第七章 网络内容安全态势评估

7.1 概述

7.2 网络内容安全态势评估模型

7.3 网络内容安全态势评估指标体系

7.4 网络内容安全态势预测与可视化

哈尔滨工程大学 HARBIN ENGINEERING UNIVERSITY

7.1 概述

7.1.1 网络内容脆弱性分析

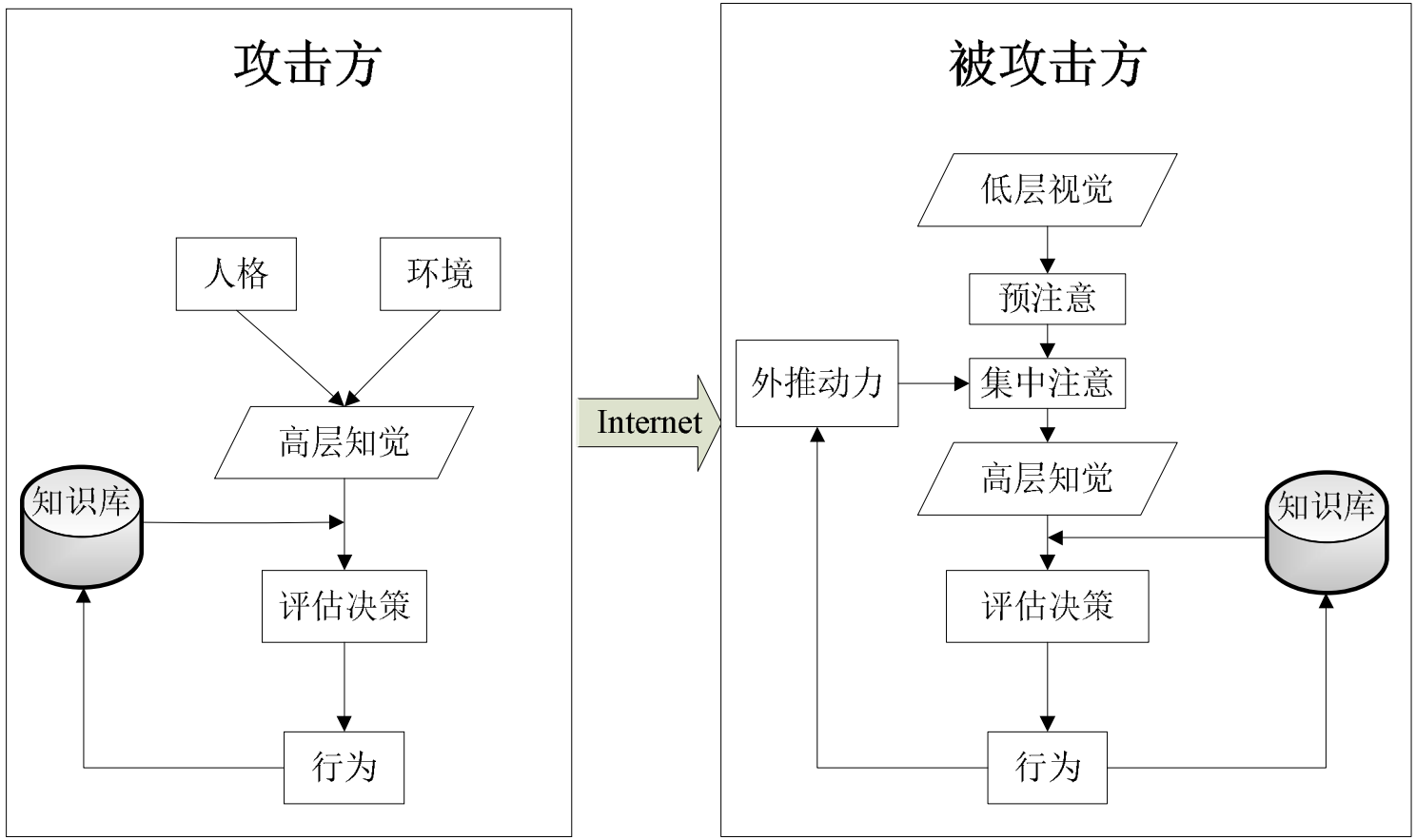
- 网络内容安全态势评估对于内容安全管理策略的制定和预防重大网络内容安全事件的发生具有重要意义。
- 1994年Libicki首次将计算机攻击分为物理层次攻击、句法层次攻击和语义层次攻击。
- Schneier认为语义攻击是攻击者强加自己的思想给网民，并认为语义攻击的目标是人与计算机的接口，即可视画面。
- Thompson等人将计算机攻击分为自治攻击和认知攻击。自治攻击是指攻击网络基础设施、计算机结构等，它不需要与用户有任何交涉，自动对计算机发起攻击；认知攻击是通过一系列措施改变用户行为，操纵用户感知的攻击。

7.1.1 网络内容脆弱性分析

■1999年中国学者管海明等人提出计算机网络攻击的四个层次：实体层次的攻击、能量层次的攻击、逻辑层次的攻击和超逻辑层次的攻击。超逻辑层次的攻击是利用计算机网络进行反动宣传，传播谣言，蛊惑人心等行为攻击。

■可以看出语义攻击、认知攻击和超逻辑层次的攻击如出一辙，都是攻击者将自己的攻击意念发布在网页上，表现形式为网络内容，网民在浏览网页时，经过视觉、感觉和知觉三个认知阶段，下意识地、不由自主地接受这种攻击意念，网络内容攻击模型如下图所示 。

7.1.1 网络内容脆弱性分析



7.1.1 网络内容脆弱性分析

(1) 存在空间：网络内容攻击存在空间包括垃圾邮件、传播扩散度高的论坛、博客、微博等、色情网站、弹出的广告网页等。

(2) 持续时间：根据网络内容攻击的持续时间不同分为长期性网络内容攻击、阶段性网络内容攻击和短期性网络内容攻击。

(3) 攻击目的：

1）政治目的：通过发放反党、反国家、反政府的信息，危害国家安全；

2) 经济目的：利用国家与国家间、企业与企业间的竞争，将掌握的国家机密卖给国外敌对分子，或将掌握的企业机密卖给别的企业，以牟取经济暴利。

7.1.1 网络内容脆弱性分析

（3）攻击目的（续）：

3）政治目的：通过发放虚假历史信息，以达到“合理”侵略国家、霸占国家财富的目的。此类信息的发放者可能是国外敌对分子，它们的发放严重影响国家的稳定发展。

4) 个人目的：一些因心理不正常就在网络上发放有攻击性的信息，或有奇怪癖好发放色情、暴力等的信息，或粗心，无意发放不文明的信息。这些信息的发放并不出于政治、经济、军事目的，但因为网络内容的高匿名性、高开放性、无地域性和零成本性，流传范围广，由此造成的危害同样不可计量。

