DOI：10.19364/j.1674-9405.2024.06.009

水利部网络威胁情报中心研究与应用

邹　希，殷　悦，张　潮，詹全忠

（水利部信息中心，北京 100053）

摘　要：为不断提高水利网络安全威胁感知、监测预警、应急响应能力，提出融合网络威胁情报的水利网络安全防护框架，基于水利部网络安全大数据平台，建立水利部网络威胁情报中心，实现网络威胁情报汇集、私有情报生产和多类型情报输出，将水利部网络威胁情报中心与水利部网络安全威胁感知决策指挥系统等进行对接，实现网络威胁情报赋能威胁狩猎、预警响应、攻击溯源等应用场景。研究成果已在水利行业网络安全日常防护、重要时期安全保障中得到应用，可有效提升水利部及水利行业单位网络安全防护水平，在网络安全防御体系构建中具有参考价值和实践意义。

关键词：网络安全；网络威胁情报；威胁感知；监测预警；应急响应

中图分类号：TP393.08　　**文献标识码：**A　　**文章编号：**1674-9405(2024)06-0055-06

0　引言

没有网络安全就没有国家安全。当前，百年未有之大变局正在加速演进，不稳定、不确定因素日益增多，国际格局复杂多变，针对关键信息基础设施的高级可持续威胁（APT）、数据窃取等事件频发，国家网络安全形势复杂严峻[1]。

在此背景下，全方位了解攻击者的信息，在网络安全对抗过程中抢占主动地位变得至关重要，而由网络威胁情报（CTI）驱动的网络安全防御是高效应对复杂网络威胁的关键[2]。与军事情报在传统战争中的作用类似，网络威胁情报作为已知或潜在网络威胁的信息，可协助网络安全人员快速甄别和了解网络威胁的来源、性质、攻击手段等，从而获取网络攻防对抗中“知己知彼”的信息优势，使得主动防御有章可循[3]。

水利是国家关键信息基础设施重要行业之一。近年来，水利部以水利网络安全顶层设计为指引，以水利关键信息基础设施为安全保护对象，坚持“实战化、体系化、常态化”理念，构建水利关键信息基础设施网络安全综合防御体系，不断提升水利关键信息基础设施“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”能力[4]。其中，水利网络威胁情报是重要的安全基础设施和服务，为水利网络安全主动防御、精准防护提供重要情报支撑。因此，为提升水利部网络安全威胁感知、监测预警、应急响应等能力，实现网络安全防护“关口前移”，水利部打通网络威胁情报汇集、分析、使用、共享等各个环节，建立水利部网络威胁情报中心[5]。

1　网络威胁情报

1.1　网络威胁情报概念

网络威胁情报至今没有统一的标准定义，相关机构和专家对网络威胁情报的定义主要有：1）著名咨询公司 Garter 定义。威胁情报是一种基于证据的知识，对网络资产可能存在或出现的风险、威胁，给出相关联的场景、机制、指标、内涵及可行的建议等，可为主体响应相关威胁或风险提供决策信息[6]。2）Friedman 等[7]定义。Friedman 等在《Definitive Guide to Cyber Threat Intelligence》中对网络威胁情报的定义是，通过各种方式收集、分析、传播的关于攻击者动机和企图及方法的知识，用于帮助各层级的安全和业务人员保护企业关键资产。3）网络安全机构 SANS 定义。SANS 在发布的《2020 SANS Cyber Threat Intelligence（CTI）Survey》中对网络威胁情报的定义是，满足利益相关者特定需求并经过分析加工的有关攻击者能力、机会和意图的信息[8]。4）网络安全公司 CrowdStrike 定义。网络威胁情报为理解威胁主体的动机、目标、攻

收稿日期：2024-06-23

基金项目：国家重点研发计划项目（2021YFB3900600）；水利青年拔尖人才资助项目（JHQB202214）

作者简介：邹希（1995—），男，湖北荆州人，硕士，工程师，主要从事水利信息化和网络安全研究工作。E-mail：zouxi@mwr.gov.cn

击行为而收集和处理及分析的数据[9]。

总结上述定义，网络威胁情报应包含以下内涵：1）网络威胁情报是一种经过加工、提炼的信息/知识；2）网络威胁情报描述了攻击者/威胁主体的意图、动机、目标；3）网络威胁情报包含了攻击者/威胁主体使用的方法、技术、工具，以及攻击行为；4）网络威胁情报提供了降低/响应相关威胁的建议。

