网络空间威胁情报共享技术综述

杨沛安[1,2] 武 杨[1,3] 苏莉娅[1,3] 刘宝旭[1,3]
(中国科学院大学 北京 100049)[1] (中国科学院高能物理研究所 北京 100049)[2]
(中国科学院信息工程研究所 北京 100093)[3]

摘 要 如今,以高级可持续威胁(APT)为代表的新型攻击越来越多,传统安全防御手段捉襟见肘,网络空间安全态势日趋严峻。威胁情报具有数据内容丰富、准确性高、可自动化处理等特点,将其用于网络安全分析中可以有效提高安全防御能力。因此,威胁情报越来越被关注,学术界和产业界已针对威胁情报分析与共享开展了相应研究。文中首先对威胁情报的价值、意义进行了分析,并对威胁情报和威胁情报厂商进行了分类;然后重点从威胁情报共享技术面临的主要问题出发,分析和总结了学术界和产业界针对这些问题进行的研究与尝试;最后展望了威胁情报共享领域未来的研究内容。

关键词 网络空间安全,威胁情报,情报共享,数据挖掘
中图法分类号 TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.06.002

Overview of Threat Intelligence Sharing Technologies in Cyberspace

YANG Pei-an[1,2] WU Yang[1,3] SU Li-ya[1,3] LIU Bao-xu[1,3]
(University of Chinese Academy of Sciences, Beijing 100049, China)[1]
(Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, China)[2]
(Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)[3]

Abstract Nowadays, new kinds of cyber-attacks, such as APT and DDoS, have lower concealment, lower attack cost and huge attack effect. These advantages can let them easily escape from the detection of traditional cyber-attack measures. Cyber-space security situation is becoming more and more severe. The detection and prevention of these attacks have become much harder. CTI(Cyber Threat Intelligence) based network defence has been proved to be a promising strategy to address this problem. In this case, both academic and business circle have put many efforts on CTI analysis and sharing. This paper introduced the meaning and value of CTI. Then aiming at the sharing for threat intelligence, it studied and reviewed the works and developments in CTI sharing deeply. In the end, it looked ahead to the future study of CTI sharing.

Keywords Cyberspace security, Threat intelligence, Intelligence sharing, Data mining

1 引言

当前网络空间的攻防战是一场“非对称”战争。利用0day漏洞的APT攻击等新型威胁和攻击层出不穷,攻击方拥有较长的准备时间、丰富且高效的攻击工具和相对较低的攻击成本。而传统的安全防护大多依靠部署于边界或特殊节点的防火墙、入侵检测系统、入侵防御系统等安全设备进行静态防御,实行以特征检测为主的网络安全监控,并基于预置规则匹配产生告警信息。这些传统方法在面对新型威胁和攻击时,防御和检测的效果甚微[1]。防守方的响应时间相对较短,缺乏有效的检测识别工具,同时需要花费相对更高的防御成本。在这种形势下,提高检测识别准确率,缩短响应时间,降低防御成本,成为网络安全领域的研究重点。威胁情报具有高度规范化的数据格式,可机读,也可人工分析;同时,威胁情报数据内容的知识密度大、准确性高、关联性强,可以为安全分析的各个阶段提供有力的数据支撑。因此,各国的安全团队都开始积极地挖掘威胁情报数据的价值,研究威胁情报分析与共享技术。

美国是最早在政府层面开展威胁情报建设的国家,在20世纪90年代后期其就已认识到信息共享将在网络安全防御保障任务中起到重要的作用,不仅在多项国家政策中倡导和促进信息共享,还将信息共享要求上升到国家战略的高度。近年来,美国政府在网络安全政策立法及促进联邦政府和私营部门之间的网络安全信息共享方面持续投入了大量精力,

到稿日期:2017-05-05 返修日期:2017-08-04
杨沛安(1988-),男,博士生,主要研究方向为网络信息安全、情报分析与共享,E-mail:yangpa@ihep.ac.cn;**武 杨**(1985-),男,博士,助理研究员,主要研究方向为网络安全、威胁情报,E-mail:youngywu@tencent.com(通信作者);**苏莉娅**(1993-),女,硕士生,主要研究方向为网络安全态势感知;**刘宝旭**(1972-),男,研究员,博士生导师,主要研究方向为网络攻防、态势感知等。

更是设立了白宫情报办公室来领导全国各级情报机构、组织和企业间的信息共享事务。美国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[2]。

根据 CNCERT 的研究[3],近年来我国逐渐成为各类网络攻击的重灾区,而其中以 APT 和 DDoS 为代表的新型攻击所占的比重越来越大[4-5]。这些新型攻击有着目标专一、持续时间长、危害大等特点,针对它们的检测与防御往往存在检测识别难度高、响应处置效果差等问题。而由于我国的威胁情报体系发展还处于起步阶段,情报分析与共享等领域都缺少深入的理论和技术研究[6],基于威胁情报的网络安全分析技术较为落后,面对新型攻击更加难以进行有效的检测与防御,网络空间安全态势极为严峻。

为了扭转这种被动局面,我国正逐步展开网络空间安全战略,根据自身需求和技术积累现状,结合云计算、大数据等前沿技术,积极开展威胁情报感知、分析和共享的研究。目前,学术界和产业界都积极开展相关技术的研究,寻求合作,并建立市场主导、政府监督、联盟协同、实体运营的国内情报共享体制,从而促进国内威胁情报技术的发展,进一步提高国家网络空间安全的整体防御能力。

通过深入研究情报分析与共享技术发现,制约情报共享的主要问题是共享数据的有效性计量和有限性约束。有效性计量的问题包括共享数据表达、共享传输规范、共享数据有效性评估等。有限性约束的问题则包括共享风险评估、情报知识产权保护、数据隐私保护等。具体可以总结为 3 个关键问题:如何确定共享数据的格式和内容、共享数据以何种方式共享交换,以及如何使共享数据得到有效保护。

本文主要从情报共享出发对威胁情报进行研究,旨在从多个角度为相关研究者介绍威胁情报共享领域的主要内容及研究现状,为开展相关研究提供参考。

2 威胁情报厂商与威胁情报

2.1 威胁情报厂商

威胁情报生产链中包含了各式各样的情报生产厂商。这些厂商中有的是依托大量设备保有量、在安全防护和分析领域具有丰富经验的硬件厂商,如思科、IBM 等;有的是拥有大量用户、通过长期从事反病毒分析工作积累了海量安全分析数据和经验的杀毒软件厂商,如赛门铁克、红伞、卡巴斯基、360 天眼等;有的是具有丰富的网络安全对抗分析经验的网络安全服务厂商,如 FireEye、CrowdStrike、微步在线等。这些威胁情报厂商通过建立的威胁情报中心进行安全事件的分析和挖掘,从网络犯罪溯源、信誉库、漏洞挖掘、恶意软件分析等多个角度满足不同用户的需求并提供专业服务。表 1 对这些威胁情报厂商的发展和产品信息进行了整理。

