(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106936637 A
(43)申请公布日 2017.07.07

(21)申请号 201710154095.6

(22)申请日 2017.03.15

(71)申请人 中国电子科技网络信息安全有限公司
地址 610207 四川省成都市双流县西南航空港经济开发区工业集中区内

(72)发明人 陈剑锋 徐锐 刘方 李春林

(74)专利代理机构 成都九鼎天元知识产权代理有限公司 51214
代理人 徐静

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/08(2006.01)
G06F 17/30(2006.01)

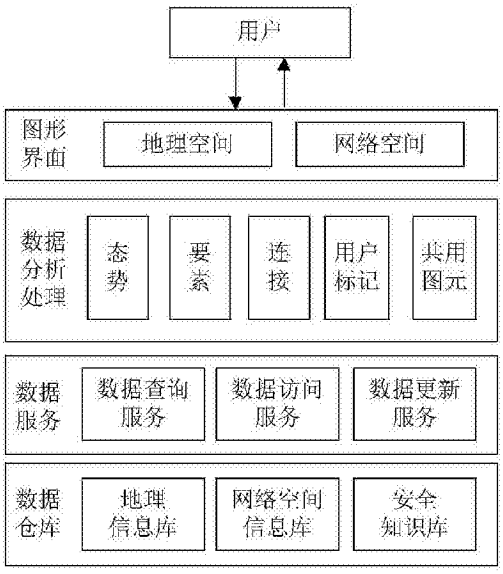
权利要求书3页 说明书7页 附图2页

(54)发明名称

一种网络空间态势的全景探索式可视化方法及装置

(57)摘要

本发明涉及网络空间态势的全景探索式可视化领域。针对现有技术存在的问题，提供一种可视化方法及装置。通过图形界面进行人机交互，将网络空间基础态势数据、攻击态势数据和防护态势数据代表的知识以可视化方式表达，用户基于交互探索方式捕获所关注重点的细微情况和变化。可以从不同视图的不同角度来发现网络空间态势的演变规律。本发明使用网络空间态势数据存储步骤中所述网络空间态势数据的按照时间、空间和态势要素类型建立索引；通过基准点设置步骤、设置比例尺步骤、绘制底图步骤以及要素连接步骤进行网络空间态势绘制；用户从观察者模式或者探索者模式的角度出发，对网络空间态势界面进行观察，接收态势界面表达的信息，全面了解事件过程。



CN 106936637 A

1.一种网络空间态势的全景探索式可视化方法，其特征在于包括：

网络空间态势数据存储步骤：数据源提供的数据按照类别分为日志化数据、协议化数据和流状的顺序化数据，在格式字典的辅助下对数据作均一化标准处理；然后按照定义的参数配置对均一化的数据处理后得到网络空间态势数据；然后将网络空间态势数据按照基础态势、攻击态势和防护态势分类存储；基础态势指网络空间构成要素的日常运行状态；攻击态势指敌对方对我方采取的攻击情况，用于判别我方受影响和受破坏的情况；防护态势指我方监测范围内对抗攻击的情况，用于协助我方采取防御应对措施；

图形数据库建立步骤：使用网络空间态势数据存储步骤中所述网络空间态势数据的按照时间、空间和态势要素类型建立索引；

态势绘制步骤，通过基准点设置步骤、设置比例尺步骤、绘制底图步骤以及要素连接步骤进行网络空间态势绘制；

用户从观察者模式或者探索者模式的角度出发，对网络空间态势界面进行观察，接收态势界面表达的信息，全面了解事件过程。

2.根据权利要求1所述的一种网络空间态势的全景探索式可视化方法，其特征在于所述态势绘制步骤包括：

基准点设置步骤：选择基准点通过指定态势呈现的地理原点，形成以该点为中心向外延展的网络空间态势；

用户选择图形数据库建立步骤中网络空间态势数据中的某个参数作为基准点；其中所述参数可以通过HTML中的<select>控件构建下拉式菜单框引导用户选取地理信息库中的某一城市/地区作为地理位置基准点；或是通过文本框输入，指定网络空间信息库中的某一域名/IP地址作为基准点，然后通过Javascript中的Ajax()异步调用方法查询公开互联网域名/IP地址地理映射服务，将其转换为地理位置基准点；

设置比例尺步骤：通过HTML中的<select>控件构建下拉式菜单框引导用户设置比例尺；

绘制底图步骤：根据基准点设置步骤得到的基准点以及设置比例尺步骤中得到的比例尺，通过HTML中的Canvas绘图机制把地理空间地图绘制至网络空间态势界面中，得到绘制底图；

要素连接步骤：在绘制底图步骤得到的绘制底图基础上，将不同类型的安全事件通过定位阶段、布局阶段和染色阶段绘制在网络空间态势界面中，然后将具备特定联系的要素进行绘制连接；将已绘制在网络空间态势界面上的事件称为要素。

