息。二是恶意节点识别技术。由于路由、交换等设备在数据传输上的重要性,汇聚传输域内的网络节点通常被恶意利用,以产生攻击跳板、路由劫持、中间人攻击等威胁行为,需要研究网络设备身份认证、目标属性判证等技术,以获取恶意节点威胁信息。

##### (3) 防护目标域威胁感知技术

防护目标域的威胁主要源于病毒、木马、未知插件等恶意代码对设备、数据等信息资产进行的恶意操作,具体技术如下。一是资产脆弱性分析,通过对域内的软硬件系统、应用程序等功能部件进行漏洞、后门测试分析,以获取其潜在风险影响。或者通过安全组件(防火墙等)对网络运行状态进行监控,以获取安全日志信息。二是攻击行为特征分析,针对进入域内的潜在威胁对象(木马程序、恶意文件等),通过静态分析(操作码、反编译等)和动态分析(API调用、沙箱执行等)相结合,提取操作行为特征作为威胁信息。

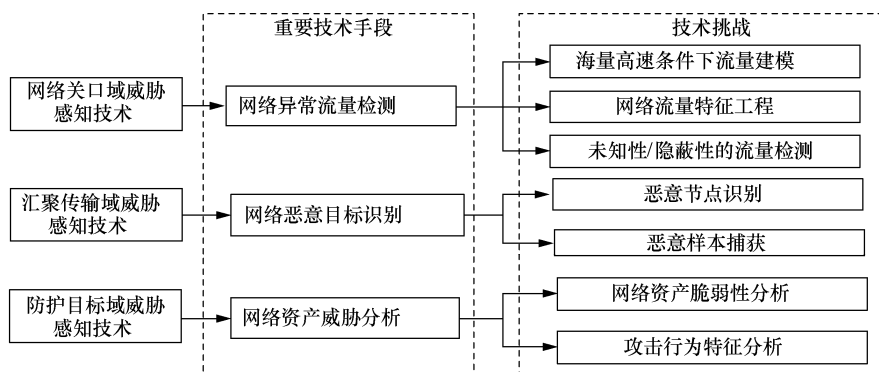


图6 基础技术层分析

Figure 6 Analysis of basic technology layer

## 4.2 面向信息融合的协同技术层

协同技术层是域间系统的核心技术环节，用于对域内系统基础威胁信息进行管理和协同利用，以生成攻击类威胁信息，并为应用层提供技术支撑。协同处理各域内威胁信息有助于实现特征间信息互补以及威胁信息碎片的串联，进而提升威胁检测的精度和效率，具体技术手段及挑战如图7所示。

### (1) 威胁大数据协同处理技术

威胁大数据的协同处理技术需要实现对各域内系统所得多源异构威胁数据进行统一处理和关联利用。一是需要研究威胁大数据预处理方法，对大量异构的基础信息进行数据集成、规约、编排、存储、查询等统一处理，提高信息利用效率；二是需要数据挖掘分析方法，对预处理后的数据原材料进行逻辑关联、关系挖掘等精加工处理，提高数据的利用价值；三是构建威胁信息的知识图谱，实现同一威胁事件或威胁源的信息关联，提升协同分析性能。例如，通过建立攻击组织的IP列表、木马工具、攻击手法等数据资源的知识图谱，可以实现目标精细监测、信息快速关联等目的。

### (2) 人机协同的智能分析技术

人机协同的攻击智能分析技术需要解决现有

检测技术仅依赖于人工研判（效率低、漏警高）或仅依赖于机器学习（缺乏可解释性、虚警率高）的问题。近年来，在大数据资源驱动下，以深度学习为代表的人工智能技术在文本、语音、图像等领域取得突破，并且正逐步向网络安全领域拓展，表1列举了部分应用。

基于分支领域的应用，人工智能技术将会向多源协同、人机交互、行为分析等网络安全的综合应用发展。为此，需要进一步开展的研究包括：一是利用循环神经网络、卷积神经网络、对抗学习网络等深度学习方法，构建具有自我学习和自动更新能力的威胁检测平台，提高检测工作效率；二是设计人机交互机制，通过引入专家知识的反馈，提高人工智能对网络威胁行为检测的可解释性，提高检测准确性。