表 1 威胁情报厂商的典型代表

Table 1 Typical representatives of threat intelligence manufactures

平台/公司名称	业务说明
FireEye	成立于 2004 年,是一家为企业提供安全防护产品的公司,总部位于美国加利福尼亚州的米尔皮塔斯。近年来,其积极开展威胁情报 TI 业务,与业界企业进行情报共享方面的战略合作。其威胁情报(AIT+)从 FireEye 全球传感器中提取威胁数据,并将它与旗下公司 Mandiant 的事件响应数据融合,产生情报产品。目前能够提供战术、战略和运营情报。
iSight Partners	成立于 2006 年,是历史最悠久的威胁情报厂商之一,目前已在 16 个国家开展业务,支持 24 种语言。公司于 2016 年 1 月被 FireEye 收购。其产品 ThreatScape 覆盖战略、运营、战术 3 方面的威胁情报,可以提供 API 和 SDK 的集成;同时提供与威胁情报相关的其他服务。
Symantec	成立于 1982 年,是信息安全领域处于全球领先地位的解决方案提供商,总部位于加利福尼亚州的 Cupertino,现已在全球 40 多个国家和地区设有分支机构。近年来开始提供威胁情报相关的产品与服务,主要产品为 DeepSight Intelligence,其能提供安全风险、漏洞、IP、URL、域名信用库等情报。
Verisign iDefense	成立于 1999 年,在 2005 年由 VeriSigan 公司以 4000 万美元收购。现拥有 40 多个专职的 TI 分析师,支持 20 种语言,提供覆盖 3 种类型的 14 种威胁情报:犯罪活动、网络犯罪和黑客主义的威胁攻击者情报;漏洞情报;IntelGraph 平台产品,允许客户进行搜索、操作及可视化分析。
CrowdStrike	成立于 2011 年,在 2015 年 7 月的 C 轮融资中得到 1 亿美元的资金。聚焦于不同类型的攻击者(国家、犯罪团伙、黑客及恐怖分子),提供战略、运营及战术层面的情报,拥有一个门户网站及相应的 API 来支持不同的使用方式。
Dell Security	成立于美国佐治亚州亚特兰大,于 2011 年被 Dell 收购,是领先的安全服务公司。客户可以独立地购买威胁情报服务,或将其作为一个完整的安全服务解决方案的组成部分。其情报服务分为两个部分:Global Threat Intelligence 和 Targeted Threat Intelligence,也提供通用及更多定制化的威胁情报。
微步在线	成立于 2015 年 7 月,致力于提供及时、准确的威胁情报,用来阻截攻击、发现威胁、溯源追踪和消除风险。主要产品有 VB(VirusBook.cn)和 TIC(威胁情报中心)。VB 是一个综合性的威胁分析平台,免费为安全人员提供一个便利的一站式分析平台。TIC 的威胁应用解决方案,使客户可以快速发现关键威胁并采取有效的行动。
奇虎 360	成立于 2005 年 9 月,其天眼系统对本地的信息进行了采集和关联分析,还综合了 IP、域名、恶意样本、攻击手法、攻击组织等一系列的信息。

2.2 威胁情报

随着产业界和学术界对威胁情报的持续关注,越来越多的威胁情报应运而生,这些情报的类型多样、内容丰富。从多个层面对威胁情报进行分析,可以加深理解,提高利用效率。下面从数据类型、情报内容、情报来源这 3 个角度对情报共享数据进行分析。

2.2.1 数据类型

从数据类型角度进行分析,威胁情报属于一种海量、多源、异构的数据。它包含了各类结构化或非结构化的数据,如结构化的 TTPs(Tactics,Techniques & Procedures)[7] 情报、非结构化的纯文本情报。Bianco 根据情报的价值和获取的难易程度,将威胁情报分为 Hash、IP、域名、网络或主机特征、攻

击工具、TTPs 6 类[8]，如图 1 所示。

对这 6 类威胁情报的数据结构进行分析可以发现，处于下三层的 Hash、IP、域名类情报属于易于获取但利用价值不高的低级情报，大多属于海量、异构、结构化的网络基础数据，其知识粒度低、关联关系差、应用场景单一，但是易机读、易处理。按照 STIX 规范，这些情报大多可以被归类到 Observables(观测度量)或 Indicator(威胁指标)[7]，用于安全分析中的初始分析阶段。

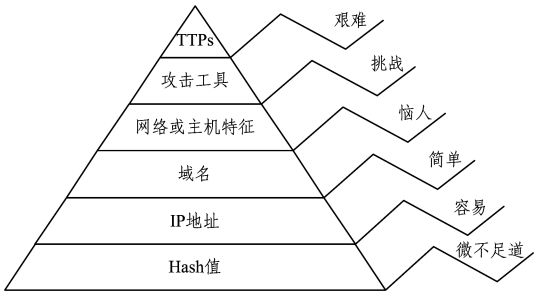

图 1　威胁情报价值及难度金字塔

Fig. 1　Pyramid of threat intelligence value and analysis diffculty

处于上三层的网络或主机特征、攻击工具、TTPs 等情报属于相对不易获取但具有较高利用价值的高级情报。这些情报大多通过对低级情报进行人工或自动化处理得到，以非结构化、具有明显语义的说明文本配合结构化属性信息的方式存储。例如，攻击工具情报对工具名称、MD5、发现时间、作者、静/动态行为特征、族群特征等属性进行结构化存储。这些高级情报包含丰富的知识内容和较强的关联逻辑关系，可以适用于较广泛的安全分析场景。对高级情报进行有效利用，可有效提高安全分析的效率和准确率。但高级情报在可机读、易读性等自动化处理方面往往存在问题，研究如何提高高级情报的自动化分析、处理的识别效率和准确率，对降低攻击检测成本，缩短攻击响应时间和提高攻击防御能力十分重要。

2.2.2　情报内容

从情报内容的角度对威胁情报进行分析可以发现，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不同。将情报内容根据其价值分为以下 3 类(以价值从低到高的顺序给出)，具体如表 2 所列。

1)基础网络类情报，如 IP 黑名单、恶意 URL 列表、CVE 漏洞信息等，是最普遍、最易获得的威胁情报类型。生产这类情报的厂商主要有两种：1)具有较强的恶意代码分析能力的杀毒软件厂商，如赛门铁克、奇虎 360 等；2)专门从事威胁情报处理工作的厂商，如 ThreatStream、微步在线等。第一种厂商开发出的杀毒软件产品拥有巨大的用户使用群体，它们可以从用户处得到海量的基础网络安全数据，如报警、日志等，通过对这些数据进行分析和处理加工，形成不同类型和不同等级的威胁情报。这些厂商在基础网络安全数据的“量”与“质”上拥有绝对的优势，其恶意软件类情报的类型多、内容广，具有较高的准确度、可信度和更新速度。第二种厂商虽然无法获得来自用户的第一手网络安全数据，但它们可以将研究重点集中在分析技术创新和用户体验优化上。通过对分析技术的不断优化，如引入可视化分析技术等，加强对分析结果的质量把控，并根据用户的反馈进行产品升级，其恶意软件类情报产品在易读性、易用性及适用性方面占有很大优势。同时，这些厂商的恶意软件情报往往较为重视产品类型和内容。目前，这类威胁情报可根据用户的需求对情报内容、更新时间、发布方式等进行定制，且定制情报在情报总量中占很大比重。但这类情报由于大多是从安全防御的某一角度入手，虽然内容相对丰富，但面对越来越高级的攻击，可利用的价值正逐渐降低。

