第 5 章

太空网络风险评估指标体系

5.1 太空网络安全风险评估指标体系结构

要保证太空网络的安全风险评估结果科学、可信，除建立科学的评估模型，采用先进的分析方法外，构建科学的安全风险评估指标体系也是必不可少的。

基于风险的组成要素，结合太空网络安全风险评估的过程，整个太空网络安全风险评估指标体系可以分为四方面：信息资产指标、威胁指标、脆弱性指标以及风险评估指标。安全风险评估指标体系结构如图 5-1 所示。

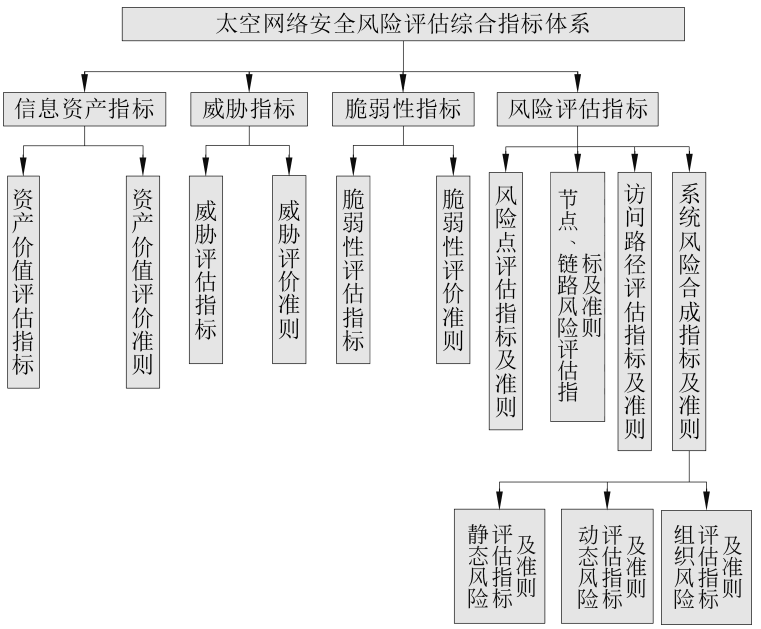

图 5-1 安全风险评估指标体系结构

由此可见，太空网络的安全风险的三个组成要素信息资产、威胁、脆弱性的指标分别由两部分组成：评估指标和评价准则。其中，评估指标是评估风险的依据，评价准则是度量风险的准绳。风险评估指标按照评估的过程分四部分。

5.2 空间信息资产评估指标

5.2.1 资产分类标准

太空网络信息资产也分为物理资产和逻辑资产两大类。前者主要指有形的实物基础设备等，如主机、服务器等，后者指无形的信息、财富、智力资源，如员工的技能、数字化信息等。需要说明的是，这里所说的信息资产指的是太空网络中所有与信息相关的资产。其中物理资产具体包括系统、硬件设备、软件资源三种；逻辑资产包括数据信息、人力资源两种。对于物理资产，按照资产所处的地理位置，以及资产完成的功能分类描述。对于逻辑资产，按照资产的功能分类描述即可。

