船海战场网络信息安全发展策略的研究

鲍敬源
(海 Z 驻武汉地区第二 J 事代表室,湖北 武汉 430064)

摘　要:针对当前船海战场网络安全的发展路线、训练不系统、海上战场信息密码保护机制的不健全、信息防御作战人员的培训不足等,该文从开发计划、行动策略、设备技术、对抗演习、人才培训等角度提出加强船舰海战网络空间信息安全保护体系建设的对策,为提高海战网络空间安全保护能力,取得信息化战争胜利提供理论基础。基于海上空间智能水平的不断提高分析了关于目前中国船海作战信息空间存在的基本问题、网络空间防御策略的优化策略以及网络空间信息安全的解决方案。

关键词:船海战场;网络信息安全;加密信息防护;信息安全制度;优化安全策略
中图分类号:TP309　　**文献标识码**:A　　**文章编号**:1673-629X(2022)0053-04

Research on Development Strategy of Network Information Security in Naval Warfare Field

BAO Jing-yuan
(The 2nd Office J of Hai Z in Wuhan, Hubei 430064, China)

Abstract: In view of the current development route, unsystematic training, imperfect information password protection mechanism and insufficient training of information defense fighters, we put forward countermeasures to strengthen the construction of information security protection system in naval warfare cyberspace from the perspectives of development plan, action strategy, equipment technology, confrontation exercises and personnel training, which provides a theoretical basis for improving the security protection ability of naval warfare cyberspace and winning the information war. Based on the continuous improvement of the intelligence level of maritime space, we analyze the basic problems existing in the information space of naval warfare in China, the optimization strategy of cyberspace defense strategy, and the solutions of cyberspace information security.

Key words: naval warfare; network information security; encrypted information protection; information security system; optimization security strategy

0　引　言

21 世纪是互联网飞速发展的时代。互联网技术广泛应用于各个领域。随着网络的快速发展,网络信息安全的重要性也凸显出来[1]。全球网络空间安全正在遭受着巨大挑战,针对互联网及物联网的攻击、勒索软件、数据泄露屡屡发生,网络安全高危漏洞频现,关键信息基础设施遭受到了严重的网络安全威胁[2]。安全意识来源于工作场所的显性安全体验和主观安全体验[3]。中国作为一个网络信息技术应用超高速发展的国家,网络信息安全的规划以及制定的整体战略都会逐步地变成关系到一个国家的命运危在旦夕的事情。网络信息安全的应用逐渐应用于各个领域和各个方面。随着网络信息安全的发展,运输对信息安全数据的要求越来越高。对于数据的实施安全也与日俱增,为了保证船舰的信息安全,也为航运提供更加优质的数据,在网络信息安全发展的推进下,也产生了很多船舶信息安全保护的方案,现在的大部分方案可以有效地对船舶信息安全进行合理的保护,保证数字化时代的信息安全。计算机化、网络化网络设施等信息设备在船舶中得到越来越广泛的应用,大大提高了信息传输的效率和在海军作战指挥中的有效性。

船舰系统的管理以及内部军用设备也变得越来越智能。船舶内部信息管理水平、船舶安全信息已经基本上依赖互联网技术,而信息则承载了很多关于船舰信息的核心,一旦防护不当则会导致船舶信息系统、船的内部信息安全风险管理和监控系统处于一个相对危险的情况。此外,还容易出现用户信息泄露、军事涉密隐私泄露[4]等安全问题。船舶网络安全对于海上装

收稿日期:2021-08-04
作者简介:鲍敬源(1977-),男,硕士,工程师,研究方向为网络信息安全、信息安全。

备和船舶的网络管理也至关重要,能够有效保障与船舶合作企业的信息安全,国家海军船舶作战信息的机密,维护乘客信息安全,甚至是生命安全。鉴于上述与船舶网络安全相关的问题,国内学者对有关中国船舶作战的网络安全进行了严谨深刻的分析。

1 船海作战网络信息安全的主要问题

1.1 舰载网络装备的关键核心未取得独立自主权

舰载信息网络设备的关键核心过于依赖外国产品和技术,例如在攻防对抗中,APT 攻击[5],正面临中国关键信息泄露别国的安全风险。目前,船海装备采购的产品芯片、元件、网络存储设备、操作系统、协议和标准很大程度上依赖于进口技术,敏感信息更容易被国外获取。在中国作战项目的建设中,外企占据了很大一部分份额,并把握着很多的核心骨干。其中大部分都是国外的通信设备和网络技术主力。所以关键的网络设施设备的信息安全对中国船海作战的安全起到了至关重要的作用。

