计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20200616
57(10):2052-2065,2020

网络安全威胁情报共享与交换研究综述

林 玥[1,2] 刘 鹏[2] 王 鹤[1,2] 王文杰[2] 张玉清[1,2]
[1](西安电子科技大学网络与信息安全学院 西安 710071)
[2](中国科学院大学国家计算机网络入侵防范中心 北京 101408)
(liup@nipc.org.cn)

Overview of Threat Intelligence Sharing and Exchange in Cybersecurity

Lin Yue[1,2], Liu Peng[2], Wang He[1,2], Wang Wenjie[2], and Zhang Yuqing[1,2]
[1](*School of Cyber Engineering, Xidian University, Xi'an* 710071)
[2](*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing* 101408)

Abstract The emerging threats in cyberspace are endangering the interests of individuals, organizations and governments with complex and changeable attack methods. When traditional network security defense methods are not strong enough, the threat intelligence sharing and exchange mechanism has brought hope to the protection of cyberspace security. Cybersecurity threat intelligence is a collection of information that can cause potential harm and direct harm to organizations and institutions. This information can help organizations and institutions study and judge the cybersecurity threats they face, and make decisions and defenses accordingly. The exchange and sharing of threat intelligence can maximize the value of threat intelligence, reduce the cost of intelligence search and allieviate the problem of information islands, thereby improving the threat detection and emergency response capabilities of all parties involved in the sharing. This article first introduces the concept of cyber security threat intelligence and mainstream threat intelligence sharing norms; secondly, it investigates the literature on threat intelligence sharing and exchange at home and abroad in the past 10 years, and analyzes and summarizes the current situation and development trend of threat intelligence sharing and exchange. The article focuses on in-depth analysis from three perspectives of sharing models and mechanisms, the distribution of benefits of the exchange mechanism, and the privacy protection of shared data. The problems in the three parts and related solutions are pointed out, and the advantages and disadvantages of each solution are analyzed and discussed. Finally, the future research trend and direction of threat intelligence sharing and exchange are prospected.

Key words cyber threat intelligence; threat intelligence sharing; benefit distribution mechanism; privacy protection; sharing model

摘 要 网络空间新生威胁正在以其复杂多变的攻击方式危害着个人、组织乃至政府的利益.在传统网络安全防御手段捉肘见襟时,威胁情报共享与交换机制的提出给网络空间安全的防护带来了一丝曙光.网络安全威胁情报是对组织和机构产生潜在危害与直接危害的信息集合,这些信息能帮助组织和机构研判所面临的网络安全威胁,并据此制定决策和进行防御.威胁情报的交换与共享可以使威胁情报价值最大化,降低情报搜集成本和改善信息孤岛问题,进而提高参与共享各方的威胁检测与应急响应能力.首先介绍了网络安全威胁情报的概念和主流的威胁情报共享规范;其次,调研了近10年来国内外有关

收稿日期:2020-08-10;**修回日期**:2020-09-05
基金项目:国家重点研发计划项目(2018YFB0804701)
This work was supported by the National Key Research and Development Program of China (2018YFB0804701).
通信作者:张玉清(zhangyq@ucas.ac.cn)

威胁情报共享与交换的文献,分析和归纳了威胁情报共享与交换的现状与发展趋势,着重从共享模型与机制、交换机制的收益分配以及共享数据的隐私保护3个角度进行了深入分析,指出了3部分存在的问题及相关解决方案,并对各方案的优缺点进行了分析讨论;最后展望了威胁情报共享与交换未来的研究趋势和方向.

关键词　网络安全威胁情报;威胁情报共享;利益分配机制;隐私保护;共享模型

中图法分类号　TP319

近年来,网络技术日益翻新,同时带来了日趋复杂的新生网络威胁.

这些新生威胁具有多矢量、多阶段的特性:多矢量指的是威胁攻击可以使用多种传播方式(如Web、电子邮件、应用程序等),多阶段指的是攻击可以在网络中渗透、传播并最终泄露有价值的数据.

表1详细介绍了4种新生威胁及其特点.一方面,新生攻击促成了新的攻击场景,从防御角度可理解为"攻击链[1]".另一方面,为了实现新生攻击,攻击者配备了最新的零日漏洞和社会工程学技术,利用先进的策略很容易避开传统的安全防御手段.

Table 1　Emerging Threats and Their Characteristics

表1　新生威胁及其特点

Emerging Threats	Characteristics
Advanced Sustainable Threat	The attackers keep trying until they enter the network and remain undetected for a long time; with the purpose of stealing data; the target is organizations in high-value information fields, such as government agencies and the financial industry.
Polymorphic Threat	For example, constantly changing (deformed) viruses, worms or Trojan horses [2]; the appearance of the code changes, but the basic functions remain unchanged; signature-based defense methods can be avoided, creating a vicious circle beneficial to attackers.
0Day Threat	Targeting publicly unknown vulnerabilities in operating systems or applications; it can be undiscovered for a long time, even if it is eventually discovered, it will still take days or even weeks to fix the vulnerabilities.
Mixed Threat	A combination of grammatical and semantic attacks[3]; combined with social engineering techniques, such as phishing attacks.

网络安全是一种权衡较量,是攻击者和防御者之间的非静态平衡行为[4].由于信息的不对称性,攻击者具有先下手为强的优势,而防御者往往处于被动的地位.

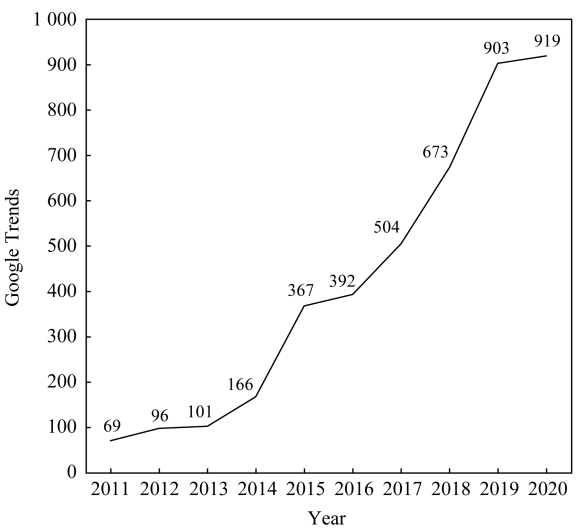
为提高网络安全防御能力,各方着眼于对威胁情报的利用,因其数据内容丰富、准确性高等特点,可以为安全分析的各个阶段提供有力的数据支撑.面对复杂的攻击形式和严重的攻击后果,依靠个人或单个组织的技术力量仅能获得局部的攻击信息,无法构建完整的攻击链,更无法准确有效地预防攻击.而威胁情报的交换与共享方法能够使威胁情报价值最大化,降低情报搜集成本,很好地改善信息孤岛问题,进而提高参与共享各方的威胁检测与应急响应能力.网络安全威胁情报的共享交换作为一种"以空间换时间"的技术方式,可以及时利用其他网络中产生的高效威胁情报提高防护方的应对能力,缩短响应时间,从而形成缓解攻防对抗不对称态势的长效机制.

作为网络空间的主导者,美国政府高度重视网络安全威胁信息的共享,早在2003年的《网络空间安全国家战略》中就提出了建立信息共享与分析中心(Information Sharing and Analysis Center, ISAC),确保能够接收实时的网络威胁和漏洞数据[5].近年来,美国政府在威胁情报信息共享的建设方面持续投入大量的精力,现已建立起了覆盖地方—联邦政府、部门(行业)、企业—政府多个层面的威胁情报分析与共享体系,极大地提高了美国应对其网络空间安全态势的感知和防御能力[6].然而,我国的威胁情报体系发展仍处于起步阶段,基于威胁情报的网络安全分析技术比较落后.不仅缺乏有效、可靠的威胁情报的采集、共享与利用规范,而且尚未建成规模化的技术完备的集数据截获、分析、转化、共享与利用为一体的现代化威胁情报中心,因而缺乏面向政府、军队、企业、设备厂商、个人或民间组织提供的威胁情报的综合服务平台.

