doi: 10.7690/bgzdh.2023.11.002

地空导弹武器系统网络安全探析

马帅帅，钱叶魁
（陆军炮兵防空兵学院郑州校区，郑州 450052）

摘要：针对地空导弹武器系统面临的网络空间威胁日益凸显的问题，对其进行分析。从近几年空袭案例来看，“网电攻击”比火力上的硬杀伤更容易突破地面防空体系，其作战隐蔽性更强；分析系统网络安全脆弱性和短板弱项。结果表明，该分析对于地面防空体系应对网络空间威胁及开展应对设计研究具有重要意义。

关键词：武器装备；脆弱性；网络安全
中图分类号：TJ762.1^{+}3　　**文献标志码：**A

Analysis on Network Security of Ground-to-air Missile Weapon System

Ma Shuaishuai, Qian Yekui
(*Zhengzhou Campus of Army Artillery Air Defense Academy*, *Zhengzhou* 450052, *China*)

Abstract: In view of the increasingly prominent problem of cyberspace threat faced by surface-to-air missile weapon system, this paper analyzes the problem. From the air attack cases in recent years, the "cyber attack" is easier to break through the ground air defense system than the hard killing of firepower, and its operational concealment is stronger; the vulnerability and weakness of the system network security are analyzed. The results show that the analysis is of great significance for the ground air defense system to deal with the threat of cyberspace and to carry out the design research.

Keywords: weapons and equipment; vulnerability; cyber security

0　引言

21 世纪以来，伴随着现代战场上网络通信大量使用，功能不断丰富，武器装备对其依赖的程度也在不断增强。当前，在陆军各兵种中，防空兵武器装备对网络空间的依赖程度最大，其各作战单元之间主要通过由计算机网络为基础延伸发展而构建的战场网络来传递空情和下达指挥控制指令，使得地空导弹武器系统能够快速、有效地拦截空中目标；因此，地空导弹武器系统的网络安全，将会成为影响其作战效能发挥的重要因素之一。

1　地空导弹武器系统通信网络概述

地空导弹武器系统主要由导弹、指挥控制系统、目标搜索指示系统、跟踪制导系统、导弹发射系统和支援保障系统等子系统组成[1-5]。各子系统由计算机终端、通信设备相互连接，组成一个具有数据和话音交互功能的综合通信网络，能够实现车载高速数传设备与话音终端、指控终端等末端设备的接入，保证各子系统之间的数据和话音通信[6]。同时，也能通过车载高速数传设备接受上级指挥所空情信息、作战指令以及远程预警雷达情报等信息。

从结构上来看，地空导弹武器系统的通信网络不是一个相对开放式的网络空间，内部网络与外部民用网络进行了物理隔离，传统手段无法接入系统内部网络；但随着技术发展，攻击者可利用无线通信接口、微波中继站、雷达天线等开放式传感器来侵入武器系统通信网络，非法访问武器系统内部计算机终端，采用网络攻击手段，彻底接管整个防空指挥网络。其拓扑结构如图 1 所示。

2　网络脆弱性分析

2.1　网络结构脆弱性分析

地空导弹武器系统的网络拓扑采取的是一种类似于星型的网络拓扑结构，武器系统的指控系统相当于中心节点，接受上级空情信息和作战指令，而后通过点对点链路连接的方式，将指控指令分别发送给（子节点）目标搜索指示系统和跟踪制导系统，当跟踪制导系统满足发射条件后，向指定的导弹发射系统发送发射指令，导弹发射系统接收指令，执行发射程序[2]。这种网络拓扑结构简单，便于集中控制，利于快节奏的作战指挥；无线组网通信过程中网络延迟总体较小，传输误差低，有助于武器系统数据的快速接收、灵活应对；网络结构拓展便捷，能够迅速完成火力单元的最大化组网配置；同时，