7.1.2 网络内容安全态势评估概念

- 态势是一种状态，一个趋势，是一个整体、全局的概念。“安全态势”一词最早出现在军事上，如“战场安全态势”，“地区安全态势”等名词，同时也应运而生了相关的态势评估技术。
- 安全态势评估是指通过技术手段从时间和空间维度来感知并获取安全相关元素，通过数据信息的整合分析来判断安全状况并预测其未来的发展趋势。安全态势评估最早出现在航空领域和军事领域，后来逐渐推广到各个技术领域，包括交通管理、生产控制、物流管理、医学研究和人类工程等。

7.1.2 网络内容安全态势评估概念

- 网络的发展使得安全态势评估开始在计算机网络领域得到应用。“积极防御，综合防范”是我国信息安全保障体系建设必须坚持的原则。
- 网络安全态势评估是指将网络原始事件进行预处理后，把具有一定相关性，反映某些网络安全事件的特征的信息，提取出来，运用一定的数学模型和先验知识，对某些安全事件是否发生，给出一个可供参考的，可信的评估概率值。也就是说评估的结果是一组针对具体某些事件是否发生概率的估计。在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

7.1.2 网络内容安全态势评估概念

- 网络内容具有高匿名性、高开放性、无地域性、零成本性、快速传播性和冲击力度大等特性。随着互联网应用技术的不断推广和普及，网络内容安全成为信息安全的一项基本内容，已经逐渐引起广泛的关注和共识。网络内容安全的脆弱性催生了网络内容安全态势评估。
- 网络内容安全态势评估的定义如下：通过技术手段获取网络内容相关数据，并对这些数据进行分析得到网络内容的安全状况并预测其未来发展趋势。

7.1.2 网络内容安全态势评估概念

随着网络信息内容安全形势愈发严峻，网络内容安全态势评估将成为信息内容安全领域的研究重点。网络内容安全态势评估对于保障网络信息内容安全具有以下重要意义：

①网络内容安全态势评估技术能够综合分析网络内容的各个安全元素；

②网络内容安全态势评估可以从整体上动态反映网络内容安全状况；

③网络内容安全态势评估可以根据一段事件内的评估结果对未来网络内容安全状况及发展趋势进行预测。

7.1.2 网络内容安全态势评估概念

网络安全态势预测的目的：对可能发生的网络内容安全威胁进行提前防护，根据事态严重程度采取应对措施，以遏制事态的发展，实现对不良信息内容大范围传播的有效控制。此外，还可以评估所采取措施的有效性，为后续措施选取提供有益参考，便于内容安全策略的制定。

7.2 网络内容安全态势评估模型

7.2.1 通用安全评估方法

安全评估是指通过系统科学的程序、理论和方法，对待评测对象所构成的系统中存在的危险因素进行辨识、分析和揭示，判断系统发生危害及损伤和影响程度的可能性及严重程度，找到消除风险、保证安全的措施，从而为制定预警与防范措施和管理决策提供科学依据，最终达到对系统的不安全性因素进行有效控制，以确保系统安全的目的。

7.2.1 通用安全评估方法

安全评估工作通常遵循一定的程序，主要有以下三个主要环节和步骤:

（1）危险 / 不安全源头和因素辨识与分析

全面收集资料，找到影响待评估对象安全的危险源以及相应的危险因素，并进行细致地辨别和分析，这是做好可行的安全评估工作至关重要的基础环节。

（2）对危险 / 不安全要素进行安全评估

主要包括建立一定层次结构的指标体系、选取科学可行的安全评估方法以进行定性和定量相结合的分析。

（3）对危险 / 不安全要素进行控制

划分危险等级以得出最终评估结论，并制订相应的安全预警应对措施，以落实减少或防范危险。

7.2.1 通用安全评估方法

1. 层次分析法

1977年，美国运筹学家、匹兹堡大学教授Saaty T.L首次提出了“层次分析法（简称AHP），它是一种定性和定量相结合的多目标决策分析方法。

层次分析法是一种定性和定量分析相结合的评估决策方法，它将评估者对复杂系统的评估思维过程数学化。其基本思路是评估者通过将复杂问题分解为若干层次和若干要素，并在同一层次的各要素之间简单地进行比较、判断和计算，就可得出不同替代方案的重要度，从而为选择最优方案提供决策依据。

1. 层次分析法

将层次分析法应用于多指标综合评估过程中，其处理步骤如下：

①设置指标的权值

②建立比较矩阵

将系统中包含的因素根据系统结构划分为多个层次，用矩形说明层次的递阶关系和因素的从属关系。

③构造判断矩阵

用三标度法来对同一层元素进行两两比较后建立一个比较矩阵并计算出各元素重要性的排序指数，将比较矩阵转化为判断矩阵。

④一致性检验

⑤加权计算得到初步的脆弱指数

⑥指数的修正

2. 模糊综合评估法

模糊数学评估法的基础是模糊数学。模糊数学诞生于1965年，它的创始人是美国自动控制专家Zadeh　L.A。这一理论提出后，开始在西方学术界为某些偏见所左右，并未引起足够重视。20世纪80年代后期，日本将模糊技术应用于机器人、过程控制、地铁机车，交通管理、鼓掌诊断、声音识别、图象处理、市场预测等众多领域。模糊数学理论在日本的成功应用和巨大的市场前景，给西方企业以巨大的震动，在学术界也得到了普遍的认同。

2. 模糊综合评估法

对于模糊综合评估方法的理论研究，主要集中在模糊数学界，因为模糊综合评估本身就是模糊数学的一项重要研究内容。在模糊综合评估中，用P 表示概率测度，用C 表示影响测度，P 和C 的域值为区间[0,1]，用下标f事件未发生，用下标s事件发生。显然有 $P_f = 1 - P_s$ 和 $C_f = 1 - C_s$