- 系统：是指位于空间、海上或地面处理和存储信息的各种子系统。这里的系统是指信息、软件、硬件资产以及任何主机、客户机或者可视为系统的服务器的结合。系统资产是最广泛的一类资产，代表一组信息、软件和硬件资产。需要特别说明的是，系统是一个有机的整体，风险评估时应当单独考虑，而不能把它分成系统的组件分别评估。因此，在安全风险评估过程中必须对系统资产加以标识。
- 硬件设备：是指太空网络的基础性物理设备，例如星上计算机裸机。这里也需要将硬件资产与系统资产区别开。比如，标识资产时，将星上计算机标识为资产，就要指明组织最重要的资产是星上计算机硬件，还是星上计算机系统。因此，在实施风险评估时，通常要强调单独考虑这些物理设备的价值。
- 软件资源：是指太空网络的软件应用程序和提供的 IT 服务等。软件应用程序和服务，如星上操作系统、数据库应用程序、空间网络软件、安全应用软件等，主要用于处理、存储和传输信息。当标识软件资产时，应当注意区别系统和软件应用程序或服务本身。如果是系统（如数据库系统），则它不仅包括软件，还包括相关的数字信息资源。这里的软件资产应该是狭义的，指的就是空间子系统的软件应用程序本身及其相关组件。
- 数据信息：指太空网络系统处理、存储的数据信息。这些数据信息包括正在空间子系统中运算加工的数据、正在空间子系统通信网络中传输的信息流、已经以书面形式或者电子形式存储的信息资源，以及用于完成组织任务的知识产权。数据信息本质上是无形的，它与太空网络紧密联系。系统存储、处理和传输驱动组织的关键信息。因此，当组织建立策略和计划以保护系统资产时，同时也保护了组织的关键数据信息（及其软件和硬件资产）。但是，要特别注意，千万不要忽略，有些关键的数据信息是以物理形式表示的（记录在纸上、胶片上等），但它们本身是无形的。
- 人力资源：指组织中拥有独特技能、知识和经验的、他人难以替代的人。人力资源是一种特殊的资产。当人被作为资产加以标识时，可能因为他拥有某种特定的技能或者能提供某种服务。人被标识为资产，实质上是人的某个方面具有代表性的特征被标识为资产，如技能水平、职业道德等方面。在人被标识为资产时，要确

定是否还有更适于标识的相关资产。例如，标识他们使用的关键系统或者他们为其他使用者提供的某类信息。

上述资产分类是为了标识组织的资产，太空网络中常见的各类资产详见附录A。

5.2.2　资产的相对价值评估指标

资产标识完成之后，就应该进一步评估资产的资产价值，以便从众多的资产中挑选出关键资产。值得注意的是，考虑太空网络的各种资产价值，是指系统的各种与信息相关资产的相对价值，而不仅是资产本身的绝对价值。这种相对价值就是要体现资产对系统的重要性。

1. 非人力资源类资产的相对价值评估指标

对于除人力资源外的资产的相对价值，主要从如下五方面的指标评价，如表5-1所示。

• 组织业务指标

该指标表征资产在完成组织功能方面的重要性。评价指标值时，主要考虑资产是否为组织完成其业务活动所必需的，如果资产的安全属性被破坏，会直接导致组织无法正常运转，那么这种资产无疑是关键资产。具体到太空网络而言，组织的核心业务就是地面测运控和天基信息支援等活动。这项核心业务又由一系列子业务组成。比如，天基信息支援活动主要包括卫星侦察、空间目标监视、卫星通信、空间测绘与环境保障等。

• 系统功能指标

该指标表征资产对实现系统功能的贡献大小。作为一个系统，其存在的价值就在于它具有某种功能，能提供某种服务。以太空网络对抗为例，主要提供如下服务：空间侦察、导弹预警、天气预报、导航定位、资源勘探、地形测绘、电磁干扰、防电磁辐射、通信传输、空间物理攻击、空间防护、空间网络管理、(计算机、网络)入侵检测、空间信息安全事件应急响应及灾难恢复等。如果资产对系统提供某项功能而言是不可或缺的，那么可以认为该资产即为关键资产。

• 经济成本指标

该指标表征资产的绝对价值大小，主要考虑资产的成本和造价，一般用于物理资产。按照通常的说法，一个东西越昂贵越重要。但是，昂贵也是相对的，对不同规模的系统而言，昂贵的标准和意义是不同的，而且不同的设备，其造价和设计的使用年限也不一样。所以，昂贵必须有一个评判的标准。这里考虑以资产的单位造价(或单位成本)即资产的造价和资产的设计使用年限的比值作为资产的昂贵程度指标。考虑太空网络本身就是一个极其昂贵的复杂系统，在选定指标时起点应该比普通系统高一些。具体的指标，可邀请专家根据整个太空网络的总造价和当时的国民经济发展状况制定。