2)攻击团体情报，包括深网/暗网[11]监控情报、网络犯罪和黑客主义的威胁攻击者情报等，如 Cyjax 公司发布的暗网活动报告。只有少数公司提供这类情报，主要原因是这类情报的分析难度较大、分析周期长，且需要丰富的分析经验，如深网或暗网中的黑客大多使用隐蔽信道(如 TOR 网络[12])和各种非对称加密通信方法对自身进行隐藏，这类攻击需要大量具有专业知识的人员长期进行有针对性的监视和分析。但这类情报往往包含针对指定黑客团体的深入挖掘分析结果，具有较高的准确性和丰富的情报内容，利用价值较高。

3)APT 分析类情报主要由业界知名的情报厂商发布，如 FireEye 公司发布的《APT28：AT THE CENTER OF THE STORM》[9]分析报告、奇虎 360 发布的《OceanLotus(海莲花)APT 报告》[10]。这些厂商首先针对 APT 攻击进行溯源分析，重建攻击场景，对 APT 攻击事件中的各要素进行挖掘和推理；然后根据分析过程和结果，形成包含各类 IOC 和攻击工具、攻击目标、攻击影响等在内的攻击事件的分析报告。在报告中，厂商还会给出针对特定攻击的防御方法或建议。APT 分析报告不仅包含对攻击事件本身的完整描述(各种攻击特征、指标等)，还对攻击的分析过程进行了详细的阐述，可以为研究者提供完整、有效的安全事件的分析和方法和模型，为其自身安全事件的分析和研究提供借鉴。该类情报包含了极其丰富的知识内容，具有极高的利用价值，是最高级的威胁情报。

表 2　威胁情报内容的分类

Table 2　Classification of content of threat intelligence

情报类别	情报内容	情报特点
基础网络情报	DNS、URL、IP、信誉信息等	这类情报的内容一般只适用于单一网络安全分析领域，内容较为单一，用于对防火墙、入侵检测系统等进行配置；其获取方便、更新快；但情报数据单一、知识粒度小，且准确率因厂商的不同而参差不同。
攻击团体情报	攻击团队、组织在深网/暗网中的交易、攻击活动分析	这类情报主要用于为用户提供攻击者画像、攻击溯源分析；其获取途径有两种：1)渗透到黑客圈、黑市中进行社工分析和定向挖掘；2)对相关攻击事件进行分析；该类情报的获取难度较大，且更新效率低；但其准确率相对较高，且具有很大的参考价值。
APT 分析类情报	APT 攻击事件溯源分析、攻击态势分析	这类情报可为企业和国家制定战术战略提供参考和支持；其来源主要是厂商对 APT 的攻击过程进行分析、拆分和复原，而后对攻击要素进行描述、凝练；由于 APT 攻击具有隐蔽性，该类攻击的分析情报一般不定期更新；但发布报告的知识粒大且准确率很高。

2.2.3 情报来源

从情报来源的角度进行分析，威胁情报主要分为两种：1)安全厂商以产品形式出售或分享；2)开源情报联盟或情报联盟以开源数据的形式分享。其中，安全厂商的安全情报产品主要通过两种方式产生：1)安全厂商通过其遍布互联网的终端软件搜集情报，并通过自身的威胁情报分析中心进行分析处理，然后得到相应的威胁情报，如我国的奇虎 360、美国的 IBM 等；2)安全厂商虽然不具备广泛深度可用的情报搜集终端，但可以通过购买非公开和搜集公开情报来得到数据，针对某些应用场景和业务需求对这些数据进行分析，然后得到相应的威胁情报，如我国的微步在线、美国的 FireEye 等。开源联盟的安全情报主要由联盟内各组织、机构或个人根据己方需求和技术能力，针对特定的安全领域进行公开分析和研究，并在该过程中实现情报信息的共享。这类情报虽然内容相对单一，但在准确性和适用性方面具有较大优势。情报联盟则在共享框架内，根据实际需求对各成员共享的情报进行融合集成，产生更有针对性、更完整且准确的威胁情报，并根据情报类型和价值以开源或有偿销售的形式对外共享。

3 数据表达与传输规范

威胁情报在安全分析中的优势在于其高度结构化的数据框架和具有丰富关联关系的数据内容。但这些特性也使得现有数据表达规范和通信传输协议在威胁情报数据表达的有效性与完整性、传输的准确性与安全性等方面存在问题，无法有效地进行威胁情报的表达和传输。主要问题有 3 个：数据格式不统一，无法相互读取；内容框架不兼容，无法相互理解；传输协议不通用，无法相互传输。针对这些问题，学术界和产业界分别在情报的相关分类与管理、传输规范和表达规范等方面进行了研究。

3.1 威胁情报的共享规范

业界各企业、组织和机构根据在情报共享实际业务中遇到的问题，开展了相关研究工作，提出了一些威胁情报表达和传输的规范。通过对威胁情报规范进行调研分析，对其中有代表性的主要规范的特征和适用范围进行了总结，如表 3 所列。

表 3 典型的威胁情报规范

Table 3 Typical threat intelligence Specification

名称	来源	特点及不足	适用范围
OpenIOC	Mandiant	可拓展、免费、支持 Mandiant 的其他规范；但存在不通用、表达能力有限等问题	识别恶意软件/活动、生成调查线索
STIX	OASIS	表达丰富、共享方便；但结构相对较复杂	威胁识别/分析、管理响应活动、共享
TAXII	OASIS	侧重于警告信息表达和共享	警告、建立/管理共享
CybOX	OASIS	表达元素全面、支持注释、具有良好的健壮性；但结构较复杂	事件分析、威胁检测、电子取证
MAEC	MITRE	侧重于恶意软件的表达	恶意软件/威胁分析、入侵检测
OVAL	MITRE	侧重于漏洞评估、补丁管理及共享	漏洞评估、补丁管理、SIMS、共享

目前，业界的主要安全厂商（如火眼、奇虎 360 等）都以 STIX 作为情报框架，以 TAXII 作为共享与传输规范的情报表达模式[13]，以 CybOX 作为情报构件内容的表达规范，如图 2 所示。究其原因，这 3 个规范都是由 OASIS 根据业界对情报分析和共享的需求，在美国国土安全局的授权下，对其相关情报共享技术进行深入研究后制定的。因此，这 3 种规范无论是在整体实用性还是情报传输有效性与表达准确性等方面，都具有很大优势，得到了业界的普遍认可。

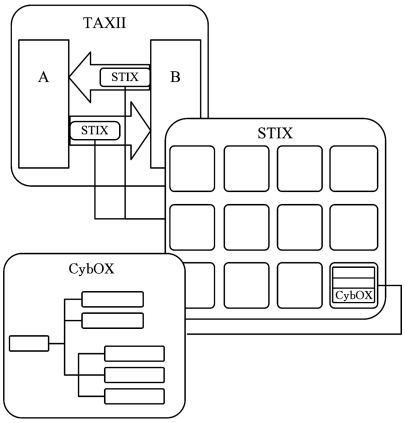

图 2 常用的 STIX，CybOX，TAXII 情报规范组合

Fig. 2 Typical combination of STIX，CybOX and TAXII

下面对情报规范组合的主要内容进行简要介绍。

3.1.1 STIX 2.0

STIX(Structured Threat Information eXpression)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 STIX 2.0 版本[14]。STIX 提供了一种结构化的通用框架来对网络威胁情报进行表达，可以提高情报的准确性、交互操作性和自动处理效率，能够有效地支持对网络威胁管理流程和应用的自动化，并为更高级的网络安全分析（如分析网络威胁、说明网络威胁的特征模式、管理网络威胁应对活动、共享网络威胁情报等）提供模型、框架和规范上的支持。为了使该框架可以适应于各种独立的场景，STIX 在设计之初就将可扩展性考虑在内。其主要构件的逻辑关系如图 3 所示。