为了扭转这种被动局面,建立和完善可靠的威胁情报共享与交换机制迫在眉睫.目前,我国正在逐步

展开以威胁情报为基础的网络空间安全态势感知战略,根据自身发展和技术积累情况积极开展情报集、共享与分析等方面的研究.学术界和产业界也都积极地进行着相关技术的研究,尝试寻求网络安全防御的合作共赢,从而建立健全的国内情报共享与交换体制,进一步推进我国威胁情报相关机制的发展,提高国家网络安全的整体防御能力[7].

虽然威胁情报共享领域的研究引起了国内外广泛关注,但仍然存在许多制约情报共享发展的问题和困难.为此,我们系统地调研了 IEEE, ACM, Springer 等期刊以及安全会议中近 10 年来有关威胁情报共享机制的文献,统计分析了近 60 篇论文,尝试总结威胁情报共享当前的研究成果并指出该领域的研究方向.图 1 显示了关键词"Cyber threat intelligence"近 10 年来在互联网上的搜索热度,每年份的纵轴数据为去年 9 月到该年 8 月的月度搜索热度(0～100)算术求和.连年增加的搜索热度反映该领域持续受到关注,相信更多的研究成果即将出现.



The annual data is the arithmetic sum of the monthly search popularity (0～100) from September last year to August of that year.

Fig. 1 Google trends of "cyber threat intelligence" in the past 10 years

图 1 Internet 搜索关键词"cyber threat intelligence"近 10 年的 Google trends 数据

本文的主要贡献有 3 个方面:

1) 系统地调研了 2010 年至今的近 60 篇威胁情报共享相关文献,指出了威胁情报共享研究的发展历程,对比了国内外威胁情报共享规范,总结相关共享模型与方案;

2) 首次从外部环境障碍、共享参与者的信任障碍和利益分配、共享数据的隐私安全和价值评估 3 个角度出发对威胁情报共享所面临的问题进行梳理,并分别给出各问题相对应的研究举措;

3) 分析了当前我国威胁情报共享研究中的不足,总结了面临的五大机遇与挑战,并指出了未来的研究趋势与下一步研究方向.

1 威胁情报

1.1 威胁情报的定义

在传统安防领域,威胁必须具有 3 个要素才能称之为威胁,它们分别是渴望达成的目的、用以支持的资源及可供实施攻击的机会、手段与工具.

随着互联网和信息化的普及,传统的安全威胁也渗透到了线上,而与之对应的是网络空间中的威胁与威胁情报.所以从历史发展观来看,网络威胁是传统威胁在介质升级后的一种新体现,网络威胁情报是传统安全情报的范围延伸.

网络威胁情报(cyber threat intelligence, CTI)是记载网络上现有的或者曾经存在的安全威胁的一种信息,但是目前整个业内对于威胁情报并没有一个十分确切的一致定义,目前最为通用的定义是 Gartner 公司在 2014 年版本的《安全威胁情报服务市场指南》[8]中给出的.

Gartner 认为,威胁情报是一种基于证据的知识,包括了情境、机制、指标、影响和操作建议.威胁情报描述了现存的、或者是即将出现针对资产的威胁或危险,并可以用于通知主体针对相关威胁或危险采取某种响应.

在 2015 年,由 Friedman 和 Bouchard 在《网络威胁情报权威指南》[9]中,也给出了一个有关威胁情报的定义:对敌方的情报及其动机、企图和方法进行搜集、分析和传播,以帮助各个层面的安全和业务成员保护企业关键资产的信息.

总之,威胁情报就是对企业产生潜在危害与直接危害的信息集合.这些信息能帮助企业研判当前发展现状与趋势,并可推算出所面对的威胁,然后由此制定决策.简而言之,对企业产生危害或者利益损失的信息,就可以称之为威胁情报,这也是目前整个业界所默认的一种定义[10].

1.2 威胁情报的内容与分类

从数据特点上来看,威胁情报是一种海量、多源、异构的信息.2014 年,FireEye 的 Bianco 在公开演讲中提出,所有事件(facts)、机器采集的原始数据(raw data)、专家所做的相关分析(expert analysis)

等,都可以被认为是有价值的威胁信息,可以用来进行集中过滤、处理,然后得到有价值的威胁情报.在该公开汇报过程中,Bianco 根据情报的潜在利用价值以及获得难度,做了一个金字塔形状的分类.金字塔从下至上分别是:Hash 值、IP 地址、域名、网络/主机特征、攻击工具、TTPs.一般而言,包含不同内容的威胁情报的使用价值不同,其获取的难易程度也有所不同.

需要特别指出的是,从威胁情报本身而言,它类似于医疗科学中的疫苗,既是预防的重要工具,同时自身也有一定的危险性,如果威胁情报的内容里含有很多敏感数据,那么在共享过程中就要进行针对性的脱敏操作,以防含有敏感信息的威胁情报被不法分子利用.

根据威胁情报应用场景的不同,可以将其分为 3 类[10]:以自动化检测分析为主的战术情报、以安全响应分析为目的的运营级情报,以及指导整体安全投资策略的战略级情报.

1) 战术级情报.战术情报的作用主要是发现威胁事件以及对报警进行确认或优先级排序.常见的失陷检测情报、有害 IP 情报都属于该范畴,它们都是可机器阅读的情报,可以直接被设备使用,自动化完成相应的安全响应.

2) 运营级情报.运营级情报是给安全分析师或者安全事件响应人员使用的,目的是对已知的重要安全事件做分析(报警确认、攻击影响范围、攻击链以及攻击目的、技战术方法等)或者利用已知的攻击手法主动查找攻击相关线索.

3) 战略级情报.战略层面的威胁情报是给有组织的安全管理者使用的,比如企业的首席策略官(chief strategy officer, CSO).它能够帮助决策者把握当前的安全态势,在安全决策上更加有理有据.包括了什么样的组织会进行攻击、攻击可能造成的危害有哪些,攻击者的战术能力和掌控的资源情况等,当然也会包括具体的攻击实例.

2　威胁情报共享

威胁情报共享作为网络安全威胁情报体系架构中的一项重要环节,对实现网络安全态势感知以应对新生网络威胁起着至关重要的作用.威胁情报共享这一概念上承数据的收集、关联聚合等技术,下启威胁情报的提取和分析方法,是建立以威胁情报为核心的网络安全防御战略体系的关键步骤.面对日益严峻的网络威胁形势,打破藩篱,加强各信息系统协同互助,构筑宽共享、全联通的信息共享环境可使威胁情报价值最大化,进而提高参与共享各方的威胁检测与应急响应能力.

2.1　威胁情报共享的发展

虽然威胁情报共享这一概念是近几年才映入人们的眼帘,但在此之前网络安全信息的共享早已成为各领域希望探讨的话题,并为威胁情报共享研究提供了扎实的理论和技术铺垫,在推动威胁情报共享快速发展方面起到了关键性的作用.与威胁情报共享相关的研究(涵盖网络安全信息共享)非常广泛,如图 2 所示,包括对网络安全信息共享的探索和调查、相关标准和平台的推出以及相关模型和机制的建立等.

Fig. 2　Research history of threat intelligence sharing models and mechanisms

图 2　威胁情报共享模型与机制的研究历程

2.1.1　探索阶段

早期对威胁情报共享机制的研究处于探索阶段,大部分的内容针对信息共享的需求与动机、问题与挑战,尝试寻找能解决这些问题的方法,并提出一些可行性意见和建议.

Vázquez 等人[11]分析了基于网络安全情报共享的防御机制面临的挑战,从网络防御合作中的动机和障碍、合作风险管理和信息价值认知、可提高政府级数据交换效率的交换模型、适用于常见网络防御数据的自动化共享机制这 4 个方面入手,探讨如何有效推动情报共享.

