战场环境下装备保障信息系统安全风险与防护

李宇明，耿斌
（总装备部军械技术研究所，石家庄 050000）

摘要：目的 研究战场环境下装备保障信息系统的安全问题。**方法** 从装备保障及装备保障信息系统的概念、分类和复杂战场环境下装备保障信息系统所面临的安全威胁入手，依照五分法把装备保障信息系统安全风险划分为5个等级，推导出风险评估模型，提出实施装备保障信息系统安全防护的技战术策略。**结果** 战场环境下，为确保整个作战进程中装备保障活动安全、有效、稳定地进行，装备保障信息系统防护必须遵循统一协调、综合利用的积极防护原则，采用有效的风险控制措施加以应对。**结论** 通过积极探索和发展装备保障信息安全与防护理论，找准战场环境信息防护中存在的薄弱环节，制定了装备保障信息安全防护策略，加强装备保障信息系统的安全管理工作，最终提高我军装备保障信息系统的防护能力。

关键词： 战场环境；装备保障；信息系统；安全防护
DOI： 10.7643/issn.1672−9242.2015.02.019
中图分类号： TJ06；TP311.52　　**文献标识码：** A
文章编号： 1672－9242(2015)02－0091－04

Security Risk and Protection of Equipment Support Information System in Battlefield

LI Yu−ming, *GENG Bin*
(Ordnance Technique University, Shijiazhuang 050000, China)

ABSTRACT: Objective To study the security risk and protection of equipment support information system in the battlefield. **Methods** Beginning from the concept and classification of equipment support information system and the security risks of the equipment support information system in the complex battlefield environment, the security scale of the equipment support information system could be divided into five grades by five−classification−method. The security risk evaluation model was deduced and the protection strategy for the equipment support information system was proposed. **Results** To ensure the safety, effectiveness and stability of equipment support during the whole battle process in battlefield environment, the equipment support information system should follow the positive protection principle of harmonization and comprehensive utilization, and effective risk control measures should be used. **Conclusion** By studying and developing the theory of equipment support information security and protection, the weakness of the information system in battlefield must be found, the protection strategy for the equipment support information system

收稿日期： 2014−08−21；**修订日期：** 2014−12−15
Received: 2014−08−21; **Revised:** 2014−12−15
作者简介： 李宇明(1976—)，男，河北人，博士，工程师，主要研究方向为装备保障理论与外军装备保障信息。
Biography: LI Yu−ming (1976—), Male, from Hebei, Ph.D., Engineer, Research focus: equipment support theory and foreign equipment support information.

should be established, and finally the protection capability of the equipment support information system would be improved.

KEY WORDS: battlefield environment; equipment support; information system; security protection

战场环境下,确保装备保障信息系统安全是装备保障安全工作的中心环节,将直接影响到装备保障任务的完成和作战进程的顺利发展。定性和定量分析战场环境下装备保障信息安全风险程度,开展装备保障信息系统安全风险评估,制定并采取适当的风险防护措施,确保整个装备保障信息系统安全,是当前我军实施装备保障信息系统安全建设的一项重要任务。

1 装备保障信息系统

装备保障是指从事装备工作的人员和组织,运用保障装备、设施和相关资源,通过物资保障和技术保障,保持或恢复装备良好状况,以确保军队作战和建设等军事需要的各项活动的统称[1]。装备保障的主要业务包括组织指挥、物资供应、维修保障等。其组成要素包括保障组织、保障装备、保障力量、保障手段、保障资源、保障活动等。装备保障信息是建立在对信息的广义理解之上,范围涉及到整个装备保障体系的各个环节和各项保障活动,涵盖了装备从生产到报废的整个寿命周期,贯穿于装备"管、修、供、训、战备"的各项业务管理过程中[2]。

装备保障信息系统为军队装备保障机构内部的作业、管理、分析和决策智能提供支持,它以装备为受控对象,以系统论和控制论为指导,由一定的组织、人员、设备和软件组成,按照规定的程序和要求,从事装备技术保障信息服务,以支持和控制装备保障活动有效的运行[3]。从层次结构区分,装备保障信息系统可分为总部、战区、军团、兵团、部队和分队等装备保障信息系统。总部级装备保障信息系统是由总部装备机关使用的自动化业务工作平台组成的计算机局域网络;战区级是由战区内装备保障机关使用的自动化业务工作平台组成的计算机局域网络;野战级是由支撑野战级装备保障信息化系统各类软件运行的硬件环境。它们的业务支撑软件包括各级的战场态势监视系统、装备保障资源可视化管理系统、远程技术支援系统、装备保障综合数据库系统等。