• 技术成本指标

该指标表征资产在技术方面的复杂程度。由于太空网络是一个融合了许多尖端技术、凝聚了众多开发人员智慧的复杂大系统，因此，技术方面也是评价资产是否为关键资产的一个重要指标。在技术上主要考虑三方面：其一，资产的技术含量多大，即资产包含了哪些主要技术；其二，这些技术的先进程度如何，先进程度一般分为国际领先、国际先

进、国内领先、国内先进、一般技术等；其三，这些技术中，哪些是有自主知识产权的。最终，可以根据资产是否包含有自主知识产权的国内先进水平以上的技术，确定资产是否属于关键资产。

• 作用范围指标

该指标表征资产受损对系统其他部分影响的强弱。由于太空网络的资产，都具有一定的功能，某些资产甚至能为其他资产提供一定的安全防护功能，因此，评价资产作用范围指标时，主要考虑被保护的其他资产的多寡。

这几个指标分别从不同的角度体现了资产的重要性。首先，无论在民事组织还是军事组织中，保护组织成员和非组织成员的生命安全，保存有生力量都是最基本、最核心的要求。其次，从研究太空网络安全风险评估的目的考虑，确保组织的业务活动正常进行，保证系统功能正常实现和系统服务正常提供是最直接、最重要的目标。最后，在保证组织业务活动和系统功能服务正常的前提下，也必须考虑关键空间资产的经济成本、技术成本及资产受损的可能影响范围等方面的因素。因此，基于上述考虑，在权重的划分上，如表 5-1 所示。

表 5-1 系统资产相对价值评估指标值及评价准则

指标项	权 重	分 值	评价标准
组织业务	0.3	3	对完成子网的关键组织业务活动不可或缺、不可替代
		2	对完成子网的关键组织的业务活动至关重要，但可以用其他资产替代
		1	对完成子网的少数非关键的组织业务活动很重要
		0	对完成子网的组织业务基本无影响
系统功能	0.2	3	对实现子网的功能与服务不可或缺、不可替代
		2	对实现子网的功能与服务至关重要，但可以用其他资产替代
		1	对实现子网的功能与服务一般重要，只对部分功能有影响
		0	对子网的功能与服务基本无影响
经济成本	0.2	3	资产的造价极其高昂，或资产的经济价值极高，一般在百万元以上
		2	资产造价很高，或经济价值很高，一般在十万元以上
		1	资产造价较高，或经济价值较高，一般在万元以上
		0	资产造价一般，经济价值也一般，一般在万元以下
技术成本	0.15	3	拥有自主知识产权的国际先进或领先技术
		2	拥有自主知识产权的国内先进或领先技术
		1	拥有自主知识产权的发明专利，或具有独创性的、实用性强的技术
		0	普通的技术

续表

指标项	权　重	分　值	评价标准
作用范围	0.15	3	为子网内40%以上的节点(或链路、或路径)提供一定程度的安全防护
		2	为子网内10%以上的节点(或链路、或路径)提供一定程度的安全防护
		1	为子网内至少一个其他的节点(或链路、或路径)提供一定程度的安全防护
		0	只与本身的安全性相关

此外,5方面的权重也可由评估专家和系统的拥有者或使用者共同制定。评估资产的相对价值目的是标识关键资产,而不是得出一个绝对的量化值数。因此,通过这5方面按照各自权重计算出资产的相对价值分值,然后按如下规则转换为资产的相对价值的等级。

2. 人力资源类资产的相对价值评估指标

对于人力资源这种特殊资产,拟分两级指标考虑。一级指标为道德水平、技术水平、发展潜力三项。各项一级指标包含的二级指标如表5-2所示。

表5-2　人力资源资产评价指标构成

一级指标	权　重	二级指标	权　重
道德水平	0.4	职业道德	0.6
		社会公德	0.4
技术水平	0.4	技术技能	0.4
		业务经验	0.4
		学历	0.2
发展潜力	0.2	年龄	0.2
		知识结构	0.2
		钻研精神	0.3
		学习能力	0.3

