Software Engineering and Applications 软件工程与应用, 2020, 9(5), 403-411
Published Online October 2020 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2020.95046

Hans汉斯

面向卫星通信网络的威胁情报关键技术

董　坤[1]，李　序[2,3*]，刘艳梅[1]，李　洋[1]，张海霞[2]，黄克振[2,3]

[1]中国卫通集团有限公司，北京
[2]中国科学院软件研究所可信计算与信息保障实验室，北京
[3]中国科学院大学，北京
Email: *lixu@tca.iscas.ac.cn

收稿日期：2020年10月2日；录用日期：2020年10月16日；发布日期：2020年10月23日

摘　要

随着卫星通信网络的逐步推广应用，如何保障此类新型网络环境的安全性成为业界的关注重点。本文提出将威胁情报相关技术引入卫星通信网络的安全防护工作，分析了卫星通信网络威胁情报面临的技术挑战，提出了面向卫星通信网络的威胁情报技术架构，对其中关键的威胁情报分析挖掘技术进行了阐述，并对未来研究工作进行了展望。

关键词

网络安全，威胁情报，卫星通信网络，数据治理，人工智能

Key Technologies of Threat Intelligence for Satellite Communication Network

Kun Dong[1], Xu Li[2,3*], Yanmei Liu[1], Yang Li[1], Haixia Zhang[2], Kezhen Huang[2,3]

[1]China Satellite Communications Co. Ltd., Beijing
[2]Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing
[3]University of Chinese Academy of Sciences, Beijing
Email: *lixu@tca.iscas.ac.cn

Received: Oct. 2nd, 2020; accepted: Oct. 16th, 2020; published: Oct. 23rd, 2020

Abstract

With the gradual promotion and application of satellite communication networks, how to ensure

*通讯作者。

文章引用: 董坤, 李序, 刘艳梅, 李洋, 张海霞, 黄克振. 面向卫星通信网络的威胁情报关键技术[J]. 软件工程与应用, 2020, 9(5): 403-411. DOI: 10.12677/sea.2020.95046

the security of this new type of network environment has become the focus of the industry. This paper proposes to introduce threat intelligence related technologies into the security protection work of satellite communication networks, analyzes the technical challenges faced by satellite communication network threat intelligence, and proposes a threat intelligence technology architecture for satellite communication networks, conducts analysis and mining technologies of key threat intelligence, and makes a prospect of the future research work.

Keywords

Cyber Security, Threat Intelligence, Satellite Communication Network, Data Governance, Artificial Intelligence

1. 引言

近年来，随着网络信息化的不断深入与创新，网络安全形势越来越严峻，高级持续性攻击成为网络空间面临的严重威胁。攻击过程精心策划，攻击方法错综复杂，常导致严重的数据泄露或者系统破坏。攻击者不断改变现有攻击方式，开发新型攻击工具，无法通过恶意程序签名实现实时检测，单纯依赖防火墙、入侵防御系统和反病毒软件已无法阻止这些攻击。急速增长的网络攻击催生了威胁情报的诞生。

Gartner 将威胁情报生命周期划分为六个阶段：定向、收集、处理、分析、传递、反馈。其中威胁情报分析对于安全态势的评估、威胁预测及防御系统的提升至关重要。威胁情报通常是多源异构的海量数据，必须对掌握的情报进行多源信息融合、挖掘有用信息、关联分析、推理预测，才能使威胁情报发挥出真正的价值，有效地推演预测未来的安全态势、攻击者身份和攻击手段，从而帮助安全人员给出恰当的应对防护措施。

网络攻击的目标对象已经从传统的网络领域逐渐扩展到以物联网、工业控制系统、大数据平台、卫星通信网络为代表的新型网络应用环境。针对此类新型网络，应用环境的安全防护也是国家网络安全等级保护制度所强调的工作内容。本文研究如何将威胁情报技术引入到卫星通信网络的安全防护中。

传统通信卫星经过长年发展，已积累了一定的网络安全技术基础，包括物理层及链路层抗干扰技术、信源及信道加解密技术等。但伴随宽带卫星网络在我国的正式应用，卫星网络的应用模式发生了巨大变化，安全环境也面临巨大挑战，主要体现在：

