网络安全态势感知技术标准化白皮书

2020年版

全国信息安全标准化技术委员会
信息安全评估标准工作组

2020年11月

全国信息安全标准化技术委员会信息安全评估标准工作组

组长：李京春
副组长：顾健、李斌、李嵩
秘书：李健、刘楠

编写单位

公安部第三研究所
新华三技术有限公司
北京神州绿盟科技有限公司
上海观安信息技术股份有限公司
三六零科技集团有限公司
中国信息安全测评中心
中国民航大学
北京锐安科技有限公司
北京天融信网络安全技术有限公司
中国电子技术标准化研究院
中国科学院信息工程研究所
工业信息安全创新中心有限公司
中移动信息技术有限公司
国家信息中心
中国南方电网有限责任公司
北京威努特技术有限公司

编写人员

陈　妍　李京春　李　斌　顾　健　上官晓丽　刘贤刚　王　龑　孙松儿
刘玉岭　叶晓虎　陆　臻　孙　彦　郭　旭　陈宇耀　万　可　杨洪起
吴天昊　张文科　谢　江　张　屹　李　旋　周景贤　刘慧芳　杨　璐
李　健　刘星材　李　宁　吴　槟　郑新华

前言 | PREFACE

网络安全态势感知平台作为网络安全的实时守护者，是实现“全天候全方位感知网络安全态势”的主要手段。为了更好地引导网络安全态势感知技术标准化工作的有序开展，全国信息安全标准化技术委员会（TC260）信息安全评估标准工作组（WG5 工作组）集众多成员单位之合力，由公安部第三研究所牵头，联合业界的主流安全厂商、典型行业用户、科研院所一起努力，最终形成本版白皮书。此外，为了更好地帮助不同行业的用户了解行业内的网络安全风险、网络安全态势感知系统的建设需求和标准需求等，由具有该行业实践经验的参编单位提供了“附录 A 行业案例”，用于给网络安全态势感知相关的研发、生产、建设和部署单位提供参考，这是参编单位的实践结果，不代表本白皮书的立场。附录 B 给出了网络安全态势感知相关的已发布及在研标准。

全书组织如下:

第 1 章介绍了本白皮书的背景。

第 2 章介绍了网络安全态势感知的典型模型，并给出了系统架构。

第 3 章分析了网络安全态势感知的标准化需求以及国内外标准化现状。

第 4 章以问题导向为原则，给出了网络安全态势感知的标准架构并对架构中的各组成部分进行描述。

第 5 章以前面各章为依据，给出了网络安全态势感知标准化工作建议。

附录 A 介绍了政务行业、网络运营服务行业及汽车行业的网络安全态势感知案例，主要分为网络安全风险分析、建设需求分析、标准现状与需求分析三部分。

附录 B 给出与网络安全态势感知相关的已发布及在研标准列表。

参考资料部分列出了本白皮书编写过程中参考的相关资料。由于编制时间仓促，编制组水平有限，错误疏漏在所难免，针对此版白皮书如有任何意见或建议，敬请联系 chenyan@mctc.org.cn。

目录 | CONTENTS

前言 2

第一章 背景 5

第二章 网络安全态势感知技术框架 8

- 典型模型 8
- 系统架构 11
  - 前端数据源 12
  - 核心态势感知 12
  - 影响态势感知的要素 13

第三章 网络安全态势感知标准化需求和现状 14

- 标准化需求 14
- 标准化现状 14
  - 国外标准 14
  - 国内标准 16

第四章 网络安全态势感知标准架构 19

- 基本原则 19
- 总体架构 20
- 组成部分 22
  - 总体框架标准 22
  - 前端数据源类标准 22
  - 数据标准 23
  - 应用标准 24
  - 数据共享标准 25
  - 业务支撑标准 26

第五章 网络安全态势感知标准化工作建议 28

- 统筹规划网络安全态势感知标准 28
- 加快开展亟需标准的制定进程 28
- 积极推进态势感知标准的应用 28

附录 A：行业案例 29

- 政务行业 29
  - 网络安全风险现状 29
  - 建设需求分析 29
  - 标准现状与需求分析 30
- 网络运营服务行业 31
  - 网络安全风险现状 31
  - 建设需求分析 32
  - 标准现状与需求分析 33
- 汽车行业 34
  - 网络安全风险现状 34
  - 建设需求分析 35
  - 标准现状与需求分析 35

附录 B：已发布及在研的标准 37

参考资料 41

第一章 背景

随着组织信息化建设规模的扩大，安全架构日趋复杂，各种类型的安全设备、安全数据越来越多，组织自身的安全运维压力不断加大。另一方面，以高级可持续威胁攻击（Advanced Persistent Threat，APT）为代表的新型威胁的兴起，随着内控与合规的深入，越来越需要组织充分利用更多的安全数据进行分析检测，对基础架构安全、应用安全、数据安全乃至业务安全中面临的各类高级威胁做出判定和响应，以支撑业务持续稳定、安全运行。

独立分割的安全防护体系已经很难应对如此复杂的安全环境。高级恶意程序已经逐渐成为主流，隐秘通道也已经开始向组织内部逐渐渗透。当前网络环境中部署的各类安全设备主要实现单点检测，检测能力受限，导致安全问题依然频繁发生，诸如勒索病毒、APT 攻击，敏感数据泄露等。特别值得注意的是，当这些安全事件发生时，单点安全设施只能给出有限、甚至无法给出相关检测信息，更有甚者有些安全威胁在网络内部发生、潜伏、破坏了数天乃至数月的时间，都难以察觉。总的来说，很多时候组织常常对自身网络安全中的各类威胁看不到、看不清、看不及时，从而给组织日常的安全保障工作带来各方面的危害和影响。

态势感知的概念最早在军事领域提出，覆盖感知、理解和预测三个层次，随着计算机网络的发展又提出了“网络态势感知（Cyberspace Situation Awareness，CSA）”，即在大规模网络环境中对引起网络态势发生变化的要素进行获取、理解、展示以及对发展趋势进行预测，从而帮助决策和行动。随着网络安全复杂性的凸显，态势感知在网络安全领域得到高度重视和广泛应用。

网络安全态势感知是一种基于环境动态地、整体地洞悉安全风险的能力，它利用数据融合、数据挖掘、智能分析和可视化等技术，直观显示网络环境的实时安全状况，为网络安全保障提供技术支撑。网络安全态势感知系统的工作过程大致分为安全要素采集、安全数据处理、安全数据分析和分析结果展示这几个关键阶段。安全要素采集是获取与安全紧密关联的海量基础数据，包括流量数据、各类日志、漏洞、木马和病毒样本等；安全数据处理是通过对采集到的安全要素数据进行清洗、分类、标准化、关联补齐、添加标签等操作，将标准数据加载到数据存储中；安全数据分析和分析结果展示是利用数据挖掘、智能分析等技术，提取系统安全特征和指标，发现网络安全风险，汇总成有价值的情报，并将网络安全风险通过可视化技术直观地展示出来。

借助网络安全态势感知，运维人员可以及时了解网络状态、受攻击情况、攻击来源以及哪些服务易受到攻击等情况；用户单位可以清楚地掌握所在网络的安全状态和趋势，做好相应的防范准备，减少甚至避免网络中病毒和恶意攻击带来的损失；应急响应组织也可以从网络安全态势中了解所服务网络的安全状况和发展趋势，为制定有预见性的应急预案提供基础。

1999 年，美国人 Tim Bass 提出网络态势感知的概念；2000 年，他将该技术应用于多个网络入侵检测系统检测结果的数据融合分析，开启了网络安全态势感知技术蓬勃发展的序幕。美国将网络安全态势感知作为其国家安全防御体系中的重要组成部分，从国家安全的整体高度进行统一规划和部署。根据 2002 年的《国土安全法案》和《联邦信息安全管理法案》，美国联邦政府于 2003 年开始启动爱因斯坦计划，建设大规模信息安全监控系统，自动收集、关联分析和共享政府机构间的安全信息，快速感知和应对网络安全面临的威胁，增强美国政府的网络安全态势感知能力和网络安全防御能力。自 2003 年开始启动“爱因斯坦 -1”计划，到 2007 年的“爱因斯坦 -2”，再到 2012 年开始“爱因斯坦 -3”，截至 2019 年 9 月，在 104 个联邦民事机构中，已有 76 个已经完全实现了“爱因斯坦 -3”计划的基本能力。美国政府期望通过爱因斯坦计划的实施，保护美国国内重要的网络信息资产，同时，还能感知监控他国互联网应用，使其成为主动防御甚至反制的工具，最终成为美国国家安全战略体系中的重要组成部分。另外，美国军方出于网络战等方面的考虑，也在积极发展网络安全态势感知能力。这些网络安全态势感知系统的建设使美军在网络空间战场中的态势感知能力和作战能力得到极大提升，也给全球网络空间的安全带来重大影响。

我国高度重视网络安全态势感知能力建设。在国家层面上，通过制定相关政策方针对网络安全态势感知能力建设和发展制定了战略规划，从而带动了“产学研用”各方面的协同发展。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上提出要“全天候全方位感知网络安全态势”。2016 年 11 月发布的《网络安全法》第五章提出将网络安全监测预警与应急处置工作制度化、法制化，为深化网络安全防护体系、实现“全天候全方位感知网络安全态势”提供了法律依据和保障。2016 年 12 月，国务院发布的《“十三五”国家信息化规划》对实现“全天候全方位感知网络安全态势”提出了具体要求：要求“加强网络安全态势感知、监测预警和应急处置能力建设。建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。建立政府和企业网络安全信息共享机制，加强网络安全大数据挖掘分析，更好地感知网络安全态势，做好风险防范工作。”该规划还要求部署建设“网络安全监测预警和应急处置工程”，包括：“建立国家网络安全态势感知平台，利用大数据技术对网络安全态势信息进行关联分析、数据挖掘和可视化展示，绘制关键信息基础设施网络安全态势地图。建设工业互联网网络安全监测平台，感知工业互联网网络安全态势，为保障工业互联网安全提供有力支持。”该规划还同时提出了要建立国家网络安全态势感知平台和党政机关网络安全态势感知系统。

国内的高校和科研院所很早就开始了态势感知相关理论和基础技术的科学研究工作，并取得了一定的成果，搭建了多个原型系统、发表了大量的学术论文；各监管机构和主管部门积极响应国家政策，从组织、策略、技术、运维等各方面为建设和应用网络安全态势感知提

供了保障和支撑；多个省、市、地区、行业以及大型企事业单位进行了网络安全态势感知系统的建设；旺盛的市场需求调动了广大安全厂商的积极性，出现了很多有特色的网络安全态势感知产品。

然而不同于传统防火墙、入侵检测、安全审计等功能相对固化的产品，网络安全态势感知的概念及应用则复杂很多。虽然很多产品和平台都宣称具备网络安全态势感知的三要素：态势获取、态势理解和态势预测，但一方面缺乏网络安全态势感知技术、框架、功能等标准，另一方面也缺少业界公认的针对网络安全态势感知的综合评价指标，导致实际部署后的应用效果千差万别，没有给用户带来实际的网络安全监测与防护效果，反而造成了资源浪费，同时给市场和监管带来了一定的混乱。另外，网络安全态势感知系统需要从多种数据源进行数据采集，并与多个其他安全产品和系统进行联动，存在较多需要定义的数据接口，目前各产品厂商、各平台建设单位各自为政，缺乏统一的数据接口，数据对接、威胁情报共享工作的实际落地较为困难。解决这些问题需要有配套的态势感知标准来对相关系统和产品的功能进行规范，保障相关产品和系统的质量；对态势感知的评价指标进行构建，保证系统输出结果的一致性；对系统间数据采集、数据共享、协同联动的接口进行统一，促进不同厂商产品和系统之间的互联互通。

网络安全态势感知标准能对态势感知能力的建设起到规范和指导作用，主要体现在如下方面：一是通过规范态势感知产品开发者、平台建设者的设计、开发和建设流程，统一系统框架，提升系统的技术水平；二是通过规范态势感知服务组织的基础安全管理、数据安全管理、系统安全管理和安全运维等，提升系统防范安全风险的能力；三是规范行业体系，对系统的数据采集、数据共享、协同联动的接口进行统一，促进不同厂商产品和系统之间的互联互通，从而进一步支撑网络安全态势感知的快速发展。为此，亟待从技术和产业发展角度加快推进网络安全态势感知的标准化工作，为我国网络安全态势感知的健康发展提供有力保障。

本白皮书对网络安全态势感知的概念和发展历史进行了分析梳理，基于相关典型模型给出了网络安全态势感知的技术框架，基于标准化需求和现状给出网络安全态势感知的标准架构，并提出开展态势感知标准化工作建议，为各级监管部门和企事业单位在进行网络安全态势感知能力建设和管理时提供标准化思路，为各系统生产厂商在进行网络安全态势感知系统设计、开发、部署和应用过程中提供标准化指导。