2 战场环境对装备保障信息系统安全威胁

战场环境下,装备保障信息系统所面临的安全威胁一般可以分为人为威胁、自然威胁与环境威胁等3类。为了削弱我军装备保障能力,敌方必将使用多种信息攻击手段,对我军的装备保障信息系统实施立体式综合打击。依据当前信息化战争的作战规模和态势,我们将装备保障信息系统安全威胁划分为电子攻击威胁、网络攻击威胁和实体攻击威胁等3类。

2.1 电子攻击威胁

电子对抗实力是夺取战场优势的重要条件,是决定作战胜负的基础因素。电子作战部队拥有遥感遥测卫星、地面电子侦察站、空中电子侦察飞机、海上电子侦察舰船、预警雷达、预警机、电子干扰机、技侦部队及各种监测系统组成的全方位立体通信侦察预警体系。电子攻击成为未来影响我军装备保障信息系统安全的重要威胁。

2.2 网络攻击威胁

战时,敌军一方面会利用各种网络命令和专用的软硬件工具,收集和判断我方装备保障信息网络系统的结构、软硬件配置等,或直接从我方网络系统中获取情报信息的侦察手段[4]。另一方面会以"黑客"入侵和病毒"植入"等方式,对我装备保障信息系统实施网络攻击,通过远程登录系统,窃取我军装备保障机密信息,扰乱我正常的装备保障工作和信息流通秩序,破坏我军装备保障信息的完整性,甚至损毁我装备保障计算机网络系统中的硬件设施。

2.3 实体攻击威胁

实体攻击威胁指装备保障信息系统的实物资源受到物理攻击所遭受的威胁。在强大的侦察监视系统与电子干扰系统的支援下,敌方会利用地面火力攻击、空中火力打击、海上火力截击和特种部队突袭等方式,对我军装备保障信息系统实体、设施实施猛烈的物理攻击。

3 装备保障信息安全风险等级划分

目前,战场环境下装备保障信息系统安全风险等级的划分还没有统一的标准,根据GB/Z 24364—2009《信息安全技术信息安全风险管理指南》中规定的风险等级,依照五分法[5]把装备保障信息系统安全风险

划分为5个等级,将风险值设定在[0,1]之间。各风险等级对应的风险值为:Ⅰ级风险0~0.2;Ⅱ级风险0.2~0.4;Ⅲ级风险0.4~0.6;Ⅳ级风险0.6~0.8;Ⅴ级风险0.8~1.0。

其中,Ⅰ级风险属于低风险等级,它的发生基本上不会影响装备保障任务的完成,可以维持现有信息防护力量的部署不变。Ⅱ级风险属于较低风险等级,它的发生将对装备保障信息系统造成轻度影响,装备保障任务完成的可能性较大。此时需要密切关注该风险,认真制定防护预案,一旦风险增大,能够立即实施控制。Ⅲ级风险为一般风险等级,它会对装备保障信息系统造成一定影响,装备保障能力可能受到一定的削弱,会在一定程度上影响装备保障任务的完成。此时应当对该风险实施控制,确保风险不再增大,同时尽可能减小其对装备保障的影响。Ⅳ级风险属于较高风险,它的发生将对装备保障信息系统产生较大的影响,装备保障能力受到严重削弱,大大降低完成装备保障任务的可能性。此时应当在立足于自身信息防护力量的基础上,选择适当的风险控制措施,对该风险加以及时的控制。Ⅴ级风险为高风险等级,它会对装备保障产生非常严重的影响,甚至造成装备保障系统瘫痪,无法完成装备保障任务。此时应当集中信息防护力量,运用有效的控制措施立即对该风险实施控制,适当时候还可以请求上级及友邻部队派遣专业信息防护力量实施支援。

4 装备保障信息系统综合安全风险评估模型

现代战争是一个复杂、动态的作战过程,装备保障信息系统安全风险也会随战场阶段的变化而不断改变。另外,由于装备系统自身的复杂性和战场环境威胁的多元性,装备保障系统信息系统所面对的安全风险绝不是单一的。要在风险评估过程中体现这种动态性和复杂性,就应当分析每个作战阶段、每个子系统安全风险的具体情况。计算某一作战阶段上装备保障信息系统安全防护的综合风险,首先考虑每个子系统的风险对整个装备保障信息系统的综合影响;然后再对作战过程中每一个阶段的风险进行综合加权处理;最终得战时装备保障信息系统安全的综合风险值。