道德水平、技术水平、发展潜力三项一级指标中,首先道德水平是第一位的。但是,技术水平同样重要,组织需要的是德才兼备的人才。因此,暂定各指标权重分别为0.4、0.4和0.2。各二级指标及其权重见表5-2。人力资源资产的评价指标值同样采用三分制,以便与前述的非人力资源资产的评价指标值保持一致。

信息资产价值等级划分标准如表5-3所示。

被评为上述任一个等级的资产,都是系统的关键信息资产,就应该被作为关键资产加以标识,只是它们的重要程度略有不同。

表 5-3 信息资产价值等级划分标准

资产相对价值分值	资 产 等 级
小于或等于 1	1
大于 1 且小于或等于 2	2
大于 2 且小于或等于 3	3

3. 节点或链路的相对价值评估准则

在得出单个资产的相对价值等级后，应该确定资产所在节点的综合价值的评价指标及其计算方法。从组织业务活动考虑，由于最关键的资产一旦受损，可能会对组织造成不可估量的后果；从安全防护的角度来说，最关键的资产往往是首先要保护的对象。因此，真正决定一个节点或链路价值的是最关键资产的存在与否以及其数目多少。所以，对于节点资产价值的确定，要避免非关键或次关键的资产影响真正的关键资产的权重。基于上述分析，制定以下节点或链路相对价值的评估准则，如表 5-4 所示。

表 5-4 节点或链路相对价值的评价准则

节 点 等 级	评 估 准 则
4	拥有 5 个以上 3 级关键资产
3	拥有 1～5 个 3 级关键资产
2	至少拥有 1 个 2 级关键资产
1	至少拥有 1 个 1 级关键资产

4. 跨节点或链路的资产的评估准则

对跨节点或链路的资产的评估，应按以下步骤进行。

首先，从系统、组织角度，按上述指标评估整个资产的相对价值等级；

然后，确定该信息资产组件的分布及其重要性；

最后，确定该信息资产在各节点上的该信息资产的组件(子资产)相对价值等级。

资产组件重要性评估准则如表 5-5 所示。

表 5-5 资产组件重要性评价准则

组 件 等 级	评 估 准 则
2	主信息资产中必不可少的组件或信息
1	主信息资产中重要的组件
0	主信息资产中无关紧要的组件

节点(或链路)上的该信息资产的组件(子资产)相对价值等级评价准则如表 5-6 所示。

最终，对风险的评判，还要结合威胁和脆弱性，考虑资产受损对系统的影响。这种影响的评判指标将在 5.3 节中给出。

表 5-6　组件(子资产)相对价值等级评价准则

资产等级	组件等级	
	2	1
3	3	2
2	2	1
1	1	1

5.2.3　子网权重评估指标

子网权重评估指标主要包括三项：子网的组织业务指标、子网实现的系统功能和子网的作用范围指标。

子网权重评估指标及评价准则如表 5-7 所示。

表 5-7　子网权重评估指标及评价准则

指标项	权重	分值	说明
组织业务	0.4	3	对完成上层网络的关键组织业务活动不可或缺、不可替代
		2	对完成上层网络的关键组织的业务活动至关重要，但可以用其他资产替代
		1	对完成上层网络的少数非关键的组织业务活动很重要
		0	基本对完成上层网络的组织业务无影响
系统功能	0.4	3	对实现上层网络的功能与服务不可或缺、不可替代
		2	对实现上层网络的功能与服务至关重要，但可以用其他资产替代
		1	对实现上层网络的功能与服务一般重要，只对部分功能有影响
		0	对上层网络的功能与服务基本无影响
作用范围	0.2	3	为上层网络内 40%以上的节点(或链路、或路径)提供一定程度的安全防护
		2	为上层网络内 10%以上的节点(或链路、或路径)提供一定程度的安全防护
		1	为上层网络内至少一个其他的节点(或链路、或路径)提供一定程度的安全防护
		0	只与本子网的安全性相关