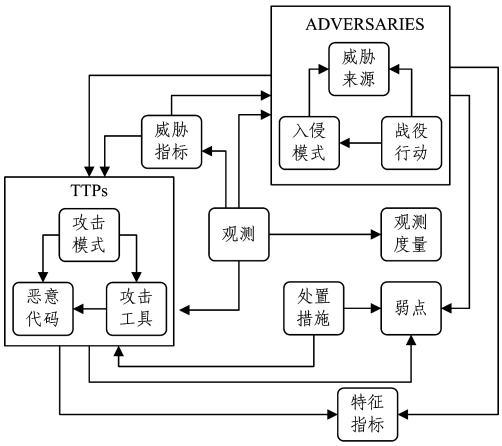

图 3 STIX2.0 组件的逻辑图

Fig. 3 Structure of SITX2.0 objectives

该框架包含了 12 个主要的构件，这些构件分别表达了网

络威胁不同维度的特征，它们在结构上相互独立，在内容上相互关联，如“入侵模式”可以根据“威胁指标”将多个“战役行动”关联到一起，并且指出其中共同的“威胁来源”。

STIX 的灵活性体现在使用者可以自由对这些构建进行组合或独立使用，选择需要的模块进行情报表达。STIX 的扩展性则体现在对各种情报表达规范的支持，即使用者可根据需要设计扩展模块，将需要使用的表达规范引进框架中。但在实际应用中，STIX 也存在着结构关系复杂、表达效率低等问题，需要根据自身的应用进行轻量化自定义使用。

3.1.2　TAXII

网络威胁信息共享已被证明是对抗当今复杂网络威胁的关键。然而，如今的网络威胁信息共享的实践，要么是一个耗时、手动的过程，要么是与特定网络威胁信息分享社区或技术相关联的、范围有限的自动化行为，亟需一种更广泛的、能跨越不同的社区和共享模型、支持不同的共享方法和更广泛的威胁数据的网络威胁信息共享方案。针对这一需求，OASIS-CTI-TC 开发了 TAXII(Trusted Automated exchange of Indicator Information)——一种基于指标信息的可信自动交换规范[15]。

TAXII 的主要内容是一组技术规范和支持文档，用于跨越组织和产品/服务的界限，共享网络威胁信息。这些文档定义了安全交换网络威胁信息的检测、预防和实时缓解网络威胁的协议和数据格式，其框架结构如图 4 所示。

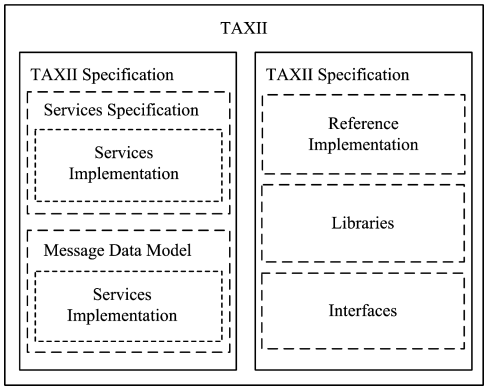

图 4　TAXII 框架结构示意图

Fig. 4　Structure of TAXII components

TAXII 规范定义了组件规范，并针对如何利用 TAXII 进行互操作给出了指导并给出了要求。TAXII 规范还包括一组支持用例。TAXII 服务规范定义了必须考虑与 TAXII 兼容来实现的服务。服务规范在一个较高的层面上描述了信息交换，不将服务绑定到任何特定的交换机制(如 HTTP，SMTP 等)中，但提供使用特定交换机制来实现服务规范的技术规范和要求。TAXII 消息数据模型定义了 TAXII 信息的结构，包括标题、有效载荷、控制和数据信息等内容。TAXII 消息数据模型默认使用 STIX 作为 TAXII 消息的有效载荷，它同样不直接将数据模型绑定到任何特定的表达格式，而是提供在使用不同表达格式(如 XML，JSON 等)来表达信息数据模型时的技术规范和要求。TAXII 工具包则用于支持 TAXII 的应用并协助兼容功能的开发，它包括可供参考的使用样例、一组开发工具及各种函数库、接口 API 等。TAXII 具有良好的可扩展性，目前还在持续更新中。

3.1.3　CybOX

CybOX(Cyber Observable Expression)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，目前已经更新到 CybOX 2.1 版本[16]。可观察对象包括文件、HTTP 会话、系统配置项等。CybOX 规范提供了一套标准且支持扩展的语法，用于描述所有可被从计算系统和操作上观察到的内容。可观察的对象可作为判断威胁的指标，如 Windows 系统中的 Registry Key。这种可观察对象由于具有某个特定值，往往作为判断威胁存在与否的指标。IP 地址也是一种可观察的对象，通常作为判断恶意企图的指标。由于 CybOX 对各类可观测指标具有充分的表达能力，因此在当前威胁情报共享领域中，STIX 框架的各类要素内容都参考 CybOX 规范进行填充。CybOX 规范的数据结构如图 5 所示。

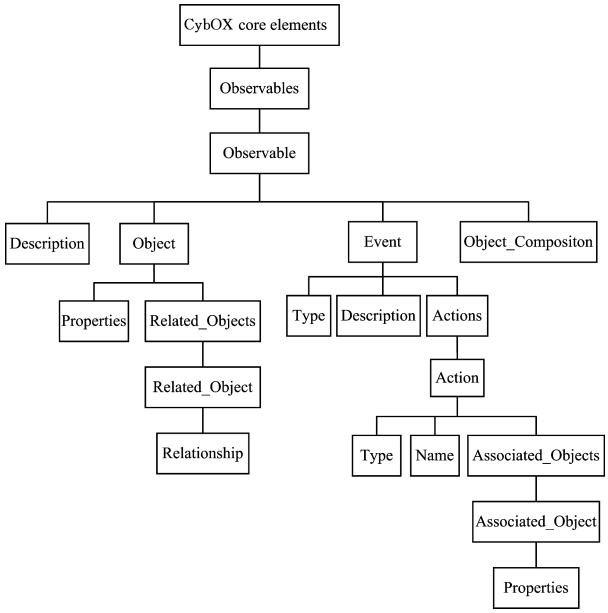

图 5　CybOX 数据框架示意图

Fig. 5　Structure of CybOX objectives

3.1.4　其他相关规范

OpenIOC(Open Indicator of Compromise)是由 MANDIANT 公司基于其多年的数字取证技术，对内部多年使用的情报规范进行整理后对外公布的一个开源的安全情报共享规范框架。该共享规范具有内容丰富、表达灵活且可机读性高等特点。受其主要面向事件响应与数字取证领域的应用限制，OpenIOC 并不完全满足当前企业对威胁情报共享的需求，因此逐步被 STIX 所取代。MAEC(Malware Attribute Enumeration and Characterization)是由 MITRE 公司开发的一种信息标准化语言，它主要被应用于恶意软件/威胁分析、入侵检测等场景中。MAEC 对基于恶意软件的行为、组件信息和攻击模式等属性进行了详细的描述。MAEC 和 STIX 在对恶意软件进行表达时的侧重点不同：MAEC 侧重于提供全面的、结构化的恶意软件样本的详细信息，而 STIX 则侧重于尽可能全面地表达恶意软件样本的基本信息。目前，大部分厂商已使用 Cybox 和 STIX 的组合来替换 MAEC 规范，但仍有少数公司