(1) 卫星通信网络结构由简单变复杂，与 IP 技术高度融合；

(2) 卫星通信网络规模由较小规模变为超大规模，百万量级的在线用户容量将是常态；

(3) 卫星通信网络业务不再受带宽制约而变得更加丰富；

(4) 通信设备面临新一轮的技术更新；

(5) 卫星通信网络面临更深层次、更广范围、更多信息类型与传输协议的威胁。

目前通用的网络安全技术多围绕地面网络展开，而卫星通信网络的应用在多个领域已经开始探索，单纯使用原有网络安全技术不足以满足其网络安全需求，近年来陆续发生了一系列相关的安全事件，印证了卫星通信网络安全机制的缺陷。针对卫星通信网络的安全防护工作，引入威胁情报相关技术，有利于帮助防御系统及时掌握面向卫星通信网络及系统的安全威胁和风险，增强精准性安全防护和主动防御。

本文第二章对卫星通信网络进行简要介绍，第三章介绍威胁情报的定义、分类及技术现状，第四章提出卫星通信网络的威胁情报技术架构，第五章阐述针对卫星通信网络的威胁情报分析挖掘技术，最后对全文进行总结。

2. 卫星通信网络

卫星通信是安置在地球上(包括海陆空)的无线电通信站之间利用卫星作中继站接收、转发、反射无线电波，在两个或多个地球站之间或手持终端或航天器之间的通信[1]，主要包括卫星固定通信、卫星移动通信、卫星直接广播和卫星中继通信四大领域。卫星通信网络是以具有星上处理功能的卫星为主要通信实体，结合相关地面网络操作控制中心、地面网关和地面用户组建的互联互通的卫星群体网络[2]。

卫星通信系统主要包括两个部分：中继接力站(通信卫星部分)和终端站(地球站部分)。通信卫星是用于信息通信的人造地球卫星，分为空间平台和有效负荷两部分，空间平台主要包括卫星的控制、监测等，有效负荷是设在空中的接力站，由天馈线和通信转发器组成；地球站包括基带设备、射频设备、天馈线设备、监控设备等。卫星通信的主要原理是将卫星发射到赤道上空 3600 km 处的对地静止轨道上，利用卫星上的通信转发器接收由地球站发射的信号，并对信号进行放大变频后，转发给其它地球站，从而完成两个地球站之间的传输。卫星通信具有频带宽、通信容量大、通信距离远、通信时不受复杂地理条件的限制、通信质量高和系统可靠性强等特点，在军用和民用领域中都得到了广泛应用，因此安全问题也日益成为卫星通信网络研究中的重要方面。

3. 威胁情报

3.1. 威胁情报相关定义

威胁情报的概念提出之后，很多机构或学者都曾对威胁情报的定义进行阐述。目前工业界和学术界对威胁情报还没有形成统一的定义，常被引用的是 Gartner 公司给出的定义[3]：“威胁情报是关于 IT 或信息资产所面临的现有或潜在威胁的循证知识，包括情境、机制、指标、推论与可行建议，这些知识可为威胁响应提供决策依据”。Forrester 公司认为“威胁情报是针对内部和外部威胁源的动机、意图和能力的详细叙述，可以帮助企业和组织快速了解到敌对方对自己的威胁信息，从而帮助提前威胁防范、攻击检测与响应、事后攻击溯源等能力”。SANS 研究院给出的威胁情报的定义为：“针对安全威胁、威胁者、利用恶意软件、漏洞和危害指标所收集的用于评估和应用的数据集”[4]。i SIGHT 认为：“网络威胁情报是关于已经收集、分析和分发，针对攻击者和其动机、目的和手段，用于帮助所有级别安全和业务员工用于保护其企业核心资产的知识”[5]。

3.2. 威胁情报分类

目前，针对威胁情报的分类多种多样，本文摘取有代表性的三种分类方法介绍如下：

3.2.1. 基于使用对象的分类

Chismon 等人[6]根据威胁情报针对的使用对象的不同，将威胁情报划分为四类：战略情报、运营情报、战术情报、技术情报。战略情报主要面向高层管理人员，包括大环境下或大背景下的攻击来源、攻击危害、攻击者使用的资源与能力等宏观信息，主要是关于攻击趋势、财务影响以及可能影响高层决策的信息；运营情报是关于针对组织即将发生攻击的信息，由高级安全人员使用，例如安全经理或事件响应团队的负责人；战术情报主要面向安全分析人员或安全响应人员，通常被称为战术、技术和程序(TTP)，是关于威胁参与者如何进行攻击的信息，帮助安全响应人员确保应对当前情况准备对应的防御战术；技术情报则为安全人员或安全设备可以直接操作或读取的情报，如具体的远控域名、恶意 IP、恶意样本哈