假设整个装备保障信息系统中包含m个子系统,每个子系统将面对n类风险,则装备保障信息系统中第j个子系统的安全风险B_j可以用式(1)表示:

$$B_j = \sum_{i=1}^{n} \psi_i C_i \quad (i=1,\cdots,n, j=1,\cdots,m) \tag{1}$$

式中:C_i为第i类风险的风险值;ψ_i为第i类风险的权重系数,表示一旦第i类风险发生,可能对该子系统造成影响的严重程度。

同理,第t个作战阶段的整个装备保障信息系统的安全风险评估值A_t表示为:

$$A_t = \sum_{j=1}^{m} \mu_j B_j \quad (j=1,\cdots,m) \tag{2}$$

式中:μ_j为第j个子系统在该阶段装备保障信息系统中的相对重要性。

如果把整个作战过程简单划分为准备、开始、僵持、结束等4个阶段,那么整个作战过程装备保障信息系统的综合安全风险评估值W表示为:

$$W = \sum_{t=1}^{4} \sigma_t A_t \quad (t=1,\cdots,4) \tag{3}$$

式中:σ_t为第t个作战阶段上装备保障信息系统所担负的保障任务的相对重要性。

式中(1),(2),(3),分别代表不同条件下的权重系数ψ_i,μ_j,σ_t和第类风险的风险值C_i。可以通过比较其在装备保障信息系统中所担负的主要任务、面临的风险比重和重要程度,采取专家打分和层次分析的方法来得到。

5 战场环境下装备保障信息系统安全风险防护

装备保障信息系统安全风险防护是针对信息系统安全风险,装备保障指挥员通过采取适当的防护措施,对信息系统安全风险进行有效控制的过程。战场环境下,装备保障会面对各类风险,因此,装备保障信息系统防护必须遵循统一协调、综合利用的积极防护原则,采用有效的风险控制措施加以应对。具体来讲,战时装备保障信息系统安全风险防护所要采取的措施应该从技术和战术两个层面进行考虑。

5.1 信息系统安全防护技术

信息系统安全防护技术是防止秘密信息或关键信息在产生、传输、存储、利用过程中被泄漏或破坏,确保军事信息的可用性、安全性、完整性、可控性和可靠性的一项技术[6]。依据装备保障信息系统所面临的主要威胁,主要包括电子防护技术和网络防护技术。

在电子对抗斗争中,装备保障所采取的电子防护技术主要包括反通信侦察技术、反电子干扰技术。由于装备保障在作战中必将面临巨大的电子干扰威胁,为了减少敌方实施的电子干扰对我装备保

障的影响，必须采取有效的反电子干扰技术，确保装备保障中各类通信电子设备的正常工作。依据装备保障特点，可采取的反电子干扰技术包括跳频技术、直接序列扩频技术、猝发通信技术、自适应技术、定向天线技术、通信组网技术以及采用抗干扰能力强的通信手段等技术。

另外，随着计算机技术的快速发展与广泛应用，计算机网络已经成为各级军事信息系统的神经中枢，战时装备保障中也大量应用了计算机网络以提高装备保障效能。由于计算机网络技术中存在的各种安全漏洞，使得装备保障面临严重的网络威胁。针对这些威胁与风险需要采取相应的信息安全防护技术来保障系统计算机网络的安全，其中包括防火墙技术、电磁屏蔽技术、数据加密技术、防计算机病毒技术、入侵检测技术以及备份技术、信息过滤技术和审计追踪技术等。

5.2 信息系统安全防护战术

依据战时装备保障信息系统安全防护特点，可以制定出以下四条具体的信息系统安全防护战术。

1）隐真示假，防敌侦察监视。侦察与监视是敌军获取我装备保障情报信息的重要方式，也是敌军对我装备保障实施信息攻击的主要手段，它既包括了空间电子通信侦察、卫星侦察，又包括了空中侦察与地面侦察。面对无处不在的“电子眼”、“千里耳”，我装备保障信息防护力量应立足自身防护能力，坚持从实际出发，采用多种多样的方式与手段，隐真示假，削弱敌军侦察监视效果。主要方式包括：利用地形、夜暗和不良天候等自然条件进行伪装；充分运用伪装网、迷彩衣、人工障碍，以及制式涂料等实施伪装，降低目标的显著性或改变目标外形；运用科学手段，设置与装备保障相关设施、装备具有相似热辐射特征的假目标实施欺骗伪装；认真研究敌侦察监视规律，灵活确定装备保障活动时间。