2. 模糊综合评估法

评估过程如下：

①建立模糊集合

首先构造风险因素集，然后构造评估集，对于风险概率和风险产生的影响，可以设立不同的评估集。

②建立隶属度矩阵

专家参照评估集对因素集中的各因素进行评估，给出各因素的评语，构造模糊映射，得到隶属度矩阵。风险因素相对于概率和影响得到不同的隶属度矩阵。

2. 模糊综合评估法

评估过程如下：

③ P_5和C_5的计算

在计算风险因素发生的概率时，各因素相应的权向量为A，对评估集V，各指标赋予相应的权重，得指标权向量B，则风险事件发生的概率为

$$P_s = AR_pB^T$$

在计算风险后果的影响发生的概率时，各因素相应的权向量为A′，对评估集V′，各指标赋予相应的权重，得指标权向量 B′，则风险事件后果的影响为

$$C_s = A'R_cB'^T$$

2. 模糊综合评估法

评估过程如下：

④系统风险评估

根据 P_5和C_5，计算系统的风险度。

$$R = 1 - P_f C_f$$
$$= 1 - (1 - P_s)(1 - C_s)$$
$$= P_s + C_s - P_s C_s$$

一般认为R>0.7为高风险系统，R<0.3为低风险系统，介于二者之间的为一般风险系统。

2. 模糊综合评估法

⑤确定各风险因素熵权系数

在上述模糊综合评判法中，对各因素相应的权向量A的确定，一般采用专家估计法，或由专家对各因素两两比较构造判断矩阵，再采用层次分析法法求得。无论哪种方法，都带有明显的主观性。此处采用熵权系数法，通过定量计算求得各因素权向量 A。

3. 距离综合评估法

所谓距离评估，顾名思义，就是通过测算距离，来对待评估对象进行排序或估值。其处理过程如下：

①指标预处理

主要是指标同向化和无量纲化。

设用 P个指标对n 个事物进行综合评估，原始数据构成如下矩阵：

$$X' = (x'_{ij})_{n\times P}$$

其中 $i = 1,2,\cdots,n \quad j = 1,2,\cdots P$，

如果P个指标中有逆指标或适度指标，则将其转化为正指标，转化后数据矩阵记为：$X = (x_{ij})_{n\times P}$

选用合适的方法对数据进行无量纲化，变换后数据矩阵记为：$Y = (y_{ij})_{n\times P}$

3. 距离综合评估法

②利用专家经验构造加权数据矩阵

设已确定出各指标的权重为 $w_1, w_2, \cdots w_P$ ，以它们为主对角线元素构造对角矩阵 W，即：

$$W = \begin{pmatrix} w_1 & & 0 \\ & \ddots & \\ 0 & & w_P \end{pmatrix}_{P \times P}$$

加权数据矩阵为

$$Y = Y'W = (y_{ij})_{n \times P}$$

3. 距离综合评估法

③利用各指标的极值确定参考样本

用所有参评样本中各指标的最大值构成最优样本，用各指标的最小值构成最劣样本，分别用Y^+和Y^-表示如下：

$$Y^+ = (y_1^+, y_2^+, \cdots, y_P^+)^T$$

$$Y^- = (y_1^-, y_2^-, \cdots, y_P^-)^T$$

其中

$$y_j^+ = \max_{1 \le i \le n} \{y_{ij}\}$$

$$y_j^- = \max_{1 \le i \le n} \{y_{ij}\}$$

3. 距离综合评估法

④计算距离

根据距离公式计算样本点到最优样本点和最劣样本点的距离。记加权数据矩阵Y中第i行的P个样本数据为

$$Y_i = (y_{i1}, y_{i2}, \cdots, y_{iP})^T$$

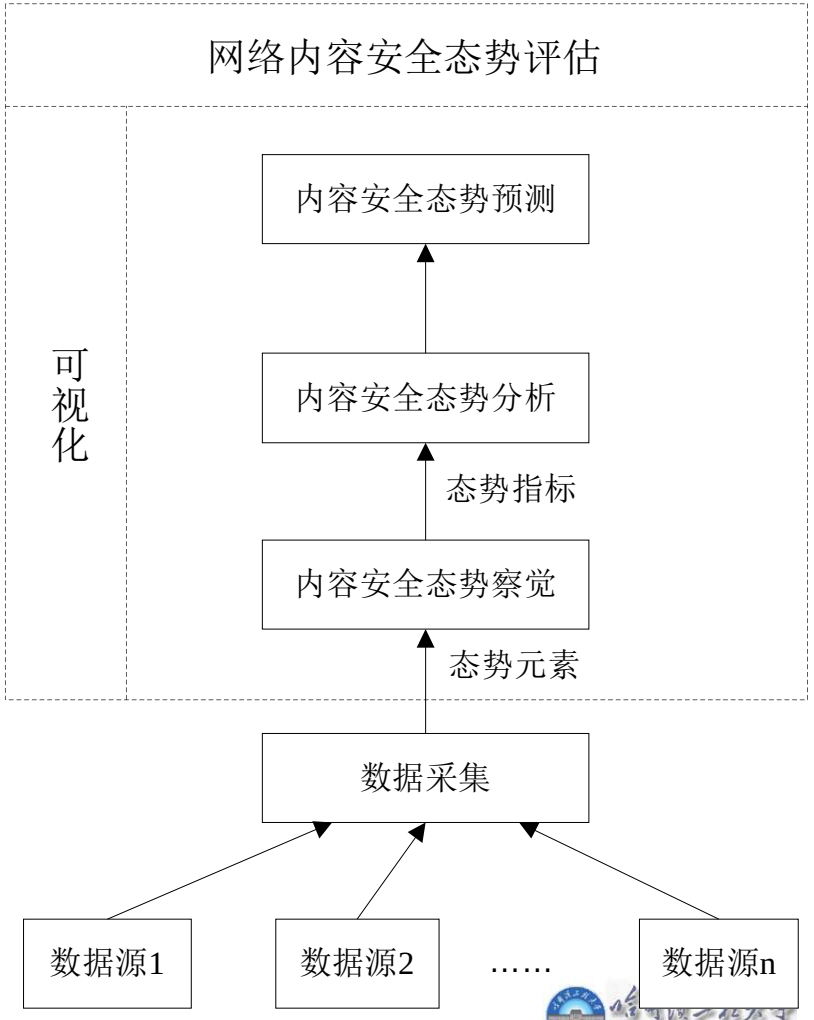
则样本点Y_i与最优样本点的相对距离为

$$d_i = \frac{(Y_i - Y^-)^T \bullet (Y^+ - Y^-)}{\left\| Y^+ - Y^- \right\|} = \frac{\sum_{j=1}^{P} (y_{ij} - y_j^-)(y_j^+ - y_j^-)}{\sqrt{\sum_{j=1}^{P} (y_j^+ - y_j^-)^2}}$$

此外，还有基于粗糙集理论的安全评估方法、基于贝叶斯网络的安全评估方法、基于灰色理论的安全评估方法以及基于智能算法的安全评估方法等。

7.2.2 网络内容安全态势评估模型

安全评估过程中对信息的了解就是时间、空间域中的当前态势元素被觉察认识、理解并被预测的处理过程，即安全态势评估具有一定的层次性。本章在基于知识的基础上构建了层次化的网络内容安全态势评估模型，如下图所示