希值等。

3.2.2. 基于应用场景的分类

基于不同的应用场景，威胁情报可以分为：归属情报、检测情报、指向情报和预测情报。归属情报根据行为证据指向特定攻击者，解决威胁行为人是“谁”的问题；检测情报识别在主机和网络上观察到的安全事件，解决威胁行为是“什么”的问题；指向情报帮助预测哪些用户、设施或者网络实体可能成为定向攻击的目标，解决威胁行为针对“谁”的问题；预测情报通过行为模式来预测威胁事件的发生，解决威胁行为接下来会“怎样”的问题，与态势感知密切相关。

3.2.3. 基于数据类型与价值密度的分类

基于情报的数据类型与价值密度，威胁情报可以分为情报数据、情报信息、情报知识三层。情报数据包括样本、IP 指纹、域名解析记录、WHOIS 信息、数字证书等，特点是数量巨大，更新频率相对较低；情报信息包括样本\IP\域名\URL\邮箱等的黑白类信誉以及 C&C 远控信息，特点是经过分析研判，具有较强的时效性；情报知识包括安全事件报告、攻击手法 TTP、黑客组织画像等，特点是量少，价值最高，非结构性强，主要由人工分析挖掘而成。

3.3. 威胁情报挖掘分析技术现状

(1) 数据提取与治理

威胁情报来源广泛，数量庞大，价值密度低，对其进行分类整理并从中提取有价值信息有助于情报分析工作。研究人员将 Map Reduce 体系结构引入到威胁情报的数据治理[7]，使用机器学习算法对威胁情报进行分类。Graf R 等人利用深度自编码器挖掘情报中潜在的语义信息，实现自动化网络事件分类[8]。Noor U 等人[9]将深度学习技术应用到高级威胁指标的提取，高级威胁指标(TTP、软件工具和恶意软件等攻击模式)在网络威胁归因中具有很大的作用，但在非结构化的技术报告中无法实现自动化的机器读取，因此通过建立针对高级威胁指标的通用词汇表，利用语义搜索技术从技术报告中直接提取高级威胁指标。

(2) 情报分析

利用关联分析、时间序列、流数据分类等技术来进行威胁情报分析，有助于从复杂的海量信息中提取出高价值的威胁特征[7]，挖掘出信息之间的隐藏关联，从而更清晰地了解攻击者的攻击手段或当前的整体安全态势。王通[10]使用本体模型对威胁情报进行关联分析，利用知识图谱可视化技术直观地展示威胁情报的要素与关系；吕宗平[11]利用获取到的威胁信息对选取的特征属性计算信息熵，通过频繁模式挖掘进行关联分析；卿斯汉[12]通过对网络蠕虫行为模式的分析，提出一种基于网状关联分析的网络蠕虫预警方法。

(3) 攻击溯源

目前大多数威胁情报分析模型都是基于攻击链模型和钻石模型[11]。攻击链模型根据攻击者对攻击目标系统入侵的不同阶段划分，将各个阶段按顺序连接起来形成完整的攻击过程，基于攻击链模型的威胁情报分析通过还原攻击的每一个阶段来还原整个攻击过程；钻石模型建立的基本元素是入侵事件，每个事件都有四个核心特征，即对手、能力、基础设施及受害者，通过连线来代表它们之间的关系，并布置成菱形。也有学者将人工智能技术引入来帮助预测威胁源[9]。

针对卫星通信网络的安全防护工作，引入威胁情报技术，需要能够为情报的不同使用对象提供相应的情报内容，同时也要能够根据应用场景、数据类型需求及价值密度需求，提供相应维度的威胁情报，因此在威胁情报分析中，要能够依据各个标准对情报进行分类，并能够综合利用治理、分析和攻击溯源等技术手段，对卫星通信网络中收集到威胁情报数据进行挖掘分析。