第二章 网络安全态势感知技术框架

本章将调研网络安全态势感知的典型模型，并在此基础上给出网络安全态势感知系统架构和主要组成部分。

典型模型

在对态势感知的研究中，学术界和行业界提出了多种相关的模型和技术，比较著名的有 Endsley、JDL 和 Tim Bass 三个经典模型，这些模型为网络安全态势感知理论和技术的发展提供了参考和借鉴。

1）Endsley 模型

Endsley 模型是在 1995 年由前美国空军首席科学家 Mica R. Endsley 仿照人的认知过程建立，主要分为核心态势感知与影响态势感知的要素两部分，其中核心态势感知包括：态势要素感知、态势理解和态势预测，如图 2.1 所示。

核心态势感知：

- 第 1 级态势要素提取：提取环境中态势要素的位置和特征等信息；
- 第 2 级态势理解：关注信息融合以及信息与预想目标之间的联系；
- 第 3 级态势预测：主要预测未来的态势演化趋势以及可能发生的安全事件。

影响态势感知的要素主要分为任务和系统要素以及个人因素，实现态势感知能力依赖于各影响要素提供的服务。态势感知系统最终的执行效果将反馈给核心态势感知，形成正反馈，不断提升态势感知的总体能力。

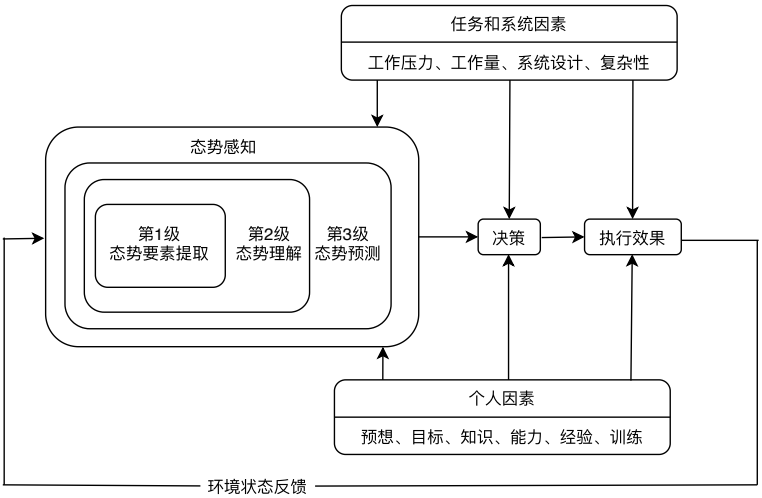

图 2.1Endsley 模型

2）JDL 模型

面向数据融合的 JDL（Joint Directors of Laboratories）模型体系，是在 1984 年，由美国国防部成立的数据融合联合指挥实验室提出，经过逐步改进和推广使用而形成。它将来自不同数据源的数据和信息综合分析，根据它们之间的相互关系，进行目标识别、身份估计、态势评估和威胁评估，通过不断的精炼评估结果来提高评估的准确性。该模型已成为美国国防信息融合系统的一种实际标准。该模型的具体结构如图 2.2 所示：

- 第 0 级数据预处理：负责过滤、精简、归并来自信息源的数据，如入侵检测警报、操作系统及应用程序日志、防火墙日志、弱点扫描结果等；
- 第 1 级对象精炼：负责数据的分类、校准、关联及聚合，精炼后的数据被纳入统一的规范框架中，多分类器的融合决策也在此级进行；
- 第 2 级态势精炼：综合各方面信息，评估当前的安全状况；
- 第 3 级威胁精炼：侧重于影响评估，既评估当前面临的威胁，也预测威胁的演变趋势以及未来可能发生的攻击；
- 第 4 级过程精炼：动态监控融合过程，依据反馈信息优化融合过程。

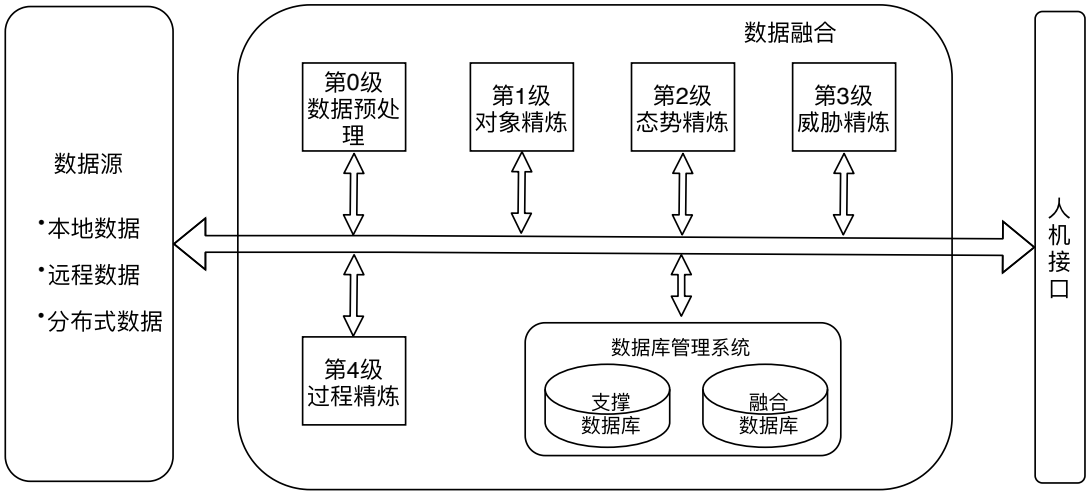

图 2.2 JDL 模型

3）Tim Bass 模型

1999 年，Tim Bass 等人在态势感知三级模型的基础上提出了从空间上进行异构传感器管理的功能模型，模型中采用大量传感器对异构网络进行安全态势基础数据的采集，并对数据进行融合，对知识信息进行比对。该模型以底层的安全事件收集为出发点，通过数据精炼和对象精炼提取出对象基，然后通过态势评估和威胁评估提炼出高层的态势信息，并做出相应的决策，该框架将数据由低到高分为数据、信息和知识三个层面。该模型具有很好的理论意义，为后续的研究提供了指导，但最终并未给出成型的系统实现。该方法的缺点是当网络系统很复杂时，威胁和传感器的数量以及数据流会变得非常巨大而使得模型不可控制。该模型的具体结构如图 2.3 所示：

- 第 0 级数据精炼：负责提取、过滤和校准原始数据；
- 第 1 级对象精炼：将数据规范化，做时空关联，按相对重要性赋予权重；
- 第 2 级态势评估：负责抽象及评定当前的安全状况；
- 第 3 级威胁评估：基于当前状况评估可能产生的影响；
- 第 4 级资源管理：负责整个过程的管理。

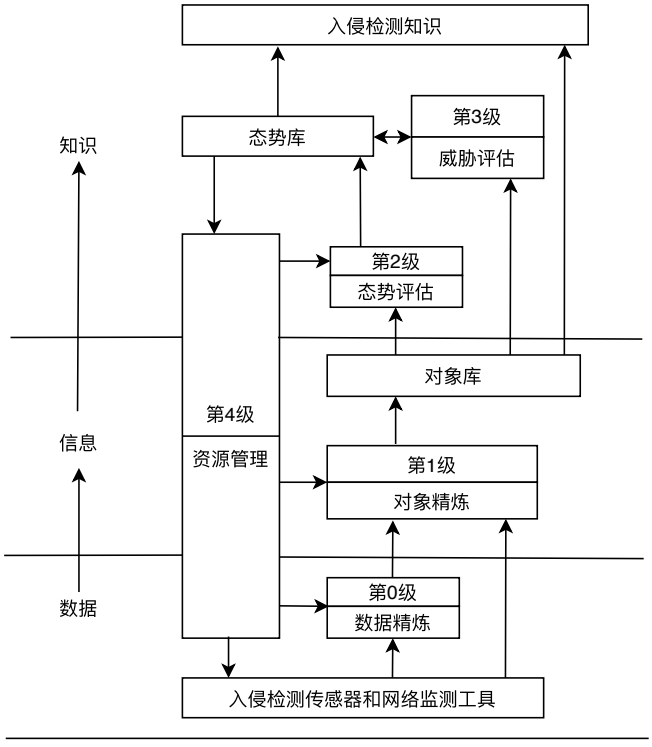

图 2.3 Tim Bass 模型

系统架构

基于以上对典型模型的分析和行业调研（详见“附录 A 行业案例”），可知网络安全态势感知能力高低主要由核心态势感知和影响态势感知的要素决定，也与前端数据源密不可分。本文提出了网络安全态势感知系统架构如图 2.4 所示，包括：1）各类前端数据源，如流量探针、服务器探针、监测平台等；2）核心态势感知：包括数据采集、数据处理、数据存储、数据分析、监测预警、数据展示、数据服务接口和系统资源管理；3）影响态势感知的要素：包括人工辅助、应急处置、安全决策和数据共享。

数据采集层主要关注采集什么数据，通过什么方式采集；数据处理主要关注如何处理采集到的数据，如何将采集到的数据进行有效融合；数据存储主要关注如何存储以及存储数据的类型；数据分析主要关注系统应具备何种数据分析能力，从而进行安全事件辨别、定级、关联分析等；监测预警主要关注监测内容和预警方式，甚至包括通过预警进行主动防御；数据展示主要关注如何进行安全态势展示、统计分析和安全告警等；数据服务接口主要关注支持的数据服务接口及格式；系统资源管理主要关注系统的安全管理要求。而在影响态势感知的要素中，可知利用系统结果进行决策和处置以及数据共享是构建网络安全态势感知能力的关键环节。此外，网络安全态势感知系统也要保证自身的安全，使其不成为网络中的安全风险点。

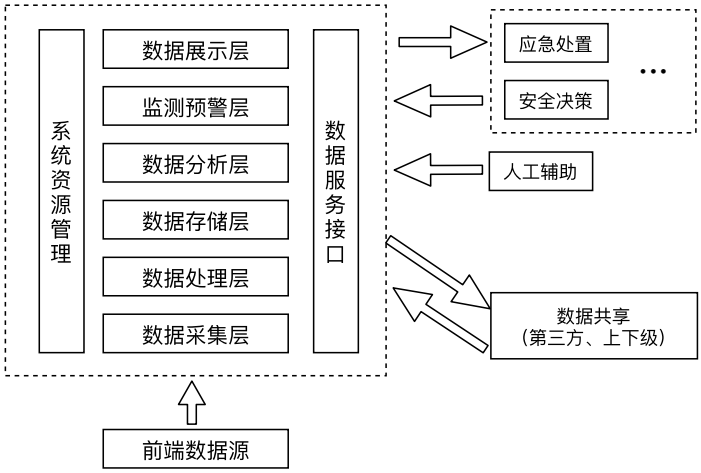

图 2.4 网络安全态势感知系统架构

需要注意的是图 2.4 给出的是网络安全态势感知的总体框图，该框图将数据能力、分析能力和应用能力充分解耦，有利于应用单位更多地接入不同前端数据，更好地使用多样化的分析模型，这样的框架更适用于大型单位的网络安全态势感知能力建设，这时候形成网络安全态势感知能力的是一个系统或多个系统。对于规模较小的单位，其也希望建立网络安全态势感知的能力，可以选择具有高度集成的网络安全态势感知产品，即对外不再展现数据服务接口等功能，而是将其封装在产品中，使用的是一家单位的全部能力。

1）前端数据源

前端数据源输出的数据是网络安全态势感知系统得以有效运行的基础。前端数据源有不同的类型，典型的包括流量探针、服务器探针、监测平台、第三方机构上报等。此外，由于工业互联网、云计算、移动互联网、物联网等新技术的应用，其前端数据源也需要重点考虑。不同的前端数据源有不同的业务处理能力及不同的数据输出格式，目前各前端数据源输出数据格式不一，导致每个网络安全态势感知系统都需要与前端数据源进行适配，另外对数据质量进行统一把控是业界的要点、难点和痛点。

2）核心态势感知

- 数据采集层

针对不同的网络环境和业务应用，网络安全态势感知系统的前端数据源会有所区别，前端数据源是大数据分析的基础与前提，准确高质量的数据能保证安全分析效果。针对用户对态势感知的场景需求，依托数据采集对象和采集内容，定义分析场景和建模。采集包括网络设备、主机、应用、安全设备等记录的日志数据和告警信息；异常流量数据和按规则匹配的网络流量数据；以及整个网络中所有的资产信息、相关的人员信息、账号信息以及与资产相关的漏洞信息、脆弱性信息和威胁情报信息等辅助信息数据，为进一步场景化的态势感知分析需求提供数据支撑。

- 数据处理层

数据处理层主要对多源、异构数据进行清洗和过滤、归一化、标识等操作，从而提高安全分析的可信度，降低误报率。其中数据清洗和过滤是将大量的重复数据进行归并，并将无效数据进行剔除；归一化是将原始数据转换为统一格式和内容的数据，为后续分析处理提供统一的标准化数据结构；数据标识是对海量数据环境下的不明数据流量进行识别，利用模式识别、深度学习、大数据分析技术和人工智能技术，识别和分离不明数据。