1.2 网络威胁情报层次

网络威胁情报可分为广义和狭义 2 类网络威胁情报，在网络安全日常运营中广泛应用的攻击 IP、域名、文件哈希（Hash）等失陷指标（IoC）均属于狭义的网络威胁情报，是广义网络威胁情报分类中的技术情报。广义的网络威胁情报还包括年度网络安全威胁分析报告和行业网络安全态势报告等宏观的、全局的、总结性的战略情报，针对特定组织即将发生或预测的与攻击有关的运营情报，以及针对具体攻击者使用的工具、手法、传播渠道的战术情报。

广义的网络威胁情报按照获取难度、准确度、价值大小，可以通过如图 1 所示的金字塔模型表示层次[10]。越往金字塔的顶端代表被攻击者越难监测和防御，这种情报的价值就越大，提供这类情报也越难[11]。

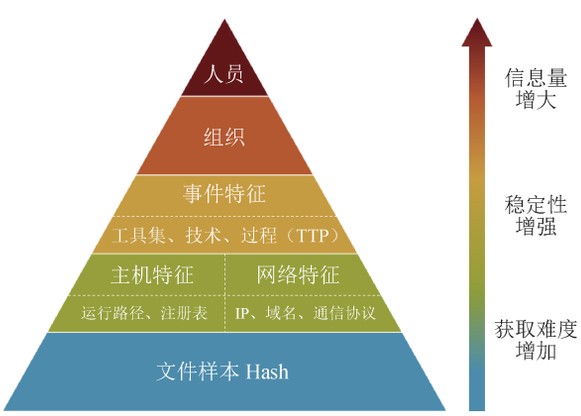

图 1 网络威胁情报层次金字塔

各类网络威胁情报的特点分析如下：

1）文件样本 Hash 是最底层的威胁情报，如恶意文件的 MD5（消息摘要算法）或 SHA（安全散列算法）值，由于散列函数具有雪崩效应，攻击者对恶意文件进行简单修改即可躲避检测，因此该类威胁情报虽能提供准确的信息但实际作用有限，防御效果较低。

2）主机和网络特征是现阶段使用最广泛的威胁情报，如恶意代码运行时写入的注册表项、文件路径，攻击者使用的 IP、域名等，这些特征可通过终端安全防护产品和网络流量检测设备获取，能提供一定的威胁情报信息，具有一定的防御效果。

3）事件特征是攻击者使用的 TTP（战术、技术和程序），通常通过对大量样本进行各个维度的相似度分析，可将同一家族的恶意软件归类到一起，这类基于事件特征的情报使得防护更具针对性，同时可显著降低防护成本。

4）组织和人员是事件特征的进一步分析，是对攻击事件背后组织者和实施者的挖掘，如同一黑客团伙可能会使用相同的攻击工具或者固定的传播渠道，通过对多个攻击事件特征的收集和分析，可分辨出攻击事件背后的同一组织或团伙，进而定位到威胁产生的根源。

1.3 主流网络威胁情报平台

目前，世界各国都越来越重视网络威胁情报的作用和价值。美国在 2015 年成立了网络威胁情报整合中心（CTIIC），负责整合分析各个部门收集到的情报，并为其他部门提供分析报告。2017 年《中华人民共和国网络安全法》颁布施行，明确建立国家网络安全监测预警和信息通报制度，为加强我国网络安全信息收集、分析和通报工作提供了法律依据。

随着网络威胁情报成为网络安全防御的重要技术手段，越来越多的组织、机构、网络安全公司建立了商业或开源威胁情报平台，包括国外的 AlienVault Open Threat Exchange，SANS Internet Storm Center，IBM X-Force，VirusTotal 和 ThreatMiner，国内的网络安全威胁情报共享平台（CNTD）、网络安全威胁信息共享平台、网络安全威胁和漏洞信息共享平台（CSTIS）、360 安全大脑情报中心、微步在线威胁分析与情报共享社区、天际友盟威胁情报中心、绿盟威胁情报中心、腾讯安全威胁情报中心等。