Serrano 等人分析了网络安全信息共享面临的 4 个主要挑战[12],并重点介绍了基于当前技术水平的技术解决方案.

Haass 等人与非营利性情报组织 ACTRA (Arizona Cyber Threat Response Alliance, Inc.)共同对威胁情报的共享模式进行了研究,重点关注异构组织情报共享技术、政策和组织协调模式等 3 方面存在的问题和可能的解决方案[13].

2.1.2 调查阶段

随着研究的不断深入,越来越多有关安全信息共享的总结性调查文献出现,从宏观的角度阐述威胁情报共享多层次、多角度的问题.

Kampanakis 等人调研了现有的情报共享和分析平台,介绍了这些方案的基本特性,确定了它们试图解决的问题,并总结了这些方案的相同点和不同点[14].对这些平台的数据进行分析后发现,这些数据大多易于理解,但难于共享和交换;跟踪研究了情报提供者之间进行情报共享时存在的热点问题;从使用者的角度对不同情境下的情报共享模式进行了阐述.

Goodwin 等人借助微软在基础设施安全管理方面多年的经验,提出了有关信息共享的历史背景,并阐述了信息共享在模型、方法和机制等方面的分类,最后对进行协作式的信息共享和交换提供了可行的建议[15].

Skopik 等人提供了一个关于网络安全信息共享维度的结构化概述[16].该文献首先详细地探索并制定了信息共享系统的需求;其次,重点介绍标准化组织在法律方面的工作,并从组织和技术方面调查了实施情况;最后,对最新技术进行了严格审查,并着重指出了将来构建有效的安全信息共享平台时应重点考虑的因素.

2.1.3 指导性文件的发布

随着前期该领域知识的积累以及相关内容的探索和调查,威胁情报共享受到各个领域的关注,推进其发展的举措也越来越多.

标准机构等类似机构就如何构建网络安全信息共享网络也出台了一系列标准,其中典型例子为 NIST 发布的《网络威胁信息共享指南》[17] 和 ENISA 文档《网络安全信息共享:监管和非监管方法概述》[18] 等.

2.1.4 共享平台的推出

针对特定的共享内容、组织形式及具体网络安全实际情形,一些威胁情报共享平台也相继被推出.

在 2016 年,卢森堡的计算机时间响应中心 (Computer Incident Response Center Luxembourg, CIRCL)的学者提出恶意软件信息共享平台(Malware Information Sharing Platform, MISP)[19] 和威胁共享项目.这是一个可信的平台,不仅可以搜集和共享针对目标攻击的重要威胁指标,也可以搜集和共享欺诈事件中使用的漏洞或财务指标等威胁信息,以帮助建立针对目标攻击的预防行动和反措施.

在 2017 年,南非科学与工业研究理事会(Council of Scientific and Industrial Research, CSIR)相关人员针对本国的网络安全现状,提出一个在国防环境中的网络威胁情报共享平台[20],系统地讨论和演示了该平台能够促使各个国防力量在国防环境中进行无缝的协作,以维持弹性的网络安全态势.

在 2019 年,Leszczyna 等人[21] 关注电力基础设施的网络安全隐患,为电力部门提出了一个实现信息交换的集中式平台;介绍了几种支持方案,包括匿名机制、数据处理和相关算法;定义了以自然语言和机器可读格式实现的网络事件信息通信的数据模型,并设计了关键组件的安全需求,旨在建立增强的威胁情报,将信息共享和细粒度的态势感知联系起来.

前期的研究在很大程度上采用体系结构的观点来看待问题,而忽略了关于安全信息共享的操作方面的指导.对于潜在的复杂网络系统,维持态势感知所需的技术和过程很少受到关注.

2.2 威胁情报共享的相关标准

威胁情报多源异构的数据特点使得现有数据表达规范和通信传输协议不能在威胁情报共享中直接使用,无法有效地进行威胁情报的表达和传输.由此看来,标准化的数据格式和统一的传输协议是高效威胁情报共享体系中必不可少的部分.基于结构化的规范情报描述标准和固定的传输协议可降低参与情报共享机构、存储库进行情报交换和数据格式转化的成本,提高所交换情报的效率和准确性,同时简化参与方的连接管理,促进各成员资源共享、协同交流[22].

2.2.1 国外主流共享规范

国外的威胁情报共享标准已经非常成熟且得到了广泛的应用.

为满足情报共享市场的需求,业界已制定了一系列相关标准用于威胁情报的交换.结构化威胁情报表述(structured threat information expression, STIX)[23] 是一种由 OASIS-CTI-TC 负责开发和维护的情报表达规范,用于对网络威胁情报的建模、分析和交换进行规范,目前已经更新至 STIX2.0 版本.

指示性信息的可信自动交换方案(trusted automated exchange of indicator information, TAXII)[24]

提供了威胁情报信息的安全传输与交换,可兼容多种传输格式的数据.

网络可观察对象描述(cyber observable expression, CybOX)[25]规范定义了一个表征计算机可观察对象与网络动态和实体的方法.

STIX 和 TAXII 作为两大标准,不仅得到了包括 IBM、思科、戴尔、大型金融机构以及美国国防部、国家安全局等主要安全行业机构的支持,还积累了大量实践经验,在实践中不断优化.

目前比较主流的情报共享平台的做法是在 STIX 规范框架下,借助 CybOX 提供的词汇描述威胁情报,并利用 TAXII 进行传输.

2.2.2　国内首例共享规范

在威胁情报共享的规范化与系统化发展方面,我国也在紧追国际发展趋势,大力推动网络安全威胁情报相关标准的制定、发布和执行.规范的威胁情报格式是实现网络安全威胁情报共享和利用的前提和基础,在推动网络安全威胁信息技术发展和产业化应用方面具有重要意义.

2018 年 10 月 10 日,我国正式发布了威胁情报的国家标准[26]《信息安全技术网络安全威胁信息格式规范》,该规范成为国内第一个关于威胁情报的相关标准.该规范给出一种描述网络安全威胁信息的结构化方法,其创建目的是实现各组织间网络安全威胁信息的共享和利用,并支持网络安全威胁管理和应用的自动化.为了更好地实现这些目标,标准定义了一个通用的网络安全威胁信息模型,旨在对威胁信息进行统一描述,从而提升威胁信息共享的效率、互操作性,以及提升整体的网络安全威胁态势感知能力.

图 3 给出了与该标准匹配的威胁信息模型,它从对象、方法和事件 3 个维度对威胁信息进行划分,采用包含可观测数据、攻击指标、安全事件、攻击活动、威胁主体、攻击目标、攻击方法、应对措施在内的 8 个组件描述威胁信息.这些组件分别表达了网络威胁不同维度的特征,它们在结构上相互独立,在