3.根据权利要求2所述的一种网络空间态势的全景探索式可视化方法，其特征在于还包括对网络空间态势中的要素进行额外标注的过程；绘制属性包括属性选择、属性定位和属性布局几个步骤；属性选择是根据当前用户配置，选取一个至多个用于显示的要素属性字段用于绘制；属性定位是根据实体的位置区域，以不遮挡显示为原则，在要素上方、下方、左方或右方调用字符串显示函数绘制信息；属性布局是根据要素位置区域的显示拥挤程度，通过力导向方法，对属性摆放的位置进行微调以达到最佳的呈现效果。

4.根据权利要求2所述的一种网络空间态势的全景探索式可视化方法，其特征在于所述要素连接步骤中布局阶段通过力导向算法调整位于相同地理区域的安全事件位置，避免彼此重叠影响展示效果；染色阶段根据安全事件代表的安全态势类型进行标注，调用涂色

函数将基础态势事件标定、攻击态势事件以及防护态势事件标定为不同颜色。

5.根据权利要求2所述的一种网络空间态势的全景探索式可视化方法，其特征在于所述绘制连接包括绘制直线和绘制曲线；绘制直线方法为：在两要素的X、Y坐标间调用直线函数绘制；绘制曲线的方法为：在两要素的X、Y坐标间调用贝塞尔曲线函数绘制；绘制连接的条件包括：1)要素代表事件的发生时间存在紧密的先后关系；2)要素代表事件的IP地址存在上下级网络关系；3)要素代表事件的描述存在一致性关系；4)要素代表事件的描述存在耦合性关系；在两要素间仅存在一条连接的情况下绘制直线，存在多条连接的情况下绘制曲线。

6.根据权利要求1所述的一种网络空间态势的全景探索式可视化方法，其特征在于所述网络空间态势数据存储步骤中数据处理包括清洗、冗余归并、时空配准和数据分类；数据清洗以均一化后的规范格式数据为输入，通过删除缺字段数据和取值异常数据得到净载荷数据；冗余归并以净载荷数据为输入，对发生时间一致且内容描述一致的数据进行删除，得到无重复数据；时空配准以无重复数据为输入，将所有数据中的时间信息调整为同一时区，将所有数据中的发生地信息调整为统一格式，得到含标准化时空标记的数据；数据分类以含标记数据为输入，按照数据中的事件类型对数据进行分类。

7.根据权利要求2所述的一种网络空间态势的全景探索式可视化方法，其特征在于所述地理空间地图由三维地球模型使用圆柱投影、圆锥投影或方位角投影方法得到，绘制过程为将基准点作为中心点，将地图按照设置比例尺步骤中比例尺的参数进行放大、缩小或裁剪，最后调用贴图函数，地图绘制在网络空间态势界面上。

8.根据根据权利要求2所述的一种网络空间态势的全景探索式可视化方法，其特征在于所述比例尺设置为“城区级”、“城市级”、“省级”和“国家级”四种级别；比例尺设置越大，网络空间态势界面中能够容纳的地理区域越大，态势呈现的全面度提升；比例尺设置越小，网络空间态势界面中的能够容纳的地理区域越小，态势呈现的精细度提升。

9.根据根据权利要求2所述的一种网络空间态势的全景探索式可视化方法，其特征在于所述观察者模式指的是观察者流程中使用全局视图、基础态势视图、攻击态势视图、防护态势视图和热点事件视图这五类视图；全局视图是由在态势绘制要素步骤中，绘制攻击态势、防护态势和基础态势三类安全事件得到的视图；基础态势视图是由在绘制要素步骤中，仅绘制基础态势安全事件得到；攻击态势视图是由在态势绘制步骤中，仅绘制攻击态势安全事件得到；防护态势视图是由在态势绘制的态势绘制步骤中，仅绘制防护态势安全事件得到；热点事件视图是由绘制要素步骤中仅绘制过去时间T内发生的安全事件得到；在观察者流程的轮询中，五类视图的切换时间由用户通过文本框方式输入指定，可设置为时间P范围内；当上一视图已显示所设的切换时间后，系统自动切换为下一视图；

探索中模式指的是用户通过下拉框选择和文本框输入配置时间探索、空间探索和属性探索三类参数，然后通过平移、放大、缩小、点击操作进行自由态势探索；时间探索参数设置：在时间探索视图中，用户可设置一个时间段，只显示发生在这一时间段中的态势事件；在空间探索参数设置：用户可设置两个区域，屏幕一分为二，在左右分别显示这两个区域的网络空间态势，以便对比观察；属性探索参数设置：用户可设置一个或多个关心属性的取值范围，将只显示具有这些属性的态势事件。

平移操作：用户使用鼠标拖拽态势地图，地图将向着用户拖拽的方向展开新的内容；放

大操作：用户使用鼠标滚轮放大态势地图，地图将减小比例尺，在相同屏幕面积中显示更少的内容；缩小操作：用户使用鼠标滚轮缩小态势地图，地图将增加比例尺，在相同屏幕面积中显示更多的内容；点击操作：用户点击一个态势要素，在该要素旁边显示关于该要素所有属性的完整信息。