7.2.2 网络内容安全态势评估模型

1.数据采集。网络信息内容的传播和扩散具有多通道性，因此对网络内容安全态势评估的第一步是采集数据，可通过网络爬虫获取数据存入数据库。

2.内容安全态势察觉。内容安全态势察觉是获取网络内容安全态势元素，可通过前面几章的信息内容识别技术进行态势察觉。

3.内容安全态势分析。内容安全态势分析是内容安全评估的核心。通过合理的评估算法、数学模型，构建行之有效的内容安全态势评估指标体系，计算网络内容的安全态势值。

4.内容安全态势预测。安全态势预测通过分析态势数据构建合理的预测模型，预知网络内容安全态势的发展趋势。

7.2.3 网络内容安全态势评估发展

纵观信息安全风险评估和网络安全态势评估，网络内容安全态势评估发展方向为：

- 手动评估到自动评估
- 从定性评估到定性评估与定量评估相结合
- 从基于知识的评估到基于模型的评估

1. 手动和自动评估

在网络内容安全态势评估工具出现之前，网络内容安全态势评估工作只能手动进行。手动评估对于管理员而言，工作量大且容易出现疏漏。具体而言，管理员需要浏览网页内容、分析当前安全实践、发现内容安全威胁、对内容安全状况及发展趋势进行预测等。

事实上，目前还没有专门针对网络内容安全态势评估的评估工具。但是，借助于网络安全态势评估工具和网络信息内容分析工具可以在一定程度上解决手动评估的局限性。

2. 定性和定量评估

定性评估是最广泛使用的评估方法。指借助对事物的经验、知识、观察及对事物发展变化规律的了解，科学地进行分析、判断的一类方法。该方法只关注于安全事件带来的损失，而忽略事件发生的概率。

目前应用较多的有安全检查表、事故树分析、事件树分析、危险度评估、预先危险性分析、故障类型和影响性分析、危险性可操作研究等。这些方法的共同特点是采用简易的计算公式，不必计算威胁发生的概率，非技术或非安全背景的员工也能轻易参与，同时评估流程和报告形式比较有弹性。

2. 定性和定量评估

定量评估是指根据统计数据、监测数据、同类或类似系统的资料数据，应用科学的方法构造数学模型进行量化评估的方法。该方法利用了威胁发生的概率和可能造成的损失。当前的网络安全态势评估方法基本上都采用了定量或定性与定量相结合的评估方法。

3. 基于知识的评估和基于模型的评估

基于知识的评估方法主要是依靠经验进行的，而经验从安全专家获取并凭此来解决相似场景的评估问题。这种方法的优越性在于能够直接提供推荐的保护措施、结构框架和实施计划。

基于模型的评估方法可以分析出系统自身内部机制中存在的危险性因素、发现系统与外界环境交互中的不正常及有害行为，从而完成对系统脆弱性和安全威胁的定性分析。

7.3 网络内容安全态势评估指标体系

网络内容安全态势评估模型是网络内容安全态势分析的基础，而网络内容安全态势量化评估是网络内容安全态势分析的核心部分。只有通过使用、准确的量化指标，才能有效地反映网络内容安全状况，为网络内容安全管理员提供综合、直观的网络内容安全信息。

7.3.1 评估指标的提取原则

1.全面性原则。作为可应用于大规模网络信息内容的安全态势评估指标体系，必须要考虑到几乎所有对网络内容安全产生影响的要素，争取能够做到全方位、多角度评价当前网络内容安全态势。

2.分层原则。网络信息内容安全态势评估指标具有层次性，有些是针对国家安全的，有些是针对企业安全的，有些是针对个人安全的，每个层次造成的影响差别较大，构建指标体系时应该分层考虑各个层次。

3.突出性原则。各评估指标的选取要全面，但应区别主次，要选取那些能体现不安全因素的指标，即找到杠杆点，因为只有杠杆点最能影响整个系统的安全性。对于网络信息内容安全态势评估指标体系而言，由于网络内容危害造成的影响不同，对于指标体系的构建一定要坚持突出性原则，才能准确把握评估工作。

7.3.1 评估指标的提取原则

3.突出性原则。各评估指标的选取要全面，但应区别主次，要选取那些能体现不安全因素的指标，即找到杠杆点，因为只有杠杆点最能影响整个系统的安全性。对于指标体系的构建一定要坚持突出性原则，才能准确把握评估工作。

4.动态性原则。虽然在构建指标体系时，应尽量选取比较有规律变化的因素，以体现指标体系的稳定性，确保其价值，但是对于网络信息内容而言，应同时注重动态性，遵循动态结合的原则。

5.科学性原则。网络内容安全态势评估指标的选择和设计应该建立在一定的统计理论基础上，并结合网络内容安全事件的具体情况，建立指标的代表性、计算方法、数据收集、指标范围、权重选择等都必须要有科学依据。

7.3.2 评估指标的选取方法

网络信息内容安全态势指标可以分为多种类型：

（1）按照网络内容安全态势范围分：国家级网络内容安全态势指标、企业级网络内容安全态势指标、个人级网络内容安全态势指标等。

（2）按照网络内容安全态势时间分：长期性网络内容安全态势指标、阶段性网络内容安全态势指标、重大网络内容安全态势指标等。

7.3.2 评估指标的选取方法

网络信息内容安全态势指标可以分为多种类型：

（3）按照网络内容表现方式分：网络文本内容安全态势指标、网络图像内容安全态势指标、网络音频内容安全态势指标、网络视频内容安全态势指标等。

（4）按照网络内容安全态势指标描述的视角分：内容敏感度、内容倾向性、内容暴露度、内容恶意度、传播扩散性等。

7.3.2 评估指标的选取方法

- 网络信息内容安全态势涉及的因素较多，可采用分析法对网络内容安全态势评估指标进行选取。
- 分析法是将指标体系的度量目标和对象分割成若干个不同的组成部分或侧面（子目标），之后逐步细分，直到各个组成部分和侧面都能用具体的统计指标来描述。这种方法是建立评估指标体系工作中较为常用的一种方法，一般来说，可以分为三步。