4. 面向卫星通信网络的威胁情报技术架构

将威胁情报应用于卫星通信网络的防护系统中，面临着以下主要挑战：一是需要广泛且可信的威胁情报来源，利用掌握的威胁情报实现安全事件的提前告警、威胁预测、风险评估等。二是卫星通信网络的拓扑架构存在动态性，诸多地面用户终端具有移动性、可扩展性的特点。三是威胁情报数据的鲜活性问题。互联网中每天包含了百万级甚至数亿的危害指标，但是根据调查[13]，57%的受访专业人士表示获得的威胁情报大多数已经过时，而且大多数可用的商业和开源威胁情报产品并没有发挥足够的作用[14]。四是威胁情报的针对性问题。卫星通信网络的安全防护需要大量针对特定设备(如 VSAT 终端设备、信关站设备等)的威胁情报，及时掌握相关设备的漏洞隐患和新型攻击方式，这方面的威胁情报数据极为缺乏。

威胁情报分析过程需要自动化分析与人工分析相结合，才能更深地挖掘出情报价值，卫星通信网络已经呈现与 IP 技术高度融合的趋势，其网络边界的特殊性、协议特殊性和传输特殊性都是现有安全技术没有深入覆盖的研究领域，对于卫星通信网络中的威胁情报分析专业人才也较为缺乏。

卫星通信网络安全需求与传统的地面网络安全需求是一致的[2]，包括：可用性(卫星网络即使受到攻击，仍然能在需要时提供有效的服务)、机密性、完整性以及身份认证(应能对通信中的对等实体和数据来源进行鉴别，如空中卫星应能够鉴别地面或终端的合法性)与访问控制。如图 1 所示，依据国家网络安全等级保护制度对新型通信网络的安全要求，围绕卫星通信网络的安全需求，将威胁情报技术架构分为四个层次，即：数据采集层、数据治理层、分析验证层、安全保障业务层。下面详细介绍技术架构的每个层次。

4.1. 情报采集层

情报采集层主要负责从各种数据源采集威胁情报数据。根据卫星通信网络保护对象的特点，将情报数据分为通用威胁情报和专项威胁情报两类。

通用威胁情报主要包括恶意文件、恶意 IP/域名、漏洞信息、攻击组织等。通用威胁情报可以来自系统内部产生的威胁信息，同时国内外有很多开源或商业威胁情报平台可以提供此类情报，国外的威胁情报提供方包括 AlientVault OTX、RSA Netwitness Live、Blue coat、SANS 等，国内有微步在线、360 网络威胁中心、绿盟、Freebuf 等。

专项威胁情报主要包括卫星通信网络专用设备、协议、应用服务相关的威胁情报，例如 VSAT 终端设备被植入的恶意文件、信关站设备的安全漏洞等。此类情报依赖于专业人员的分析，可以通过对相关网页、论坛、博客等网站进行信息爬取获取对应信息，更主要的是通过专项的漏洞挖掘和渗透测试工作，挖掘分析卫星通信网络专业设备、网络协议及应用服务所存在的漏洞、恶意文件等情报要素。

4.2. 数据治理层

数据治理层负责对采集的多源异构威胁情报数据进行清洗、标准化、标签、融合、质量管理等工作。

数据清洗是对采集到的威胁情报数据进行筛选，清除重复数据、噪声数据和无效数据，并对数据准确性进行验证。数据标准化对异构的数据进行统一格式化处理，形成标准格式、统一维度的威胁情报数据，便于存储和分析使用；数据标签是根据数据来源、类型、时间、影响对象、地区、行业等维度对威胁情报数据进行标记，作为后续自动关联分析的基础[15]；数据融合是利用多源融合技术对采集到的数据进行归并和关联，解决数据中可能存在的冲突信息等；数据质量管理是对生成的各类威胁情报及其原始数据的质量进行评价、反馈和管控，以期不断提高威胁情报数据对于卫星通信网络安全保障工作的实际效果。