10.一种网络空间态势的全景探索式可视化装置，其特征在于包括：

网络空间态势数据存储模块：数据源提供的数据按照类别分为日志化数据、协议化数据和流状的顺序化数据，在格式字典的辅助下对数据作均一化标准处理；然后按照定义的参数配置对均一化的数据处理后得到网络空间态势数据；然后将网络空间态势数据存储；将网络空间态势数据分为基础态势、攻击态势和防护态势；基础态势指网络空间构成要素的日常运行状态；攻击态势指敌对方对我方采取的攻击情况，用于判别我方受影响和受破坏的情况；防护态势指我方监测范围内对抗攻击的情况，用于协助我方采取防御应对措施。

图形数据库建立模块：使用网络空间态势数据存储模块中所述网络空间态势数据的按照时间、空间和态势要素类型建立索引；

态势绘制模块，通过基准点设置模块、设置比例尺模块、绘制底图模块以及要素连接模块进行网络空间态势绘制；

用户从观察者模式或者探索者模式的角度出发，对网络空间态势界面进行观察，接收态势界面表达的信息，全面了解事件过程。

一种网络空间态势的全景探索式可视化方法及装置

技术领域

[0001] 本发明涉及网络空间态势的全景探索式可视化领域，尤其是一种网络空间态势的全景探索式可视化方法及装置。

背景技术

[0002] 网络空间是人工制造的，由多种传感器、控制器、连接器、计算平台、存储平台和人类等要素参与并持续演变的复杂巨系统。为了更有效利用网络空间，必须首先对网络空间进行准确感知、认知。网络空间态势“看不清、辨不明”等问题，已长期制约了我国对网络空间掌控和改造能力的提升。在网络管理、安全管理和应急响应领域，网络空间态势可视化已经有一定的研究和应用成果，但其机制以统计数据、指标体系、简单标定为主，效果以固定角度展示、静态展示和视图切换展示为主，技术和能力水平尚未达到国际主流标准，难以满足瞬息万变网络空间中态势把握、威胁发现、风险预警和高效运维的需求。当前面临的困难主要包括：

[0003] (1)与地理空间或虚拟空间单一主体平面的呈现机制、原理、方法不同，网络空间态势相关的数据来源多样，其种类涵盖了经由地理层、逻辑层与认知层感知获取的大量信息，因而与之适配的可视化模型、坐标系及渲染算法需要专门化、定制化研究；

[0004] (2)网络空间态势的构成数据常以海量化、结构化和高速变化的方式存在，由于通常的显示设备难以支持也无必要将全要素同时展示，因而需根据用户的关注重点与求解目标对数据进行动态选择、映射、编排和布局，以展示效果最清晰为原则进行要素的精化、筛选构图；

[0005] (3)静态、平面化的图形受到图层遮挡、视野区域、操作模式等机制的限制，用户缺乏身临其境的感知效果，特别是对网络空间这类结构复杂、关联关系众多、层次丰富、内容繁杂的复杂巨系统而言，需要为用户设计革新性、直观性的探索机制，激活用户的隐性知识，形成感悟态势、把控局势、判断趋势的重要辅助支撑手段。

发明内容

[0006] 本发明所要解决的技术问题是：针对现有技术存在的问题，提供一种网络空间态势的全景探索式可视化方法及装置。本发明要解决的技术问题主要是网络空间态势的全景探索式可视化问题，提出地理空间与网络空间的时空关联可视化探索方法，构建的网络空间地图包括地理因素和网络拓扑结构模型，从多角度对网络空间的整体态势进行综合展示。通过图形界面进行人机交互，将网络空间基础态势数据、攻击态势数据和防护态势数据代表的知识以可视化方式表达，用户基于交互探索方式捕获所关注重点的细微情况和变化。一方面可以从不同视图的不同角度来发现网络空间态势的演变规律，另一方面可以比较不同地区、不同网系间网络空间态势的差异，形成整体、全面和系统化的态势认知。

[0007] 本发明采用的技术方案如下：

[0008] 一种网络空间态势的全景探索式可视化方法包括：

[0009] 网络空间态势数据存储步骤：数据源提供的数据按照类别分为日志化数据、协议化数据和流状的顺序化数据，在格式字典的辅助下对数据作均一化标准处理；然后按照定义的参数配置对均一化的数据处理后得到网络空间态势数据；然后将网络空间态势数据存储；将网络空间态势数据分为基础态势、攻击态势和防护态势；基础态势指网络空间构成要素的日常运行状态；攻击态势指敌对方对我方采取的攻击情况，用于判别我方受影响和受破坏的情况；防护态势指我方监测范围内对抗攻击的情况，用于协助我方采取防御应对措施。

[0010] 图形数据库建立步骤：使用网络空间态势数据存储步骤中所述网络空间态势数据的按照时间、空间和态势要素类型建立索引；

[0011] 态势绘制步骤，通过基准点设置步骤、设置比例尺步骤、绘制底图步骤以及要素连接步骤进行网络空间态势绘制；

[0012] 用户从观察者模式或者探索者模式的角度出发，对网络空间态势界面进行观察，接收态势界面表达的信息，全面了解事件过程。

[0013] 进一步的，所述态势绘制步骤包括：

[0014] 基准点设置步骤：选择基准点通过指定态势呈现的地理原点，形成以该点为中心向外延展的网络空间态势；用户选择图形数据库建立步骤中网络空间态势数据中的某个参数作为基准点；其中所述参数可以通过HTML中的<select>控件构建下拉式菜单框引导用户选取地理信息库中的某一城市/地区作为基准点；或是通过文本框输入，指定网络空间信息库中的某一域名/IP地址作为基准点，然后通过Javascript中的Ajax()异步调用方法查询公开互联网域名/IP地址地理映射服务，将其转换为地理位置基准点；