2）战技结合，防敌通信干扰。电子战是当前信息作战的基本作战样式，也是作战过程中中敌军将贯穿始终的主要信息攻击方式。装备指挥与通信是装备保障行动实施有效控制的重要保障，也是敌军电子干扰的重要对象。为了防敌通信干扰与破坏，我装备保障信息防护力量必须采取战技结合的方式。一方面，从技术上采取扩频技术、捷变频技术、数字稳频技术、合资适应频谱处理技术等技术手段，从电子装备的结构、原理等方面提高抗干扰能力；另一方面，从战术上采取电子信号静默、电子信号佯动、电子信号欺骗等手段，欺骗迷惑敌人。

3）借力防护，防敌火力打击。作战中，敌军各种火力对装备保障信息防护实体的生存构成了巨大威胁。由于装备保障信息防护力量对敌军火力打击的防卫能力极为有限，因此必须借助联合作战部队的防卫作战力量才能够有效地压制住敌军对我装备保障的火力优势。基本做法为：各保障群（队）始终贴近作战部队，借助作战部队建构的“盾牌”来隐蔽和掩护自己，抵御敌军的各种火力攻击，提高生存能力。

4）加强网络安全管理，防敌网络攻击。网络攻击的发生主要与网络安全管理制度的落实、网络安全意识的强弱以及软硬件设施的安全性能等因素有关。只有在提高网络设施等硬件设施安全性能的同时，加强网络安全意识，强化安全责任制度，落实各项管理制度，才能够真正保证我装备保障网络的畅通与安全。具体包括人员安全管理、网络设施安全管理、信息安全管理和网络运行安全管理。

6 结语

目前，我军装备保障信息化建设已经步入了新的历史发展时期，装备保障信息化水平有了明显的提高。为了达到习主席提出的“能打仗，打胜仗”的目标要求，确保整个作战进程中装备保障活动安全、有效、稳定地进行，就必须积极探索和发展装备保障信息安全与防护理论，立足战场环境，找准信息防护中存在的薄弱环节，科学地制定装备保障信息安全防护措施和方案，有针对性地加强装备保障信息系统的安全管理工作，最终提高我军装备保障信息系统的防护能力。

参考文献：

[1] 俞康伦. 装备保障系统运行理论研究[D]. 石家庄：军械工程学院，2002.
YU Kang-lun. Research on Equipment Support System Running Theory[D]. Shijiazhuang: Ordnance Engineering University, 2002.

[2] 张玉锋. 装备保障信息集成中间件关键技术的研究与实现[D]. 长沙：国防科学技术大学，2007
ZHANG Yu-feng. Research and Achievement on Intermediate Key Technique of Equipment Support Information[D]. Changsha: Defence Science and Technique College, 2007.

[3] 张海川，王盼卿，陈家文. 基于SOA的装备保障领域信息系统集成研究[J]. 微计算机信息，2006，22(6)：158—160.
ZHANG Hai-chuan, WANG Pan-qing, CHEN Jia-wen. Re

（下转第124页）

等，来改善舰艇的适居性，提高艇员海上生活的舒适性，进而提高舰艇的战斗力。

参考文献：

[1] 张晓静，连之伟，兰丽. 改善潜艇舱室热舒适和空气品质的技术探讨[J]. 中国舰船研究，2012，7(4)：11—17.
ZHANG Xiao-jing，LIAN Zhi-wei，LAN Li. Improving Measures of Thermal Comfort and Air Quality in Submarine Cabin [J]. Chinese Journal of Ship Research，2012，7(4)：11—17.

[2] 王世忠，周爱民，施红旗，等. 船舶舱室内热舒适性参数的选取[J]. 舰船科学技术，2012，34(10)：118—122.
WANG Shi-zhong，ZHOU Ai-min，SHI Hong-qi，et al. The Determination of Thermal Comfort Parameters in Ship Chambers[J]. Ship Science and Technology，2013，34(10)：118—122.

[3] 胡晓芳，梁斌，汤皓泉. 舰艇生活舱室色彩设计方法初探[J]. 中国舰船研究，2012，7(1)：52—56.
HU Xiao-fang，LIANG Bin，TANG Hao-quan. Method of Chromatic Design in Living Quarters of Ship[J]. Chinese Journal of Ship Research，2012，7(1)：52—56.