三项指标中，显然以第一项、第二项为主，实际情况下，第三项指标在前两项中已经有所体现。因此，各项指标所占比重暂定为 40%、40%和 20%。当然，此比重也可根据实际情况修正、确定。

5.3 太空网络威胁评估指标

5.3.1 威胁分类标准

威胁是指可能导致信息安全事故和系统信息资产损失的活动。威胁源被定义为任何可能危害组织资产的环境或事件，是威胁的发起者。评估威胁首先要识别威胁源，在识别威胁源中要考虑可能危害 IT 系统及其处理环境的所有潜在威胁源。按照威胁源的性质，太空网络面临的威胁主要来自四方面：人为故意行为、人为意外行为、系统问题和自然环境问题，如表 5-8 所示。另外，由于空间环境和地面环境差别很大，太空网络在空间环境下面临的威胁与在地面环境下面临的威胁又有很大不同，因此，制定整个系统威胁标识的指标时有必要分别考虑。具体的常见威胁列表见附录 B。

表 5-8 威胁源描述

威 胁 源	描 述	示 例
自然环境问题	指可能对组织信息技术系统产生影响的自然灾害、基础服务结构和运行环境方面的问题，使其他一些组织维护的系统失效，这是组织无法控制的	宇宙射线、洪水、地震、飓风、泥石流、雪崩、雷电风暴、长时间电力故障、污染、化学液体泄漏、水管破裂、长途通信中断等及其他类似事件
系统问题	与信息技术系统相关的问题，这是组织无法控制的	硬件缺陷、软件缺陷、相关系统无效或失效、病毒、恶意代码和其他与系统相关的问题
人员问题(故意)	那些由人员(包括组织内外的人员)因某些目的故意激发或引发的事件(如基于网络的攻击、恶意软件上传、对保密信息未经授权的访问)，可能破坏组织的资产	黑客、计算机罪犯、恐怖分子、工业(或其他)间谍、内部组织成员
人员问题(意外)	那些由人员(包括组织内外的人员)无意识地激发或引发的事件(如疏忽的数据条目)	组织外合法用户、内部组织成员

5.3.2 威胁评估指标

威胁评估指标除威胁源标识外，还要将威胁源分为自然威胁和人为威胁。自然威胁的评估指标主要有发生的频率和威胁后果如表 5-9 所示。

评估人为攻击(威胁)的一级指标主要有攻击者发起攻击的可能性、攻击者攻击成功的可能性和攻击后果三项。需要说明的是，这三项指标不是简单的加权关系，后续的风险评估将分别应用这三个指标，因此，在评价风险时，这三个指标没有权重之分。然而，为便于单纯评价威胁大小，表 5-10 中给出的指标中，二级指标包括攻击的主角、攻击动机、攻击者的技术水平、攻击者的攻击成本、攻击者的攻击频率、攻击者的已有条件、业务影响指标、生命影响指标、信誉影响指标、经济影响指标、社会影响指标及网络影响指标 12 项。

表 5-9　自然威胁评估指标描述

一级指标	权　重	二级指标	权　重	描　　述
自然威胁发生的频率	0.4	—	1	自然灾害或系统故障发生的频率
攻击(威胁)后果	0.6	业务影响	0.2	威胁对组织的业务活动的影响
		生命影响	0.2	威胁对组织有生力量的影响
		信誉影响	0.2	威胁对组织的权威、威信和信誉带来的影响
		经济影响	0.2	威胁对组织在经济方面的影响
		社会影响	0.1	威胁危害组织和系统后,对社会造成的影响
		网络影响	0.1	威胁对系统的网络平台的影响