[0015] 设置比例尺步骤：通过HTML中的<select>控件构建下拉式菜单框引导用户设置比例尺；

[0016] 绘制底图步：根据基准点设置步骤得到的基准点以及设置比例尺步骤中得到的比例尺，通过HTML中的Canvas绘图机制把地理空间地图绘制至网络空间态势界面中，得到绘制底图；

[0017] 要素连接步骤：在绘制底图步骤得到的绘制底图基础上，将不同类型的安全事件通过定位阶段、布局阶段和染色阶段绘制在网络空间态势界面中，然后将具备特定联系的要素进行绘制连接；将已绘制在网络空间态势界面上的事件称为要素。

[0018] 进一步的，一种网络空间态势的全景探索式可视化方法还包括对网络空间态势中的要素进行额外标注的过程；绘制属性包括属性选择、属性定位和属性布局几个步骤；属性选择是根据当前用户配置，选取一个至多个用于显示的要素属性字段用于绘制；属性定位是根据实体的位置区域，以不遮挡显示为原则，在要素上方、下方、左方或右方调用字符串显示函数绘制信息；属性布局是根据要素位置区域的显示拥挤程度，通过力导向方法，对属性摆放的位置进行微调以达到最佳的呈现效果。

[0019] 进一步的，所述要素连接步骤中布局阶段通过力导向算法调整位于相同地理区域的安全事件位置，避免彼此重叠影响展示效果；染色阶段根据安全事件代表的安全态势类型进行标注，调用涂色函数将基础态势事件标定、攻击态势事件以及防护态势事件标定为不同颜色。

[0020] 进一步的，所述绘制连接包括绘制直线和绘制曲线；绘制直线方法为：在两要素的

X、Y坐标间调用直线函数绘制；绘制曲线的方法为：在两要素的X、Y坐标间调用贝塞尔曲线函数绘制；绘制连接的条件包括：1)要素代表事件的发生时间存在紧密的先后关系；2)要素代表事件的IP地址存在上下级网络关系；3)要素代表事件的描述存在一致性关系；4)要素代表事件的描述存在耦合性关系。在两要素间仅存在一条连接的情况下绘制直线，存在多条连接的情况下绘制曲线。

[0021] 进一步的，所述网络空间态势数据存储步骤中数据处理包括清洗、冗余归并、时空配准和数据分类；数据清洗以均一化后的规范格式数据为输入，通过删除缺字段数据和取值异常数据得到净载荷数据；冗余归并以净载荷数据为输入，对发生时间一致且内容描述一致的数据进行删除，得到无重复数据；时空配准以无重复数据为输入，将所有数据中的时间信息调整为同一时区，将所有数据中的发生地信息调整为统一格式，得到含标准化时空标记的数据；数据分类以含标记数据为输入，按照数据中的事件类型对数据进行分类。

[0022] 进一步的，所述地理空间地图由三维地球模型使用圆柱投影、圆锥投影或方位角投影方法得到，绘制过程为将基准点作为中心点，将地图按照设置比例尺步骤中比例尺的参数进行放大、缩小或裁剪，最后调用贴图函数，地图绘制在网络空间态势界面上。

[0023] 进一步的，所述比例尺设置为“城区级”、“城市级”、“省级”和“国家级”四种级别；比例尺设置越大，网络空间态势界面中能够容纳的地理区域越大，态势呈现的全面度提升；比例尺设置越小，网络空间态势界面中的能够容纳的地理区域越小，态势呈现的精细度提升。

[0024] 进一步的，所述观察者模式指的是观察者流程中使用全局视图、基础态势视图、攻击态势视图、防护态势视图和热点事件视图这五类视图；全局视图是由在态势绘制要素步骤中，绘制攻击态势、防护态势和基础态势三类安全事件得到的视图；基础态势视图是由在绘制要素步骤中，仅绘制基础态势安全事件得到；攻击态势视图是由在态势绘制步骤中，仅绘制攻击态势安全事件得到；防护态势视图是由在态势绘制步骤中，仅绘制防护态势安全事件得到；热点事件视图是由绘制要素步骤中仅绘制过去时间T内发生的安全事件得到；

[0025] 在观察者流程的轮询中，五类视图的切换时间由用户通过文本框方式输入指定，可设置为时间P范围内；当上一视图已显示所设的切换时间后，系统自动切换为下一视图。

[0026] 一种网络空间态势的全景探索式可视化装置包括：

[0027] 网络空间态势数据存储模块：数据源提供的数据按照类别分为日志化数据、协议化数据和流状的顺序化数据，在格式字典的辅助下对数据作均一化标准处理；然后按照定义的参数配置对均一化的数据处理后得到网络空间态势数据；然后将网络空间态势数据存储；将网络空间态势数据分为基础态势、攻击态势和防护态势；基础态势指网络空间构成要素的日常运行状态；攻击态势指敌对方对我方采取的攻击情况，用于判别我方受影响和受破坏的情况；防护态势指我方监测范围内对抗攻击的情况，用于协助我方采取防御应对措施。