- 数据存储层

数据存储层主要是网络安全态势感知系统对采集的不同类型数据进行分级分类存储，以满足数据分析的要求。采用分级、分类、分层的模式，汇聚资源数据、网络运行数据、网络安全事件、威胁情报等重要数据，实现各类网络安全数据的统一融合，为数据分析、数据共享提供数据基础。该层需要实现对不同数据源同一类型的数据进行汇聚，并根据数据存储需求，对数据存储的类型、内容、方式和周期等进行约定。

- 数据分析层

网络安全态势感知的数据分析层是利用流量识别、协议分析、文件还原等手段，通过特征检测、规则分析、算法分析、行为分析等方法，结合人工智能、深度学习、行为建模、场景构建等技术，采用数据整理分类、对比统计、重点识别、趋势归纳、关联分析、挖掘预测的数据处置策略，从海量数据中自动挖掘出有价值的信息，最大的发挥数据的价值。数据分析是态势感知能力建设的核心，而分析模型、分析技术的正确使用是网络安全态势感知建设的关键。因此该层的重点在于数据分析模型的设计，从而实现风险、威胁和异常行为的分析，并给出其评价指标和方法。

- 监测预警层

网络安全态势感知的监测预警是数据分析

的应用，是依据数据分析结果，实现网络安全事件告警、态势评估、安全预警、追踪溯源等应用。通过利用态势感知，实现对采集数据的统计分析、能力评估、关联分析、数据挖掘等操作，生成态势感知平台所需的安全运行态势、安全风险态势、网络威胁态势等基础态势信息。在基础态势分析基础上，充分结合态势关联、威胁情报等，并对其进行科学、合理的组合，得出网络安全指数，调用各类基础数据和知识库信息，提炼攻击手段，还原攻击过程，溯源攻击者，为事件预警和应急指挥提供参考依据，以全面支撑安全事件快速响应和应急处置工作。监测预警有利于更好、更快地发现网络中的风险，从而支撑安全决策。

- 数据展示层

网络安全态势感知的数据展示层主要通过展示界面展示网络运行状态、网络攻击行为、安全事件、整体安全态势等，并能够持续的、多维度的监测信息资产和相关的威胁、脆弱性、安全事件、安全风险等分类态势指标变化情况，同时展示告警信息。目前各个产品和系统对安全的展示五花八门，让用户看不懂、看不明白，很多时候会忽略重点，因此该层的重点在于展示的内容要规范、合理，从而让用户快速了解网络安全状况。

- 数据服务接口

数据服务接口主要为网络安全态势感知系统的数据交换、数据分析、威胁处置提供数据访问调用服务。能够支持数据的推送服务，如数据汇聚 / 下发、数据交换和推送；能够支持模型分析服务，该服务根据业务需要，对数据进行统计、分析、规律性探索、预测等，并返回结果，以支撑应用层业务场景复杂、多变的需求，包括数据集碰撞类服务、分析类服务和预测类服务等。将数据作为服务提供给分析模型、第三方应用和其他单位能提升平台的可扩展性和能力。

- 系统资源管理

为保证网络安全态势感知系统的正常运行，需要能够对各类系统资源进行管理、对各种过程进行控制，因此系统资源管理应该是通过人工或自动化的方式对各种安全策略、数据分析过程、数据质量、知识库、上下级部署等进行管理，以支撑系统的有效运转。合理、有效的系统资源管理将提升系统的运转效率和实际效果。

- 自身安全

网络安全态势感知系统需要接入到信息系统的网络中进行数据采集，因此其自身安全也非常重要，包括标识与鉴别、角色管理、远程管理、自身审计等。

3）影响态势感知的要素

网络安全态势感知的能力建设除需要前端数据源及核心态势感知的支撑外，影响态势感知的要素，如人工辅助、应急处置、安全决策、数据共享等内容也需要重点关注和研究。比如，人工辅助需要考虑不同等级、不同能力的人员如何支撑网络安全态势感知的工作；应急处置是明确应对应急事件和安全事件的处置方法、处置流程、处置具体内容；安全决策基于网络安全态势感知系统的输出结果进行研判和决策，包括明确决策的组成要素和决策流程的统一；数据共享是实现网络安全态势感知协同防御的基础，主要实现安全事件及威胁情报等的共享。

第三章 网络安全态势感知标准化需求和现状

本章将对网络安全态势感知的标准化需求进行调研和分析，对国内外组织的网络安全态势感知的标准化现状进行梳理。

■ 标准化需求

在传统的网络安全防护体系建设中，更多依靠的是单个设备的能力、强调的是单点防护，缺少整体协同。网络安全态势感知系统基于多源数据从整体上对网络中的安全风险进行识别和预测，但其建设需要从不同数据源进行数据采集，并与其它安全产品和系统进行联动，因此存在较多需要定义的数据接口，包括前端采集接口、数据分析接口、数据共享接口等。目前各网络安全态势感知产品的开发厂商、各平台建设单位缺乏统一的数据接口，给平台对接、数据交换和威胁情报共享等增加了工作量、带来了困难。此外，网络安全态势感知系统建设单位在建设时由于没有统一的标准，导致对态势感知的认识不到位，系统架构设计不合理，在后期无法对系统能力进行扩展；导致态势感知功能模糊不清、能力参差不齐，无法真正实现网络安全态势感知；导致前端采集源与平台、平台内部高度融合，无法与其他优秀的前端采集源、分析能力进行异构兼容。

随着发布网络安全态势感知产品厂商的增多，以及各级网络安全态势感知系统的建设和实践，需要有配套的网络安全态势感知标准来对相关功能进行规范；对态势感知的评价体系进行构建；对平台间数据采集、数据共享、协同联动的接口进行统一，促进不同产品和平台之间的互联互通，从而进一步增强网络安全态势感知能力，最终形成国家的网络安全态势感知能力。

■ 标准化现状

1）国外标准

- ISO/IEC JTC1

ISO/IEC JTC1/SC27（信息 技术委员会 / 安全技术分委员会）开展了信息安全标准化工作，制定了脆弱性的披露标准 ISO/IEC 29147《信息技术 安全技术 脆弱性披露》(Information Technology -- Security Techniques -- Vulnerability Disclosure），用于实现脆弱性相关信息的规范化发布。这可以作为基础类标准对网络安全态势感知系统进行业务上的支撑。

- ITU-T

ITU-T 的 SG17（安全研究组）负责安全标准的制定，其中 Q4 关注网络空间安全，Q7 关注安全应用，Q8 关注云计算和大数据安全。

Q4 制定了 X.1500-X.1599 网络安全信息交换系列标准（Cybersecurity information exchange），包括 ITU-T 针对网络安全信

息制定了相关的交换标准，如X.1500《网络安全信息交换概述标准》（Overview of Cybersecurity Information Exchange）、X.1520《通用漏洞和暴露风险》（Common Vulnerabilities and Exposures）、X.1521《通用漏洞评分系统》（Common Vulnerability Scoring System）、X.1524《通用缺陷列表》（Common Weakness Enumeration）、X.1525《通用缺陷评分系统》（Common Weakness Scoring System）、X.1526《用于漏洞的公开定义和系统状态评价的语言》（Language for the Open Definition of Vulnerabilities and for the Assessment of a System State）、X.1528《通用平台列举》（Common Platform Enumeration）、X.1541《事件对象描述交换格式》（Incident Object Description Exchange Format）、X.1544《常见攻击模式枚举与分类》（Common Attack Pattern Enumeration and Classification）、X.1570《网络安全信息交换发现机制》（Discovery Mechanisms in the Exchange of Cybersecurity Information）等。这些标准可以用于网络安全态势的数据共享，也可以作为基础标准支撑态势感知业务。

Q7在2017年新立项了X.tfss《运营商提供的安全服务技术框架》（Technical Framework for Security Services Provided by Operators），其中提及的网络安全态势感知相关章节，可指导运营商提供网络安全态势感知服务。

Q8在2019年新立项了X.nssacc《云计算网络安全态势感知平台要求》（Requirements of Network Security Situational Awareness Platform for Cloud Computing），主要针对云计算网络，从数据采集、计算存储、分析、感知、可视化等方面提出了态势感知平台基本功能要求。

- OASIS

OASIS（结构化信息标准促进组织，Organization for the Advancement of Structured Information Standards）是一个推进电子商务标准的发展、融合与采纳的非盈利性国际化组织。相比其他组织，OASIS在形成了较多Web服务标准的同时也提出了面向安全的标准，同时在针对公众领域和特定应用市场的标准化方面也付出了很多的努力。

OASIS制定了《结构化威胁信息表达式》（Structured Threat Information eXpression，STIX）、《情报信息的可信自动化交换》（Trusted Automated Exchange of Intelligence Information，TAXII）、《网络可观察表达式》（Cyber Observable eXpression，CybOX）等标准，规范了用于交换威胁情报的格式、语法和协议，可用于网络安全态势感知系统对威胁情报数据的采集和交换。

- IETF

国际互联网工程任务组（The Internet

Engineering Task Force，IETF）的主要任务是负责互联网相关技术标准的研发和制定。在安全领域的安全事件轻量级交换工作组，研究和制定了支持计算机和网络安全事件管理的标准。已发布的 RFC 7970《安全事件描述交换格式（版本 2）》（Incident Object Description and Exchange Format Version 2，IODEF v2）、RFC8134《管理安全事件轻量级交换实现报告》、RFC8274《安全事件描述和交换格式使用指南》（Incident Object Description Exchange Format Usage Guidance）、RFC 8600《使用 XMPP 协议进行安全信息交换》（Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange）等系列标准定义了在不同计算机安全事件响应小组之间交换信息安全事件可使用的数据格式，可以用于指导网络安全态势感知系统对安全事件的采集和交换。

- NIST

美国国家标准与技术研究院（NIST）在 2017 年发布了电力行业态势感知系统实施指南 NIST SP 1800-7《电力设施态势感知 》（Situational Awareness for Electric Utilities），该指南结合电力行业的实例给出了态势感知系统的参考设计，有助于我们更好地理解态势感知系统的功能、架构和解决方案，对制定更为通用的态势感知系统技术要求类标准具有很高的指导和参考价值。

美国国家标准技术研究所还曾发布 NIST SP 800-150《网络威胁信息共享指南》Guide to Cyber Threat Information Sharing），为组织建立和参与网络威胁信息共享提供指导方针，涉及了信息源的选择，威胁情报类型，数据源的选择，威胁指标等内容，可为网络安全态势感知系统进行数据共享提供有效指导。

2）国内标准

- TC260

全国信息安全标准化技术委员会（TC260）开展过《信息安全技术 网络安全态势感知通用技术要求》和《信息安全技术 网络安全态势感知数据规范》两个标准研究项目，对网络安全态势感知的总体框架、组成部分和各部分的要求以及数据预处理进行了深入的研究并提出了后续的标准化建议。基于这些研究结果和建议，TC260 于 2020 年新立项了《信息安全技术 网络安全态势感知通用技术要求》、《信息安全技术 政务网络安全监测平台技术规范》、《信息安全技术 网络安全信息报送与态势研判指南》、《信息安全技术 网络安全信息共享指南》等与态势感知的总体框架和功能要求、行业应用、安全决策、数据共享相关的标准制定项目以及研究如何进行网络安全态势评价的《信息安全技术 网络安全态势感知评价指标》标准研究项目。

此外，TC260 制定的 GB/T 20985.1-2017《信息安全事件管理 第 1 部分：事件管理原理》、GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》目前修订中）、GB/T 24363-2009《信息安全应急响应计划规范》、GB/T 28458-2012《信息安全技术

安全漏洞标识与描述规范》、GB/T 28517-2012《网络安全事件描述和交换格式》、GB/T 30276-2013《信息安全技术 信息安全漏洞管理规范》、GB/T 30279-2013《信息安全技术 安全漏洞等级划分指南》（该标准正在修订，目前处于报批稿状态，且标准名称更改为《信息安全技术 网络安全漏洞分类分级指南》）、GB/T 32924-2016《信息安全技术 网络安全预警指南》、GB/T 33561-2017《信息安全技术 安全漏洞分类》、GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》、GB/T 37027-2018《信息安全技术 网络攻击定义及描述规范》、《信息技术 安全技术 信息安全事件管理 第 2 部分：事件响应规划和准备指南》（在研）等标准可以用于指导网络安全态势感知系统中的态势评估、共享交换、应急管理等过程。

- TC28

全国信息技术标准化技术委员会（TC28）信标委的工作范围是信息技术领域的标准化，涉及信息采集、处理、传输、交换、描述、管理、组织、存储、检索等的标准化工作，其制定的GB/T 37722-2019《信息技术 大数据存储与处理系统功能要求》和GB/T 38676-2020《信息技术 大数据 存储与处理系统功能测试要求》用于规范网络安全态势感知系统的数据存储和处理等过程，可为数据类标准提供参考。