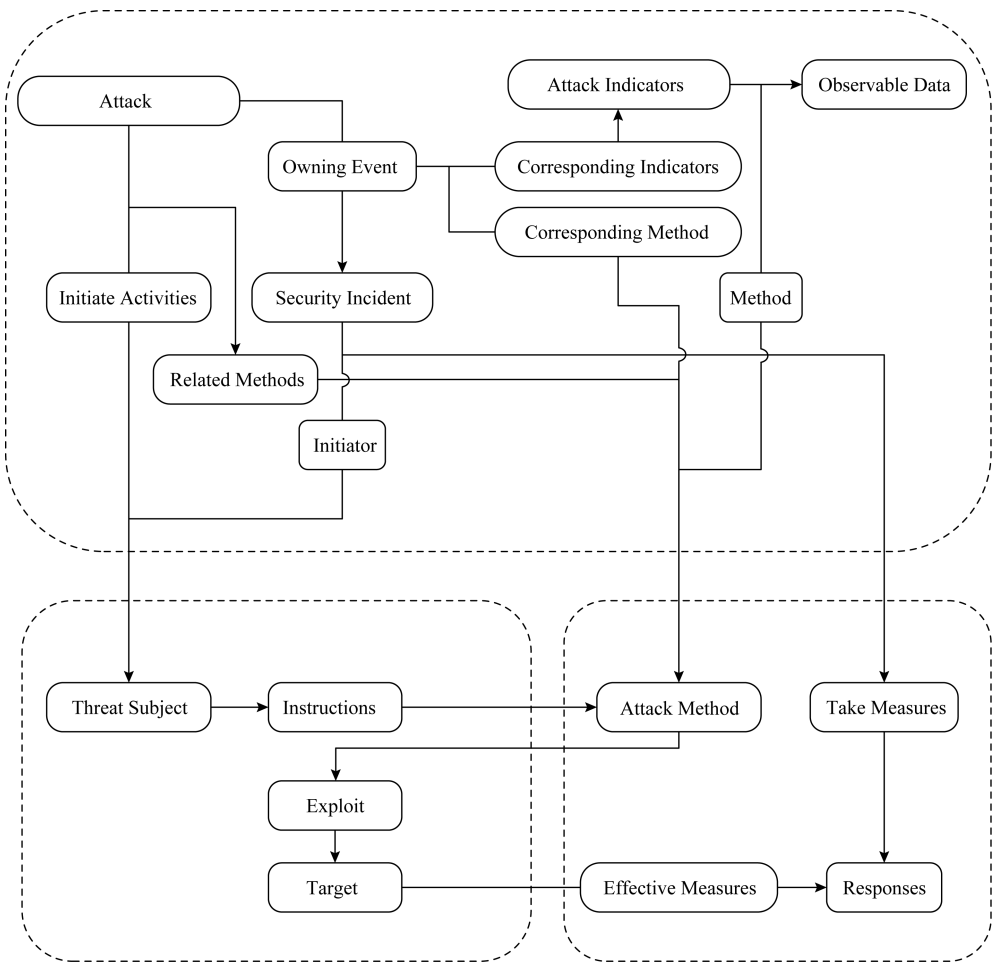


Fig. 3　Threat information model

图 3　威胁信息模型

内容上相互关联,如“攻击指标”是用来识别特定“攻击方法”的技术指标,它是多个“可观测数据”的组合,是用来检测“安全事件”的检测规则.

2.3 威胁情报共享的模型与方案

面对网络威胁的复杂性、多样性,不断有学者在尝试寻求能够实现威胁情报共享的模型与机制.不管是早期的网络安全信息共享还是现今的威胁情报共享,能够为共享过程提出合理的共享方案将更好地推进网络安全态势感知技术的发展.

通过调研和跟踪本文发现,在 2010 年,德克萨斯大学圣安东尼奥分校的学者[27]讨论了众多实践经验,说明了现有访问控制模型在安全信息共享方面的局限性,包括自主访问控制、强制访问控制和基于角色的访问控制,并针对性地提出以组为中心的安全信息共享(g-SIS)模型的研究工作如何直接解决现有模型的局限性.在 2012 年,该团队针对信息分享的必要性和社区网络安全威胁进行了研究,定义了社区网络安全的威胁警戒级别,并讨论不同级别对信息共享的影响,提出了一个以组为中心的合作信息共享框架,并阐述了共享过程中可能遇到的问题及进一步的研究内容[28].2014 年,该团队的学者又做了进一步的研究,更加关注共享过程中的细节,为该信息共享框架设计了一个正式的策略模型,旨在提高社区网络安全[29].

经过几年的研究,g-SIS 方案的提出在共享方面提供了良好的思路和创新性,但仍然存在着几点不足之处.例如,该共享方案并不能得到广泛的采用,并且共享的信息侧重面窄,缺少统一标准的数据格式,最重要的是无法解决共享参与者之间的信任问题.在 g-SIS 框架之外,针对威胁情报共享的分布式方案相继提出,更加注重以威胁情报为核心的共享模型.

在 2019 年,Li 等人为了丰富 P2P 僵尸网络检测方法,提出了将分布式威胁情报共享系统应用于 P2P 僵尸网络检测的新思路[30].在分布式的部署结构下,设计了一个分级的情报共享机制,通过该机制可以将结构化的多维威胁情报共享给所有成员,确保系统能够监测和预测网络威胁.

Lin 等人提出了一种基于黑板模型的社区协作威胁情报共享方案[31],该方案可用于识别潜在风险,在早期阶段预防网络攻击并推动社区的应急响应.文章根据中国国家标准对威胁情报共享类型进行划分,并且将黑板监控机构设计为多智能体系统,以实现分布式功能特点.

表 2 对目前较成熟的威胁情报共享机制从共享规范、控制粒度、信任、隐私保护和早期检测防御等 5 个方面进行了详细的对比.

Table 2 Comparison of Threat Intelligence Sharing Mechanisms

表 2 威胁情报共享机制比较

Sharing Plan	Sharing Norms	Access Control	Trust Issues	Privacy Protection	Early Detection and Defense
g-SIS Model[29]	Not Considered	Coarse-grained	Not Considered	Not Considered	Not Considered
Distributed Model[30]	STIX and TAXII	Coarse-grained	Not Considered	Not Considered	Considered
Blackboard Model[31]	China National Standard	Fine-grained	Not Considered	Not Considered	Considered
iShare[32]	Not Considered	Coarse-grained	Considered	Not Considered	Not Considered
Blockchain Model[33]	STIX 2.0	Fine-grained	Considered	Considered	Not Considered

3 威胁情报共享的问题与举措

从理论上来说,共享威胁情报是一件很有意义的事情.但在互联网安全领域,这件“美好的事情”要实现并非那么容易.

从外部环境来看,完成共享过程需要一定的信息技术做安全支撑,如果缺乏专业操作,共享参与者将无法推进威胁情报共享的进行.除此之外,从共享参与者的角度考虑,存在共享信任障碍和共享利益难分配的问题;从共享数据的角度考虑,存在敏感数据泄露和数据价值难评估等问题.本节将进一步描述威胁情报在共享方面的问题以及相应举措.

3.1 鼓励威胁情报共享的外部举措

许多国家和国际组织通过对威胁防御者之间的合作和协调进行支持来鼓励威胁信息或情报的共享.一些组织关注漏洞和事件响应,而另一部分则专注于识别入侵和潜在威胁.综合来说,这些服务为成员提供了通用且连贯的信息技术基础设施的安全框架.本节简要回顾了大多数知名组织及其主要角色和作用.

3.1.1 事件响应团队和国际合作

从区域角度来看,计算机应急响应团队(computer emergency response teams, CERTs)是每个网络安全

生态系统的重要组成部分.他们搜集有关新威胁的信息,发出早期预警,并可根据要求提供帮助.CERT合作已被证明是区域内最为有效的措施,网络威胁的全球性也要求国际合作,CERTs在国际上也有着良好的联系.以我国为例,作为国家级应急中心,国家计算机网络应急技术处理协调中心(CNCERT)的主要职责是:按照"积极预防、及时发现、快速响应、力保恢复"的方针,开展互联网网络安全事件的预防、发现、预警和协调处置等工作,维护公共互联网安全,保障关键信息基础设施的安全运行.

事件响应和安全小组论坛(Forum of Incident Response and Security Teams, FIRST)在建设CERTs国际社区方面发挥着有效的作用.FIRST汇集了来自政府、商业和教育机构的各种计算机安全事件响应团队,旨在促进预防事件方面的合作和协调,促进对事件的迅速反应,以及成员和整个社区之间的信息交流.

Euro-CERT小组于2000年5月成立了一个名为TF-CSIRT (TF-Computer Security Incident Response Teams)的特别工作组.其主要目标是通过观察共享事件的统计数据,制定一项欧洲信赖机制.该组织同时还承担了教育、培训新工作组的任务.