继续使用 MAEC 和 STIX 的组合规范进行情报共享。OVAL 也是由 MITRE 公司开发的一种描述语言，在漏洞分析中常被用来定义检查项、脆弱点等漏洞技术的细节内容。OVAL 使用标准的 XML 格式组织内容，它提供了足够的灵活性，可以用于分析 Windows，Linux，Unix 以及各种嵌入式操作系统的系统状态、漏洞、配置、补丁等情况，并且具有较好的可机读性，能直接应用到自动化的安全扫描中。但同样由于表达内容、应用场景的局限性，OVAL 并不适用于当前各厂商对威胁情报共享的普遍需求，因此逐步被 STIX 所取代。

3.2 学术界的相关研究

在该领域，学术界有很多研究机构、团体和个人进行了较为广泛的研究。研究主要集中在两个方向：1)针对现有情报共享规范进行优化，目的在于提高共享数据的有效性和共享的效率；2)结合具体的应用场景，进行新型共享规范的设计研究，目的在于提高共享规范的适用性和准确性。具体地，分为情报内容定义与情报分类、情报传输规范、情报表达规范 3 方面，如表 4 所列。

表 4 学术界在情报共享规范领域的研究

Table 4 Research fields of threat intelligence sharing specifications

研究方向	研究内容	研究现状
内容定义与分类	主要研究威胁情报分类与情报内容定义	目前的主要研究大多处于应用需求阶段，集中于如何提高情报的适用性、利用价值和效率。缺少从情报论角度系统地对网络威胁情报的内容进行定义和分类等的研究。
传输规范	针对在传输适应性、准确性方面的需求，对现有规范进行优化和重写	目前主要集中于对点对点情报共享的研究，即研究者仅根据己方对情报传输的需求，结合己方情报内容及格式的特点，基于现有规范进行相关规范的设计和开发；缺少针对具有多成员、需要跨网域共享的情报联盟的共享传输规范的研究。
表达规范	针对现有共享规范在表达适用性和准确性上的不足进行研究，基于 STIX 等规范设计新型情报表达规范	目前主要研究集中在提高安全事件表达的准确性、适用性和可读性方面。该领域内存在两个问题：1)由于情报类型和应用场景不同，相关研究的结果不具有很好的通用性；2)大多研究集中在解决威胁情报可机读性的效率问题上，而在情报易读性、情报内容分类表达等方面的研究较少。

3.2.1 情报的分类与管理

Burger 等人[17]提出使用本体论对情报类型进行整理，进行共享情报的分类计数，建立了一种基于网络安全词项的专家词库来对情报进行描述、比较及区分。该研究在情报分类方面具有一定的借鉴意义，但其情报分类的准确性依赖于安全词库中词项的全面性和完整性，对未知情报的分类效果并不理想。Liao 等人[18]提出在海量数据中对 IOC 信息进行提取时存在效率、适用性、自动化等方面的问题，并给出了一种创新的自动 IOC 提取方法。该方法可以自动化地定位、识别和分析技术文献中出现的 IOC，然后通过语义关系封装得到的 IOC，形成 OpenIOC[19]数据。这些数据不仅包含 IOC 指标项，还包含这些指标项的备注信息(如获取方式、发现位置等)。该研究的重点是基于文本的威胁情报，其研究成果可以有效提高自动化处理这类情报的效率和准确率，但在提高适用性方面并没有进行深入研究。Brown 等人[20]首先讨论了网络安全情报共享对提高网络安全防御能力的重要意义；然后指出由于威胁情报种类多、数据类型繁杂，导致对现有情报的凝练和分析存在困难，同时需要对这些大量情报进行有效的分类和管理，以提高情报的利用价值和利用效率；最后对现有的情报管理平台和共享平台进行了研究和分析，并对平台的优缺点进行了阐述。

3.2.2 情报的传输规范

Field 等人[21]定义了一种来源导向的情报共享方案。该方案提供一种基于 HTTP(s)、使用 Atom+XML 的情报传输规范，对基于 STIX 结构的网络交换信息进行传输。该方法适用于在稳定的共享成员(如情报联盟成员)间进行广泛、深入的情报共享，但在面对低通信频率的共享双方间进行快速、实时的信息交换时，传输效率和准确性欠佳。Steinberger[22]对高速网络中流数据的交换模式和协议进行了调研，对其进行了分类，比较了这些模式与协议在高速网络环境中进行共享传输的效果；为了解决流数据传输中缺少并发协同的问题，提出了一种结构简明、易于部署和整合、适用于威胁情报自动化处置的情报交换格式 FLEX，并通过实验验证了其可以有效提高高速网络中情报共享的效率[23]。Kampanakis 等人[24]重点关注了情报共享中的自动化传输，对现有适用于自动化传输的规范进行了详细分析，给出了不同规范可能适用的应用场景，并针对动态目标防御网络的防护目的提出了一种自动化的情报传输方案。

3.2.3 情报的表达规范

Takahashi 和 Miyamoto[25]提出一种情报表达框架，其用于共享各方在互联网中交换高信息密度的情报。该框架对 IODEF 规范进行了扩展，用以表达如基于 XML 格式的结构化数据。他们从设计、部署并使用多个阶段对该框架的应用进行了详细描述，并通过具体用例验证了该框架的有效性。Ussath[26]针对 STIX 等现有情报表达协议对攻击事件中的关联关系属性表达不够详细的问题进行了研究，提出可以对 STIX，IOC，CybOX 等进行扩展，以更好地适应安全事件分析中的情报共享；并针对在 APT 攻击追踪溯源分析方面的具体需求，提出了一种安全调查模型，该模型支持对多源异构的情报进行处理和分析，以支持自动化和半自动化的溯源分析[27]。Asgarli 等人[28]指出，通用、高效的情报交换可以促进高效、智能、自动化地响应网络攻击，进而有效提高国土防卫能力；而现有的常用的 STIX，IODEF，OpenIOC 等基于 XML 的情报表达规范大多由独立的研究团队根据各自的需求开发，不具备很好的通用性，且在易读性方面受到很大限制。针对这一问题，他们使用本体论和图书馆信息学对这些规范进行分析，找出各种规范的相似度或差异度，然后通过语义学模型分析各自的特征和优势，并在易读性方面对其进行比较。