[0028] 图形数据库建立模块：使用网络空间态势数据存储模块中所述网络空间态势数据的按照时间、空间和态势要素类型建立索引；

[0029] 态势绘制模块，通过基准点设置模块、设置比例尺模块、绘制底图模块以及要素连接模块进行网络空间态势绘制；

[0030] 用户从观察者模式或者探索者模式的角度出发，对网络空间态势界面进行观察，

接收态势界面表达的信息，全面了解事件过程。

[0031] 综上所述，由于采用了上述技术方案，本发明的有益效果是：

[0032] (1)网络空间态势数据的可视结构转换能力。融合网络空间测绘日志化、协议化和顺序化数据源的不同特征信息，从利于可视处理的角度进行数据的形式化规约，形成支撑检索、操作、推理和管理的标准化数据集。

[0033] (2)面向视图的态势数据析取和置备能力。

[0034] 根据所需视图的逻辑特性和呈现目标，对网络空间态势数据集进行析取和映射，包括在目标参数控制下的数据清洗、冗余归并、时空配准、数据分类和实体映射，等过程，将网络空间态势数据集转换为全景展示所需的精化数据。

[0035] (3)全景探索式可视化展现能力。从时间、空间、属性等特征出发构建全景、纵深多层次的数据视觉感知体系，贴合网络空间态势认知的具体需求，将安全数据信息形象化，将人类的感知综合化，极大提升管理、操作人员对网络空间态势现及发展趋势的感知全面度和准确率。

附图说明

[0036] 本发明将通过例子并参照附图的方式说明，其中：

[0037] 图1是网络空间可视化系统结构框架。

[0038] 图2是网络空间态势数据准备流程图。

[0039] 图3是网络空间态势绘制流程图。

[0040] 图4是网络空间态势全景探索流程图。

具体实施方式

[0041] 本说明书中公开的所有特征，或公开的所有方法或过程中的步骤，除了互相排斥的特征和/或步骤以外，均可以以任何方式组合。

[0042] 本说明书中公开的任一特征，除非特别叙述，均可被其他等效或具有类似目的的替代特征加以替换。即，除非特别叙述，每个特征只是一系列等效或类似特征中的一个例子而已。

[0043] 数据分类以含标记数据为输入，按照数据中的事件类型对数据进行分类，如事件类型取值为“警告”或“攻击”则分类为攻击态势，如取值为“通知”或“基础”则分类为基础态势，取值为“管理”则分类为防御态势；

[0044] 本发明包括数据仓库层、数据服务层、数据分析处理层和图形界面层，如附图1所示；

[0045] ●数据仓库：提供基于大数据的地理信息库、网络空间信息库和安全知识库的数据支撑。

[0046] ●数据服务层：屏蔽具体数据仓库操作的实现细节，为数据分析处理层和图形界面层提供与网络空间态势关联信息的、统一易用的数据查询、数据访问和数据更新服务。

[0047] ●数据分析处理层：对从数据服务层获取的数据按照用户当前视图和探索模式进行选择、整编和处理，得到一致的，可以用于图形界面呈现的态势数据。

[0048] ●图形界面层：对用户提供网络空间态势的展示效果，同时接收用户的交互指令，

实现对网络空间的主动探索能力。

[0049] 本方法包括：

[0050] 网络空间态势的全景探索式可视化方法包括数据准备、态势绘制和探索交互三个部分组成。

[0051] (1)数据准备

[0052] 数据准备是将数据源中的原始数据经处理后转换和提升为高质量的态势数据，并存储至数据仓库的过程。数据准备的流程如附图2所示。

[0053] 网络空间态势的数据源是网络中广泛存在的终端、服务器和通信、安全设备，数据源提供的原始数据按照类别和内容分为日志化数据、协议化数据和流状的顺序化数据，在格式字典的辅助下对数据作均一化标准处理；然后按照定义的参数配置对均一化的数据进行清洗、冗余归并、时空配准、数据分类和实体映射，得到可用于网络空间态势数据呈现所需的结构化信息。

[0054] 具体地，数据清洗以格式标准化后的规范格式数据为输入，通过删除缺字段数据和取值异常数据得到净载荷数据。冗余归并以净载荷数据为输入，对发生时间一致且内容描述一致的数据进行删除，得到无重复数据；时空配准以无重复数据为输入，将所有数据中的时间信息调整为同一时区，将所有数据中的发生地信息调整为统一格式，得到含标准化时空标记的数据；数据分类以含标记数据为输入，按照数据中的事件类型对数据进行分类，如事件类型为“警告”或“攻击”则分为攻击态势，如事件类型为“通知”或“基础”则分类为基础态势，如事件类型为“管理”则分类为防御态势。