- CCSA

中国通信标准化协会（CCSA）的标准化工作侧重于电信和互联网领域，其中安全方面的标准主要由 TC8（网络与信息安全技术委员会）的 WG1（有线网络安全工作组）、WG2（无线网络安全工作组）、WG3（安全管理工作组）和 WG4（安全基础工作组）来负责制定。CCSA 已经在电信、工业互联网等领域开展了网络安全态势感知相关的探索，目前已发布的 YD/T 3734-2020《基础电信企业网络安全态势感知系统技术要求》针对基础电信企业这一特定的行业领域中的态势感知系统提出了要求。其他正在制定中的标准包括《电信网和互联网网络安全态势感知系统安全要求》、《工业互联网安全态势感知系统技术要求》、《物联网安全态势感知技术要求》、《物联网业务安全态势感知系统技术要求》、《物联网终端安全态势感知系统技术要求》、《移动智能终端安全态势感知平台技术要求》等，结合通信领域中一些更加细化的应用场景，对不同的态势感知系统提出了更加具体的要求。

此外，CCSA 正在制定中的《公共安全大数据 第 4 部分：采集与预处理》标准，规定了公共安全领域内的数据源、数据类型、数据采集技术与方法等采集要求，以及数据预处理要求，可用于网络安全态势感知系统中的数据采集和预处理阶段；制定中的《公共安全大数据 第 7 部分：共享与互联》对于数据的共享提出了相关要求。另外，CCSA 也制定了 YD/T 2388-2011《网络脆弱性指数评估方法》、YD/T 2389-2011《网络威胁指数评估方法》、《网络安全评价指标体系研究》等标准，可以作为态势感知系统中安全评价指标体系的有效参考。

- 公共安全行业标准

公共安全行业正在制定的网络安全事件威胁行为监测系列标准，包括《网络安全事件威

胁行为监测 第 1 部分：基于流量的威胁行为监测技术要求》、《网络安全事件威胁行为监测 第 2 部分：基于安全日志的威胁行为监测技术要求》、《网络安全事件威胁行为监测 第 3 部分：网站与服务器安全监测技术要求》、《网络安全事件威胁行为监测 第 4 部分：机构报送网络安全事件格式规范》，都旨在对采集探针及其输出数据进行进一步规范，适用于网络安全态势感知系统的数据采集。

公共安全行业发布了资源服务总线系列标准，包括 GA/T1375.1-2017《资源服务总线 第 1 部分：体系架构》、GA/T1375.2-2017《资源服务总线第 2 部分：技术要求》、GA/T1375.3-2017《资源服务总线第 3 部分：注册格式》、GA/T1375.4-2017《资源服务总线第 4 部分：查询报文格式》、GA/T1375.5-2017《资源服务总线第 5 部分: 请求报文格式》、GA/T1375.6-2017《资源服务总线 第 6 部分: 提供报文格式》、GA/T1375.7-2017《资源服务总线 第 7 部分：内容格式》等，这些标准规定了资源服务总线的体系架构、技术要求、注册格式、查询报文格式、请求报文格式、提供报文格式等。该系列标准可以为网络安全态势感知数据服务接口标准提供参考。

公共安全行业发布的通报预警系列标准 GA/T 1717.1-2020《信息安全技术 网络安全事件通报预警 第 1 部分：术语》、GA/T 1717.2-2020《信息安全技术 网络安全事件通报预警 第 2 部分：通报预警流程规范》、GA/T 1717.3-2020《信息安全技术 网络安全事件通报预警 第 3 部分：数据分类编码与标记标签体系技术规范》及在制定中的《信息安全技术 网络安全事件通报预警 第 4 部分：威胁情报交换规范》为如何更好地使用和管理网络安全态势感知平台提供了有效参考，可用于态势感知系统的管理工作。

第四章 网络安全态势感知标准架构

本章围绕组织在进行网络安全态势感知能力建设、厂商在开发和设计网络安全态势感知产品时面临的问题，以问题导向为原则，给出了网络安全态势感知的标准架构并对架构中的各组成部分进行描述。

■ 基本原则

网络安全态势感知系统建设是较为复杂的一项工程，组织在进行网络安全态势感知能力建设、厂商在开发和设计网络安全态势感知产品时经常由于无标准可依，需自行进行框架设计、功能开发、接口适配等，导致各网络安全态势感知平台能力参差不齐、接口多种多样，且需花费大量的时间、精力和财力。有些系统建设单位对网络安全态势感知了解不多，对哪些部分需要标准化也无从下手，导致最终建成的系统没有达成预期效果，且系统的扩展性较差。为了更好地解决网络安全态势感知系统建设过程中面临的问题，本部分以问题导向为原则，给出了网络安全态势感知的标准架构，该架构可指导网络安全态势感知系统的参与各方进行网络安全态势感知的标准化建设，但随着网络安全态势感知技术的发展，该架构在未来可能会有一定的调整。

需要注意的是，并不是标准架构中的每一部分都要形成单独的国家标准，可考虑在一个标准中覆盖多个方面；可考虑充分复用现有标准；但对于网络安全态势感知系统建设中特别重要且需由标准支撑的部分则建议形成独立的国家或行业标准。另外，有些部分可以在现有标准的基础上结合行业和团体的新需求进行细化和扩展，制定新的行业或团体标准，以此共同构建网络安全态势感知标准体系。

本文给出的网络安全态势感知的标准架构是从态势感知平台的数据处理流程来进行分类。除此之外，标准架构还可以依据标准在网络安全态势感知中的作用进行分类。根据标准的作用来分，态势感知系统的标准可以分为：基础类、安全要求类、实施指南类和检测评估类标准。

其中基础类标准旨在提供网络安全态势感知基础性的术语、接口、框架；安全要求类标准主要基于网络安全态势感知的通用功能和行业特性功能，提出具体的要求，包括安全功能要求和自身安全功能要求；实施指南类标准主要围绕安全要求的落实，基于最佳实践，给出具体的实施指导；检测评估类标准主要是围绕具体的实施是否满足要求展开，主要是涉及网络安全态势的数据评估、技术使用能力（能力成熟度）评估、决策效果评估及目标满足性评估（业务导向）的标准，这类标准对于产品、平台的功能、数据的服务能力的评价具有积极作用。

基于标准作用的分类方法，应能充分利用已有的标准规范，互相配合，加强协同，比如基础类标准之间保持一致，并明确数据共享的类型和方法；安全要求类标准要能把握网络安全态势感知的核心，抽象出具体的要求；在实施指南类标准中应从数据流和业务流方向进行考虑，贴近业务的实际需要；检测评估类标准应量化能力评估的方法，提高认知的准确度和效率。

两种分类从不同的维度进行网络安全态势感知标准的划分，每种维度都有其优势和劣势。这两种划分维度应该互相补充和配合，从而更好地帮助网络安全态势感知平台的建设和使用，最终形成全天候全方位的网络安全态势感知能力。

总体架构

基于图 2.4 网络安全态势感知系统架构，本节设计了基于数据处理流程的网络安全态势感知标准架构，具体见图 4.1。其中图 2.4 中的数据采集层、数据处理层、数据存储层、数据服务接口对应标准架构图 4.1 中的数据标准；考虑到分析模型较难用标准定义，因此在标准架构图 4.1 中不体现数据分析层的内容，而主要规范结果；图 2.4 中的监测预警层、数据展示层、系统管理管理对应标准架构图 4.1 中的应用标准；图 2.4 中的安全处置、安全决策和人工辅助则对应图 4.1 中的业务支撑标准。

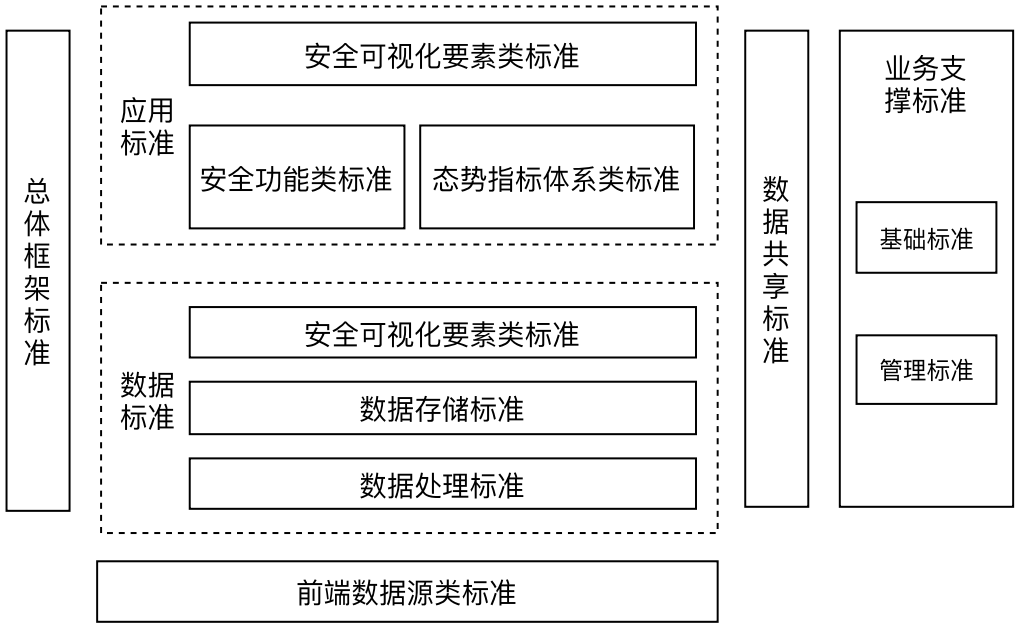

图 4.1 网络安全态势感知标准架构

综上所述，网络安全态势感知标准架构主要包括总体框架标准、前端数据源类标准、数据标准、应用标准、数据共享标准和业务支撑标准。其中数据标准包括数据预处理标准、数据存储标准和数据服务接口标准；应用标准包括安全功能类标准、安全指标体系类标准和安全可视化要素类标准；业务支撑标准包括基础标准和管理标准。

通过梳理国内外标准化现状并结合图 4.1 网络安全态势感知标准架构，给出了图 4.2 网络安全态势感知标准图谱，该图谱的横坐标分别是已发布国内标准、在研的国内标准，以及可供网络安全态势感知系统建设参考的国外标准，此外，该图谱还专门给出了需重点推进的网络安全态势感知标准（包括已立项的和迫切需要的）建议，从而与 5.2 节的内容相呼应。其中，该谱图中已发布的国内标准、在研的国内标准、可供参考的国内外标准具体名称见附录 B。