## 4.3 面向安全预警的应用技术层

应用技术层是域间管理系统的辅助技术环节，其目的是对协同层的攻击类威胁信息进行综合分析，以生成高价值的威胁信息，并支撑安全预警响应，重点关注的技术如下。

### (1) 网络安全态势分析技术

网络安全态势分析是基于协同层的攻击信息，提炼出包含攻击行为的战术、技术、过程等

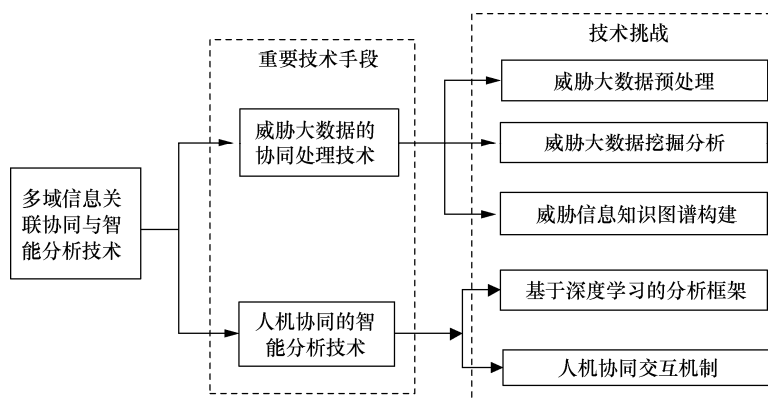


图7 协同技术层分析

Figure 7 Analysis of collaborative technology layer

表1 网络安全中的人工智能应用举例

Table 1 Examples of artificial intelligence application in network security

| 安全域   | 应用场景                   | 智能算法                  |
|-------|------------------------|-----------------------|
| 网络关口域 | 异常流量检测，恶意域名检测……        | 以支持向量机、深度学习等有监督学习算法为主 |
| 汇聚传输域 | 僵尸网络检测，网络舆情分析……        | 以K近邻、高斯模型等无监督学习算法为主   |
| 防护目标域 | 恶意文件检测，恶意应用检测，系统漏洞分析…… | 以半监督算法为主（有监督和无监督相结合）  |

意图的高价值威胁信息。具体支持技术包括：一是安全风险度量技术，通过对威胁信息进行定量描述，为安全态势的数值化分析和精确度量奠定基础；二是安全态势推理技术，基于量化的威胁信息，利用数理模型、逻辑推导、群体智能等理论工具，挖掘网络威胁态势中的潜在规律或意图。

## (2) 网络威胁预警响应技术

网络威胁预警响应技术主要是利用域间和域内系统提供的威胁信息，指导预警策略的生成。该技术结合威胁信息的具体特征和跨域协同模式的结构特点，以最优化解理论为指导，形成预警响应的指导策略。例如，根据威胁信息的价值大小决策响应操作的强度和广度，根据攻击威胁的技术手段决策预警信息作用的安全威胁域，根据威胁信息的安全态势决策预警操作时间分配。

## 5 应用场景

基于上述跨域协同预警模式的功能框架和技术体系，本节阐述威胁信息在该网络预警模式中的具体应用，如图8所示，其中，短虚线表示域间纵向场景，长虚线表示域内横向场景。

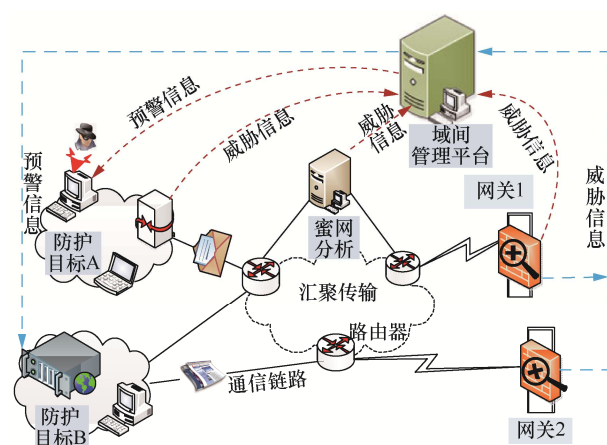


图8 跨域协同模式应用场景

Figure 8 Application scenario of cross domain and collaboration model

在纵向应用场景中，网络关口1的流量分析、汇聚传输域的蜜网分析以及防护目标域的防火墙日志在工作过程生成了相应的基础威胁信息（如可疑的IP、恶意的邮件信息、隐蔽通信的痕迹），通过域间管理平台对基础威胁信息的协同关联分析，得到攻击类威胁信息（即“某黑客组织通过钓鱼攻击方式对防护目标A进行窃密型攻击”）。

根据攻击信息的指导，制定预警策略，对目标A内黑客正在攻击或可能攻击的重要终端设备进行安全防护。

在横向应用场景中，网络关口1和网络关口2通过分析各自的流量数据得到，有大量的外部IP通向境内同一IP的流量数据，进而各自将该情况作为威胁信息上报共享。域间管理系统对网络关口的域内信息进行协同分析，得到境内IP对应的防护目标B内的重要服务器正遭受外来DDoS攻击，进而生成相应的预警信息，对防护目标B进行安全防护。

基于上述设计，本文研发的域间原型系统的测试界面如图9所示。在某数据平台的测试表明，该系统通过日志检索、目标管理、流量IP等信息的综合处理，能够及时有效地发现木马、蠕虫、黑市工具、僵尸网络、APT攻击、勒索软件等网络威胁。