1.2 网络安全意识薄弱,缺乏信息安全保护系统化设计

中国对于信息安全的重视程度没有跟上时代的节奏,安全防护的体系缺乏一个整体的设计。随着发展,初步建立了信息安全保障机构,专门负责信息安全保护、检测、响应和评估,形成了信息安全组织、标准规范、技术科研设备建设体系。但是,关键问题还是信息安全防护体系顶层设计滞后,核心关键技术阻碍,加上关键硬件和软件缺乏动态保护能力,信息安全保护体系没有得到完善。这样会导致整体性能效率的降低以及安全信息可靠性的下降,防护能力不足会造成安全性较低,由此无法对重要的保密系统和很多机密的设备和装置进行有效的保障,无法保障它们不受到外界高强度的破坏。

1.3 网络平台存在安全漏洞,网络架构的安全防护信任度低

中国目前的计算机、服务器、网络设备、存储设备、外围设备在关键的基本平台中存在明显的安全问题,安全等级相对较低。部分原因是采用了网络平台外部关键硬件和软件中存在国外预设的威胁,另一个原因是使用传统架构,自身的架构存在一定的缺陷。这两种安全问题是无法通过现有的网络信息防护就可以解决的。这就是为什么即使网络信息平台已采取安全防护措施,但防护效果仍不充分的原因。因为关键的基础平台是关于网络军事信息系统,这些军事设备是对于民用等其他重要保障设备的安全保障,如果国家最为保密的设备都存在一定的网络信息泄露的安全隐患,那么人们在日常生活中的信息更加轻而易举的获得。但是最为重要的还是其在安全方面全面保护中的隐患和漏洞直接影响军事部门设备和其他安全防护设备的安全操作正常发挥保护作用。

2 船海作战网络安全防护发展的关键方向

2.1 优化网络空间安全,完善信息安全防护力量

网络空间安全的主要特征是信息主导和网络化方位特点、智能竞争、技术对抗等方面。对于船海战场信息获取、传输、处理、存储和应用对于信息化时代都要跟随网络的发展[6]。随着各个国家信息安全的威胁,迫切需要构建一个完善的船海战场信息安全防护体系才能保证海军作战的效能。目前,海战网络空间安全也存在着发展主线路线不明确、训练演习不系统,且对于如船舰保密信息、情报信息、密码信息等野外保护机制不健全,信息防御作战人员培训不系统,海战领域存在信息安全保护不足等问题。因此,需要对于船海战场的安全保护制定发展战略、行动战略、装备技术、对抗实训、人才培养等方面的系统化的体系。在能够保护自身网络空间安全的根本上,逐渐拉近和别国的距离,逐步使中国在保护网络信息安全领域上,能够在全球具有一席之地。

2.2 提升船海战场信息防护能力,开发虚拟对抗环境

首先,要对船海战场的网络空间的具体行为进行仿真和发展。搜集一些信息可以对别国的作战方略和技术手段有一定研究。训练海战场的网络空间信息保护队伍,它应该是合理和准确的确定信息运营的要求、科学规划和统一标准,以达到网络覆盖范围与实战密切相关,并最大化虚拟范围。最终,它将成为海上战场网络空间信息对策实践环境,促进新战术和防护技术成果的形成[7]。另一方面,对于安全平台也需要加强防护,例如计算机、服务器、网络设备等外围设备可能面临着很大的信息安全问题。最重要的一点就是本身的网络安全架构就存在这一些根本上的问题。要时刻防护关键硬件、软件被他人入侵和破坏。这给中国海上战略系统的安全性能带来重大的隐患。要提高密码保障能力、监测预警能力、入侵防御保护以及应急响应和信任保障。对关键的网络信息安全技术以及核心设备的研制任务进行合理的规划。

2.3 对船海网络信息安全防护人才加大培养力度

首先整合教育资源,加强人员培训。海战场网络空间信息安全人员队伍建设有待加强实现专业人才的培养状态并有效整合他们分散在各级指挥机关,高等学校,科研院所(机构)和作战部门团队的信息安全防护人员,通过新的战术培训,新的装备培训,新技术轮换培训等有效发挥人才培养规律的方法示范[8],建立了军队与大学之间的联合教学与培训机制人才培养环

境从校园扩展到军队和科研单位组合训练模式。坚持“战斗训练一致”的原则,坚持实战贴近实际设备,加强培训体系的开发,建立真实的正常运行安装完善的培训环境,注重信息安全保护的完整性链接能力。二是依靠科研机构提高人才培养效率。通过确保海上战场网络空间的信息安全和信息安全保护人员必须具有特殊的政治素养,扎实的理论基础以及系统的专业知识,熟练的指挥能力,强大的创新能力满足多元化岗位的需求[9]。并且,要开发新型的教学模式和教学内容,对信息化人才的培养也要设计更加周密的计划安排,对于一些极为具有天赋的人才有针对的进行培训。只有不断地优化和创新教学体系,进一步优化教学方式和培养特色,才能更好地得到对于信息安全防护人才带来的反馈[10]。