3.3 共享规范的应用

目前，以 STIX 为主的情报共享规范已被广泛应用于网络威胁的表达与共享中。下面以 STIX 规范为例，对共享规范的应用场景进行简要说明。

如图 6 所示，STIX 的主要应用场景有 4 种：分析网络威胁、明确网络威胁的指标特征、管理网络威胁响应活动和共享网络威胁信息。

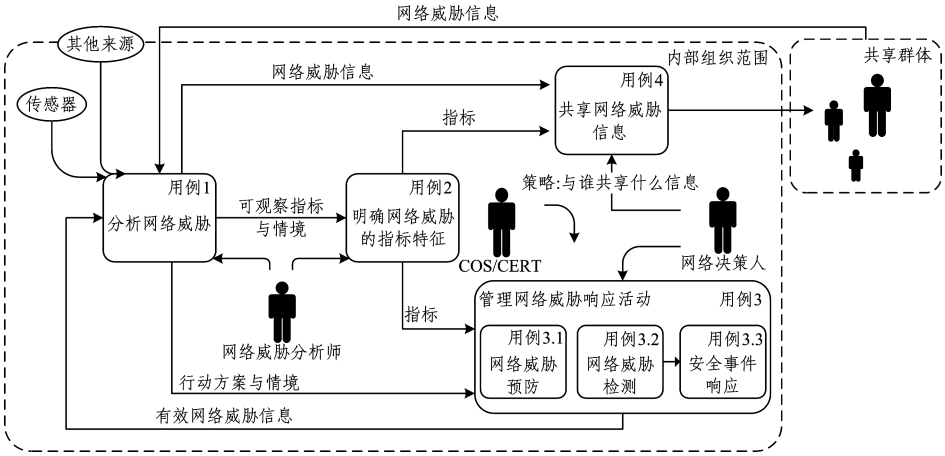

图 6　STIX 应用场景示意图

Fig. 6　Typical STIX application scenes

3.3.1　分析网络威胁

在这一应用场景中,分析人员需要对多源异构的网络威胁信息进行识别、评估和分类,以保证威胁关联的所有信息都得到充分描述并随时更新。基于对这些信息的理解与特征归纳,分析人员可以继续对关联威胁指标特征进行研读和分析,并根据分析结果给出响应威胁活动的建议措施。例如,在对潜在钓鱼攻击进行分析时,分析人员对可疑的钓鱼邮件进行评估分析,以确定相关邮件的附件与链接是否为恶意;评估钓鱼攻击目标与内容的普遍性,确定恶意附件是否打开过或包含链接,同时对所有的分析进行记录。

3.3.2　明确网络威胁的指标特征

在该应用场景中,分析人员需要规定不同的网络威胁情境及其相关元数据的可观测度量,然后对这些威胁特征指标的比对结果进行分析和处理。例如,在确定钓鱼攻击发生后,分析人员首先通过分析钓鱼邮件得到相关的可观测度量(如源/目的 IP、邮件主题、URL、附件等),并识别钓鱼攻击中的相关 TTP,对攻击进行溯源分析和重建;然后在此基础上设置对应的威胁指标,给出合适的响应建议,并生成自动化规则(如 Snort,OVAL 等);最后对所有信息进行整合,从而形成针对该钓鱼攻击的威胁情报。

3.3.3　管理网络威胁响应活动

在该应用场景中,安全管理人员在对特定的安全事件进行检测和调查后,可以通过使用包括处置措施在内的威胁情报对网络中可被利用的漏洞、缺陷或不当配置进行修复和管理。例如,在确认钓鱼攻击发生并具有明确的威胁指标时,安全管理人员可以通过共享得到的钓鱼攻击威胁情报对当前的攻击态势、网络环境威胁、潜在安全隐患等进行分析和评估,并根据威胁情报提供的处置措施进行预防或检测。

3.3.4　共享网络威胁信息

在该应用场景中,网络管理人员一方面需要通过共享得到网络威胁信息,明确威胁类型,确定检查及处置威胁的方法,提高自身的安全防护能力;另一方面,也需要将自身的威胁指标、入侵模式、观测度量等威胁情报共享给他人。例如,在确认钓鱼攻击发生并经过分析和处理得到相关威胁指标、处置方式等情报后,网络管理人员可根据事先确定的情报共享策略与他人自动或手动共享相关情报,实现针对该类型钓鱼攻击的威胁情报共享,提高其检测和防御水平。

4　共享模式

在情报交换的过程中,双方不可避免地会遇到情报共享的有效性和公正性问题。针对这两个问题,学术界和产业界分别从共享平台、共享模型与机制、共享收益分配 3 个方面进行了研究。其中,共享模型与机制的研究包括情报购买方式、情报推送方式等,解决了共享的有效性问题;共享收益分配的研究包括数据价值评估、收益计量等,解决了交易的公正性问题。

4.1　共享交换平台

产业界普遍倾向于从实际业务出发,结合企业发展需求建立情报共享平台,尝试进行情报共享。目前,国外比较典型的威胁情报共享平台有 ThreatCrowd 的威胁搜索平台、VirusTotal 和 VirusBook 的威胁情报在线分析系统、AlientVault 的 OTX 以及 IBM 的 X-force 情报共享平台等。通过对情报共享平台的组织性质、共享内容以及共享机制进行研究,可以将共享平台分为战略合作联盟、威胁情报联盟、互信交换平台和威胁情报集成平台 4 类,各类平台所占的市场份额如图 7 所示。

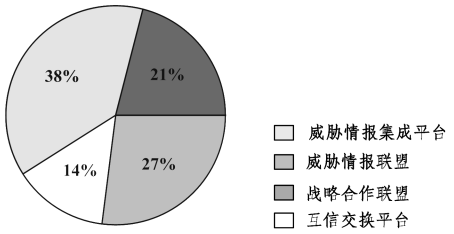

图 7　共享交换平台的分类

Fig. 7　Classification of threat intelligence sharing platform

战略合作联盟主要依赖于安全厂商间的商业运作模式来进行。合作双方一般都有自己侧重的安全领域和技术优势,

通过购买和转让的方式得到对方擅长但己方不擅长的数据和情报；再结合自己的相关数据和情报进行整合分析，组合形成符合各自需求的威胁情报产品。基于这种形式的共享平台有OSINT，IID，iSIGHT Partners，NetClean 等。

威胁情报联盟主要是由相互独立的安全软件厂商（互联网公司、云安全公司、传统安全公司、安全研究人员以及金融、银行等具有较高相似度的行业中的各机构）组成的联盟，它们之间的情报交换可增进企业之间的互信互补，促进参与方对攻击者 TTP 及总体战略的理解，使参与方有机会获取因自身视野存在盲点或信息渠道狭窄而无法搜集到的情报。组成联盟的这些厂商一般都在安全分析的某一领域比较具有权威性，通过联盟的形式共享威胁情报。基于这种形式的共享平台有 Mcafee 和 Symantech 的情报共享联盟等。

互信交换平台大多依托于安全厂商自己的大数据分析平台。大型厂商基于自己多年积累的海量数据，结合其业务需求进行分析，得到大量的威胁情报，并将这些情报存储在自己的大数据平台上。厂商为用户提供查询接口和 API，通过一系列可信度检验和认证机制将威胁情报数据共享给用户，同时允许用户一定程度地更新和维护这些威胁情报。基于这种形式的共享平台有 IBM 的 X-FORCE 和奇虎 360 的天眼等。

威胁情报集成平台主要由专门从事情报分析与处理的情报厂商提供。这类生产厂商自身不采集基础数据，它们搜集或购买相对低级的威胁情报数据，然后根据用户需求、产品定位、技术能力等对低级情报进行加工处理，从而生产更高级别的威胁情报数据，这些数据会以开源或有偿使用的方式进行共享。这类平台包括 ThreatCrowd 和 VirusTotal 等厂商的威胁情报共享平台。

4.2 学术界的相关研究

学术界的研究主要集中在两个方向：共享模式与机制的研究和共享收益分配的研究。前者旨在解决共享过程中数据分发与情报交互缺少有效模型机制的问题，而后者的目标则是解决数据价值评估难度大、收益不易计量等问题，具体描述如表 5 所列。