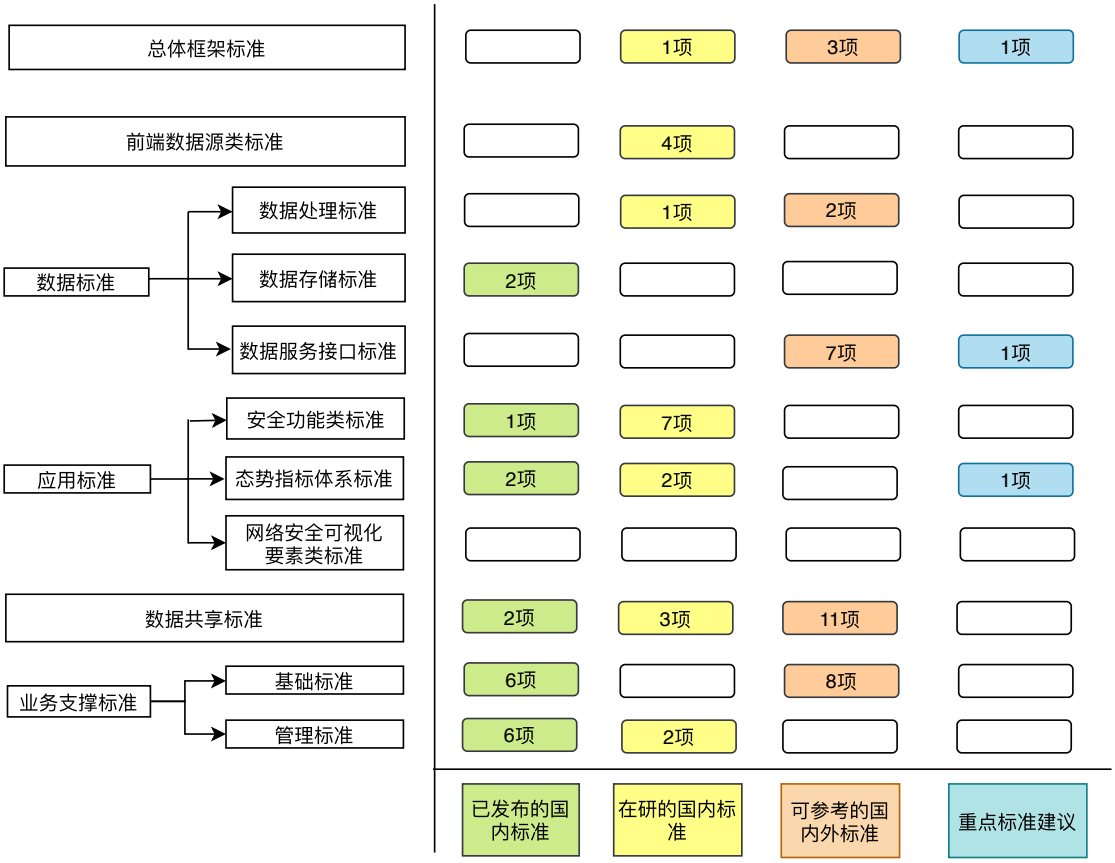

图 4.2 网络安全态势感知标准图谱

■ 组成部分

1）总体框架标准

网络安全态势感知总体框架标准作为总纲性标准，是其他标准制定的前提和基础，为网络安全态势感知其它标准的制定提供框架性要求和方向指导。

网络安全态势感知总体框架标准主要包括术语和定义、安全体系架构和基本安全要求。

术语和定义是网络安全态势感知标准中的基础部分。该标准需要给出网络安全态势感知领域的常用术语和定义，能够统一业界对关键术语和定义的认识和理解，规范术语定义和术语之间的关系，有利于技术交流和研究。需要重点关注的事项有：1）借鉴《信息安全技术 术语》中相关的规范化定义；2）尽量与国际标准化组织（ISO）、国际电工委员会（IEC）、美国国家标准与技术研究院（NIST）、我国国家网络安全态势感知标准化总体组等国内外标准化组织已发布的网络安全态势感知相关标准中的术语和定义保持一致。安全体系架构部分通过梳理分析网络安全态势感知的典型技术路线、面临的威胁、可能的风险等因素，构建网络安全态势感知系统模型，规范网络安全态势感知体系结构，切实保障网络安全态势感知系统的安全。NIST 已经发布的 SP 1800-7《电力设施态势感知》、ITU-T SG17 在研的《运营商提供的安全服务技术框架》和《云计算网络安全态势感知平台要求》可以为本部分标准制定提供借鉴和参考。

基本要求部分是网络安全态势感知标准的基础，可规范网络安全态势感知系统的规划、设计、开发和部署，需对数据采集、数据处理、数据存储、数据分析、监测预警、数据展示、数据服务接口、系统资源管理等模块的主要内容提出基本安全要求。目前，TC260 已经立项了《信息安全技术 网络安全态势感知通用技术要求》，后续需尽快推进该标准的制定工作。

2）前端数据源类标准

数据是网络安全态势感知的基础，前端数据源输出数据的质量关系到网络安全态势分析和呈现的效果。前端数据源类标准主要是对各类前端数据源输出的数据内容和格式进行规范。

如图 2.4 所示，网络安全态势感知系统的数据采集层主要通过主动、被动等方式获取各种数据，态势感知的前端数据源面临以下现状：1）数据种类繁多，包括资产数据、网络流量数据、运行状态数据、设备告警数据、脆弱性数据、安全事件数据和威胁情报数据等；2）不同场景下的数据类型不同，即不同场景下需要根据实际业务需求采集汇聚不同类型的态势要素数据；3）前端数据源来源不同，包括流量探针、服务器探针、监测平台、第三方上报、威胁情报数据接入、业务数据导入等；4）同一类型前端数据源可能存在不同的格式，由于数据来自于不同型号设备或不同厂商，缺乏产品告警或安全事件输出格式的规范。因此，为了提高数据融合、关联的精准分析和深度发掘能力，需要对前端数据源进行统一规范，对数据质量进行统一把控。

鉴于前端数据源形式多样，如流量探针一

般是部署在关键网络节点的硬件设备；服务器探针一般是部署在服务器上的代理，用于获取服务器的安全运行状态、系统日志等数据；监测平台会将监测的结果（一般来说是经过人工验证）进行上报；同时前端数据源也包括工控设备、物联网感知设备等，因此在态势感知平台进行数据类型和格式的统一定义并不合适。需要对每一类前端数据源制定相应的标准，对其功能和输出格式进行规定；同时建立一套元数据标准，保障各个前端数据源采集的数据能够统一存储，支撑整个网络安全态势感知的整体工作。目前，公安在研的行标《网络安全事件威胁行为监测 第 1 部分：基于流量的威胁行为监测技术要求》、《网络安全事件威胁行为监测 第 2 部分：基于安全日志的威胁行为监测技术要求》、《网络安全事件威胁行为监测 第 3 部分：网站与服务器安全监测技术要求》、《网络安全事件威胁行为监测 第 4 部分：机构报送网络安全事件格式规范》等都是前端数据源类的重要组成部分。

3）数据标准

- 数据处理标准

在前端数据源类标准的基础上，数据处理标准用于规范网络安全态势感知平台数据处理层的基础能力和技术要求，为网络安全态势感知平台数据接入后的预处理工作提供指导。

数据处理层主要是按照一定的规则对采集到的各类数据进行处理，以保证数据的质量。一般的数据处理流程包括数据筛选（包括必填字段缺失、重要字段格式错误、重复数据等）、数据转换、数据标识等。考虑到数据类型的不同，数据处理层也应能支持离线和在线多种处理方式。考虑到各平台面临的网络环境、数据类型、数据量的差异，数据处理方式会有所区别，可根据各行业的特点，建立各行业的数据处理标准，同时制定统一的国家标准规范网络安全态势感知的预处理流程和方法，整体上提高数据质量，增强全网安全态势感知能力。其中 GB/T 37722-2019《信息技术 大数据存储与处理系统功能要求》、GB/T 38676-2020《信息技术 大数据 存储与处理系统功能测试要求》对数据处理和存储的框架、功能及测试方法等提出了要求，但这两个标准提出的处理要求是对于处理模块自身的相关功能，不涉及处理流程，只能作为参考。CCSA 正在制定中的《公共安全大数据 第 4 部分：采集与预处理》对于数据预处理提出了相关要求。

- 数据存储标准

数据存储标准是用于规范和统一网络安全态势感知平台数据的存储能力和存储格式的要求。其中存储能力要求包括数据存储量要求、读写能力要求及数据资源管理能力要求等；数据存储格式要求则包括数据分类要求、存储格式要求和数据编码要求等。

网络安全态势感知平台目前较为主流的数据分类方法是原始库、资源库、知识库、主题库等；其中原始库主要是由前端数据源采集的各类数据；资源库是对原始库进行关键要素的分析、提取而形成的；知识库是各类知识的汇聚，包括威胁情报库、安全事件库、漏洞库等；主题库则是利用原始库、资源库、知识库等信息进行分析、提取后形成的。具体分类可由各行业根据实际业务需求进行。统一的网络安全态势感知平台数据存储标准将有利于促进安全事件分类分级的统一，是实现多源异构数据整合和多方数据共享的基础。GB/T 37722-2019《信息技术 大数据存储与处理系统功能

要求》、GB/T 38676-2020《信息技术 大数据 存储与处理系统功能测试要求》对数据处理和存储的框架、功能及测试方法等提出了要求。

- 数据服务接口标准

面向不同的行业用户或网络安全管理需求，网络安全态势感知平台，会有较大的功能要求差异，如业务功能差异、业务流程差异、管理粒度差异等。同时，网络安全态势感知平台的数据为多源采集，数据与业务应用的高度耦合将会使业务应用难以充分满足网络安全管理业务需求的多样化。数据服务接口是网络安全态势感知多样化业务应用与底层多源数据充分解耦的关键。

数据服务接口标准的制定应以网络安全态势感知的总体框架为基础，以充分支撑上层业务应用多样化为目标，以底层功能支撑和数据提供的服务化封装为技术手段，并充分结合现有实践经验。公共安全行业发布了资源服务总线系列标准，该系列标准为网络安全态势感知系统建立数据服务接口标准提供参考，但无法直接使用。

4）应用标准

- 安全功能类标准

安全功能类标准主要是梳理网络安全态势感知的通用功能要求，包括安全事件识别功能、安全事件分级功能、安全策略管理功能和自身安全功能等。

网络安全态势感知平台的核心能力之一是网络安全事件发掘，分析层是其中的核心，也是整个平台的大脑。数据分析主要基于业务安全和网络安全分析引擎，从海量数据中挖掘和量化安全风险事件以及系统安全特征和指标。考虑到不同系统的数据分析模型差别很大，在标准中不适合直接描述模型。然而，网络安全态势感知平台具有不同的应用形式，比如，可以为监管侧提供网络安全的整体态势，从而支撑网络安全事件通报、打击网络犯罪；可以为企业侧提供企业内网络的安全威胁情况，为企业的网络安全决策提供依据；可以具有通用安全能力。综合考虑各个形式态势感知平台的异同，可以编制网络安全态势感知安全能力要求标准。

网络安全态势感知功能类标准，需要：1）从网络安全事件的识别定级、关联分析、异常行为分析、潜在危害分析、安全趋势分析等分析的效果进行规范性要求；2）为保证平台的有序运行，应规范平台自身的安全策略、知识库、前端数据源的管理能力；3）考虑平台的自身安全，包括标识与鉴别、角色管理、远程管理、安全审计等。考虑到不同行业、不同层级对于网络安全态势感知的需求可能不同，可在通用安全能力要求的基础上，制定行业相关的安全能力要求进行细化和完善。目前，TC260 已经立项了《信息安全技术 政务网络安全监测平台技术规范》，用于规范在政务网络中态势感知系统的安全功能。另外，已发布的 YD/T 3734-2020《基础电信企业网络安全态势感知系统技术要求》、及在研的《工业互联网安全态势感知系统技术要求》、《电信网和互联网网络安全态势感知系统安全要求》、《物联网安全态势感知技术要求》、《物联网业务安全态势感知系统技术要求》、《物联网终端安全态势感知系统技术要求》、《移动智能终端安全态势感知平台技术要求》等相关行业标准的制定可以为本行业内网络安全态势感知系统的设计、开发、部署和应用提供指导，

提升行业乃至全国的网络安全态势感知能力。

- 态势指标体系类标准

网络安全态势指标体系是反映网络安全特性，且有一定关联关系的集合，是形成对网络安全态势标准化定量评价的依据。态势指标体系类标准需以辅助网络安全管理决策为目标，结合特定网络安全业务应用场景，实现对网络安全状况的综合评估。态势指标体系类标准应能够对网络安全态势提出基本的评价指标，并结合特定场景，提出额外的评价指标，从而实现对网络安全态势感知平台的指导和规范。

网络安全态势感知的数据主要是两类：一类是直接从前端数据源获得的原始数据，包括资产数据、告警数据、漏洞数据、威胁情报等；另一类是通过关联关系基于原始数据及知识库进行分析得到的安全事件数据，这部分主要对关联评估方法进行规范。在指标体系构建时，需要提取这两类数据的对象，形成具体对象的指标，指标的构建可基于现有的指标体系，如 YD/T 2388-2011《网络脆弱性指数评估方法》、YD/T 2389-2011《网络威胁指数评估方法》。网络安全态势是随着环境不断变化的，该变化是网络中各个要素互相作用和影响的结果，因此，在进行指标体系建设时，需要考虑各个要素之间的关联关系，尤其要根据不同的场景建立适合自己的指标体系。因此，一套完整的网络安全态势感知指标体系标准是非常必要的，能够帮助决策者、运维者了解系统真实的运行状态，保障系统的安全运行。TC260 的研究项目《信息安全技术 网络安全态势感知评价指标》、CCSA 的研究项目《网络安全评价指标体系研究》正在对指标体系相关问题进行研究。

- 网络安全可视化要素类标准

网络安全可视化是网络安全态势感知平台的主要功能之一，是网络安全态势感知平台面向用户输出安全告警、安全事件及态势分析结果等信息的主要窗口，其所需呈现的信息与用户的网络安全管理业务需求息息相关。然而，各个行业的网络安全管理者在使用网络安全态势感知平台的过程中，会对网络安全可视化产生不同的要求。

网络安全可视化要素类标准旨在解决网络安全可视化功能需求多样化的前提下，如何统一网络安全可视化呈现基本要素的能力问题。通过制定网络安全可视化要素类标准，可对网络安全可视化功能提出最基本的要求，从而规范呈现的网络安全基本要素，如资产或对象态势、脆弱性态势、网络攻击态势、安全事件及告警态势和应急处置业务态势等宏观性基本要素，同时亦应对细粒度基本要素提出规范要求，如资产分布、趋势分析、各类排名，乃至安全告警应呈现的信息内容要素等。

网络安全可视化要素类标准不是功能性规范，不直接对网络安全可视化提出功能要求，而是以网络安全可视化多样性需求为基础，充分抽象和提取其共性要素，形成以要素具备与否为判定基准的标准。网络安全可视化要素类标准应具备足够的包容性，充分兼容多样化的网络安全管理需求，同时应具备落地性，为网络安全态势感知系统网络安全可视化功能提供准入要求和认定标准。该类标准不一定单独形成标准，可与其他标准进行高度融合。