3.1.2　ISACs:信息共享和分析中心

信息共享与分析中心(Information Sharing and Analysis Center, ISAC)是促进威胁信息共享的第一个正式机制[34].它是由美国政府提出的,并在1998年出版的《总统直接决定第63号》(PDD-63)中作了描述.此外,美国CERT(USCERT)还与ISACs合作,主办仅限于保护关键国家基础设施的相关组织的会议.ISACs搜集、分析并向行业和政府传播私营部门的威胁信息,并向成员提供减轻风险和增强复原能力的工具.它作为一个框架,使利益相关者能够跨不同的攻击链步骤开发他们的防御策略.许多ISACs现已建立,涵盖不同的行业和部门.

3.1.3　其他协调措施

欧洲网络与信息安全机构(European Network and Information Security Agency, ENISA)是主要的欧洲机构,旨在通过鼓励网络和信息安全威胁、方法和结果的交流,避免重复的工作,提高欧洲不同机构和成员国工作的一致性.

国家标准和技术研究所(National Institute of Standards and Technology, NIST)在响应计算机安全事件时,通过确定有关的标准、方法、程序和过程,对现有的CSIRTs之间的协同合作进行支持.NIST就如何在处理计算机安全事件时进行合作提供指导和最佳实践.

这些举措同样存在局限性,法律的要求、数据的敏感性等都是不愿扩大合作背后已知的普遍性问题.法律规定特别关注国际合作,而在威胁数据的敏感性方面,参与的公司仍然不愿对其同行和政府透露潜在威胁.另一个重要问题是缺少用于交换信息的总体方法.所有这些局限性都限制了从信息共享中获得的益处,从而限制了参与者之间的合作.

3.2　自动化处理与相应举措

往期威胁情报共享的发展,往往把静态的模型作为主要的研究课题,如威胁情报的表示、点对点的威胁情报交换协议等,但是威胁情报是无时无刻不在发生,如果依赖人来甄别、分析、响应,那么共享的效率将会大大降低,甚至有可能导致共享的美好期望被信息的滞后性所拖累,所以自动化的网络威胁情报甄别、发布变得尤为关键.例如2017年5月的勒索病毒WannaCry在教育网肆虐,如果威胁情报能及时地发出并得到响应,那么大部分高校、组织将得以避免入侵.

2020年4月,北京邮电大学的课题组提出了一个名为HinCTI的系统,该系统基于异构信息网络(heterogeneous information netwark, HIN),采用了数据挖掘方法[35],可以对网络威胁情报进行建模,在该文定义的威胁基础设施相似度的基础上,采用基于元路径和元图实例的异构卷积网络方法来识别网络威胁情报中涉及的基础设施节点和威胁的类型,并提出了一种基础设施节点威胁类型的识别方法,该方法可以提升威胁类型识别的性能.

同样是基于自然语言处理技术,北京航空航天大学和美国密歇根州立大学的学者,提出了一个名为TIMiner的网络威胁情报提取系统[36],该系统的目标是从社交数据中自动提取威胁情报并进行分类.因为现有的方法无法识别妥协指标(indicators of comprise, IoC),而且不能生成指示威胁情报所属范围的标签.这篇文章针对该难点,实现了一个基于卷积神经网络的高效率领域标签识别器,该识别器可以识别威胁情报的所属目标域.另外,该文还提出了一种基于词嵌入和句法依赖的折衷抽取方法,该方法能够识别不可见的IoCs类型.TIMiner通过综合利用上述2项技术,可以将提取的IoC及其域标记结合,生成一个具有特定域的威胁情报.

总的来说,将元数据经由自动化处理算法生成

威胁情报是非常有意义的,而且可以大大解放人力参与,同时提升威胁情报的反馈与响应速度.

3.3 共享信任障碍与相应举措

威胁情报在本质上是高度敏感的,由于共享者在不同的信任边界内操作,其产生的信任问题会导致隐私担忧.如果威胁情报处理不当或泄露,可能会对情报来源组织造成有不利影响;更有可能会受到攻击者的进一步利用,造成其声誉受损,进而导致收入损失.共享者需要保持敌意,同时也要确保接收者仍然信任信息(即使是未知源),这两者之间的冲突是参与威胁情报共享的障碍.换言之,这种固有信任障碍可能会抑制共享者参与威胁情报共享的积极性.

针对威胁情报共享过程中的信任问题,Wagner等人提出了一种新的信任分类方法来建立可信的威胁情报共享环境[37],并分析比较了30个流行的威胁情报平台的信任功能.其提出的信任分类方法无法抵挡共谋攻击等相关安全问题,因此该文也相应给出了减轻攻击的可能解决方案.Gao等人针对大规模异构威胁情报,提出了一种基于图挖掘的多维特征信任评估机制[38].该机制通过集成信任感知的智能体系结构模型、基于图挖掘的智能特征提取方法和自动可解释的信任评估算法,为威胁情报共享平台提供了一种可行的方案,实现了信任评估任务.

近年来,区块链技术发展迅猛,其去中心化特性使得共享参与者即使在无可信第三方的情况下也能够进行有序、可信的共享操作.由于区块链技术在其他行业信息共享方面的研究工作已经取得了一定进展,因此很多学者选择从此方向进行突破.Rawat等人[32]提出了基于区块链的iShare框架,参与iShare框架的成员间仅可分享网络安全防护的方案或概述,未涉及威胁情报的共享工作.Homan等人实现了一种威胁情报共享区块链网络原型,作为一种试验台可供相关方案进行验证[33].该文利用超级账本允许可信参与方以私有的方式传播高度敏感的数据,同时仍然参与整个网络.虽然能够克服共享过程中固有的信任屏障和数据隐私问题,但该模型局限于欧盟体制下,未能体现网络威胁情报共享的广泛性和通用性.

针对威胁情报难以共享这个问题,Riesco等人提出了一个基于区块链的模型[39],鼓励所有参与者在各个层次上动态地共享相关信息.该方案有助于支持和部署动态风险管理框架,使风险随时保持在可接受水平之下.在该方案中,参与者可根据其扮演角色的不同(生产者、消费者、投资者、捐赠者和所有者)来分享、投资和消费威胁情报与风险情报信息.同时,该文提议建立一个Ethereum区块链智能合同市场,以更好地激励所有相关各方共享知识.

3.4 收益分配困难与相应举措

在威胁情报共享中,如何公平地进行收益分配,从而激励各个组织共享更多的威胁情报是影响威胁情报共享发展的关键问题之一.当前在网络威胁情报共享利益分配中的主要问题分为3类:技术问题,耦合问题和市场问题.

1) 技术问题.在一般的威胁信息描述方法中,只针对技术细节进行了刻画,但是对于潜在的价值方面无能为力,因为"价值"是与市场相关的经济学概念,纯技术无法也不能自动解决定价问题.

2) 耦合问题.利益分配与共享模式有着千丝万缕的联系,而且与技术实现能否支持也密切相关,一个扩展性不好的威胁信息表达技术,也不利于后期建设利益分配便利的共享机制.

3) 市场问题.早期威胁情报共享的广泛运用必然导致社区内的相关用户大大提升自己的安全性,同时打击攻击者的积极性;经过一段时间的发展,社区的热度会因为整个行业的安全性提高而降低.以自身利益为导向共享参与者就会仅发布自己掌握的少数威胁信息,以保持安全生态中的部分受攻击的现状,从而实现自身收益可持续化.这显然是一个市场心态问题,而且一旦成为事实,也不利于安全行业整体的健康.

针对上述问题,国内外专家进行了许多研究.2015年,Tosh等人根据博弈论的简单思路,建立了一个朴素的威胁信息交换模型,并根据这个博弈模型得出结论:当企业彼此之间共享更多信息时,参与交换的企业受激励程度会更高,而企业自身的安全投资还有助于最大化地获取来自其他公司的安全支持[40].然而该模型并没有对交换的细节进行详细描述,比如,双方是否可以互相信任的问题,而这些问题在实际操作中是需要真正面对的.同一时间,该团队发表的另一篇文章也是利用了博弈论思想,对云计算平台中的用户进行分析得出结论:当在发现漏洞的可能性非常低的情况下,所有参与者都不会去投资漏洞研究,也不会分享任何漏洞;此外,如果漏洞太易于发现,用户将不会共享漏洞[41].