这些国内外网络威胁情报平台主要依靠收集掌握的互联网 IP、域名、域名系统（DNS）解析记录、文件样本等数据进行情报生产，具有数据量大、跨行业跨地域等特点，但同时也存在购买成本较高、无法完全符合行业单位特定需求等缺点，特别是面对越来越普遍的针对性攻击行为，商业或开源情报往往无法提供更多有价值的情报支持。

经过多年的建设，水利部已建成覆盖全国 32 个省级水行政主管部门的水利骨干网，并通过流域省区网、水利地区网延伸至市县级水利部门，部署了防汛抗旱、水资源管理等信息系统，显著提升了水利业务

数字化、网络化、智能化水平，但同时也带来越来越严峻的网络安全挑战，迫切需要提升水利行业网络安全威胁感知、监测预警、应急响应等能力。因此，根据水利行业网络环境和业务需求，基于水利行业网络安全数据，开展水利行业私有情报生产逐渐成为水利网络安全建设的重要内容。

2　水利部网络威胁情报中心研究

2.1　现状基础

水利部在部机关互联网、水利骨干网等网络出口边界，以及内部业务区和互联网服务区等网络区域，配备了流量探针、入侵检测、蜜罐等设备，并接入主机、终端等日志，采集网内流量日志和安全告警，在水利骨干网各节点部署流量监测设备，收集行业各单位水利业务网流量日志和安全告警，统一存储到水利部网络安全大数据平台。目前，水利部网络安全大数据平台已存储 PB 级的数据，日均增长数据近 2 TB，形成原始库、基础库、主题库、实时数据库等多个数据仓库。同时，建设了水利部网络安全威胁感知决策指挥系统，研发了威胁检测、异常检测、行为分析等算法模型，用于网络安全威胁感知、分析决策、事件处置等，具备了网络威胁情报生产的数据基础和应用场景。

2.2　技术框架

按照水利网络安全总体框架的布局，网络威胁情报数据属于网络安全数据采集的重要组成部分[12]，为网络安全威胁感知、决策指挥提供情报支撑。因此，水利部网络威胁情报中心情报包括通过加密的 API 接口接收外部的第三方情报，以及将水利网络安全数据中发现的攻击行为、漏洞数据、恶意文件等转换为对应的私有情报数据。

水利部网络威胁情报中心先利用水利部网络安全大数据平台提供的存储、计算资源，汇集安全数据和生产私有情报，形成水利网络威胁情报。再通过查询接口等，将网络威胁情报提供给水利部网络安全威胁感知、决策指挥等系统，辅助实现更为精准高效的威胁感知、分析决策、事件处置等。与此同时，水利部网络安全威胁感知系统的告警结果也重新反馈到水利部网络威胁情报中心，用以改进和优化威胁情报的质量及效果。此外，水利部网络威胁情报中心还向水利行业单位提供情报服务，并实现与上级主管部门的协同。基于威胁情报的水利网络安全防护框架如图 2 所示，水利部网络威胁情报中心架构如图 3 所示。

水利部网络威胁情报中心包括情报汇集、生产、输出等功能模块。以内部安全数据和外部获取情报为数据底座，以大数据处理技术和情报分析算法为生产引擎，以分等级高质量情报输出为目标，水利部网络威胁情报中心实现对多源网络安全数据的集中汇集、私有情报的生产，输出规范、可用、有价值的情报，进而赋能威胁感知、决策指挥等过程，并形成一个相互促进的循环。

2.3　威胁情报汇集

情报汇集是基础，指从第三方获取外部情报数据。水利部通过加强与网络安全主管部门、网络安全科研院所、第三方安全公司等合作，建立威胁情报共享机制，不断拓宽外部威胁情报的来源渠道。威胁情报汇集如下：

1）网络安全主管部门。水利部与中央网络安全和信息化委员会办公室（以下简称中央网信办）、公安部等有关平台实现系统对接，通过在线方式获取权威威胁情报，及时接收中央网信办、公安部等通报信息