5）数据共享标准

多源异构数据接入能力是网络安全态势感

知平台的基础能力，跨行业跨平台的数据共享能力作为构建我国全天候全方位态势感知及协同防御能力的基础，可为该能力提供可行性保障。跨行业跨平台的数据共享既包括网络空间安全监管行业和被监管行业之间的数据共享，也包含行业单位向上级单位进行安全数据汇聚的数据共享。数据共享标准可对网络安全态势感知平台共享的各类数据进行规范，用于实现跨行业跨平台的数据汇聚和利用。

数据共享标准包含了数据共享格式标准和数据共享接口标准两部分。数据共享格式标准在网络安全态势感知数据存储标准的基础上制定，用于同一跨平台共享数据的格式要求，应与存储标准中数据分类要求、数据编码要求等保持一致。数据共享接口标准用于统一跨行业跨平台数据共享过程中的传输方式和接口定义。在部分场景下，网络安全态势感知平台可能作为上级单位或网络安全监管部门网络安全态势感知系统的数据源，因此，数据共享标准的制定可以参考前端数据源标准，保证网络安全态势感知系统的数据共享与前端接入标准之间的兼容性。在相关标准制定工作中，可参考已发布的 X.1500《网络安全信息交换概述标准》、X.1541《事件对象描述交换格式》、X.1570《网络安全信息交换发现机制》、RFC7970《安全事件描述交换格式》、OASIS《结构化威胁信息表达式 (STIX) 》等国外标准，可直接使用 GB/T 28517-2012《网络安全事件描述和交换格式》和 GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》等国内标准。此外，TC260 正在制定的《信息安全技术 网络安全信息共享指南》、公安行标正在制定的《信息安全技术 网络安全事件通报预警第 4 部分：威胁情报交换规范》及 CCSA 正在制定的《公共安全大数据 第 7 部分：共享与互联》也可指导网络安全态势感知数据的共享。

6）业务支撑标准

- 基础标准

基础标准主要规范网络安全态势感知的基础要素，包括元数据标准、漏洞及脆弱性标准、攻击威胁标准和安全事件标准。

元数据方面，考虑到平台需要接收不同前端数据源的数据并统一存储，因此需要制定一套完整的、经常维护的元数据编码标准。该套标准将对数据的名称、类型、字段、是否必填字段等进行规定。而实际现状是不同行业、不同领域、不同平台根据自身业务实际建立了不同的元数据标准，这导致了数据交换和共享的困难性，因此需要从国家或行业角度建立一套元数据标准，促进网络安全态势感知国家能力的建设。

漏洞和脆弱性方面，国际上有一系列标准，如 CVE、CCE、CPE、XCCDF、OVAL、CVSS、ITU-T 的 X.1520-1528 系列标准，可以作为漏洞方面的参考性标准。TC260 也针对安全漏洞，从漏洞描述、等级划分、漏洞管理、漏洞发布等发布了相关标准，漏洞的系列标准为网络安全漏洞的规范统一管理提供了支撑，适用于计算机信息系统安全管理部门进行安全漏洞信息发布、定级和管理，同样适用于指导漏洞库建设。在网络安全态势感知系统建设过程中，安全漏洞的规范统一管理至关重要，可以采纳已有标准作为网络安全态势感知的基础性标准。

攻击威胁描述、安全事件定义方面的若干

已有标准，可参考如 X.1544《常见攻击模式枚举与分类》，可使用 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》、GB/T 37027-2018《信息安全技术 网络攻击定义及描述规范》等，这些可为网络安全态势感知的安全事件识别、发现和分析奠定基础。

- 管理标准

通报和处置在网络安全态势感知中的地位较为特殊，其与用户单位的性质（如监管型、运营型等）息息相关，这部分的内容较为复杂，也更为形式多样。例如，对于中小型网络，通报和处置的功能可能由平台自身实现；对于大型网络，可能由单独的通报预警处置平台与态势感知平台进行联动。而且通报与处置通常不是平台的技术方面所能解决的，而更依赖于相关的组织管理和管理手段进行约束，因此把这一部分定义为管理标准。

管理标准为网络安全态势感知平台的有序运行提供支撑，主要包括通报预警、应急响应、安全保卫、威胁处置等相关内容。目前已经发布和在研的包括：GB/T 20985.1《信息技术 安全技术 信息安全事件管理 第 1 部分：事件管理原理》、GB/T 24363-2009《信息安全应急响应计划规范》、GB/T 32924-2016《信息安全技术 网络安全预警指南》、《信息技术 安全技术 信息安全事件管理 第 2 部分：事件响应规划和准备指南》（在研）、GA/T 1717.1-2020《信息安全技术 网络安全事件通报预警 第 1 部分：术语》、GA/T 1717.2-2020《信息安全技术 网络安全事件通报预警 第 2 部分：通报预警流程规范》、GA/T 1717.3-2020《信息安全技术 网络安全事件通报预警 第 3 部分：数据分类编码与标记标签体系技术规范》、《信息安全技术 网络安全信息报送与态势研判指南》（在研）。需要指出的是，在制定相关管理标准时，需要考虑一致性，保证各标准之间不存在冲突，且有关联关系。

第五章 网络安全态势感知标准化工作建议

网络安全态势感知作为实现网络安全实时监测和防护的一种手段，其作用至关重要。但由于网络安全态势感知能力建设的复杂性，即使如美国等网络安全强国也一直在摸索相关方案，我国也一样在摸索中前进。网络安全态势感知的标准化工作需要系列标准来规范。在《网络安全法》的指引下，紧密围绕国家网络安全战略需要，持续完善和优化我国网络安全态势感知的标准体系建设。网络安全态势感知标准体系建设一方面可以为网络安全态势感知的标准编制工作提供方向性指导；另一方面也能为网络安全态势感知研发、生产和检测单位开展规范化科研、生产和检测提供依据。

■ 统筹规划网络安全态势感知标准

我国高度重视网络安全态势感知的标准化工作，各标准化组织也已开展了卓有成效的相关标准研究与制定工作。考虑到不同行业都在制定相关的网络安全态势感知标准，因此在国家层面，需充分调研国内态势感知标准需求，强化标准梳理，**统筹规划网络安全态势感知标准**，用于指导网络安全态势感知标准的制定和相关标准的修订工作。

■ 加快开展亟需标准的制定进程

建立网络安全态势感知安全标准化工作推进计划，按照“急需先行”的思路研制态势感知标准，加速开展重点领域和关键标准的研制工作，有序推进态势感知标准化。**一是加快已立项标准的制定进程**：针对已经立项的网络安全态势感知总体框架标准《信息安全技术 网络安全态势感知通用技术要求》、数据共享标准《信息安全技术 网络安全信息共享指南》和业务支撑标准《信息安全技术 网络安全信息报送与态势研判指南》等，需加快其制定流程，特别是框架标准能够为后续网络安全态势感知相关标准的制定提供指导和参考；**二是启动亟需标准的制定工作**，包括实现网络安全态势感知多样化业务应用、底层多源数据充分解耦的数据服务标准，以及实现对网络中安全态势统一评判的评价指标类标准等；**三是开展态势感知行业标准的制定工作**，网络安全态势感知有明显的行业属性，因此需在网络安全态势感知国家标准的基础上，根据行业特性、业务特点，制定各行业、各领域的行业标准。

■ 积极推进态势感知标准的应用

为提升网络安全态势感知标准的有效性和可操作性，解决目前态势感知系统建设多头无序的现状，建议强化态势感知标准的应用实践工作。**一是完善态势感知标准试点机制**，选取典型的态势感知场景，开展标准适用性和实施效果评价，以“实践跟踪－问题发现－经验总结－完善标准”的思路，推动态势感知标准化工作的高效开展；**二是完善态势感知标准研究、宣贯和应用推广机制**，组织高校、科研院所和企业建立“产学研用”的一体化联盟，共同攻关态势感知标准化难点，探索态势感知标准宣贯和应用的新形式、新举措，在应用中不断促进网络安全态势感知产业的良性发展。

附录 A | 行业案例

■ 政务行业

1）网络安全风险现状

随着政务部门信息化建设的逐步推进，我国政府信息化网络也飞速发展。一般政务行业的网络由涉密网络和非涉密网络构成，本章节所讨论的政务网络为非涉密的政务网络。政务网络一般包括承载互联网业务的互联网区以及与各政务部门业务连接的公用网络区，当前已实现了网络与边界防护、监控与审计防护、主机安全防护以及应用安全防护，形成了较为全面的安全防护体系。

基于互联网建设的政务网络，其跨地区、跨部门的网络连接架构，大大增加了网络攻击风险，同时增加了网络安全管理的复杂性。

面对新的安全形势，被动防御已经无法应对当前安全形势，只有切实落实好安全监测工作，持续监测、主动发现、及时预警，才能做到“知己知彼，百战不殆”。

根据政务网络的特点，从场景化的角度出发，政务网络中主要面临以下风险：

- 网络情况复杂难于监管：政务网络分为互联网区和公用网络区，政务部门的政务网络通过骨干的城域网和广域网连接各部门、通过互联网出口连接互联网，覆盖范围广、云计算和大数据技术应用广泛，且面临来自互联网和各部门、下级单位的攻击风险，技术监管难度大。

- 安全保障能力参差不齐：政务网络一般是中央、省、市、县的架构，层级多，各层级的安全保障能力差距较大，有些部门的安全保障单纯靠传统安全产品的堆砌，呈现的维度较为单一，且存在大量误报。

- 业务众多易遭受攻击：政务网络的互联网区和公用网络区承载着大量的应用，受到国内外攻击者的关注。时刻存在着攻击者用病毒木马或者内部主机的漏洞等脆弱面进行的攻击以及内部人员违规操作的风险，各 IT 系统所面临的威胁严峻。

- 内部资产难以摸清：在政务网络最难的一个环节就是摸清家底，内部到底有多少资产，有多少资产存在漏洞，这些漏洞的风险级别如何，会不会给网络带来危害等，都是政府行业用户所关心的，摸清内部资产情况能够提早发现并规避大量风险。

2）建设需求分析

结合政务系统特点，适用于政务系统的网络安全态势感知系统，实质就是通过实现对政府网络系统的整体安全状态的 7x24 小时实时监控，从资产、攻击、漏洞、运行、威胁和风险各个维度全方位感知整个网络系统的安全状态与发展趋势。

具体而言，政务系统的态势感知系统首先要进行数据的自动采集和指标提炼，将数据转化为信息，直观展示网络安全现状；其次，通过信息的归纳演绎和集成建模，将信息转化为

知识，形成安全事件融合和关联分析所需要的规则；实现网络安全事件智能分析与实时预警；最终利用知识发现所获取的模式信息，规范、约束、推导、修正和补充安全态势模型，将知识转化为智慧，最终形成全局网络安全态势，实现对网络系统的全方位防护。

政务网络的网络安全态势感知系统的建设不仅仅是一个技术实现，更是一个系统工程。它的建设目标，是形成一套全方位的网络安全保障体系，构建一个闭环的安全态势感知及处置平台。通过感知政务系统的网络安全态势，提前发现系统风险以及薄弱环节，防患于未然，做到事前感知；当网络受到外部攻击或发生重大安全事件时，即刻发现并精确定位，做到协同处置；事后，通过调查取证，发现薄弱环节，进行系统加固，同时，完善情报库，提高感知能力，确保信息系统不发生安全事件、少发生安全事件或者在发生安全事件时能够得到及时处置。

3）标准现状与需求分析

1：标准现状

在网络安全态势感知监测国家标准、行业标准方面，除了《网络安全法》和一些政府的内部政策可供参考以外，还有相关的监测标准及电子政务行业相关的标准，具体如下：

- 《GB/T 36635-2018 信息安全技术 网络安全监测基本要求与实施指南》该标准规定了网络安全监测的基本要求，给出了网络安全监测的框架和实施指南。

- 《GW 0203-2014 国家电子政务外网安全监测体系技术规范与实施指南》该标准给出了国家电子政务外网安全监测的体系框架以及实施指南。

- 《信息安全技术 政务网络安全监测平台技术规范》（2020 新立项）该标准规定了政务网络安全监测平台的技术框架、安全技术要求以及测试评价方法。

- T/CIIA 系列监测标准结合了中央级政务外网安全监测平台建设的实践经验，用于推动和指导全国政务网络安全监测体系的建设、规范安全监测业务服务。

- 《T/CIIA 005-2019 政务网络安全监测平台总体技术要求》规定了政务网络安全监测平台的基本要求，提出了政务网络安全监测平台技术框架和相应的技术要求。

- 《T/CIIA 007-2020 政务网络安全监测平台数据总线结构规范》规定了政务网络安全监测平台数据总线的格式内容要求及管理规范，主要用于规范平台内部各功能模块之间的数据交互、不同厂家 / 类型的监测分析子平台的数据格式统一标准化、指导行业内上下级平台之间的数据级联对接以及与第三方平台之间的数据对接。