7.3.2 评估指标的选取方法

（1）分析评估工作实质是什么、涉及哪些方面，每方面又包含哪些分支。

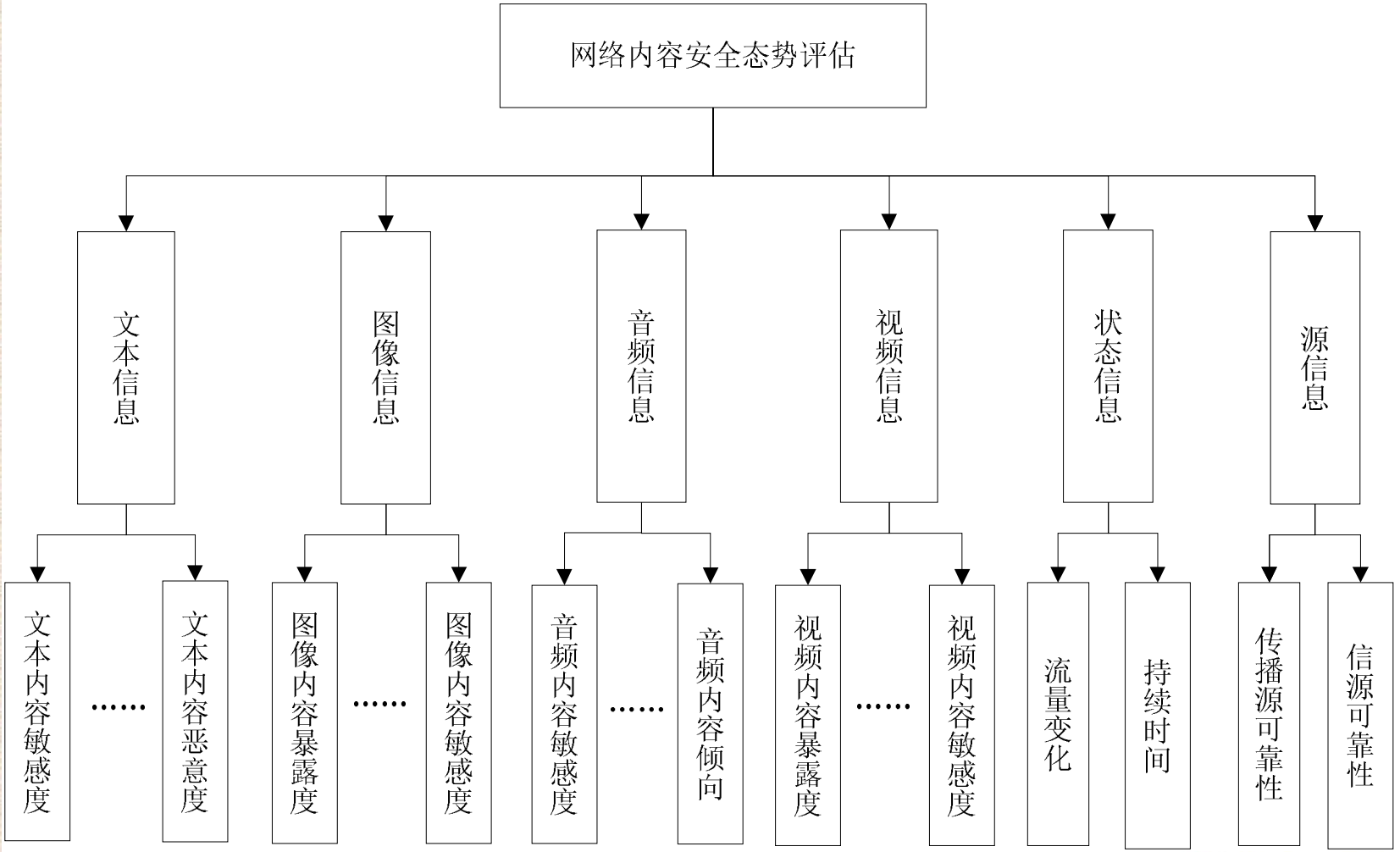
例如，在评估前我们应该首先了解网络内容安全态势的意义，它表现为哪几个方面？在此基础上，分析影响网络内容安全的各种因素，把态势评估的总体目标分解为各种子目标。

（2）细分各个子目标或侧面，直到各子目标或侧面都可以用明确的、可量化的指标描述为止。

（3）设计并确定指标层中的各个指标。

根据分析法形成如下图所示的网络内容安全态势评估指标层次结构。

7.3.2 评估指标的选取方法



7.3.3 指标体系构建与分析

虽然网络安全态势评估正成为网络安全领域的一个研究热点，已受到国内学者的高度关注，但是目前对网络安全态势评估的研究工作仍集中在网络化系统自身的物理安全评估问题上，对于网络信息内容安全态势评估的研究还很少，集中在网络舆情安全态势评估上。本节在上节的基础上构建了一个分级的网络信息内容安全态势评估指标体系，如下表所示，并对指标做简要分析。

7.3.3 指标体系构建与分析

一级指标	二级指标	三级指标
内容敏感度	文本内容敏感度	文本敏感词汇频率
	图像内容敏感度	图像敏感词汇频率
	音频内容敏感度	音频敏感词汇频率
	视频内容敏感度	视频敏感词汇频率
内容暴露度	图像内容暴露度	图像裸露面积
		敏感部位裸露程度
	视频内容暴露度	视频帧裸露面积
		敏感部位裸露程度
		裸露视频帧比例
内容恶意度	文本内容恶意度	文本内容主动干扰的程度
内容影响度	内容影响度	网站质量
		浏览人数
		回复次数
		发布时间

7.3.3 指标体系构建与分析

一级指标	二级指标	三级指标
内容倾向性	文本内容倾向性	文本内容的倾向
		文本内容的倾向强度
	图像内容倾向性	图像内容的倾向
		图像内容的倾向强度
	音频内容倾向性	音频内容的倾向
		音频内容的倾向强度
	视频内容倾向性	视频内容的倾向
		视频内容的倾向强度
信息稳定性	流量变化	流通量变化值
	持续时间	持续时间
传播扩散性	传播源可靠性	传播速度
		传播规模
		传播源网站质量
	信源可靠性	信源网站质量

7.3.3 指标体系构建与分析

1.传播源可靠性。传播源可靠性与传播速度和传播规模相关，传播速度越快，且传播范围越广，那么信息越受关注，对人民产生的影响越大。网络信息的传播主要是通过浏览和转载来完成的，即浏览人数越多，信息产生的影响越大；同理，转载信息的网站的质量越高，信息产生的影响也越大。

2.信源可信性。信源可靠性是对信源网站质量的评估。好的网站发出的信息往往具有比较高的质量，其内容安全性要比差的网站发出的信息内容安全性高。而且好网站的浏览人次一般都会比较多，因而它对社会产生的影响就比一般网站更深远。