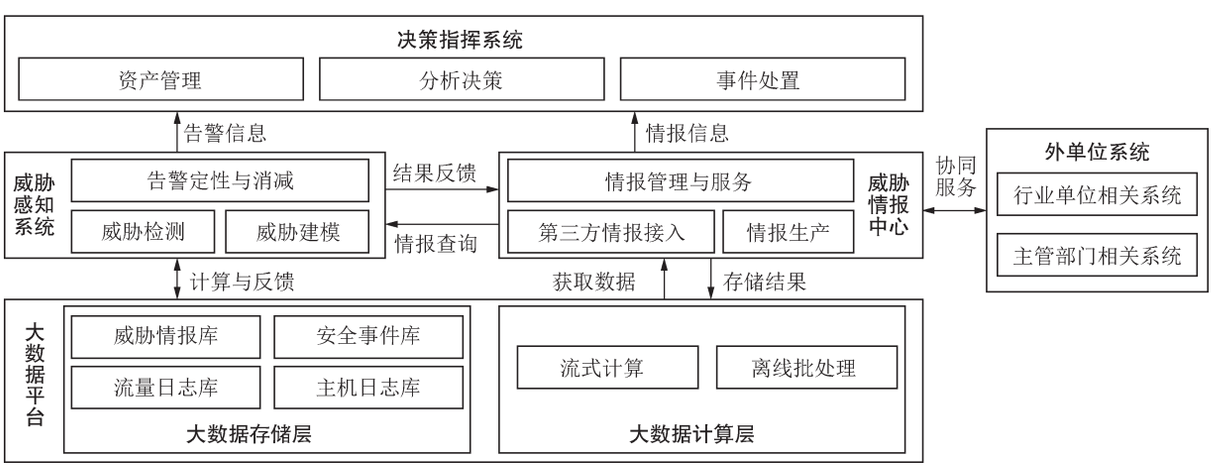

图 2　基于威胁情报的水利网络安全防护框架

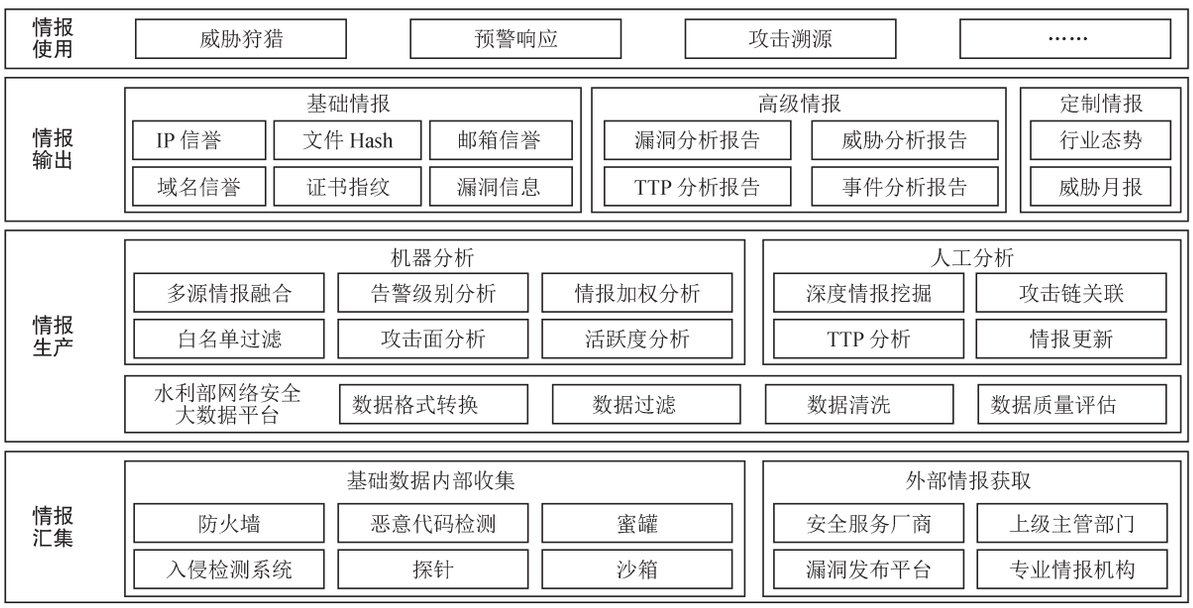

图 3 水利部网络威胁情报中心架构图

和预警提示，并转化为行业威胁情报数据。

2）网络安全科研院所。水利部与有关科研机构及高校合作，共享黑客组织、漏洞、恶意文件、失陷 IP 等情报。

3）第三方安全公司。水利部与国内知名网络安全公司合作，通过接口调用、推送更新等方式获取各厂商商业威胁情报，并合作开展互联网和暗网上涉及水利行业的情报监控收集。

2.4 威胁情报生产

情报生产是重点，指利用水利部网络安全大数据平台汇集的水利行业网络流量、安全日志等网络安全数据，生成水利行业私有情报数据。不同的网络安全设备记录的数据格式不尽相同，同时，同一网络访问行为的流量记录经过反向代理、负载均衡、安全网关等设备后，IP 地址也各不相同，因此不同来源的网络安全数据需要经过标准化处理、关联分析、深度挖掘后，才能转换为适用于水利行业日常网络安全运营的高质量私有威胁情报。威胁情报生产具体步骤如下：

1）通过正则表达式匹配等方法，从不同来源的流量和告警数据中提取告警时间、原因、IP 等字段。

2）采用 IP 地址关联、同源识别聚类、时间窗口分析、攻击关系图分析等算法，将同一访问行为、相同告警 IP、相似攻击行为的告警进行关联，生成初步的私有威胁情报。

3）结合告警数据的来源权重、严重级别、活跃频次、攻击范围等 4 个方面，为私有威胁情报生成置信度、严重程度等标签。a. 来源权重。根据告警数据来源（告警设备）本身的可信度衡量私有威胁情报的置信度。不同告警设备的可信度权重，通常根据日常运营中此类告警设备产生告警的准确度经验值设定。b. 严重级别。根据告警设备对告警的严重级别定义衡量私有威胁情报的严重程度。