表 5 学术界在情报共享模型领域的研究

Table 5 Research fields of threat intelligence sharing model

研究方向	研究内容	研究现状
共享模型与机制研究	主要研究共享过程中数据分发和情报交互的模型与框架	该领域的研究重点集中在两方面：1）针对合作伙伴间的情报共享模式进行研究，目的在于提高合作双方在情报共享中的有效性和稳定性；2）针对多角色的共享联盟内部及相互间的情报共享机制进行研究，目的在于提高共享的适用性和可靠性。这些研究缺少针对共享联盟间情报共享过程的系统研究。
收益分配研究	主要研究共享情报的数据价值评估、收益分配等问题	针对威胁情报共享收益分配的研究主要集中在针对特定共享模式下的收益分配上，研究结果缺乏普适性和系统性；另外，该领域的研究没有充分引入金融、经济等交叉学科的内容，使得现有收益分配机制缺乏较高的有效性和适用性。

4.2.1 共享模型与机制研究

Zhao[29] 针对信息分享的必要性和社区网络安全威胁进行了研究，讨论了警告分级方法及针对不同级别信息的分享思路，提出了一种基于合作的社区信息分享体系，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。Kampanakis[30] 调研了现有的情报共享和分析平台，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。Vázque[31] 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 方面入手，探讨如何有效推动情报共享。Haass 等人[32] 与非营利性情报组织 ACTRA 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在技术、政策和组织协调模式 3 方面存在的问题和可能的解决方案。Sandhu[33] 指出传统的面向企业的情报管理模式在具有高动态、分布式等特性的多组织情报传输场景中并不适用，需要一种灵活且严谨的情报共享模式，并针对性地提出了基于角色依赖的新型共享模型，该模型使得参与共享的用户可以自动化地选取角色，大大提高了情报共享各方的适应能力。Tosh 等人[34] 提出了一种基于非合作网络安全情报共享理论的情报共享模型，该模型可以帮助企业独立分析自己是否需要加入到网络情报交换中并共享情报，同时通过利用共享成本动态激励机制来吸引公司进行自主共享，从而获得更高的收益。

4.2.2 共享收益分配研究

近年来，情报共享领域的收益分配问题越来越受到重视，该方面的研究主要集中在针对指定的共享模式研究共享团体收益的分配模型。该领域的研究存在以下几个问题：1）在研究普适性方面，相关研究聚焦于特定的共享团体，结合其具体需求研究收益的分配模式，缺少具有普适性的收益分配体系的系统研究；2）在研究结果的验证方面，由于缺少具体的应用场景与实际部署环境，难以评价研究成果的有效性；3）在研究方法方面，已有研究大多聚焦于信息安全领域的研究思路和方法，较少引入相关交叉学科（如金融学、心理学等）的方法与技术来对收益评估、收益分配体系等收益分配中的关键问题进行研究。

Kamhoua 等人[35] 创造性地将博弈论的相关模型引入到网络安全信息共享研究中，以分析共享的经济收益及非共享的负面影响和损失。他们将微观经济学作为理论基础，以进化博弈的激励方式对人类社会建立模型，以此来研究信息共享的影响；在此基础上，提出了一种动态成本适应机制和分布的启发式学习方法，以帮助组织在共享过程中选取可稳定进化的共享策略；进一步地，研究了异构情报交换参与者对自属性进行共享的意义。Garrido-pelaz 等人[36] 指出多源情报共享可以有效应对愈发难以识别、危害愈发广泛的网络攻击，但情报共享面临着包括收益分配在内的诸多挑战；针对此问题，他们通过模拟不同的网络环境和攻击条件对共享策略进行研究，分析存在依赖关系的组织间进行情报共享的收益效果。

5　数据共享风险的把控

数据的非法使用、非法窃取和篡改以及用户越权访问等问题严重影响着数据共享方对情报共享的积极性，降低了情报共享活动的安全性和有效性。因此，共享风险的把控也是情报共享领域需要重点研究的内容，包括共享数据的脱敏、鉴权、销毁等。

数据脱敏需要建立数据脱敏规则，提供数据匿名化处理方法，并对个人的隐私信息进行匿名化处理。数据鉴权需要对个人的隐私数据提供相应的验证方法，限制各级用户对数据信息的访问权限，同时需要提供预防措施来保证数据的完整、准确、及时和可用。数据销毁需要依照数据分类，分级建立相应的数据销毁机制，提供全面有效的审计制度和方法，对违规共享中涉及到的数据进行销毁。由于数据脱敏在云端存储和计算环境中也有同样的需求，因此已经有了一些研究成果。其中，针对云平台的数据脱敏技术有同态加密[37]、数值混淆、密文检索[38-39]、区块链[40-41]等。但是，一方面，威胁情报共享与云共享在服务类型和用户群体上存在一定区别；另一方面，威胁情报共享在共享主题的结构和内容上存在较大的差异性。这两方面的差异性使得云共享中的数据脱敏及其他相关隐私保护技术并不能完全适用于威胁情报共享，需要根据服务、数据类型和结构的不同进行优化和重建。

目前，国内外针对情报共享领域中数据风险把控方面的研究相对较少。一方面是由于国内情报共享大环境还处于萌芽状态，尚无有效的情报共享机制，因此在更深层次的共享数据风险把控方面的研究缺少可依据的法律法规；另一方面，由于不同共享模式下的数据类型和服务类型不同，需要形成具有较好适应性、有效性的风险分析与评估模型，而目前威胁情报领域在风险评估方面缺少体系研究，知识积累不足。针对上述问题，可研究和借鉴现有大数据平台、云平台的相关成熟技术，结合交叉学科的相关知识进行深入的探索。

结束语　威胁情报体系的出现为安全态势日趋严峻的网络空间带来了一缕曙光。以威胁情报为核心，利用威胁情报种类多、内容丰富、准确率高的特点，可有效提高网络攻击的检测识别能力与响应处理能力。而威胁情报的共享则可以最大程度地提高情报的价值和利用效率，降低安全防御成本，提高防御的响应能力。本文聚焦于威胁情报共享技术，对威胁情报厂商和情报类型进行了介绍，而后针对情报共享中传输与表达规范研究、数据风险把控等领域的研究现状进行了整理和分析。

目前，在威胁情报共享方面的研究还存在较多问题。我国在威胁情报共享领域的研究还处于起步阶段，学术界和产业界都没有对共享规范、共享模式等进行系统的研究；针对不同的情报共享模式和共享对象，要确保共享与传输过程的有效性、准确性和安全性，需要集中对组织、企业以及政府的研究力量进行深入研讨，并建立相关的法律法规、标准框架作为共享技术推广的法律依据和理论技术参考。同时，随着共享技术的发展，在情报共享过程中如何进行共享数据的隐私保护和风险把控，以及在共享后如何进行合理、有效的共享收益分配，都是亟待解决的关键问题。为了能够有效解决这些问题，不仅需要依赖现有信息安全领域的相关技术，如在大数据平台方面的用户隐私保护、数据计费技术等，还需要借鉴金融、经济、情报学等学科的相关知识体系和技术，如合作伙伴间的收益分配原则、基于供应链的企业收益分配等方面的研究，并根据威胁情报共享的具体需求对这些技术进行优化和调整。

参 考 文 献

[1] 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. (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.

[2] MA M H, FANG T, WANG Y. 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.

[3] CNCERT/CC. 2016 中国移动互联网发展状况及其安全报告[R]. 北京：互联网应急响应中心, 2016.