[0055] 网络空间态势数据由三种类型的安全事件组成，即基础态势事件、攻击态势事件和防护态势事件。态势数据中的三类安全事件均包括事件ID、发生时间、终止时间、发生地点、IP地址、事件描述、备注等共性字段，另外增加与本类态势相关的专用字段。其中，基础态势指网络空间构成要素的日常运行状态，增加资源属性、协议、标识、特征等字段；攻击态势指敌对方对我方采取的攻击情况，增加攻击行为、手段、目标、效果等字段，用于判别我方受影响和受破坏的情况；防护态势指我方监测范围内对抗攻击的情况，增加安全力量分布、安全策略执行、安全任务开展、安全防护目标等字段，用于协助我方采取防御应对措施。

[0056] 数据准备阶段完成后的数据存放在数据仓库中网络空间信息库内，按照时间、空间和态势要素类型建立索引，用以在后续态势绘制的绘制要素阶段提升运行性能。

[0057] (2)态势绘制

[0058] 态势绘制的的整体流程包括选择基准点、设置比例尺、绘制底图、绘制要素、绘制连接、绘制属性等步骤，其流程图如附图3所示。

[0059] 1)选择基准点

[0060] 选择基准点通过指定态势呈现的地理原点，形成以该点为中心向外延展的网络空间态势。用户通过下拉式菜单框可以选择地理信息库中的某一城市/地区作为基准点，或是通过文本框输入，指定网络空间信息库中的某一域名/IP地址作为基准点，然后通过查询公开互联网域名/IP地址地理映射服务，将其转换为地理位置基准点。

[0061] 2)设置比例尺

[0062] 设置比例尺是确定态势缩放级别的过程。用户通过下拉式菜单框，将比例尺设置为“城区级”、“城市级”、“省级”和“国家级”四种级别。比例尺设置越大，屏幕中能够容纳的

地理区域越大，态势呈现的全面度提升；比例尺设置越小，屏幕中的能够容纳的地理区域越小，态势呈现的精细度提升。

[0063] 3)绘制底图

[0064] 绘制底图是根据基准点和比例尺，把地理空间地图绘制至屏幕中的过程。其中地理空间地图由三维地球模型使用圆柱投影、圆锥投影或方位角投影方法得到，绘制过程为将基准点作为中心点，将地图按照前一步骤中比例尺的参数进行放大、缩小或裁剪，最后调用贴图函数，地图绘制在屏幕上。

[0065] 4)绘制要素

[0066] 绘制要素是将不同类型的安全事件绘制在屏幕中的过程，将已绘制在屏幕上的事件称为要素。绘制要素包括定位、布局和染色三个步骤。

[0067] 在定位阶段，对于底图的每一地理区域，利用在数据准备阶段建立的索引快速查询到发生在该区域内、待展示的安全事件，根据当前比例尺设置缩放倍数，最后调用图标函数绘制在底图上。

[0068] 在布局阶段，通过力导向方法调整位于相同地理区域的安全事件位置，避免彼此重叠影响展示效果。

[0069] 在染色阶段，根据安全事件代表的安全态势类型进行标注，调用涂色函数，其中基础态势事件标定为蓝色，攻击态势事件标定为红色，防护态势事件标定为绿色。

[0070] 5)绘制连接

[0071] 绘制连接是在要素间具备特定联系的条件下，在要素间进一步绘制直线、曲线连接以增强认知效果。

[0072] 绘制直线的方法为：在两要素的X、Y坐标间调用直线函数绘制。

[0073] 绘制曲线的方法为：在两要素的X、Y坐标间调用贝塞尔曲线函数绘制。

[0074] 绘制连接的条件包括：1)要素代表事件的发生时间存在紧密的先后关系；2)要素代表事件的IP地址存在上下级网络关系；3)要素代表事件的描述存在一致性关系；4)要素代表事件的描述存在耦合性关系。在两要素间仅存在一条连接的情况下绘制直线，存在多条连接的情况下绘制曲线。

[0075] 6)绘制属性

[0076] 绘制属性是对网络空间态势中的要素进行额外标注的过程。绘制属性包括属性选择、属性定位和属性布局几个步骤。属性选择是根据当前用户配置，选取一个至多个用于显示的要素属性字段用于绘制。属性定位是根据实体的位置区域，以不遮挡显示为原则，在要素上方、下方、左方或右方调用字符串显示函数绘制信息。属性布局是根据要素位置区域的显示拥挤程度，通过力导向方法，对属性摆放的位置进行微调以达到最佳的呈现效果。

[0077] (3)探索交互

[0078] 探索交互是用户与态势界面进行互动的主要方式，用户从观察者或者探索者的角度出发，对网络空间态势进行观察，接收态势界面表达的信息，全面了解事件过程，并将其转化为自身的知识。探索交互方法包括观察者流程和探索者流程，用户可以在使用的时候选择或切换。

[0079] 其流程图如附图4所示。

[0080] 1)观察者流程

[0081] 在观察者模式下，用户的侧重点在于对网络空间的细致的观察，需要兼顾全局和热点区域。观察者流程中使用全局视图、基础态势视图、攻击态势视图、防护态势视图和热点事件视图这五类视图。