[4] 赵欣，李震，王为宗. 潜艇舱室密闭环境中微生物在线监测技术研究[J]. 装备环境工程，2007，4(4)：71—74.
ZHAO Xin，LI Zhen，WANG Wei-zong. Research on On-line Supervision Technique of Microbe in Obstructing Environment of Submarine Cabin[J]. Equipment Environment Engineering，2007，4(4)：71—74.

[5] 李经. 常规潜艇舱室大气环境控制技术与研究[J]. 舰船电子工程，2009，1：42—45.
LI Jing. Study on the Cabin Atmosphere Control Technology of Submarines[J]. Ship Electronic Engineering，2009，1：42—45.

[6] 彭光明. AIP潜艇舱室大气环境控制系统研究[J]. 中国舰船研究，2006，1(2)：62—65.
PENG Guang-ming. A Study on the Cabin Atmosphere Control System of AIP Submarines[J]. Chinese Journal of Ship Research，2006，1(2)：62—65.

[7] 谢志辉，叶齐政，陈林根，等. 净化潜艇舱室空气的新技术探讨[J]. 舰船科学技术，2005，27(3)：16—19.
XIE Zhi-hui，YE Qi-zheng，CHEN Lin-gen，et al. Discussion on New Technologies of Air Cleaning for Cabins in Submarine [J]. Chinese Journal of Ship Research，2005，27(3)：16—19.

[8] REGINA P，HILARY D，STEPHEN P，et al. The Perfect Boring Situation—Addressing the Experience of Monotony during Crewed Deep Space Missions Through Habitability Design[J]. Acta Astronautica，2014，94(1)：262—276.

[9] COBLENTZA，FOSSIER E，IGNAZIG，et al. Habitability Design of European Spacecraft Hermes-Ergonomic Aspects[J]. Acta Astronautica，1988，17(2)：223—225.

[10] MCART C，BLASDEL H，HASSID S. Methods for the Development of Shipboard Habitability Design Criteria[J]. Applied Ergonomics，1975，6(3)：183.

[11] 张磊，王平. 军辅船环境工程管理工作体系建立的作用[J]. 装备环境工程，2008，5(6)：93—95.
ZHANG Lei，WANG Ping. Effect for Establishment of Working System of Environment Engineering Management for Auxiliary Ship[J]. Equipment Environment Engineering，2008，5(6)：93—95.

[12] 于欧. 航海环境下军人不良心理反应的影响因素及干预措施分析[J]. 海军工程大学学报，2013，10(4)：64—67.
YU Ou. Analysis of Influencing Factors of and Interventions in Unhealthy Psychological Reacting of Servicemen in Marine Environment[J]. Journal of Naval University of Engineering，2013，10(4)：64—67.

[13] 周跃芬，高军，孙立军. 环境分析技术应用探讨[J]. 装备环境工程，2011，8(2)：89—92.
ZHOU Yue-fen，GAO Jun，SUN Li-jun. Discussion on the Application of Environmental Analysis Technology[J]. Equipment Environment Engineering，2011，8(2)：89—92.

[14] 方晶晶，何艳兰，许林军，等.舰艇舱室封闭环境中挥发性化合物分析[J].舰船科学技术，2013，35(6)：90—95.
FANG Jing-jing，HE Lan-yan，XU Lin-jun，et al. Analysis of Volatile Compounds in the Closed Ship Cabins[J]. Ship Science and Technology，2013，35(6)：90—95.

[15] 刘红敏，连之伟. 室内空气污染与改善[J]. 环境与健康杂志，2002，19(6)：468—469.
LIU Hong-min，LIAN Zhi-wei. Contamination and Improvement of Indoor Air[J]. Journal of Environment and Health，2002，19(6)：468—469.

(上接第94页)

search on Equipment Support Information System Integration Based on SOA[J]. Microcomputer Information，2006，22(6)：158—160.

[4] 中国人民解放军总参谋部通信部. 军事信息系统安全[M]. 北京：解放军出版社，2004.
General Staff Communication Department of PLA. Military Information System[M]. Beijing：PLA Publishing House，2004.

[5] 孔凡. 渡海登岛作战装备保障信息防护问题研究[D]. 石家庄：军械工程学院，2008.
KONG Fan. Research on Inofrmation Protective Problem of Equipment Support in Crossing Sea and Landing War[D]. Shijiazhuang：Ordnance Engineering University，2008.

[6] 韩林，李建华，孙克兴. 军事电子信息系统安全[M]. 北京：军事科学出版社，2002.
HAN Lin，LI Jian-hua，SUN Ke-xing. Military Electron Information System Security[M]. Beijing：Military Science Publishing House，2002.