2017年,Vakilinia和Tosh等学者使用动态博弈理论,建立了一个博弈模型并模拟了普通型参与者、CybEX共享平台自身以及攻击型参与者的三方博弈(3-way game),通过为每个参与者设计适当的

收益函数,并将组织的隐私部分纳入共享模型来分析每个参与者的最佳策略[42].通过分析得出:隐私是交换这些关键信息的瓶颈;该文最终得出了普通参与者获得最大净利益的最佳策略.与此同时,该模型还通过对普通参与者的最佳策略的分析,反向确定了 CybEX 平台应设置怎样的激励金额以及参与者的参与成本.

鉴于博弈论本身假设前提的局限性,即参与者必须是绝对利己且绝对理性的,三方博弈模型在实际应用中会存在问题.2017 年,陆正福等学者,根据 Asokan 在 1998 年的有关电子商务公平性的课题[43]进行拓展研究,提出了一种基于实际的、用户只有有限理性的公平数据交换协议[44],虽然该研究领域属于单纯的信息交换协议,但是对于威胁信息的交换仍具有一定的启发性,该文定义了有限理性公平概念,并基于有限理性假设,设计了有限理性公平数据交换协议(Fair Data Exchange Protocol-Bound Rational, FDEP-BR).并且从理论分析上证明,与 REP(Rational Exchange Protocol)相比,FDEP-BR 虽然牺牲了一定效率,但具有容错性和有限理性公平性,能够抵抗非合作攻击,并且更适合于实际用途.

从博弈论角度出发的非合作博弈的解,即非合作博弈 Nash 均衡,仅仅能够保证彼此都不亏,但是对于理想中的双赢局面是无法达成的.与非合作博弈不同,合作博弈强调集体主义和团体理性,起初经济学家对于这种合作博弈束手无策,直至 Shapley 给出有关公理化描述.

Shapley 值方法由 Shapley 在 1953 年提出[45],该方法对于解决集体利益分配问题有着非常强的说服力,在网络威胁情报共享的场景中,该理论具有非常好的利用价值.Shapley 值方法适用于由不同的参与者构成的利益集团进行内部利益分配的问题,其中该集团一致对外提供服务获取收益.由于这种模式限制,该方法适用于 B2C(Businesses-to-Consumer)模式.Shapley 值是合作博弈中一个非常重要的解,在威胁情报共享合作博弈模型中,利用 Shapley 值解决联盟利益的公平分配问题具有很强的说服力.

3.5　数据隐私问题与相应举措

共享过程中不可避免地存在着敏感信息的传递和组织,这严重阻碍着共享参与者的积极性,降低了情报共享活动的安全性和有效性,因此威胁情报中所包含的隐私信息是制约威胁信息交换的一大瓶颈.由于信息的敏感性和私有性,共享网络威胁情报对组织而言代价高昂,与此同时,做出是否共享信息的决定是一项具有挑战性的任务,并且需要解决共享优势和隐私暴露之间的权衡.因此,提出共享数据的隐私保护方案也是情报共享领域需要重点研究的内容.虽然针对其他领域的隐私保护技术相当成熟,但因威胁情报共享在用户群体和服务类型以及共享内容结构上都存在差异,需要根据服务、数据类型和结构的不同进行优化和重建.

随着研究的不断深入,有效的隐私保护技术与威胁情报相结合的解决方案相继提出.例如,结合标准的格式保持和同态加密[46],并利用 STIX 标准数据格式提出一种保证私有数据转发和聚合的网络安全共享方案,针对应用在共享过程中的不受信任的基础设施实现了数据的隐私保护;以匿名技术为核心建立一个威胁情报共享平台[47];基于身份加密和阈值秘密共享方案解决私有数据的共享问题;对隐私信息检索技术进行改进,以确保用户与云服务进行威胁情报共享时的隐私安全[48];以区块链技术[33]划分网络,允许可信参与者传播高度敏感数据.

除此之外,许多文献侧重于相关数据隐私法规对威胁情报共享的限制,例如,依托《一般数据保护条例(General Data Protection Regulation, GDPR)》,为共享的威胁情报定义完善的保护级别[49].

网络安全信息交换框架(Cybersecurity Information Exchange Framework, CybEX)[50]是由 ITU 建立一个新兴的标准.在 CybEX 架构下,不仅存在对利益分配问题的研究,越来越多的学者关注信息交换过程中的数据隐私及访问控制问题.2017 年 Vakilinia 等人在 CybEX 框架中实现了基于属性的访问控制[51].该方案利用半可信共享服务器对 CybEX 中的基于属性的访问控制进行建模,提出了基于密文策略属性加密和 STIX 的机制.2019 年,Sadique 等人提出了网络安全信息隐私交换(CybEX-P)框架[52].CybEX-P 是一个结构化的信息共享平台,保证了数据的最大安全和隐私.CybEX-P 采用盲处理、隐私保护和可信计算范例,使其成为一个通用的、安全的信息交换平台.

3.6　数据价值评估与相应举措

从长远角度看,威胁情报是一种有经济价值的商品.目前共享利益分配机制设计的首要问题是解决威胁信息数据价值评估难度大、威胁信息交易收益不易计量的问题.造成威胁情报估值难的主要问题是没有通用的方法来评估威胁信息的有效性,并且利益分配与共享模式之间有很大联系,如果共享模式认为威胁信息的共享应该是收费的,那么某用户

或买家在获取威胁信息之前就应根据价格推测该威胁信息的重要性,然而定价方由谁来扮演是个难以抉择的问题.总结起来价值衡量问题可以分为技术和市场2方面:技术方面是由于现在业界尚未对威胁信息的商品化定价、估值达成共识,也没有相应的算法可以估算某威胁情报的市场价值;市场方面是由于从买家角度出发,买方必然希望可以从市场价格推断出该威胁情报的实际使用价值.

当前尚无一种完全客观的评估威胁信息价值的确切方法或者算法.粗糙集(rough sets)理论在处理各种数据,包括不完整的数据以及拥有众多变量的数据方面具有很大优势.李远远[53]给出了一种基于粗糙集理论的指标体系和综合评价方法.基于该文,文献[54]将评估项目分为5个部分:价格、功能、性能/质量、服务、声誉/资格,并依此给出了一个从用户角度评估威胁情报的综合性方法.选择特定的参数并运用这种评估模型,可以对威胁信息提供商的威胁信息产品进行评估、分级.

对用户而言,同一社区下的信息发布者和发布平台所代表的含义是类似的,究竟该关注哪些威胁情报提供者常常是个难以确定的问题.如果不关注质量,盲目选择很多威胁信息提供商,可能会导致自己所运营的系统产生大量的误判、误警,反之则会漏掉很多真正有价值的威胁信息.Meier等人针对这个问题,给出了一个名为FeedRank的模型[55],该模型根据大量威胁信息元数据的原创性,以及被其他威胁信息源所引用多少,来生成一个关系图.该算法可以不依据任何固有事实和反馈,就可以找到威胁信息提供源之间的时空联系.该文的思想对威胁信息估值有一定积极作用,被FeedRank定义为异常的信息来源,其所含的信息若定价过高则不合理.

4 机遇与挑战

在综述现有研究的同时,本文尝试总结威胁情报共享领域当前面临的主要挑战,并结合相关研究进展给予展望.表3列举了目前我国在威胁情报共享方面的问题与机遇.机遇总是与挑战并存,如何发掘现有的知识储备、研究新的方法来解决当前的难题,具有十分重大的未来战略意义.

Table 3 Challenges and Opportunities in Threat Intelligence Sharing Research

表3 威胁情报的共享研究面临的挑战与机遇

Challenges	Opportunities
Lack of laws and regulations Lack of normalized data Lack of systematic research on sharing mode Lack of fair distribution of benefits Face data security risks	Construction goals are centered on national power. Network security threat information format specification has been released. A large amount of scientific research is being carried out. Big-Data and cloud technology have been matured.