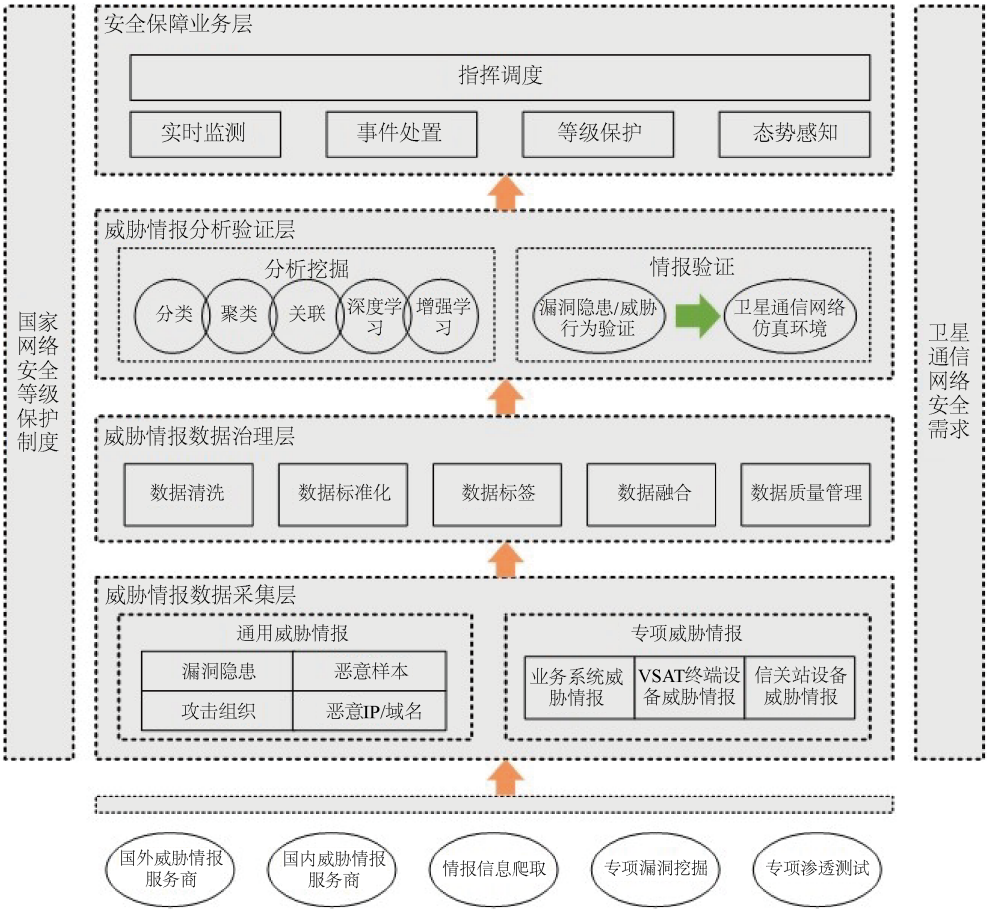

Figure 1. Threat intelligence technology framework for satellite communication network
图 1. 面向卫星通信网络的威胁情报技术架构

4.3. 分析验证层

分析验证层一方面采用关联分析、数据分类等数据挖掘算法和新型人工智能算法，对威胁情报要素数据进行分析挖掘。其中，关联分析对威胁情报的各个维度进行关联，发现其中的相关性，进而实现事件分析、攻击溯源等，例如通过对关联预警信息中的 IP、域名、漏洞信息等，可以掌握安全事件的上下文，从而制定响应措施；数据分类即对威胁情报根据使用对象、应用场景、数据类型和价值密度进行分类，以满足不同人员、使用场景的业务需求；新型人工智能算法典型的如深度学习、增强学习等神经网络算法，对于提高隐含知识发掘、深度关联信息发掘、威胁情报智能推理、未知威胁预测能力等具有显著效果。

另一方面，分析验证层通过搭建卫星通信网络的模拟仿真环境，对采集到的各类威胁情报数据(如漏洞隐患、恶意样本文件等)以及分析预测结果进行仿真环境验证，以确认其对实际网络的影响程度和影响范围，支撑卫星通信网络的安全保护实战工作。

4.4. 保障业务层

基于威胁情报数据的采集、治理、分析，为卫星通信网络提供指挥调度、实时监测、态势感知、事件处置、等级保护等安全保障业务支撑。指挥调度是依据卫星通信网络的安全策略，围绕当前安全状况、资产状况、网络威胁状况、漏洞隐患状况等，通过分析、研判、会商，提出安全决策，指挥相关模块完