3　船舰网络信息安全可信化

3.1　信息系统安全体系建设

根据国家军事可信计算平台的要求,给出了通用计算机平台信任的计算实施框架和安全级别保护要求。提出关于船舰信息安全部署的重要体系,从而把握对整个安全系统的数据进行保护和加密,增强对绝密信息的保护。舰载战斗系统逐渐满足高安全等级的要求并提供技术支持。

信息系统安全性的体系结构如图 1 所示,这种结构是涉及到三个维度的结构,即结构层次、系统单元、安全特性。其中结构层次表示从上至下将信息化分的方式;系统单元主要是指信息系统所涉及到外界环境单元;安全特性则表示了对于网络信息系统的安全要求等级。

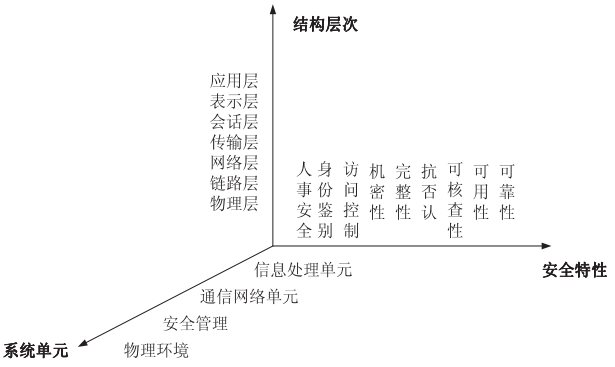

图 1　信息系统安全性的体系结构

此体系结构的完整性相对较高,应用该体系能够在理论角度上解决网络信息安全的一些相关问题。在舰载信息安全保护的过程中,受信任的计算基础提供密码服务和密钥保护,并实现从基本硬件平台到基本软件平台的完全信任链结构,这样可保护和提升信息平台身份验证和平台数据安全性,从而为舰载信息提供基础结构的安全级别要求。这种情况客观有效地加强了船海网络空间的信息安全保护水平,确保海上作战有效使用武力和提升保密性,更加有安全保障。

3.2　船海战术网络信息安全风险解决方案

上述的结构框架只是在理论角度论证的信息安全的相关风险,没有实践的验证。在此部分重点分析一下对于战术网络信息安全风险的解决方案[11]。网络信息安全风险解决方案如图 2 所示。

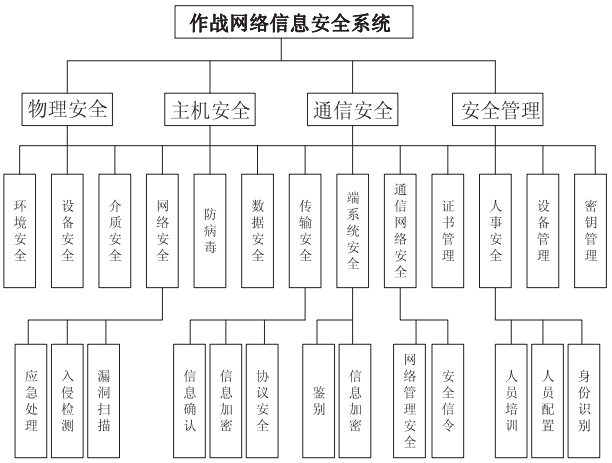

图 2　网络信息安全风险解决方案

4　优化船海战场信息安全防护顶层设计

4.1　制定发展网络空间安全,海战信息安全保护系统

信息化已经逐步的涉及到各个方面,网络空间对于未来竞争方式的一个重要发展空间。各个国家正在加大网络空间战斗力的建设,这是他们在这场信息化比赛中掌握主力的第一机会。国家安全理事会的建立和国家网络空间安全战略的制定都是确保国家安全的重要措施,必须加快组成制定网络空间安全运营策略的团队,并给予他们相应的分工和任务,加快网络空间信息安全发展的推进。船海战场的网络空间是我军网络空间防御的重要组成部分,海洋所拥有的自主权的把握关系到一个国家在军事领域的核心地位[12]。涉及边岸、水上,水下,海空等领域,这一部分面积异常巨大,因此对于他们的信息安全防护也是提升综合国力的一个重要部分。