7.3.3 指标体系构建与分析

3.内容敏感度。内容敏感度是出现敏感信息的程度，由敏感词汇自身的危害程度和出现频率来决定。敏感信息具有时效性，具体表现为在一段时期内，某些信息容易对国家或人民造成危害，变成不良信息。如在2020年，词汇“新冠肺炎”是敏感词汇，出现“新冠肺炎”多的网页，很可能是鼓吹“新冠肺炎”传播的虚假消息。该指标包括文本内容敏感度、图像内容敏感度、音频内容敏感度和视频内容敏感度四个二级指标。

4.内容恶意度。内容恶意度是对信息内容主动干扰的程度。采用中文主动干扰技术对敏感关键词进行各种变形，使得变形后的敏感关键词难以被检测和提取，但又不影响信息内容的语义表达。例如将“法轮功”变形为“ Fa论功”。内容恶意度越高，信息内容的不安全性越高。

7.3.3 指标体系构建与分析

5.内容影响度。内容影响度是指信息内容对人民造成的影响。主要与点击次数、回复人数、网站质量、发布时间等相关。网站质量越高、发布时间越长，被转载和被回复的几率越大，回复次数和转载次数越多，对人民造成的影响也越大。如果是不良内容，内容影响度越大，其危害程度也越大。

6.内容倾向性。内容倾向性包括内容的倾向和内容的倾向程度。内容的倾向主要是指内容的情感倾向。情感倾向分为正向和负向，正向和负向对信息内容安全的影响不是单独存在的。内容的倾向强度是对内容情感倾向的一个量化，如将情感倾向分成十级，其中正向五级，负向五级。

7.3.3 指标体系构建与分析

7.内容的暴露度。 内容的暴露度主要针对黄色图片或视频帧而言的，它与皮肤裸露面积和敏感部位有关。裸露面积越大，暴露度也越大，信息内容的危害程度就越大。

8.流量的变化。网络信息流量的变化是指在一定的统计时期内某一信息通过网络不同的数据源通道形成的报道数、帖子数、博文数等相关信息总量的变化值，它总是通过网络页面数的变化来呈现的。

9.持续时间。持续时间是指信息的时效性，由单位时间内浏览信息的人次来衡量。持续时间指标主要是用于阶段性网络信息内容安全态势评估和长期性网络信息内容安全态势评估中。

7.3.4 网络内容安全等级划分

通过对网络内容整体安全态势做出量化评分，实现对危险的控制和管理，可以对网络内容安全态势评估的结果进行等级化处理。参照GB/T 20984-2007，将内容安全状况划分为五级，等级越高，危险越高。

等级	评语	描述
5	重度危险	将产生非常严重的不良社会影响，如国家、政府、党或组织信誉严重破坏、严重影响到人们的正常生活，社会影响非常恶劣
4	中度危险	将产生较大的不良社会影响，如国家、政府、党或组织信誉受到破坏、较大地影响到人们的正常生活，社会影响恶劣
3	轻度危险	将产生不良社会影响，但造成的不良社会影响不大，影响到人们的正常生活
2	相对安全	产生的不良社会影响程度很轻微，通过简单措施就能弥补
1	绝对安全	不会产生不良社会影响

7.3.4 网络内容安全等级划分

- 网络内容安全等级值是关于评估指标的函数。等级处理的目的是为安全态势评估过程中对不同危险的直观比较，以确定组织安全策略。管理人员应当综合考虑危险控制成本与危险造成的影响，制定相应等级应急措施。
- 网络内容安全等级的划分可用于阶段性网络内容安全等级评估和长期性网络内容安全等级走势评估中。管理人员根据阶段性网络内容安全等级评估结果可以考虑提高近期频发内容安全事件类别的优先级，有效遏制该类别内容安全事情的发生。长期性网络内容安全等级走势评估结果可以为管理人员提供内容安全态势的知识支持，对于制定网络管理策略，预防重大内容安全事件的发生都具有很大意义。

7.4网络内容安全态势预测与可视化

7.4.1 态势预测技术

- 预测就是“鉴往知来”，借对过去的探讨，而得到对未来的了解，具体是指根据准确、及时、系统、全面的调查统计资料和信息，运用统计方法或其他数学模型，对未来事件、现象发展的规模、水平、速度和比例等量的关系的测定。
- 预测过程一般分为三个步骤：分析历史数据和信息，发现或识别数据模式或规律；通过一定的数学模型来描述这种模式或规律；将建立的数学模型在时间域上扩展完成预测。
- 两种预测方式：点预测和区间预测。点预测只是对待预测值的最佳估计；区间预测是在一定置信度（如95%）下得到的对待预测变量取值范围的估计。