[0082] 全局视图是由在态势绘制步骤中，绘制攻击、防护和基础全部三类安全事件得到。

[0083] 基础态势视图是由在态势绘制步骤中，仅绘制基础类安全事件得到。

[0084] 攻击态势视图是由在态势绘制步骤中，仅绘制攻击类安全事件得到。

[0085] 防护态势视图是由在态势绘制步骤中，仅绘制防护类安全事件得到。

[0086] 热点事件视图是由在态势绘制步骤中，仅绘制过去10分钟内发生的攻击、防护和基础全部三类安全事件得到。

[0087] 在观察者流程的轮询中，五类视图的切换时间由用户通过文本框方式输入指定，可设置为5秒-180秒范围内。当上一视图已显示所设的切换时间后，系统自动切换为下一视图。

[0088] 2)探索者流程

[0089] 在探索者模式中，用户的侧重点在于对网络空间新知识的获取和发现。需要以沉浸、专注的方式探索网络空间态势的特征规律。在探索者流程中用户通过下拉框选择和文本框输入配置时间探索、空间探索和属性探索三类参数，然后通过平移、放大、缩小、点击等操作进行自由态势探索。

[0090] 时间探索参数设置：在时间探索视图中，用户可设置一个时间段，只显示发生在这一时间段中的态势事件；在空间探索参数设置：用户可设置两个区域，屏幕一分为二，在左右分别显示这两个区域的网络空间态势，以便对比观察；属性探索参数设置：用户可设置一个或多个关心属性的取值范围，将只显示具有这些属性的态势事件。

[0091] 平移操作：用户使用鼠标拖拽态势地图，地图将向着用户拖拽的方向展开新的内容；放大操作：用户使用鼠标滚轮放大态势地图，地图将减小比例尺，在相同屏幕面积中显示更少的内容；缩小操作：用户使用鼠标滚轮缩小态势地图，地图将增加比例尺，在相同屏幕面积中显示更多的内容；点击操作：用户点击一个态势要素，在该要素旁边显示关于该要素所有属性的完整信息。

[0092] 本发明并不局限于前述的具体实施方式。本发明扩展到任何在本说明书中披露的新特征或任何新的组合，以及披露的任一新的方法或过程的步骤或任何新的组合。

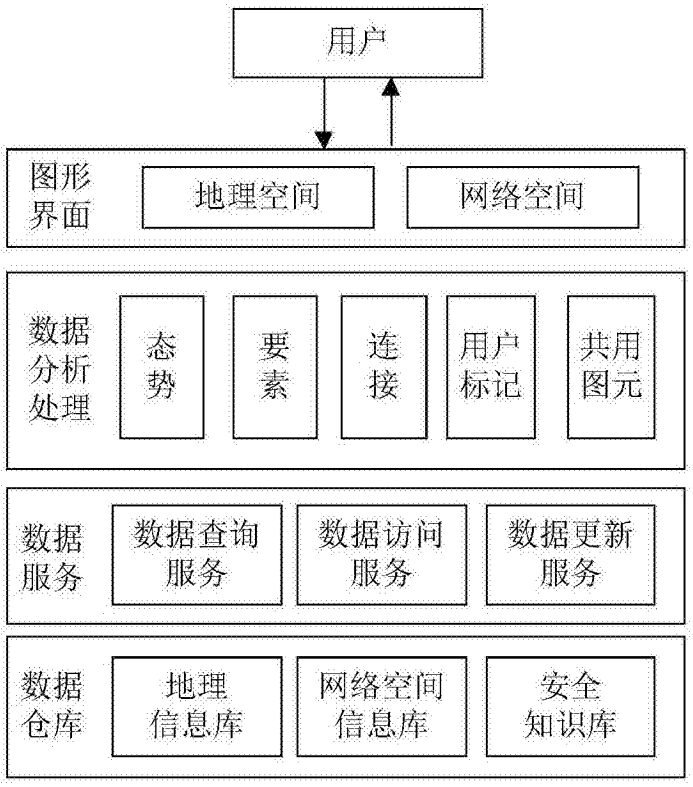

用户
图形界面
地理空间
网络空间
数据分析处理
态势
要素
连接
用户标记
共用图元
数据服务
数据查询服务
数据访问服务
数据更新服务
数据仓库
地理信息库
网络空间信息库
安全知识库