成安全保障工作；实时监测是利用威胁数据对卫星通信网络的安全状况进行实时监控分析，发现或预测正在发生或将要发生的安全事件；态势感知是在实时监测的基础上，对卫星通信网络的总体安全态势进行评估展示，并感知重要威胁、重大漏洞的威胁形势；事件处置是根据预定的应急预案，针对监测发现的安全事件采取有效的处置措施，及时弥补安全漏洞，消除安全事件影响，恢复系统正常运行；等级保护是按照国家网络安全等级保护制度，围绕等级保护技术要求和管理要求，开展卫星通信网络及应用系统的安全定级、备案、建设、整改、委托测评等工作。

5. 卫星通信网络的威胁情报分析挖掘技术

本章基于前面所给出的威胁情报技术架构，针对卫星通信网络的安全需求，阐述以下三类关键技术的核心内容。

5.1. 威胁情报大数据治理

卫星通信网络覆盖范围广泛，网络攻击形式复杂，威胁情报数据的来源异构多样，数据的种类繁杂、数量庞大，需要对威胁情报数据进行全方位的存储管理和治理工作，提高威胁情报数据的准确性、有效性和鲜活性，同时保证威胁情报数据的安全，避免数据被越权使用。

大数据治理技术已在金融、电信、能源等行业中得到了应用，国内外学者针对数据治理也进行了一系列的研究[16]，提出了很多数据管理模型，综合考虑了数据安全、隐私保护、质量管理、数据分析等方面的需求。

大数据治理技术种类多样、功能各异，不同技术的相互融合会带来更好的效果，目前主要有四种大数据治理模式：

(1) 元数据治理模式以元数据治理为核心，同时融合数据标准治理和数据安全治理，以确保元数据管理服务的规范性和安全性；

(2) 质量治理模式通过质量检验指标的制定与维护、数据质量告警、质量问题的分析和管理等，实现对数据的绝对质量管理与过程质量管理；

(3) 安全治理模式，利用数据加密工具、数据脱敏工具、数据库安全工具、数据防泄漏工具、数字水印技术、身份认证技术等保障企业数据的安全；

(4) 主数据治理模式通过对业务数据的整合、管理，提供数据建模、数据地图、数据集市和数据全生命周期管理。

面向卫星通信网络的威胁情报大数据治理要有效融合上述四种治理模式，从而对威胁数据进行系统化的治理，有效支撑卫星通信网络的安全保障工作。

5.2. 业务驱动的威胁情报挖掘

在互联网时代，几乎所有行业包括金融、电信、能源、医疗、教育等都面临着严峻的网络安全挑战。搜集威胁情报，通过挖掘分析来感知正在发生或将要发生的网络威胁，将会对各个行业的网络安全防护工作至关重要。

卫星通信网络所使用的终端设备、信关站设备、网络协议及相关业务应用与其他行业存在较大差异，卫星网络用户的业务种类繁多、需求不同、通信内容繁杂，因此针对卫星通信卫星通信网络的安全威胁、攻击方式、攻击组织、攻击资源等情报要素也必然与其他行业不同，需要结合卫星通信网络中威胁情报使用者的业务特征和安全需求，采集符合卫星业务安全需求的威胁情报，设计适合的威胁情报分析流程及挖掘算法，结合业务特征进行情报挖掘，才能使威胁情报在卫星网络安全保障中发挥实战作用。

5.3. 基于人工智能的威胁情报分析推理

近年来，人工智能技术在很多研究领域中取得了非常好的成果，包括制造业、零售业、金融业、教育业等等。人工智能技术是充分挖掘数据的潜在价值的有效手段[17]，有研究人员将人工智能应用到网络威胁情报的分析中，可以实现对威胁情报的智能推理，并对其发展的态势进行推演，有利于提升系统的安全防御能力。