7.4.1 态势预测技术

要选择一个恰当的预测算法必须考虑如下几个因素：

①现有的信息；

②预测形式的要求（点预测或区间预测）；

③数据的模式和规律；

④对预测精度的要求；

⑤预测的实时性要求（数据量，时间）；

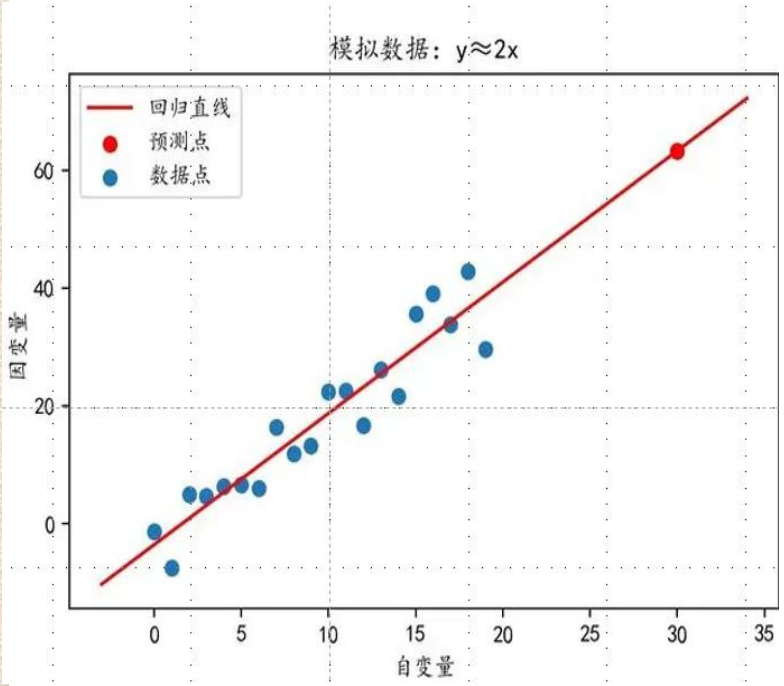
⑥可理解性和可操作性。

7.4.1 态势预测技术

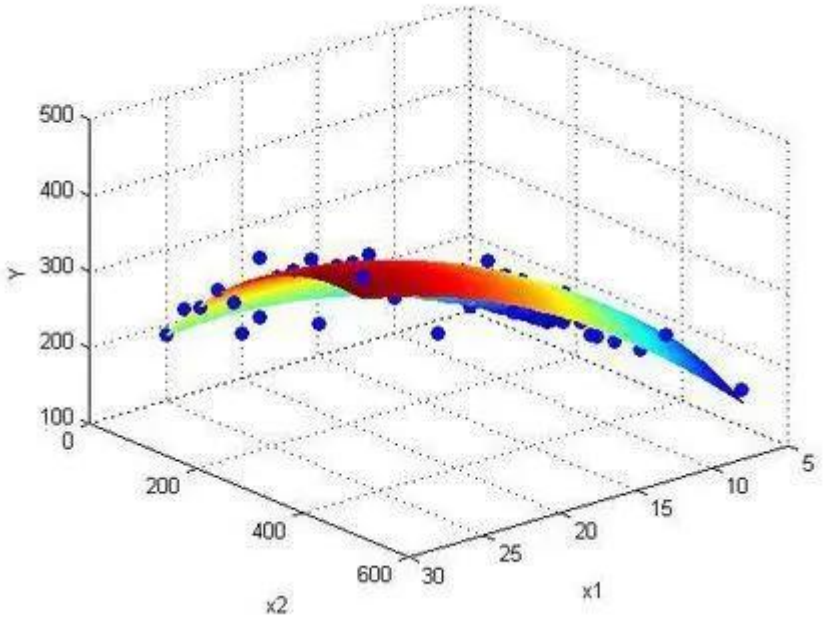
1.回归(regression)分析法。把两个或两个以上定距或定比例的数量关系用函数形式表示出来，就是回归分析要解决的问题。

解决问题：判别自变量是否能解释因变量的显著变化；判别自变量能够在多大程度上解释因变量；判别关系的结构或形式——反映因变量和自变量之间相关的数学表达式；预测自变量的值；当评估一个特殊变量或一组变量对因变量的贡献时，对其自变量进行控制。

7.4.1 态势预测技术



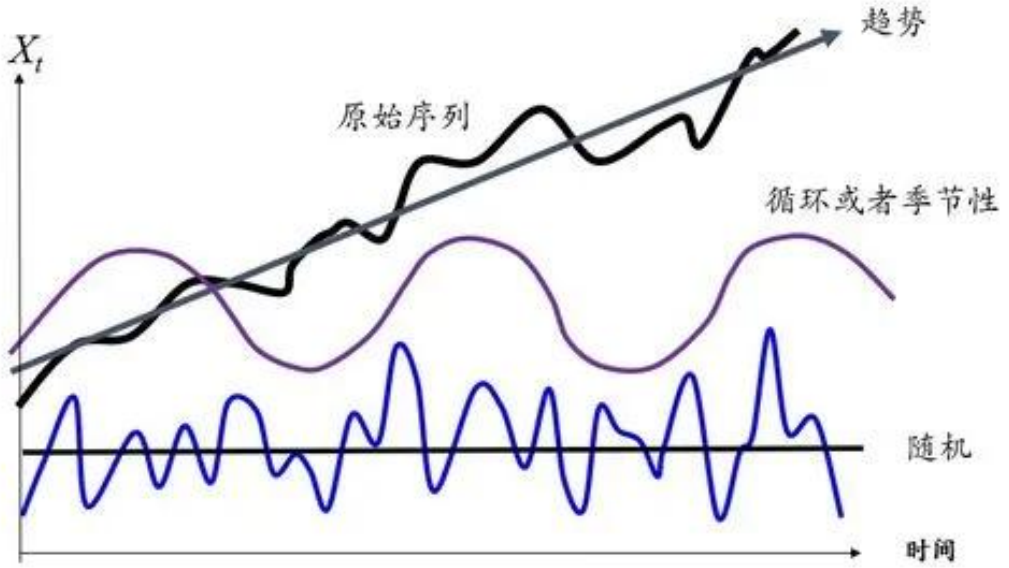
一元线性回归



多元线性回归

7.4.1 态势预测技术

2.时间序列预测法。 时间序列预测法是将预测目标的历史数据按时间的顺序排列成为时间序列，然后分析它随时间的变化趋势，外推预测目标的未来值。



7.4.1 态势预测技术

2.时间序列预测法。时间序列预测法主要用于分析影响事物的主要因素比较困难或相关变量资料难以得到的情况。时间序列预测法可分为确定性时间序列预测法和随机时间序列预测法。

时间序列分析具有以下三种变化分解式。

①趋势变动

指现象随时间变化朝着一定方向呈现出持续稳定地上升、下降或平稳的趋势。

②周期变动

指现象受季节影响，按某固定周期呈现出的周期波动变化。

③随机变动

指现象受偶然因素的影响而呈现出的不规则波动。

7.4.1 态势预测技术

3.灰色模型法。灰色理论的实质就是对原始随机数列采用生成信息的处理方法来弱化其随机性，使原始数据序列转化为易于建模的新序列。灰色预测的基本原理就是确定一条通过系统的原始序列累加生成的点群的最佳模拟曲线。

灰色预测的特点是所需的样本数较少，计算简单，因此，比传统的预测方法与有优越性。但是，基本的灰色算法也存在如对于光滑离散函数建模，在数据序列随机性较大时预测结果误差较大等缺陷。灰色预测方法可以用较少的数据建立微分方程模型，特别适于宏观预测。