通常将严重程度分为严重、高、中、低、信息 5 个程度，分别赋予 5，4，3，2，1 分。c. 活跃频次。针对攻击 IP 等威胁情报在不同告警设备上的告警次数与出现天数进行统计和计算，从而确定私有威胁情报的活跃度。d. 攻击范围。对攻击 IP 等威胁情报产生告警的告警设备数量进行统计，从而确定私有威胁情报的攻击面。

对本地流量、告警数据进行分析生成本地私有威胁情报后，还需要与第三方威胁情报数据进行比对。对于存在第三方威胁情报库的威胁情报，结合第三方威胁情报数据对本地私有威胁情报进行上下文富化。

2.5 威胁情报输出

情报输出是目的。威胁情报生成后，威胁情报以文件 Hash 和 IP 信誉、域名信誉、邮箱信誉、证书指纹等形式存储在水利部网络威胁情报中心，并同步发送至水利部网络安全大数据平台。目前，水利部网络威胁情报中心主要有以下 6 种情报：1）恶意攻击者情报，包括攻击者 IP、归属地、危险级别、攻击资产、攻击手段等信息；2）恶意文件情报，包括文件名称、后缀名、MD5 值、影响危害、受影响资产等信息；3）资产高危漏洞情报，包括资产 IP、所属单位、漏洞情况、被攻击情报、修复建议等信息；4）重要系统攻击预警情

报，包括系统名称、部署范围、漏洞情况、攻击者等信息；5）失陷资产情报，包括资产 IP、所属信息系统、所属单位、失陷方式、横向探测情况、攻击者等信息；6）零日漏洞情报，包括漏洞名称、影响软硬件、紧急修复建议、受害资产等信息。

此外，水利部网络威胁情报中心根据接入的流量、告警、情报等数据，综合分析生成 TTP、漏洞、威胁、事件等分析报告，也可以根据网络安全运营人员指定输入，生成威胁月报、行业态势报告等。

截至 2024 年 6 月，水利部网络威胁情报中心有 IP 信誉 28.2 亿条，IoC 97.8 万个，安全漏洞 29.6 万个，零日漏洞 131 个，高级情报报告 263 份。