- 《政务网络安全监测业务服务规范（征求意见稿）》规定了政务网络安全监测业务服务所需的服务原则、服务条件、服务内容、服务过程及服务管理的相关要求，用于指导监测业务服务的选择和开展。

- T/CIIA 系列监测标准已经用于规范中央级政务外网安全监测平台和省级政务外网安全监测平台的建设完善及级联对接工作。

2：需求分析

总体来看，政务系统态势感知标准规范已经有了一定的基础，形成了一定的体系。但是政务系统监测的层级较多、参建厂商较多，在政务监测体系的建设过程中可能会遇到各种不同类型态势感知平台的数据交换场景，建议进一步完善《T/CIIA 007-2020 政务网络安全监测平台数据总线结构规范》；在和第三方平台的数据交换上，需要顶层的标准规范和参考，建议出台《网络安全态势感知系统数据交换标准》；另外，政务系统态势感知系统的建设存在大量采购服务的场景，对于监测服务的开展，建议进一步完善并发布《政务网络安全监测业务服务规范（征求意见稿）》，建议出台《网络安全态势感知系统服务规范》为政务系统态势感知服务提供参考。

■ 网络运营服务行业

1）网络安全风险现状

大数据、人工智能、物联网、云计算、工业互联网等新技术、新业务不断促进电信技术的发展和业务创新、推动电信业发展、提升电信服务质量。各种新技术、新业务在丰富了网络应用的同时，业务、网络、应用、数据的安全问题也相互交织，违法不良信息扩散、高危漏洞利用、特种病毒传播、APT 攻击等非传统安全威胁逐步增多，威胁不可预知的情况加剧和安全事件频发，运营商通信网络面临着前所未有的压力和挑战。

随着 5G 网络的到来，运营商作为 5G 技术应用的最前沿，面临网络连接数量海量增长、网络流量巨幅增加等挑战。为了适应变化，运营商要不断优化网络架构、提升网络质量、扩大覆盖面，确保提供优质的网络服务。随之而来的是流量过快增长导致无法实现全面安全监控、网络设备和架构的变化导致传统安全防护手段的失效、业务不断扩展导致暴露面不断增加等安全问题。

为了解决上述问题，运营商网络中部署了大量的网络安全设备，初步形成了防护体系，但目前网络内部署的安全设备大多为单点检测，只能单维度分析过去已发生或现在正在发生的事件，无法厘清安全事件的前因后果，未来的演变趋势。同时，由于缺乏专业的运营人员对数据进行分析处理，也缺少必要的技术手段对大量的安全数据进行集中的管理和分析，导致目前网络安全监测主要以解决单个安全攻击为主，无法实现全局的网络安全分析和预警。并且由于运营商网络直接面向用户、面向互联网，导致其极容易成为黑客的攻击目标，不但要抵御传统的、常见的网络攻击，还要面对大量潜伏、隐藏的潜在威胁和未知威胁，这些高级威胁攻击经常隐藏在巨大的流量数据中，需要通过长期大规模的数据分析，进行大量的关联分析和行为分析，方能实现完整的攻击行为识别。

在数据安全方面，运营商掌握了大量的敏感信息，其中不但有公民的个人基本信息，更有能对用户进行个体化行为分析的业务数据。面对海量的敏感数据和隐私数据，如何实现全面、高效、安全的防护，也是目前所要面临的主要挑战。

综上所述，运营商的网络安全面临着网络安全环境快速变化，网络安全防御体系不协调、数据泄漏等诸多方面的压力挑战，同时也面临国家、主管部门等方面的监管要求。

2）建设需求分析

1：政策合规角度

习总书记在 “419 讲话”中明确提出了关于在信息系统中建立态势感知机制的重要性。近些年国家出台了《网络安全法》；主管单位也发布了针对电信和互联网行业相关要求，如《省级基础电信企业网络与信息安全工作考核要点与评分标准》、《通信网络安全防护符合性评测》、《移动业务运营支撑系统业务技术规范》、《基础电信企业网络安全态势感知平台建设指南》等，按照监管部门对保卫基础信息设施的工作部署要求，统一明确建设网络安全一体化态势感知平台，实现安全数据中心建设、安全威胁分析、安全监控预警、安全威胁处置以及安全运营管理等要求。以集中化建设、分阶段演进为总体思路，遵循“安全三同步、先立后破、近源防护、能力持续提升、安全运营可持续”原则，实现安全威胁分析与预警、威胁应对与快速处置、资源整合与统筹指挥的能力。以业务技术支撑部、网络管理部、信息安全管理部三大主要部门为主，进行业务融合、数据共享、统一建设运营。

2：运维角度

依托逐年建设的安全平台工程，运营商构建了事前控制、事中防护、事后审计的常态化管控体系。在开展常态化安全管控工作中，能够源源不断产生高价值的安全数据。如何有效挖掘安全数据的价值，将对安全事件的响应从事后处理提前至事中控制或事前识别，需要通过革新升级安全分析手段，提升对安全态势的感知能力。目前主要存在以下几个问题：

- 传统技术架构面对海量数据的集中化处理和存储无法解决安全运营中的管理“痛点”。
- 已具备如不良信息监测、垃圾短彩信监控、电信防诈骗、伪基站监控及客户敏感信息监控等多种安全管控技术手段，然而目前各系统独立运行，缺乏整体性安全分析及管控能力。
- 现有的基于规则的分析方法无法应对当下多变快速的攻击威胁。
- 现有数据处理能力无法有效发现高级、持续的敏感信息泄露及业务操作轨迹。
- 在重大活动保障中缺乏有效的快速处置及应急响应能力，无法有效整合分散在企业环境中的人力资源、安全资源、系统资源和流程规范。
- 安全运营效果难以衡量，安全工作中缺少有效的运营评价体系。

网络攻击一旦发生，没有快速事件响应，业务网络不仅被控制和破坏，还要面临业务数据泄露。从实际出发，面对越来越严格的监管和企业责任意识的增长，修复工作的速度和可测性变得更加重要。在提升安全响应效率的时候，不仅从单点（譬如单纯从端点或者网络）去考虑，还需要从全网整体安全运维的角度去考虑，将分散的检测与响应机制整合，通过智能化、自动化来减少安全人员花在重复繁琐事务上的时间。

在解决以上问题的过程中，主要应用了如下方法：

- 建立安全数据管理中心，以实现各部门异构数据统一采集、标准化和共享。

- 建立统一威胁分析中心，以业务驱动构建安全分析场景，补充单点分析手段。

- 建立统一情报中心，引入内外部情报数据。

- 形成流程化处置手段，根据攻击属性和影响范围对事件进行分类分级，关联资产及责任人，对事件进行工单派发、处置和反馈跟踪。

3：决策角度

对于运营商领导者来说，每年对安全建设和安全维护投入大量成本，定期内部安全会议得到的汇报材料不够全面，每年应对上级单位的安全检查总是漏洞百出，投资建设没有可靠的数据支撑。对于网络安全体系的顶层设计，网络安全的目标必须从“完美”阻止 / 允许决策转向持续的风险和信任评估，以便在发生恶意事件时快速检测和响应，使攻击者感染其他系统、造成损坏、窃取信息或创建服务交付失败的影响最小化。

为进一步量化投入产出能力，需要给管理者提供有效的实时攻击仪表和汇报素材，因此在平台建设期间，也要考虑友好的攻击实况展现和预警手段，以便于决策者给出工作指示。

4：增值角度

随着新技术快速发展，国家把网络与信息安全提升到更高层面，同时工信部与运营商自身也对安全重视程度越来越高，每年都面对监管部门、集团公司的安全考核，所以在满足安全合规性要求的同时，也需要基于自身业务安全需求投资一些安全产品和安全服务。

在建立集中化态势平台时，应重点考虑给业务部门带来的潜在效益，如投产后，攻击成功次数的下降，提前知情攻击意图，发现可能被攻破的脆弱点等，并尽可能保证风险在可见、可知、可控的范围。

3）标准现状与需求分析

1：标准现状

目前在网络安全态势感知领域，并没有较为完备的国家、行业标准和规范，只有《网络安全法》和一些政府的内部政策提供了指导性意见，造成了各运营商之间、各运营商内部的态势感知平台建设技术差异很大，长期处于各自为战的状态。近期，工信部牵头发布了《基础电信企业网络安全态势感知平台建设指南（试行）》（以下简称建设指南），开始通过标准化手段对基础电信企业的态势感知平台建设进行指导，并结合技术规范开展相关的考核工作。但从内容来说，建设指南主要规定了态势感知系统应具备的功能，没有对数据标准化、数据接口等进行详细的规定，并没有解决数据标准不统一造成数据孤岛、态势感知平台不能有效开展全面安全分析的技术难点。与此同时，基础电信企业内部制定了本企业的相关标准，如中国移动制定了《中国移动业务支撑网络安全威胁分析与预警平台技术规范》，详细规定了中国移动业务支撑领域的网络安全威胁分析与预警平台的主要功能、实现方法、接口要求、数据要求等内容。但是，此类标准通常仅适用于企业内特定领域内，无法在整个行业内进行广泛推广。

2：需求分析

虽然目前运营商行业在态势感知标准规范

方面已经有了一定的基础，但尚未形成较为完备的标准体系。因此，亟待在国家和行业层面出台更为详细的态势感知建设标准，统一建设标准，打通数据孤岛，实现国家、行业级的统一管理。涉及到与网络安全态势感知系统技术要求的建议出台《网络安全态势感知系统数据采集要求》、《网络安全态势感知系统数据交换标准》等，并对各类网络安全数据采集设备提出数据支撑要求，以此支撑运营商行业态势感知系统建设。

态势感知系统的数据来源主要是前端采集设备及节点，但由于目前各类数据源所产生的数据标准格式不统一、数据内容不一致、数据质量参差不齐，直接导致态势感知系统采集的安全数据可用性低，无法支撑全面化、精准化分析。因此，建议出台针对数据源的数据采集要求，对各类数据源进行分类，并在此基础上提出针对性的数据格式要求和采集要求，切实保证态势平台采集数据的可用性。

同时，由于态势感知平台和诸如资产管理、工单管理、威胁情报、网络安全管理平台等众多外部第三方系统存在数据接口，并进行频繁的数据交换，为保证数据交换过程中的数据安全性、可用性、完整性，建议对数据交换的全过程进行规定，从数据传输内容、传输方式、权限管理等方面进行规定，提高态势感知系统和外部系统的数据交换效率和安全性。

■ 汽车行业

1）网络安全风险现状

汽车制造行业，是高技术的制造行业，要在这个行业获得成功，必须具备全方位的技术保障。汽车制造行业与国民经济是有一定关联程度的行业，在国定资产投资中具有一定的地位，是国家的支柱行业。

汽车制造行业，也是依靠精益生产降低成本，从而获取利润的行业。企业管理者对于库存的管理非常严格，由于工序一环扣一环。某个工序生产的库存会影响另一个工序的排产计划，这些系统一旦被干扰将造成巨大的经济损失，尤其是总装车间的制造系统一旦出现问题，其它车间也不得不因为库存积压原因停工，以某个日产 300 辆乘用车的生产基地为例，每停产一天，将直接造成将上千万的经济损失。

汽车行业面临的网络安全风险主要包括以下几个方面：

1：系统分散，主机安全管理难，风险突出

汽车制造行业，是典型的离散制造行业，工序较为分散，提供生产系统的供应商多而杂，一方面，这些系统被安装了各式各样的上位机组态软件，而基于不同组态软件的兼容性要求，相应的上位机操作系统也千差万别，系统安全加固工作复杂；另一方面，由于部分系统是国外供应商生产，远程维护调试的现象突出，主机安全管理困难重重，风险突出。

2：制造系统的工控设备多、品牌不一，工控设备漏洞修复困难

在汽车制造环节的冲压、车身、涂装、总

装四大工艺中，使用了大量 PLC、扫描枪、平板电脑、无线控制模块和机器人等各类设备。这些设备的责任人分属于不同的车间、甚至不同的部门，存在多级管理、责任分散的问题，因此，与之对应的漏洞管理和修复工作复杂而艰巨。

3：生产基地分布在全国各地，缺乏统一和全面的安全管理平台，安全维护困难

汽车制造行业的生产基地较为分散，各个基地与总部之间通过企业专线贯通，安全边界多，各个基地安全投入不一，选择的安全产品也各不相同，各安全系统分散部署、安全日志分散，未形成信息安全防护的合力，缺乏统一的资产管理、漏洞管理、风险管理、事件处置平台，安全管理工作存在实际困难。

2）建设需求分析

汽车行业网络安全态势感知建设迫切需求主要体现在以下几方面：

- 随着工业互联网在汽车制造行业内的不断推进，汽车制造行业的内涵不断扩大，组成其工业互联网平台的各类硬件、软件、系统，以及各类人员都有可能成为威胁主体，软硬件的后门、漏洞、缺陷，包括对人员的诱惑都是攻击工业互联网平台的常用手段。正是由于攻击源的多样性、防范对象的不确定性和安全边界的模糊性也就造成了汽车制造行业的信息安全保障防不胜防。