在大规模、大容量、IP 融合化应用的卫星通信网络中，依靠人工推理远远无法实现及时地安全决策和应对，人工智能技术将在很大程度上提升威胁情报的处理速度，根据卫星网络安全状况的实时监测数据，根据威胁情报要素建立卫星网络安全知识图谱，直观展示网络中重大安全事件或威胁源的信息，利用 MapReduce 和 Spark 实现基于人工智能的图谱推理算法，实现对未知安全威胁及行为的预测，这方面的典型技术有卷积神经网络(CNN)、递归神经网络(RNN)、长短时记忆网络(LSTM)等，利用此类神经网络技术对卫星通信网络中的大量威胁情报进行快速学习、迭代和智能推理，能够为安全事件的监测发现、应急处置、预警预测提供准确、及时的参考依据。

6. 小结

本文主要介绍了当前卫星通信网络的安全形势以及目前的威胁情报相关技术，提出了卫星通信网络的威胁情报技术架构。将威胁情报引入卫星通信网络的安全防护工作，可以全方位掌握威胁信息，对当前的网络安全环境做出判断，进而预测未来即将发生的威胁。针对卫星通信网络的威胁情报工作，情报数据的挖掘分析是实现目标的关键，包括对已有数据的关联分析、数据挖掘、质量评估等技术。为了实现自动化的威胁预警和智能推理，需要将大数据治理、人工智能相关技术手段与现有的挖掘分析技术相结合，以卫星通信网络的安全防护需求为驱动，提高威胁情报的准确性、鲜活性，重点关注卫星通信网络专业设备、协议、应用服务等相关情报数据的采集和分析，从而有效提高卫星通信网络的安全防护和主动防御能力。

参考文献

[1] 张更新. 卫星移动通信系统[M]. 北京: 人民邮电出版社, 2001.

[2] 王晓梅, 张铮, 冉崇森. 关于宽带卫星网络安全问题的思考[J]. 电信科学, 2002(12): 38-41.

[3] McMillan, R. (2013) Definition: Threat Intelligence. Gartner Research. G002 49251.

[4] Southern African Neuroscience Society (2016) SANS Information Security Research. http://www.sans.org

[5] Fire Eye Inc. (2016) I SIGHT Parters. http://www.isightpartners.com

[6] Chismon, D. and Ruks, M. (2015) Threat Intelligence: Collecting, Analysing, Evaluating. MWR Infosecurity, UK Cert, United Kingdom.

[7] Graf, R. and King, R. (2018) Neural Network and Blockchain Based Technique for Cyber Threat Intelligence and Situational Awareness. In: 2018 10*th International Conference on Cyber Conflict*, Tallinn, 29 May-1 June 2018, 409-426. https://doi.org/10.23919/CYCON.2018.8405028

[8] 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.

[9] Noor, U., Anwar, Z., Amjad, T., *et al.* (2019) A Machine Learning-Based FinTech Cyber Threat Attribution Framework Using High-Level Indicators of Compromise. *Future Generation Computer Systems*, **96**, 227-242.

[10] 王通. 威胁情报知识图谱构建技术的研究与实现[D]: [硕士学位论文]. 北京: 中国电子科技集团公司电子科学研究院, 2019.

[11] 吕宗平, 钟友兵, 顾兆军. 基于攻击链和网络流量检测的威胁情报分析研究[J]. 计算机应用研究, 2017, 34(6): 1794-1797, 1804.

[12] 卿斯汉, 文伟平, 蒋建春, 马恒太, 刘雪飞. 一种基于网状关联分析的网络蠕虫预警新方法[J]. 通信学报, 2004(7): 62-70.

[13] Ponemon (2013) Live Threat Intelligence Impact Report 2013. Tech. Rep., Ponemon Institute Research Report.

[14] Ring, T. (2014) Threat Intelligence: Why People Don't Share. *Computer Fraud & Security*, **2014**, 5-9. https://doi.org/10.1016/S1361-3723(14)70469-5

[15] 薄明霞, 唐洪玉, 冯晓冬. 基于大数据的安全威胁情报分析与共享平台技术架构研究[J]. 电信技术, 2019(11): 5-9.

[16] 马朝辉, 聂瑞华, 谭昊翔, 林嘉洺, 王欣明, 唐华, 杨晋吉, 赵淦森. 大数据治理的数据模式与安全[J]. 大数据, 2016, 2(3): 83-95.

[17] 郭平, 王可, 罗阿理, 薛明志. 大数据分析中的计算智能研究现状与展望[J]. 软件学报, 2015, 26(11): 3010-3025.