4.2　优化网络空间安全组织结构,加强海战场信息安全保护

海战领域信息安全防护建设必须从组织系统的顶部设计并优化海军战场信息安全保护系统组织[13]。从信息命令、命令流程和方法进行改善,确保信息命令可以快速重建、可以对战场信息共享进行控制,并确保武器装备充分有效,应将海战领域的信息充分调查,建设对于攻击、防御、控制相互结合的安全保护部队,进行海军战场信息防御。有效保护海军信息系统和信息技术的作战行动设备安全[14-15]。

4.3 颁布有关网络空间安全和标准化海战法规

首先,将加快海洋战场信息安全保护规章制度的形成和改善,有权制定正确的作战和系统军事信息安全法规,一些不确定性问题尽可能规范[16]。需要加紧对于海洋信息安全保护法规的制定和安排,开发对于涉密信息和军事化信息保密的一个标准规范,逐步实现对船海作战设备的安全性能评估标准的规范化。建立军事情报的安全监督、执行、奖惩制度,保护军事情报安全依法管理系统,完善信息安全保护规则标准化级别。

5 结束语

船海战场作为一种重要的作战环境,随着网络空间的普及其工作战争平台和各式武器装备的信息化正在增加。船海战场的网络化安全形势也逐渐被我们所重视。对于这种情况客观上要求我们有效地加强船海网络空间的信息安全保护水平,确保海上作战有效使用武力和提升保密性。创立战略规划并进行调整极为关键。同时应该与指挥机构合作,以增强作战能力储备,并加强战斗人员总体安全意识,以进一步完善海战领域安全防护系统的军事的发展。战略信息的防护是每个国家都必须关注的问题,因此该文主要针对现代船海战场军事信息系统进行分析,介绍了传统战术与现阶段网络空间结合的结构、功能、作用以及主要的风险问题。通过分析提出了对于这一系列问题的改进方案,传统形势下网络军事化信息建设需要得到相应的改进,当今战略信息化的数据传输也成为了一个重要的信息节点。为了提高防护实力和机密信息的安全性和稳定性,传统的网络信息化安全的防护等级可能等级并不高。为了改善这一点,在以下内容中,出于转换的目的,结合以前的研究来了解一种信息系统安全体系结构,并主要分析战术性互联网信息安全风险解决方案。

参考文献:

[1] YU Guangxu, VARATHARAJAN R. Research on computer network information security based on improved machine learning[J]. Journal of Intelligent & Fuzzy Systems,2021,40(4):6889-6900.

[2] 网络空间:未来战争的首战场[J]. 军事文摘,2020(11):6-7.

[3] INHO H, ROBIN W, SANGHYUN K, et al. Security awareness:the first step in information security compliance behavior[J]. Journal of Computer Information Systems,2021,61(4):345-356.

[4] ZHU J, YAN L, GUO S. Research on ship network security based on game theory[C]//2019 2nd international conference on safety produce informatization (IICSPI). Chongqing, China:[s. n.],2019:78-81.

[5] RAFAL L, MICHAL R W. Threat intelligence platform for the energy sector[J]. Software:Practice and Experience,2019,49(8):1225-1254.

[6] 张楚渝,戴 菁,陈学海. 军事信息化的数据安全系统的研究[J]. 自动化与仪器仪表,2019(6):212-214.

[7] 王 崴,瞿 杨,李培林,等. 分布式虚拟装配训练通用平台研究[J]. 计算机测量与控制,2014,22(6):1944-1946.

[8] 姚燕青,刘建伟,李舟军. 网络空间安全基础理论课研究型教学方法初探[J]. 工业和信息化教育,2019(4):36-41.

[9] 郭 华,兰雨晴,高 莹,等. 密码学课程群教学方法探索与实践[J]. 工业和信息化教育,2019(4):52-55.

[10] 宗华丽,秦 娜,朱 宏. 海委信息安全中的等级保护与分级保护浅析[J]. 海河水利,2017(3):65-67.

[11] 付 钰,严 博,吴晓平. 海战场网络空间信息安全防护体系建设对策研究[J]. 海军工程大学学报:综合版,2019,16(3):23-26.

[12] 王昱镔. 工业控制系统信息安全防护工具研究[C]//中国计算机学会. 第 31 次全国计算机安全学术交流会论文集. 合肥:中国科技大学出版社,2016,515-518.

[13] 王晓儒. 计算机网络安全及防范—评《计算机网络及其信息安全管理研究》[J]. 中国科技论文,2021,16(2):255.

[14] 王 刚,李万阳,李富鹏. 计算机网络信息安全及其防护对策探讨[J]. 数码世界,2021(2):248-249.

[15] 汪 源. 计算机网络信息安全技术及其发展趋势[J]. 信息记录材料,2021,22(2):208-209.

[16] 李先鹏. 计算机网络安全问题与防范策略研究[J]. 电脑知识与技术,2021,17(3):69-70.