图9 域间原型系统测试界面

Figure 9 Test interface of inter domain prototype system

## 6 结束语

针对传统网络威胁检测模式的不足，本文以网络空间纵深防御思想为指导，设计跨域协同的网络威胁预警模式，提升网络威胁预警能力的主动性和联动性。所提模式的特点可以概括为“跨域框架、技术协同、联动响应”，具体技术贡献如下。一是设计“合纵连横”的跨域预警功能框架，实现对现有独立网络安全能力的有机整合与赋能提效，避免各安全功能组件的各自为战、重复建设。二是编排以威胁大数据感知和智能化处理为核心的协同技术体系，实现碎片化威胁信息的综合利用，提升高价值网络威胁情报的生产能

力。三是具备全局化的联动响应能力,改变现有自我预警响应的方式,通过威胁信息共享和预警策略生成,实现各安全域的联动响应与预先防护。当前,APT攻击、网络勒索等新威胁向网络空间安全提出了严峻挑战,后续研究将加快推进对所提预警模式的功能机制和关键技术的研发、实验和优化工作。

### 参考文献:

- [1] 方滨兴. 定义网络空间安全[J]. 网络与信息安全学报, 2018, 4(1): 1-5.  
FANG B X. Define cyberspace security[J]. Chinese Journal of Network and Information Security, 2018, 4(1): 1-5.
- [2] 黄韬, 刘江, 霍如, 等. 未来网络体系架构研究综述[J]. 通信学报, 2014, 35(8):184-197.  
HUANG T, LIU J, HUO R, et al. Survey of research on future network architectures[J]. Journal on Communications, 2014, 35(8):184-197.
- [3] 谭晶磊, 张红旗, 雷程, 等. 面向SDN的移动目标防御技术研究进展[J]. 网络与信息安全学报, 2018, 4(7): 1-12.  
TAN J L, ZHANG H Q, LEI C, et al. Research progress on moving target defense for SDN[J]. Chinese Journal of Network and Information Security, 2018, 4(7): 1-12.
- [4] 邬江兴. 拟态计算与拟态安全防护的原意和愿景[J]. 电信科学, 2014, 30(7): 2-7.  
WU J X. Meaning and vision of mimic computing and mimic security defense[J]. Telecommunications Science, 2014, 30(7): 2-7.
- [5] 付钰, 李洪成, 吴晓平, 等. 基于大数据分析的APT攻击检测研究综述[J]. 通信学报, 2015, 36(11): 1-14.  
FU Y, LI H C, WU X P, et al. Detecting APT attacks: a survey from the perspective of big data analysis[J]. Journal on Communications, 2015, 36(11): 1-14.
- [6] 张蕾, 崔勇, 刘静, 等. 机器学习在网络空间安全研究中的应用[J]. 计算机学报, 2018, 41(9): 1943-1975.  
ZHANG L, CUI Y, LIU J, et al. Application of machine learning in cyberspace security research[J]. Chinese Journal of Computers, 2018, 41(9): 1943-1975.
- [7] 杨德全, 刘卫民, 俞宙. 基于蜜罐的主动防御应用研究[J]. 网络与信息安全学报, 2018, 4(1): 57-62.  
YANG D Q, LIU W Q, YU Z. Research on active defense application based on honeypot[J]. Chinese Journal of Network and Information Security, 2018, 4(1): 57-62.
- [8] 杨沛安, 武杨, 苏莉娅, 等. 网络空间威胁情报共享技术综述[J]. 计算机科学, 2018, 45(6): 9-18.  
YANG P A, WU Y, SU L Y, et al. Overview of threat intelligence sharing technologies in cyberspace[J]. Computer Science, 2018,

45(6): 9-18.

- [9] Antiy CERT. 从“方程式”到“方程组”EQUATION攻击组织高级恶意代码的全平台能力解析[EB].  
Antiy CERT. From “equation” to “equation group”, full platform capability solution of advanced malicious code of EQUATION attack organization[EB].
- [10] 李建华. 网络空间威胁情报感知、共享与分析技术综述[J]. 网络与信息安全学报, 2016, 2(2):16-29.  
LI J H. Overview of the technologies of threat intelligence sensing, sharing and analysis in cyber space[J]. Chinese Journal of Network and Information Security, 2016, 2(2): 16-29.

### [作者简介]



熊钢(1986-), 男, 四川绵阳人, 博士, 盲信号处理实验室助理研究员, 主要研究方向为网络安全设计、网络异常检测。



葛雨玮(1991-), 男, 四川成都人, 硕士, 盲信号处理实验室工程师, 主要研究方向为网络流量分析、二进制分析。



褚衍杰(1982-), 男, 山东枣庄人, 博士, 盲信号处理实验室副研究员, 主要研究方向为网络体系安全、态势感知。



曹卫权(1989-), 男, 河北宁晋人, 博士, 盲信号处理实验室助理研究员, 主要研究方向为软件安全、智能信息处理。