7.4.1 态势预测技术

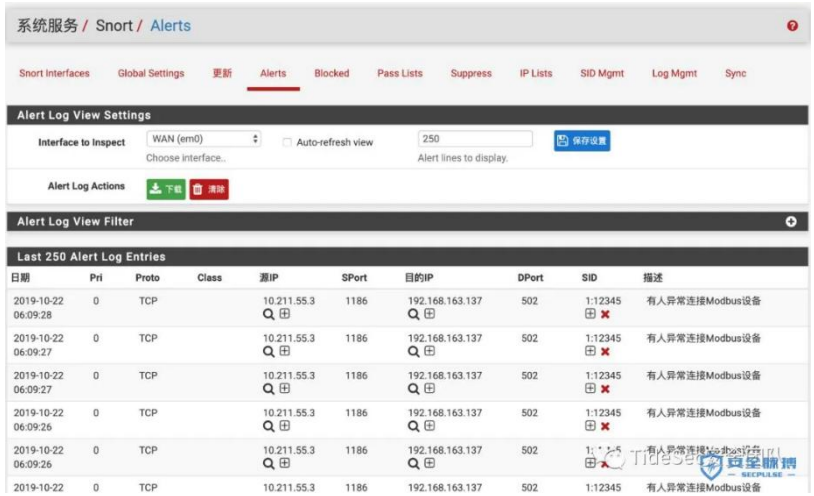
4.贝叶斯预测算法。贝叶斯动态模型及预测算法不仅仅是依赖于 时刻以往的历史数据和根据模型的知识进行预测，而且包括专家的经验信息以及主观的判断来进行预测，相对于传统的时间序列方法而言，贝叶斯通过人的主观经验给出先验分布，使得数据的要求大大减少，而得到同样精度的预测。

5.神经网络预测法。神经网络是模拟人脑神经网络的结构与功能特征的一种技术系统。它用大量的非线性并行处理器来模拟众多的人脑神经元，用处理器间错综灵活的连接关系来模拟人脑神经元间的突触行为，是一种大规模并行的非线性动态系统。

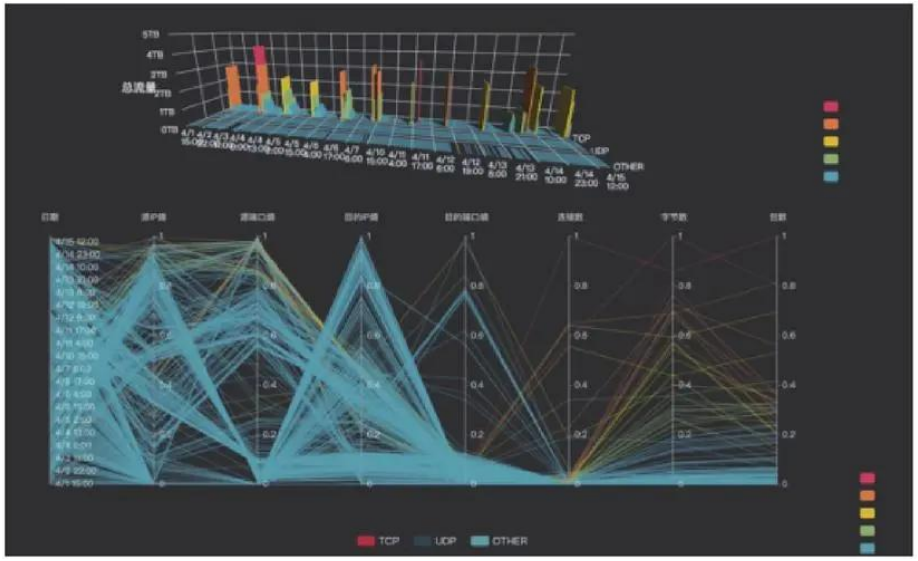
7.4.2 可视化技术

- 安全态势可视化是依据大量数据的分析结果来显示当前状态和未来趋势，而通过传统的文本形式，无法直观地将结果呈现给用户。可视化技术正是通过将大量的、抽象的数据以图形的方式表现，实现并行的图形信息搜索，提高可视化系统信息处理的速度和效率。
- 具体技术
  - 基于日志数据的可视化系统
  - 基于数据流的可视化系统
  - 基于多数据源、多视图的可视化系统
  - 基于NetFlow 的个可视化系统

7.4.2 可视化技术


系统服务 / Snort / Alerts
Snort Interfaces
Global Settings
更新
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Alert Log View Settings
Interface to Inspect
WAN (em0)
Choose interface..
Auto-refresh view
250
Alert lines to display.
保存设置
Alert Log Actions
下载
清除
Alert Log View Filter
Last 250 Alert Log Entries
日期 Pri Proto Class 源IP SPort 目的IP DPort SID 描述
2019-10-22 06:09:28 0 TCP 10.211.55.3 1186 192.168.163.137 502 1:12345 有人异常连接Modbus设备
2019-10-22 06:09:27 0 TCP 10.211.55.3 1186 192.168.163.137 502 1:12345 有人异常连接Modbus设备
2019-10-22 06:09:27 0 TCP 10.211.55.3 1186 192.168.163.137 502 1:12345 有人异常连接Modbus设备
2019-10-22 06:09:26 0 TCP 10.211.55.3 1186 192.168.163.137 502 1:12345 有人异常连接Modbus设备
2019-10-22 06:09:26 0 TCP 10.211.55.3 1186 192.168.163.137 502 有人异常连接Modbus设备
2019-10-22 0 TCP 10.211.55.3 1186 192.168.163.137 502 1:12345 有人异常连接Modbus设备


外部主机扫描内部应用数据透视
180.163.222.194-7910 > HTTP
TELNET
HTTP
百家号/网深科技


总流量
TCP
UDP
OTHER

7.4.2 可视化技术


HUAWEI
实时威胁
资产风险
威胁源
主区域
主区域(隐藏Chart)
综合态势大屏
2018/11/19/21:14:48
概述
事件处理率
97%
50%
威胁事件
7,382,746
38,362
资产数
接入总资产数
248,732
威胁类型TOP
982 疑似挖矿行为
1,872 中国菜刀
2,176 木马
1,356 IPS检测暴力破解
漏洞类型TOP
1 A5安全配置错误 1,270
2 注入类型漏洞 2,654
3 AB跨站请求伪造 1,700
4 Web安全 1,500
流量趋势
b/s
2,000
1,500
总流量
安全资讯
2018-11-19，CVE-2018-0952：Windows Stand…
2018-11-19，WebLogic Server远程高危漏洞预警
2018-11-19，CVE-2018-0952：Windows Stand…
2018-11-19，WebLogic Server远程高危漏洞预警
实时威胁
疑似挖矿行为 2018/11/19 21:14:48
123.125.15.50印度 47.75.254.67
资产风险 低危
DGA域名请求 2018/11/19 21:14:48
203.18.60.111英国 140.205.220.96
资产风险 高危
中国菜刀 2018/11/19 21:14:48
59.145.168.16美国 140.15.220.96
资产风险 高危
资产风险TOP
1 123.125.115.110 失陷
2 123.129.254.12 失陷
3 203.18.60.111 中危
威胁源TOP
英国 7,270
阿拉伯联合酋长国 3,654
南非 5,700
美国
巴西
英国
德国
葡萄牙
西藏
重庆
上海
辽宁
埃及
苏丹
南非
印度
澳大利亚