3　水利部网络威胁情报中心应用

网络威胁情报的应用可以贯穿于网络安全攻击防御的整个环节：网络攻击发生前，利用网络威胁情报提前感知风险，防患于未然；网络攻击发生时，基于网络威胁情报精准识别攻击线索，提升安全设备告警处置准确度；网络攻击发生后，借助网络威胁情报高效溯源[13]。网络威胁情报在网络攻击前中后 3 个阶段的应用可以抽象为威胁狩猎、预警响应及攻击溯源 3 个方面。

水利部网络威胁情报中心提供了 3 种情报迅速分发渠道，分别是通过水利数据交换平台进行情报数据交换共享，通过水利蓝信等通信工具进行通知提醒，通过页面查询和接口调用等进行情报查询检索。各水利单位可通过接收水利部共享的情报数据，或通过 IP、域名、MD5、情报来源、资产名称、攻击方式等多角度进行情报查询。

3.1　威胁狩猎

依托水利部网络威胁情报中心，以及水利蓝信、水利网络安全工作平台等信息通报平台，水利部建立水利网络安全联防联控机制，围绕网络安全脆弱性、威胁和事件等情报，实现情报共享、内外协同、上下联动[14]。对于恶意攻击者、恶意文件、资产高危漏洞、零日漏洞等急需处理的情报，水利行业相关单位收到共享的情报数据后，结合本单位终端安全检测、漏洞扫描、资产测绘、流量探针等设备及其日志数据，对情报数据的攻击者和受攻击资产进行归类分析整理，开展潜在威胁、攻击者的搜索排查，迅速发现潜在的攻击企图和相关系统的漏洞，组织展开内部排查和漏洞协同修复，从而在攻击发动之前提前消除隐患，将攻击阻断在发生之前。

3.2　预警响应

网络攻击发生时，水利部网络安全威胁感知系统通过调用水利部网络威胁情报中心的情报接口，实现文件 Hash 和 IP 信誉及恶意域名等的实时自动查询，在情报数据的精准支撑下，利用恶意 IP 访问扫描、重要资产恶意外联等与情报相关的检测算法模型，迅速匹配攻击 IP 和受影响资产等，产生网络安全告警信息。

同时，水利部网络安全决策指挥系统在进行安全编排和自动化响应处置时，将情报数据查询研判加入处置预案中，对于恶意攻击者、失陷资产等情报数据，决策指挥系统直接联动防火墙、Web 应用防火墙、主机防护系统等网络安全设备，通过下发拦截、拉黑、禁止区域访问、禁止外联等各类动作策略，有效提高预警响应的效率。

3.3　攻击溯源

网络攻击发生后，除对攻击行为进行预警响应外，还需要进一步收集、分析攻击线索，还原攻击过程，追溯攻击者。在某次网络安全攻防演练活动中，溯源分析人员在对网内失陷资产和攻击者 IP 等情报数据进行分析后，及时调整多台网络设备的部署位置，加强重点边界、区域情报收集。对弱口令爆破、Webshell（网页脚本）上传、异常外联等网络安全告警或事件进行聚合，重构攻击链条，提取攻击 IP、攻击载荷、回连地址等攻击特征，通过威胁情报查询进行快速关联分析溯源，发现与此次攻击相关的关联域名及域名注册信息等，进一步进行攻击者画像，最终成功定位到攻击者的个人社交信息。

4　结语

面对日益严峻的网络安全形势，网络安全防御亟须从被动防御、告警处置，向主动防御、威胁发现转变，实现攻防对抗的关口前移，做到知己知彼。水利部积极探索威胁情报在网络安全中的应用，在广泛汇集第三方丰富的情报数据的基础上，创新性地利用水利行业网络安全数据开展了水利私有情报生产，构建了水利部网络威胁情报中心，成功实现了网络威胁情报汇聚、分析、输出等全流程的自动化和集约化及标准化，并向水利行业各单位开放共享，为威胁狩猎、预警响应、攻击溯源等提供了丰富准确的情报支撑，在水利网络安全综合防御中发挥了积极作用。目前，水利网络威胁情报生产主要依靠统计、聚类、关联分析等简单算法，情报数据主要用于网络安