目前,我国在威胁情报共享领域的研究还处于起步阶段,基于威胁情报的网络安全技术相对落后.未来,对威胁情报共享理论与技术的研究还需要长时间的探索与积累,需要根据本国国情和技术积累情况找寻全面了解大规模网络攻击情况的关键步骤,积极开展以威胁情报为核心的战略研究.

1) 以国家力量为核心建设目标

由于我国情报共享大环境还处于萌芽状态,没有对共享规范、共享模式等进行系统的研究,因此尚无有效的情报共享机制,并且在更深层次的研究中缺少可依据的法律法规.针对上述问题,需要集中个人、组织、企业、政府的力量加大以威胁情报共享为核心的科研投入,制定相应标准规范和法律法规作为共享技术推广的法律依据和理论技术参考,对威胁情报共享体系进行规范化、实用性建设.此外,将更多具有网络威胁防范能力的企业、组织动员到威胁情报共享体系的建设活动中去,是提升网络空间安全态势感知水平的另一重要手段.

2) 交叉学科加以辅助

威胁情报共享领域的研究目标多、研究范围广,在一定程度上仅依赖于信息安全领域的理论知识和技术无法实现完善的共享机制,需要借助经济学、情报学和运筹学等交叉学科的内容来加以配合,从而能够建立一个健康持久、公平有序的威胁情报共享机制.

3) 成熟技术的运用

虽然目前在威胁情报共享方面对数据的评估、隐私保护等环节缺少体系研究,知识积累不足,但是其他平台的相关技术或已成熟,比如大数据平台方面的用户隐私保护、数据计费技术,以及区块链技术在医疗信息共享和物联网信息共享方面的应用等.因此,研究和借鉴现有平台的相关成熟技术,根据不同

共享模式下的数据类型和服务类型的不同加以优化和重建,从而形成具有较好适应性和有效性的威胁情报共享体系.

除此之外,我们还可以得到关于建立健全威胁情报共享机制的一些启示.一方面,为充分保障情报共享者的权益,应设立强有力的奖惩制度,调动各方共享情报的积极性,并严厉打击"搭便车"行为以防止其对健康共享环境造成的负面影响;另一方面,在已建立的共享关系中引导道德舆论,形成共享实体之间的心理契约,达成共享圈中共同的价值观对于促进协同合作,约束投机者的行为也具有重要意义.

5　结束语

在网络技术日益翻新的今天,洞悉行业的威胁情报,并及时根据情报指南增强安全应对策略,是保障系统正常运作的关键."大医治未病",利用威胁情报的共享技术和方法及时把将要发生的安全事件扼杀于摇篮中,是代价最小、损失最少的策略.各行各业彼此共享威胁情报是实现共赢的必要条件.

本文总结了威胁情报共享方面的最新研究,梳理了威胁情报共享在外部环境、共享参与者、共享数据3个方面的问题及相应举措,并给出我国当前所面临的机遇与挑战.

在未来我们将持续关注威胁情报及其共享的学术研究及产业应用,特别是在发展我国独立自主可扩展的威胁信息表达与传输协议、建立合理且有实际效益的威胁情报质量评估、隐私保护机制等方面.

参　考　文　献

[1] Hutchins E M, Cloppert M J, Amin R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains [J]. Leading Issues in Information Warfare & Security Research, 2011, 1(1): 80-106

[2] Piper S. Definitive Guide to Next Generation Threat Protection [M]. Annapolis, MD: CyberEdge Group, 2013

[3] Choo K-K R, Smith R G, McCusker R, et al. Future directions in technology-enabled crime: 2007-09 [M]. Canberra: Australian Institute of Criminology, 2007

[4] Schneier B. How changing technology affects security [J]. IEEE Security & Privacy, 2012, 10(2): 104-104

[5] Li Yu, He Jianbo, Li Junhua, et. al. Analysis on the technical framework and standards of US cyber threat intelligence sharing [J]. Security Science and Technology, 2016, (6): 16-21 (in Chinese)
(李瑜, 何建波, 李俊华, 等. 美国网络威胁情报共享技术框架与标准浅析[J]. 保密科学技术, 2016, (6): 16-21)

[6] Ma Minhu, Fang Ting, Wang Yue. Analysis and enlightenment of US cybersecurity information sharing mechanism [J]. Journal of Intelligence, 2016, 35(3): 17-23 (in Chinese)
(马民虎, 方婷, 王玥. 美国网络安全信息共享机制及对我国的启示[J]. 情报杂志, 2016, 35(3): 17-23)

[7] Yang Peian, Wu Yang, Su Liya, et al. Overview of threat intelligence sharing technologies in cyberspace [J]. Computer Science, 2018, 45(6): 9-18, 26 (in Chinese)
(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, 26)

[8] McMillan R, Pratap K. Market guide for security threat intelligence services, (G00259127) [R]. Stamford, CT: Gartner, Inc., 2014

[9] Friedman J, Bouchard M. Definitive Guide to Cyber Threat Intelligence: Using Knowledge About Adversaries to Win the War Against Targeted Attacks [M]. Annapolis, MD: CyberEdge Group, 2015

[10] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks [J]. Computers & Security, 2018, 72: 212-233

[11] Vázquez D F, Acosta O P, Spirito C, et al. Conceptual framework for cyber defense information sharing within trust relationships [C] //Proc of the 4th Int Conf on Cyber Conflict. Piscataway, NJ: IEEE, 2012: 1-17

[12] Serrano O, Dandurand L, Brown S. On the design of a cyber security data sharing system [C] //Proc of 2014 ACM Workshop on Information Sharing & Collaborative Security. New York: ACM, 2014: 61-69

[13] Haass J C, Ahn G-J, Grimmelmann F. Actra: A case study for threat information sharing [C] //Proc of the 2nd ACM Workshop on Information Sharing and Collaborative Security. New York: ACM, 2015: 23-26

[14] Kampanakis P. Security automation and threat information-sharing options [J]. IEEE Security & Privacy, 2014, 12(5): 42-51

[15] Goodwin C, Nicholas J P, Bryant J, et al. A framework for cybersecurity information sharing and risk reduction [R]. Washington: Microsoft, 2015: 2-21

[16] Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing [J]. Computers & Security, 2016, 60: 154-176

[17] Johnson C, Badger M, Waltermire D, et al. Guide to cyber threat information sharing [R]. Gaithersburg, MD: National Institute of Standards and Technology, 2016

[18] Bedrijfsrevisoren D, De Muynck J, Portesi S. Cyber security information sharing: An overview of regulatory and non-regulatory approaches [R]. Athens: European Network and Information Agency, 2015

[19] Wagner C, Dulaunoy A, Wagener G, et al. MISP: The design and implementation of a collaborative threat intelligence sharing platform [C] //Proc of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. New York: ACM, 2016: 49-56

[20] Mutemwa M, Mtsweni J, Mkhonto N. Developing a cyber threat intelligence sharing platform for South African organisations [C] //Proc of 2017 Conf on Information Communication Technology and Society. Piscataway, NJ: IEEE, 2017: 1-6

[21] Leszczyna R, Wróbel M R. Threat intelligence platform for the energy sector [J]. Software: Practice and Experience, 2019, 49(8): 1225-1254

[22] Li Jianhua. 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 (in Chinese)
(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)

[23] Barnum S. Standardizing cyber threat intelligence information with the structured threat information eXpression (STIX™) [R]. Bedford, UK: Mitre Corporation, 2012: 1-22

[24] Connolly J, Davidson M, Schmidt C. The trusted automated exchange of indicator information (TAXII™)[R]. Bedford, UK: Mitre Corporation, 2014: 1-20

[25] Casey E, Back G, Barnum S. Leveraging CybOX™ to standardize representation and exchange of digital forensic information [J]. Digital Investigation, 2015, 12: S102-S110