图1

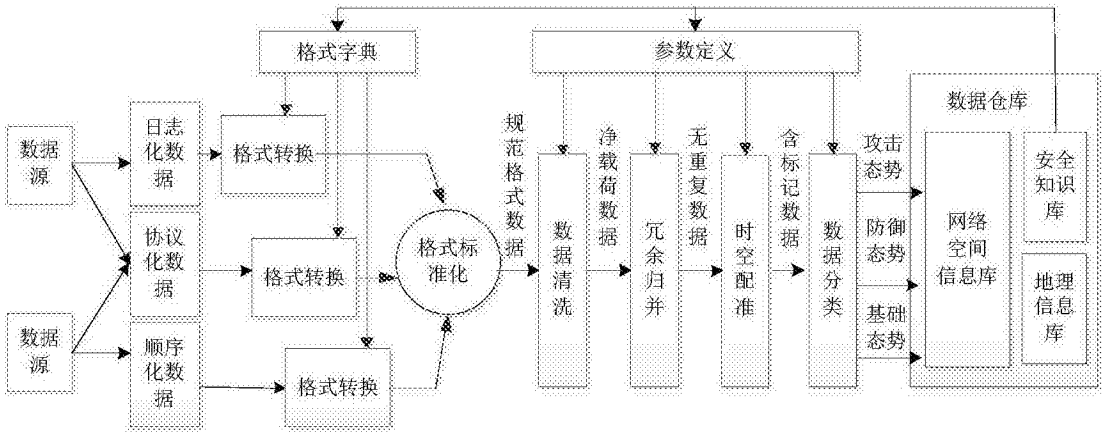

格式字典
参数定义
数据仓库
数据源
数据源
日志化数据
协议化数据
顺序化数据
格式转换
格式转换
格式转换
格式标准化
规范格式数据
数据清洗
净载荷数据
冗余归并
无重复数据
时空配准
含标记数据
数据分类
攻击态势
防御态势
基础态势
网络空间信息库
安全知识库
地理信息库

图2

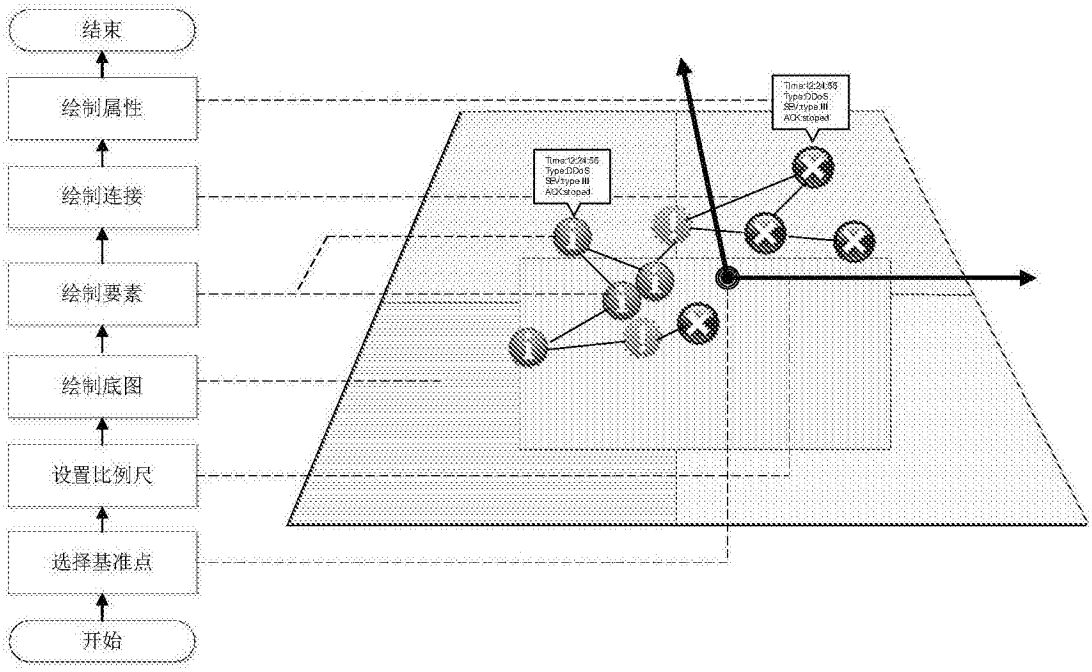

结束
绘制属性
绘制连接
绘制要素
绘制底图
设置比例尺
选择基准点
开始

图3

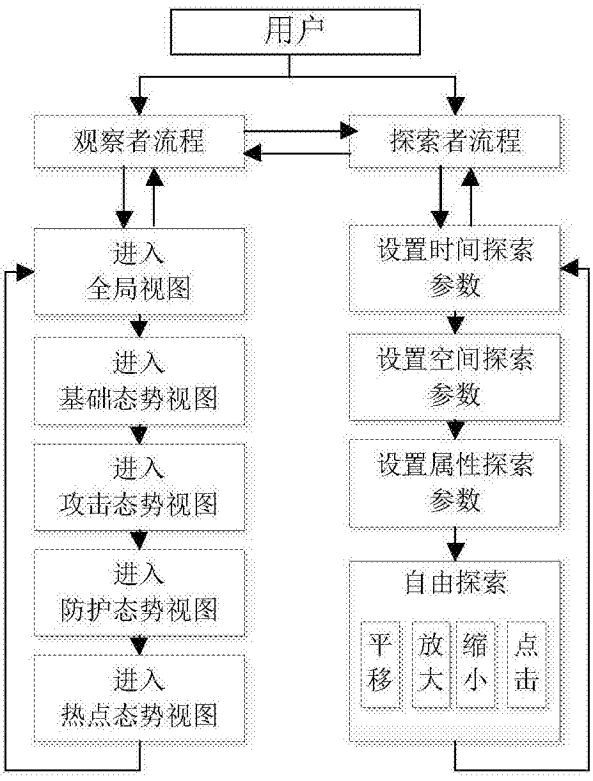

用户
观察者流程
探索者流程
进入
全局视图
进入
基础态势视图
进入
攻击态势视图
进入
防护态势视图
进入
热点态势视图
设置时间探索
参数
设置空间探索
参数
设置属性探索
参数
自由探索
平移
放大
缩小
点击

图4