全日常监测、网络攻击预警响应等环节，因此情报生产算法较为单一、情报生命周期管理较为粗放、情报应用场景较为局限等问题明显，网络威胁情报的真正价值未完全得到释放，还需要不断对网络威胁情报进行优化完善。

随着深度学习、自然语言处理技术，特别是知识图谱、生成式人工智能技术的快速发展，网络威胁情报自动处理、分析、挖掘将变得更加容易，同时，智能传感器、物联网、移动互联网的广泛应用，也将促使网络威胁情报的产生、获取、汇集等发生变革，网络威胁情报将在技术发展和数字化浪潮的驱动下不断演进和创新。下一步，将重点围绕情报挖掘、融合、生命周期管理和共享等方面开展研究应用，探索建立更为全面高效的水利网络威胁情报体系，为水利网络安全提供更加有力的支撑。

参考文献：

[1] 郭涛.抓好“重中之重”，守好“神经中枢”，切实筑牢国家网络安全防线：加强关键信息基础设施安全保护体系和能力建设实践[J].中国信息安全，2023 (9)：21-24.

[2] 吴沛颖，王俊峰，崔泽源，等.网络威胁情报处理方法综述[J]. 四川大学学报（自然科学版），2023，60 (5)：7-24.

[3] 李庆华，郭晓黎，张锋军，等.攻防对抗视角下的网络安全主动防御体系研究[J]. 信息安全与通信保密，2024 (1)：77-85.

[4] 蔡阳，付静，詹全忠，等.贯彻“三化六防”理念，保护水利关键信息基础设施安全[J].水利信息化，2021 (6)：1-4，21.

[5] 张潮，房志刚，郭冉.面向智慧水利的网络安全技术体系构建[J].中国水利，2023 (11)：41-44.

[6] 林晨希，薛丽敏，韩松.浅析网络安全威胁情报的发展与应用[J].网络安全技术与应用，2016 (6)：12-13，15.

[7] FRIEDMAN J，BOUCHARD M. Definitive Guide to Cyber Threat Intelligence[M]. Annapolis：CyberEdge Group，2015：1-8.

[8] LEE R. 2020 SANS Cyber Threat Intelligence（CTI）Survey[R/OL]. [2024-05-05]. https：//sansorg.egnyte.com/dl/lv3jkzophv.

[9] CrowdStrike. What is Threat Intelligence?[EB/OL]. [2024-05-05]. https：//www.crowdstrike.com/cybersecurity-101/threat-intelligence.

[10] 汪列军.威胁情报的层次分析[J].保密科学技术，2016 (6)：22-27.

[11] 徐丽萍，郝文江.美国政企网络威胁情报现状及对我国的启示[J].信息网络安全，2016 (9)：278-284.

[12] 詹全忠，张潮.智慧水利总体方案之网络安全 [J].水利信息化，2019 (4)：20-24，29.

[13] 李沁东，陈兴蜀，唐文佚. 开源威胁情报生产与应用综述[J].网络空间安全科学学报，2023，1 (1)：59-80.

[14] 付静.水利关键信息基础设施安全保护探索与实践[J].信息网络安全，2023，23 (8)：121-127.

Research and application of cyber threat intelligence center of Ministry of Water Resources

ZOU Xi，YIN Yue，ZHANG Chao，ZHAN Quanzhong

（*Information Center*，*Ministry of Water Resource*，*Beijing* 100053，*China*）

Abstract：To enhance capabilities in preception，monitoring，warning，and responding to cybersecurity threats in water conservancy，this study proposes a cybersecurity protection framework integrating cyber threat intelligence. Leveraging the Ministry of Water Resources' cybersecurity big data platform，the cyber threat intelligence center was established to enable threat intelligence aggregation，private intelligence generation，and multi-type intelligence dissemination. The center is integrated with systems such as the Ministry's Cybersecurity Threat Perception and Decision Command System，enabling applications in threat hunting，warning responses，and attack tracing. This framework has been implemented in routine cyber security protection and critical period security assurance within the water conservancy sector，effectively improving cybersecurity defenses for the Ministry and affiliated units. The findings provide valuable references and practical insights for constructing cybersecurity defense systems.

Key words：cybersecurity；cyber threat intelligence；threat perception；monitoring and warning；emergency response

（责任编辑：陆　燕）