表 5-10　人为威胁评估指标描述

一级指标	权 重	二 级 指 标	权重	描　　述
发起攻击的可能性	0.2	攻击的主角	1/3	指威胁源或攻击者
		攻击动机	1/3	攻击者攻击的决心或欲望
		攻击频度	1/3	用于评定威胁发生的概率
攻击成功的可能性	0.3	已有条件	1/3	实施攻击所具备的条件
		技术水平	1/3	攻击者的攻击技术水平
		攻击成本	1/3	实施当前攻击目标所需的成本
攻击(威胁)后果	0.5	业务影响	0.2	威胁对组织的业务活动的影响
		生命影响	0.2	威胁对组织有生力量的影响
		信誉影响	0.2	威胁对组织的权威、威信和信誉带来的影响
		经济影响	0.2	威胁对组织在经济方面的影响
		社会影响	0.1	威胁危害组织和系统后,对社会造成的影响
		网络影响	0.1	威胁对系统的网络平台的影响

威胁的影响(包括自然威胁后果和人为威胁后果)评估指标是威胁指标的一个重要方面。威胁的影响是指威胁可能给系统造成什么样的危害,可能给组织带来什么样的损失与后果。评估威胁对组织造成的影响时,主要考虑以下几方面的指标。

• 业务影响指标

该指标主要表征威胁对组织的业务活动的影响程度。对太空网络而言,组织的目标是要保证其核心业务顺利进行。但是,由于威胁的存在,可能导致组织不能正常按照既定的计划和部署完成太空网络的各项任务。具体的影响如通信不畅、测控或指控不力等。

• 生命影响指标

该指标主要表征威胁对组织有生力量的影响程度。人的生命是最宝贵的,尤其是对太空网络这样一个综合系统而言更是如此。因此,在威胁存在的情况下,组织的有生力量

是否受损，是否有人员伤亡，有多少人员伤亡，是衡量该威胁严重程度的一个重要指标。

• 信誉影响指标

该指标主要表征威胁对组织的权威、威信和信誉带来的影响程度。如果太空资产受到损害，比如发射失败、卫星通信中断等，组织的权威就会受到挑战，组织的威信荡然无存，组织的信誉面临威胁，因此，组织的信誉也是评价威胁影响的重要指标之一。

• 经济影响指标

该指标主要表征威胁对组织在经济方面的影响程度。一般而言，一个组织的经济承受能力都是有限的。然而，太空网络是一个成本高昂、技术复杂的综合系统，一旦面临威胁，导致系统受损，维修、恢复系统都将付出巨大的代价，给组织带来沉重的经济压力。因此，以经济的损失作为衡量威胁严重程度的一个方面是合理的。

• 社会影响指标

该指标主要表征威胁危害组织和系统后，对社会造成的影响程度。这种影响是一种间接的影响。太空网络作为高技术条件下的信息资产，可以说是一个国家（或组织）科技水平、经济实力和国防能力的集中体现。如果这样一个系统面临外来威胁时，不能完成自身的使命，必将对社会造成影响，甚至可能引发动乱。因此，考虑威胁的社会影响也是评估威胁的重要指标之一。

• 网络影响指标

该指标主要表征威胁对系统的网络平台的影响程度。这是从系统的角度考虑的。空间信息网络是太空网络的主要平台和重要支撑。如果网络面临威胁，受损网络带来的影响主要有两方面：其一，受损节点本身将直接导致系统功能不能正常实现；其二，节点的受损数目体现了威胁危害整个系统的作用范围。因此，网络影响作为评价威胁影响的一个指标是合理的。

5.3.3 威胁评估准则

基于上述分析，下面列出威胁分析的相关指标的评估准则（如表 5-11～表 5-16）。其中，为了便于划分风险等级，拟将威胁影响的严重程度按照三分制评估。

表 5-11 威胁发生频率评估准则

频 发	肯 定 发 生	可能会发生	一般不会发生	不可能发生
大于或等于 1	80%～100%	5%～79%	4%以下	0～0.1%
4	3	2	1	0

表 5-12 攻击的动机指标评估准则

动 机 等 级	评 估 准 则
2	敌意或恶意攻击行为
1	故意的恶作剧行为
0	无意