- 汽车制造行业信息系统的安全运维工作，比起其他行业的运维工作有较大的不同，相关的运维知识已经超出了传统信息系统的范畴，尤其是对于工业设备固件升级的工作，往往需要依托工业控制系统集成商或厂商完成，因此，汽车制造行业安全运维人员虽然能够了解到工控系统本身的脆弱性以及可能引发的危害，但在实际工作中，往往使用传统信息安全的漏洞扫描产品，无法及时发现相应漏洞，很难组织人力开展定期的修复工作，安全的最后一道防线无法落地。

- 汽车制造企业尽管在技术层面上已经完成了各类安全产品的部署，具备基础安全防护措施。但从整体安全体系角度而言，并未形成完整的安全管理体系，尤其是安全运维管理缺乏信息系统支撑，安全管理要求的落地更多的依靠领导考核和员工自发自觉的行动的能力，缺乏流程固化工具保证运维流程的规范性，流程规范难以保证，统计分析困难，部分管理工作均手工完成，有关记录仍为纸质形式，安全管理工作的信息化程度与业务信息化程度较不匹配。

3）标准现状与需求分析

1：标准现状

在工业网络安全态势感知监测的国家标准、行业标准方面，目前发布的标准中有《信息安全技术 网络安全监测基本要求与实施指南》（GB/T 36635-2018）、《信息安全技术 信息系统安全管理平台技术要求和测试评价方法》（GB/T 34990-2017）、《信息安全技术 网络安全等级保护安全管理中心技术要求》（GB/T 36958-2018）。

工业领域长期以来注重功能安全，缺乏针

对性的信息安全标准，往往只能参考上述列举的通用的信息安全标准。而针对态势感知的标准缺失，目前尚无可查询到的正式发布的国家/行业态势感知相关标准。由于缺乏顶层标准指导，汽车行业也缺乏行之有效的，有针对性的行业标准。

2：需求分析

在汽车行业，除了在制造环节中存在的安全需求，在汽车销售之后的车联网环节也存在安全需求，因此在态势感知的能力设计方面，感知能力不仅仅涉及某个车间、某个生产基地、某个集团，而是需要覆盖汽车生产、物流、销售的全生命周期。因此，除了包含满足基础的安全感知能力，还需要满足云计算、车联网等方面的安全感知能力。

目前汽车行业急需以下标准以规范和推动态势感知的发展和支持态势感知系统的建设运行。

- 网络态势感知系统总体通用标准：建议出台网络态势感知系统国家标准，从顶层给出态势感知系统架构和通用要求。

- 汽车行业网络态势感知系统技术要求标准：建议根据国家标准制定汽车行业的行业标准，结合国家标准的通用要求和上述列出的汽车行业的行业特色，制定具有较强可操作性的行业标准，指导企业生产和态势感知系统运维。

- 网络态势感知术语标准：建议出台网络态势感知术语国家标准，规范术语定义以减少歧义。

- 网络态势感知评价标准：建议出台网络态势感知评价标准，用于对态势感知系统进行评价。目前态势感知系统缺乏统一标准，用户也无法很好的全面提出需求，导致了各家态势感知系统的质量层次不齐，由于缺乏评价标准，无法对产品进行评价，可能出现劣币驱逐良币的现象，对企业的生产和用户的使用造成很大困扰。

附录 B | 已发布及在研的标准

序号	主题及分类		标准名称	标准编号	备注
1	总体框架标准		信息安全技术 网络安全态势感知通用技术要求	在研（TC260）	在研的国内标准
2			电力设施态势感知	NIST SP 1800-7	可供参考的国内外标准
3			运营商提供的安全服务技术框架	在研（ITU-T）	
4			云计算网络安全态势感知平台要求	在研（ITU-T）	
5	前端数据源类标准		网络安全事件威胁行为监测第 1 部分：基于流量的威胁行为监测技术要求	在研（公安行标）	在研的国内标准
6			网络安全事件威胁行为监测第 2 部分：基于安全日志的威胁行为监测技术要求	在研（公安行标）	
7			网络安全事件威胁行为监测第 3 部分：网站与服务器安全监测技术要求	在研（公安行标）	
8			网络安全事件威胁行为监测第 4 部分：机构报送网络安全事件格式规范	在研（公安行标）	
9	数据标准	数据处理标准	信息技术 大数据存储与处理系统功能要求	GB/T 37722-2019	可供参考的国内外标准
10			信息技术 大数据 存储与处理系统功能测试要求	GB/T 38676-2020	
11			公共安全大数据 第 4 部分：采集与预处理	在研（CCSA）	在研的国内标准
12		数据存储标准	信息技术 大数据存储与处理系统功能要求	GB/T 37722-2019	已发布的国内标准
13			信息技术 大数据 存储与处理系统功能测试要求	GB/T 38676-2020	

14		数据服务接口标准	资源服务总线 第 1 部分：体系架构	GA/T 1375.1-2017	可供参考的国内外标准
15			资源服务总线 第 2 部分：技术要求	GA/T 1375.2-2017	
16			资源服务总线 第 3 部分：注册格式	GA/T 1375.3-2017	
17			资源服务总线 第 4 部分：查询报文格式	GA/T 1375.4-2017	
18			资源服务总线 第 5 部分：请求报文格式	GA/T 1375.5-2017	
19			资源服务总线 第 6 部分：提供报文格式	GA/T 1375.6-2017	
20			资源服务总线 第 7 部分：内容格式	GA/T 1375.7-2017	
21	应用标准	安全功能类标准	基础电信企业网络安全态势感知系统技术要求 YD/T 3734-2020	YD/T 3734-2020	已发布的国内标准
22			信息安全技术 政务网络安全监测平台技术规范	在研（TC260）	在研的国内标准
23			工业互联网安全态势感知系统技术要求	在研（CCSA）	
24			电信网和互联网网络安全态势感知系统安全要求	在研（CCSA）	
25			物联网安全态势感知技术要求	在研（CCSA）	
26			物联网业务安全态势感知系统技术要求	在研（CCSA）	
27			物联网终端安全态势感知系统技术要求	在研（CCSA）	
28			移动智能终端安全态势感知平台技术要求	在研（CCSA）	
29		态势指标体系标准	网络脆弱性指数评估方法	YD/T 2388-2011	已发布的国内标准
30			网络威胁指数评估方法	YD/T 2389-2011	
31			信息安全技术 网络安全态势感知评价指标	在研（TC260）	在研的国内标准（研究项目）
32			网络安全评价指标体系研究	在研（CCSA）	

33	数据共享标准		网络安全事件描述和交换格式	GB/T 28517-2012	已发布的国内标准
34			信息安全技术 网络安全威胁信息格式规范	GB/T 36643-2018	
35			信息安全技术 网络安全信息共享指南	在研（TC260）	在研的国内标准
36			信息安全技术 网络安全事件通报预警 第 4 部分：威胁情报交换规范	在研（公安行标）	
37			公共安全大数据 第 7 部分：共享与互联	在研（CCSA）	
38			网络威胁信息共享指南	NIST SP 800-150	可供参考的国内外标准
39			网络安全信息交换概述标准	X.1500	
40			事件对象描述交换格式	X.1541	
41			网络安全信息交换发现机制	X.1570	
42			安全事件描述交换格式（版本 2）	RFC 7970	
43			管理安全事件轻量级交换实现报告	RFC 8134	
44			安全事件描述和交换格式使用指南	RFC 8274	
45			使用 XMPP 协议进行安全信息交换	RFC 8600	
46			结构化威胁信息表达式 (STIX)	OASIS	
47			情报信息的可信自动化交换 (TAXII)	OASIS	
48			网络可观察表达式（CybOX）	OASIS	
49	业务支撑标准	基础标准	信息安全技术 信息安全事件分类分级指南	GB/Z 20986-2007（修订中）	
50			信息安全技术 安全漏洞标识与描述规范	GB/T 28458-2012	已发布的国内标准

51			信息安全技术 信息安全漏洞管理规范	GB/T 30276-2013	
52			信息安全技术 安全漏洞等级划分指南	GB/T 30279-2013（修订中）	
53			信息安全技术 安全漏洞分类	GB/T 33561-2017	
54			信息安全技术 网络攻击定义及描述规范	GB/T 37027-2018	
55			信息技术 安全技术 脆弱性披露	ISO/IEC 29147	可供参考的国内外标准
56			通用漏洞和暴露风险	X.1520	
57			通用漏洞评分系统	X.1521	
58			通用缺陷列表	X.1524	
59			通用缺陷评分系统	X.1525	
60			用于漏洞的公开定义和系统	X.1526	
61			通用平台列举	X.1528	
62			常见攻击模式枚举与分类	X.1544	
63		管理标准	信息安全事件管理 第 1 部分：事件管理原理	GB/T 20985.1-2017	已发布的国内标准
64			信息安全应急响应计划规范	GB/T 24363-2009	
65			信息安全技术 网络安全预警指南	GB/T 32924-2016	
66			信息安全技术 网络安全事件通报预警第 1 部分：术语	GA/T 1717.1-2020	
67			信息安全技术 网络安全事件通报预警第 2 部分：通报预警流程规范	GA/T 1717.2-2020	
68			信息安全技术 网络安全事件通报预警第 3 部分：数据分类编码与标记标签体系技术规范	GA/T 1717.3-2020	
69			信息技术 安全技术 信息安全事件管理 第 2 部分：事件响应规划和准备指南	在研（TC260）	在研的国内标准
70			信息安全技术 网络安全信息报送与态势研判指南	在研（TC260）	

参考资料

1 Endsley, Mica R. "Design and evaluation for situation awareness enhancement." Proceedings of the Human Factors Society annual meeting. Vol. 32. No. 2. Sage CA: Los Angeles, CA: SAGE Publications, 1988.

2 Endsley, Mica R., and Daniel J. Garland, eds. Situation awareness analysis and measurement. CRC Press, 2000.

3 Steinberg, Alan N., Christopher L. Bowman, and Franklin E. White. "Revisions to the JDL data fusion model." Sensor Fusion: Architectures, Algorithms, and Applications III. Vol. 3719. International Society for Optics and Photonics, 1999.

4 Bass, Tim. "Multisensor data fusion for next generation distributed intrusion detection systems." Proceedings of the IRIS National Symposium on Sensor and Data Fusion. Vol. 24. No. 28. COAST Laboratory, Purdue University, I, 1999.

5 Jajodia S, Liu P, Swarup V, et al. Cyber Situational Awareness: Issues and Research[J]. 2009.

6 Kott A , Wang C , Erbacher R F . Cyber Defense and Situational Awareness[J]. 2014.

7 Peng L, Jajodia S, Wang C. Theory and Models for Cyber Situation Awareness[J]. Lecture Notes in Computer Science, 2017, 10030.

8 Tadda, George, et al. "Realizing situation awareness within a cyber environment." Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006. Vol. 6242. International Society for Optics and Photonics, 2006.

9 Tadda G P, Salerno J S. Overview of cyber situation awareness[M]//Cyber situational awareness. Springer, Boston, MA, 2010: 15-35.

10 Xi Rong-rong, Yun Xiao-chun, et al. Overview of network security situation awareness[J], Computer Applications, 2012, 32(1):1-4

11 Franke U, Brynielsson J. Cyber situational awareness–a systematic review of the literature[J]. Computers & Security, 2014, 46: 18–31.

12 M. M. Kokara,C. J. Matheusb, and K. Baclawskic, “Ontology-based situation awareness[J],” Information Fusion, vol. 10, pp. 83–98, 2009.

13 V. Mavroeidis and S. Bromander, “Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence[C],” in Intelligence and Security Informatics Conference(ISI), pp. 91–98, 2017.

14 Guan L, Hu G J, Wang Zhuan. Research on network security situational awareness technology based on big data[J]. Netinfo Security, 2016(9): 45–50.

15 Yang X N, Wang W, Xu X F, et al. Research on the construction of a novel cyberspace security ecosystem[J]. Engineering, 2018, 4(1): 47–52.

16 Wu J, Ota K, Dong M X, Big data analysis based security situational awareness for smart grid[J], IEEE Transactions on Big Data, 2016, PP(99): 1.

17 Yang X, Kong L, Zhi L, et al. Machine Learning and Deep Learning Methods for Cybersecurity[J]. IEEE Access, 2018, PP(99):1–1.

18 Jibao, Lai, Wang Huiqiang, and Zhu Liang. "Study of network security situation awareness model based on simple additive weight and grey theory." 2006 International Conference on Computational Intelligence and Security. Vol. 2. IEEE, 2006.

19 韦勇 , 连一峰 , 冯登国 . 基于信息融合的网络安全态势评估模型 [J]. 计算机研究与发展 ,2009,46(03):353–362.

20 龚俭 , 臧小东 , 苏琪 , 胡晓艳 , 徐杰 . 网络安全态势感知综述 [J]. 软件学报 ,2017,28(04):1010–1026.