[4] SUN Z. The Attack and Defense Technology Research of Advanced Persistent Threat [D]. Shanghai: Shanghai Jiao Tong University, 2015. (in Chinese)
孙增. 高级持续性威胁(APT)的攻防技术研究[D]. 上海：上海交通大学, 2015.

[5] CUI Y H, YAN L S, LI S F, et al. SD-Anti-DDoS: Fast and Efficient DDoS Defense in Software-Defined Networks [J]. Journal of Network and Computer Applications, 2016, 68: 65-79.

[6] YANG Z M, LI Q, LIU J R, et al. Research of Threat Intelligence Sharing and Using for Cyber Attack Attribution [J]. Journal of Information Security Research, 2015, 1(1): 31-36. (in Chinese)
杨泽明，李强，刘俊荣，等. 面向攻击溯源的威胁情报共享利用研究 [J]. 信息安全研究, 2015, 1(1): 31-36.

[7] OASIS. stix-v2.0-csprd01-part1-stix-core[EB/OL]. [2017-02-24]. https://oasis-open.github.io/cti-documentation/stix/review.

[8] BIANCO D J. The Pyramid of Pain: Intel-Driven Detection & Response to Increase Your Adversary's Cost of Operations[EB/OL]. http://rvasec.com/slides/2014/Bianco_Pyramid%20of%20Pain.pdf.

[9] FireEye. APT28: At the Center of the Storm [EB/OL]. [2017-01-11]. https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html.

[10] 360 天眼实验室. OceanLotus(海莲花)APT 分析报告[EB/OL]. http://bobao.360.cn/news/detail/1601.html.

[11] 秉泽. "暗网"：你所不了解的互联网 [J]. 保密工作, 2016(2): 47-48.

[12] LI X. Research and Implementation of Identification for Tor Anonymous Communication Based on Meek[D]. Beijing: Beijing Jiaotong University, 2016. (in Chinese)
李响. 基于 Meek 的 Tor 匿名通信识别方法的研究和实现[D]. 北京:北京交通大学, 2016.

[13] Eclectic Iq. ABOUT STIX AND TAXII[OL]. https://www.eclecticiq.com/stix-taxii.

[14] OASIS Cyber Threat Intelligence (CTI) TC. About STIX[EB/OL]. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-stix.

[15] OASIS Cyber Threat Intelligence (CTI) TC, The MITRE Corporation. TAXII 2.0 Draft 2[OL]. https://docs.google.com/document/d/1eyhS3-fOlRkDB6N39Md6KZbvbCe3CjQlampiZPg-5u4.

[16] OASIS Cyber Threat Intelligence (CTI) TC. CybOX 2.1[OL]. [2014-01-23]. https://cyboxproject.github.io/releases/2.1.

[17] BURGER E W, GOODMAN M D, KAMPANASKIS P, et al. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies [C]// Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security (WISCS'14). New York: ACM, 2014: 51-60.

[18] LIAO X J, YUAN K, WANG X F, et al. Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence[C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16). New York: ACM, 2016: 755-766.

[19] MANDIANT. Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC[EB/OL]. http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf.

[20] BROWN S, GOMMERS J, SERRANO O. From Cyber Security Information Sharing to Threat Management[C]// Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. New York: ACM, 2015: 43-49.

[21] FIELD J, BANGHART S, WALTERMIRE D. Resource-Oriented Lightweight Information Exchange draft-ietf-mile-rolie-01 [EB/OL]. (2015-12-02). https://tools.ietf.org/html/draft-ietf-mile-rolie-01.

[22] STEINBERGER J, SPEROTTO A, GOLLING M, et al. How to exchange security events Overview and evaluation of formats and protocols [C]// IFIP/IEEE International Symposium on Integrated Network Management. New York: IEEE, 2015: 261-269.

[23] STEINBERGER J, SPEROTTO A, BAIER H, et al. Collaborative attack mitigation and response: A survey[C]// IFIP/IEEE International Symposium on Integrated Network Management. New York: IEEE, 2015: 910-913.

[24] KAMPANAKIS P, PERROS H, BEYENE T. SDN-based solutions for Moving Target Defense network protection[C]// IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks. New York: IEEE, 2014: 1-6.

[25] TAKAHASHI T, MIYAMOTO D. Structured cyber security information exchange for streamlining incident response operations[C]// NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium. New York: IEEE, 2016: 949-954.

[26] USSATH M, JAEGER D, FENG C, et al. Pushing the Limits of Cyber Threat Intelligence: Extending STIX to Support Complex Patterns[M]// Information Technology: New Generations. New York: Springer International Publishing, 2016: 25-44.

[27] USSATH M, FENG C, MEINEL C. Concept for a security investigation framework[C]// International Conference on New Technologies, Mobility and Security. New York: IEEE, 2015: 1-5.

[28] ASGARLI E, BURGER E. Semantic ontologies for cyber threat sharing standards[C]// 2016 IEEE Symposium on Technologies for Homeland Security (HST). Waltham: IEEE, 2016: 1-6.

[29] ZHAO W, WHITE G. A collaborative information sharing framework for Community Cyber Security[C]// Homeland Security. New York: IEEE, 2012: 457-462.

[30] KAMPANAKIS P. Security Automation and Threat Information-Sharing Options [J]. IEEE Security & Privacy Magazine, 2014, 12(5): 42-51.

[31] VÁZQUEZ D F, ACOSTA O P, BROWN S, et al. Conceptual framework for cyber defense information sharing within trust relationships [M]. New York: IEEE, 2012.

[32] HAASS J C, AHN G J, GRIMMELMANN F. ACTRA: A Case Study for Threat Information Sharing[C]// Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS 2015). New York: ACM, 2015: 23-26.

[33] SANDHU R, KRISHNAN R, WHITE G B. Towards Secure Information Sharing models for community Cyber Security[C]// International Conference on Collaborative Computing: Networking, Applications and Worksharing. New York: IEEE, 2010: 1-6.

[34] TOSH D, SENGUPTA S, KAMHOUA C A, et al. Establishing evolutionary game models for cyber security information exchange (CYBEX) [J/OL]. Journal of Computer & System Sciences, http://www.sciencedirect.com/science/article/pii/S0022000001630085X?via%3Dihub.

[35] KAMHOUA C, MARTIN A, TOSH D K, et al. Cyber-Threats Information Sharing in Cloud Computing: A Game Theoretic Approach[C]// IEEE CS Cloud. New York: IEEE, 2015: 382-389.

[36] GARRIDO-PELAZ R, PASTRANA S. Shall We Collaborate?: A Model to Analyse the Benefits of Information Sharing[C]// ACM on Workshop on Information Sharing and Collaborative Security. New York: ACM, 2016: 15-24.

[37] QIAN P, WU M, LIU Z. A Method on Homomorphic Encryption Privacy-preserving for Cloud Computing [J]. Journal of Chinese Computer Systems, 2015, 36(4): 840-844. (in Chinese)
钱萍, 吴蒙, 刘镇. 面向云计算的同态加密隐私保护方法[J]. 小型微型计算机系统, 2015, 36(4): 840-844.

[38] WANG S H, HAN Z J, CHEN D W, et al. New construction of secure range query on encrypted data in cloud computing [J]. Journal of Communications, 2015, 36(2): 33-41. (in Chinese)
王少辉, 韩志杰, 陈丹伟, 等. 云环境下安全密文区间检索方案的新设计 [J]. 通信学报, 2015, 36(2): 33-41.

(下转第 26 页)