[26] China Information Security Standardization Technical Committee. GB/T 36643—2018 Information security technology-Cyber security threat information format [S]. Beijing: State Administration for Market Regulation of the P. R. C and Standardization Administration of the P. R. C, 2018 (in Chinese)
(全国信息安全标准化技术委员会. GB/T 36643—2018 信息安全技术网络安全威胁信息格式规范[S]. 北京: 国家市场监督管理总局、中国国家标准化管理委员会, 2018)

[27] Sandhu R, Krishnan R, White G B. Towards secure information sharing models for community cyber security [C] //Proc of the 6th Int Conf on Collaborative Computing: Networking, Applications and Worksharing. Piscataway, NJ: IEEE, 2010: 1-6

[28] Zhao Wanying, White G. A collaborative information sharing framework for community cyber security [C] //Proc of 2012 IEEE Conf on Technologies for Homeland Security. Piscataway, NJ: IEEE, 2012: 457-462

[29] Zhao W, White G. Designing a formal model facilitating collaborative information sharing for community cyber security [C] //Proc of the 47th Hawaii Int Conf on System Sciences. Piscataway, NJ: IEEE, 2014: 1987-1996

[30] Li Jiabin, Xue Zhi. Distributed threat intelligence sharing system: A new sight of P2P botnet detection [C] //Proc of the 2nd Int Conf on Computer Applications & Information Security. Piscataway, NJ: IEEE, 2019: 1-6

[31] Lin Yue, Wang He, Yang Bowen, et al. A blackboard sharing mechanism for community cyber threat intelligence based on multi-agent system [C] //Proc of Int Conf on Machine Learning for Cyber Security. Berlin: Springer, 2019: 253-270

[32] Rawat D B, Njilla L, Kwiat K, et al. iShare: Blockchain-based privacy-aware multi-agent information sharing games for cybersecurity [C] //Proc of 2018 Int Conf on Computing, Networking and Communications. Piscataway, NJ: IEEE, 2018: 425-431

[33] Homan D, Shiel I, Thorpe C. A new network model for cyber threat intelligence sharing using blockchain technology [C] //Proc of the 10th IFIP Int Conf on New Technologies, Mobility and Security. Piscataway, NJ: IEEE, 2019: 1-6

[34] English C D. The georgia information sharing and analysis center: A model for state and local governments role in the intelligence community [R]. Monterey, CA: Naval Postgraduate School, 2004

[35] Gao Yali, Li Xiaoyong, Peng Hao, et al. HinCTI: A cyber threat intelligence modeling and identification system based on heterogeneous information network [J]. IEEE Transaction on Knowledge and Data Engineering, 2020: 1-1

[36] Zhao Jun, Yan Qiben, Li Jianxin, et al. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data [J]. Computers & Security, 2020, 95: No.101867

[37] Wagner T D, Palomar E, Mahbub K, et al. A novel trust taxonomy for shared cyber threat intelligence [J]. Security and Communication Networks, 2018: No.9634507

[38] Gao Yali, Li Xiaoyong, Li Jirui, et al. Graph mining-based trust evaluation mechanism with multidimensional features for large-scale heterogeneous threat intelligence [C] //Proc of 2018 IEEE Int Conf on Big Data. Piscataway, NJ: IEEE, 2018: 1272-1277

[39] Riesco R, Larriva-Novo X, Villagrá V A. Cybersecurity threat intelligence knowledge exchange based on blockchain [J]. Telecommunication Systems, 2020, 73(2): 259-288

[40] Tosh D K, Sengupta S, Mukhopadhyay S, et al. Game theoretic modeling to enforce security information sharing among firms [C] //Proc of the 2nd IEEE Int Conf on Cyber Security and Cloud Computing. Piscataway, NJ: IEEE, 2015: 7-12

[41] Kamhoua C, Martin A, Tosh D K, et al. Cyber-threats information sharing in cloud computing: A game theoretic approach [C] //Proc of the 2nd IEEE Int Conf on Cyber Security and Cloud Computing. Piscataway, NJ: IEEE, 2015: 382-389

[42] Vakilinia I, Tosh D K, Sengupta S. 3-way game model for privacy-preserving cybersecurity information exchange framework [C] //Proc of 2017 IEEE Military Communications Conf (MILCOM 2017). Piscataway, NJ: IEEE, 2017: 829-834

[43] Asokan N. Fairness in electronic commerce [D]. Zürich: IBM Research Division, 1998

[44] Lu Zhengfu, Pu Yanhong, Ni Shengbin, et al. Design and simulation of fair data exchange protocol with bounded rationality [J]. Computer Science, 2018, 45(11): 115-123 (in Chinese)
(陆正福, 普艳红, 倪盛斌, 等. 有限理性公平数据交换协议的设计与仿真[J]. 计算机科学, 2018, 45(11): 115-123)

[45] Shapley L S. A value for n-person games [J]. Contributions to the Theory of Games, 1953, 2(28): 307-317

[46] de Fuentes J M, González-Manzano L, Tapiador J, et al. PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing [J]. Computers & Security, 2017, 69: 127-141

[47] Wagner T D, Palomar E, Mahbub K, et al. Towards an anonymity supported platform for shared cyber threat intelligence [C] //Proc of the Int Conf on Risks and Security of Internet and Systems. Berlin: Springer, 2017: 175-183

[48] Dara S, Zargar S T, Muralidhara V. Towards privacy preserving threat intelligence [J]. Journal of Information Security and Applications, 2018, 38: 28-39

[49] Albakri A, Boiten E, De Lemos R. Sharing cyber threat intelligence under the general data protection regulation [C] //Proc of the Annual Privacy Forum. Berlin: Springer, 2019: 28-41

[50] Rutkowski A, Kadobayashi Y, Furey I, et al. Cybex: The cybersecurity information exchange framework (x.1500)[J]. ACM SIGCOMM Computer Communication Review, 2010, 40(5): 59-64

[51] Vakilinia I, Tosh D K, Sengupta S. Attribute based sharing in cybersecurity information exchange framework [C] //Proc of 2017 Int Symp on Performance Evaluation of Computer and Telecommunication Systems. Piscataway, NJ: IEEE, 2017: 1-6

[52] Sadique F, Bakhshaliyev K, Springer J, et al. A system architecture of cybersecurity information exchange with privacy (CYBEX-P) [C] //Proc of the 9th IEEE Annual Computing and Communication Workshop and Conf. Piscataway, NJ: IEEE, 2019: 0493-0498

[53] Li Yuanyuan. Research on the construction of indicator system and comprehensive evaluation method based on rough set [D]. Wuhan: Wuhan University of Technology, 2009 (in Chinese)
(李远远. 基于粗糙集的指标体系构建及综合评价方法研究[D]. 武汉: 武汉理工大学, 2009)

[54] Li Qiang, Jiang Zhengwei, Yang Zeming, et al. A quality evaluation method of cyber threat intelligence in user perspective [C] //Proc of the 17th IEEE Int Conf on Trust, Security and Privacy in Computing and Communications/12th IEEE Int Conf On Big Data Science and Engineering. Piscataway, NJ: IEEE, 2018: 269-276

[55] Meier R, Scherrer C, Gugelmann D, et al. FeedRank: A tamper-resistant method for the ranking of cyber threat intelligence feeds [C] //Proc of the 10th Int Conf on Cyber Conflict. Piscataway, NJ: IEEE, 2018: 321-344

Lin Yue, born in 1995. Master. Her main research interest is network security situational awareness.

Liu Peng, born in 1996. PhD candidate. His main research interest is system security.

Wang He, born in 1987. PhD, lecturer of Xidian University. Her main research interests include cryptography, quantum cryptography and quantum communication protocols.

Wang Wenjie, born in 1964. PhD, associate professor of University of Chinese Academy of Sciences. His main research interests include information security and intelligent information processing.

Zhang Yuqing, born in 1966. PhD, professor, PhD supervisor. His main research interest is information security.