收稿日期：2023-07-02；**修回日期：**2023-08-05
第一作者：马帅帅（1991—），男，河南人，硕士。

网络结构的可靠性较高，当其中的一个子节点发生故障时，能够快速完成故障定位和诊断，不会影响与其他子节点间的网络通信，比较适合快速、高效的作战模式。

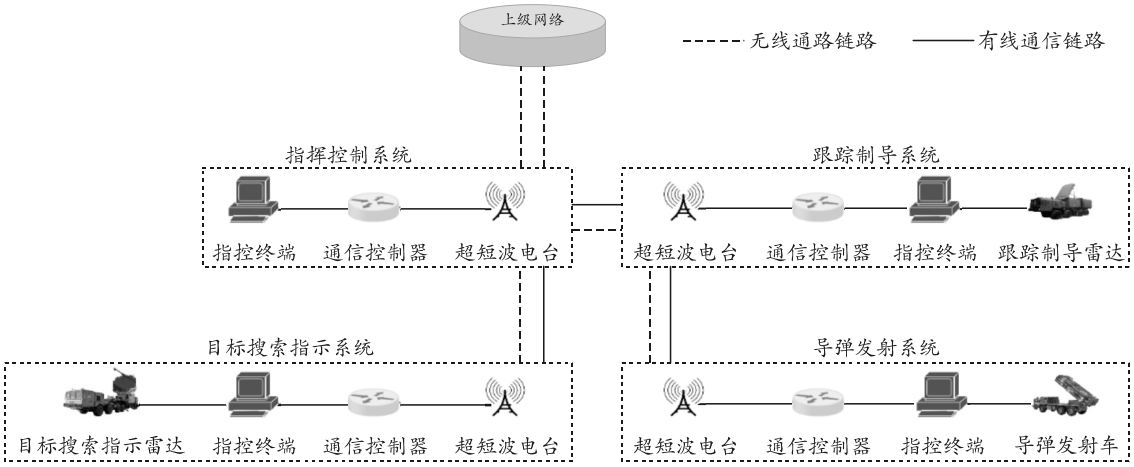

图 1　网络拓扑结构

从结构的安全性来看，其不足之处也较为突出。该拓扑结构中心化特征比较明显，指控系统作为中心节点，接受上级空情信息和指控指令，是武器系统连接外部网络的唯一关口。从网络渗透攻击的角度来看，如果通过缴获通信装备或者破译网络通信参数，就可能突破这层限制，轻而易举地进入武器系统内部网络，通过采取植入后门、更改数据参数等手段，操控和干扰武器系统指控终端正常工作，进而削弱武器系统作战效能。

2.2　终端系统脆弱性分析

目前，地空导弹武器系统多采用美国微软公司研发的 Windows 操作系统和嵌入式实时操作系统。

1) Windows 操作系统是一种通用的微内核系统，基于 C++语言、C 语言以及汇编语言编写，采用 TCP/IP 协议作为网络通信规则。从 1985 年发布的 Windows 1.0 到 2021 年发布的 Windows 11，微软公司一共发行了 11 种版本，是目前计算机采用的主流操作系统。武器系统的计算机终端也多采用此系统，由于受到军队武器装备保密性要求，加之武器装备的特殊性，武器系统计算机终端不能像民用计算机可以从互联网下载、安装微软官方发布的系统补丁，做到及时更新、升级，从而导致大量已经公开的系统漏洞长期存在于武器系统计算机终端中，存在严重的网络安全隐患。以 Windows XP 版本为例，目前仍有部分武器系统的计算机终端使用，通过查询国家信息安全漏洞共享平台(CNVD)、国家信息安全漏洞库(CNNVD)、赛门铁克漏洞库等权威操作系统漏洞公布平台，该版本操作系统存在大量已公开漏洞。在 CNNVD 中检索 2008 年以来已发布的漏洞有 283 条，分布情况如图 2 所示。其中危害性比较大，具有代表性，也最容易复现的漏洞为编号 CVE-2008-4250 的“代码注入”类型漏洞和编号 CVE-2017-0143 的“输入验证错误”类型漏洞，两者均是利用 Windows 系统服务漏洞来获取系统最高权限，从而可以完全控制目标计算机终端。

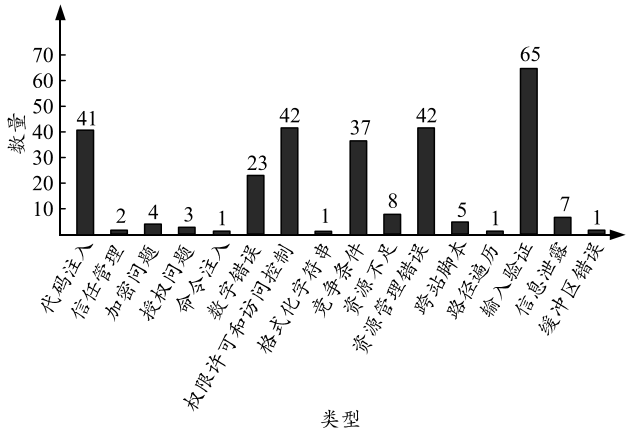

图 2　CNNVD 中 Windows XP 系统漏洞分布

2) 嵌入式实时操作系统是一种专用的操作系统，其系统精简，系统响应时间短，实时性高，能够支撑多任务，稳定性、可靠性和专用性较强。目前，嵌入式实时操作系统有 Vxworks、QNX、Palm OS、Windows CE、LynxOS 等。武器系统中应用较多的嵌入式操作系统为 Vxworks 操作系统，是由美国风河(wind river)公司设计开发，基于 wind 内核，自带 TCP/IP 协议栈，具有任务间切换时间短、中断延迟小、网络流量大的特点。它以良好的可靠性、较强的稳定性和卓越的实时性被广泛应用于航空、航天、军事等高精尖技术及实时性要求极高的领域中。由于早期版本在安全设计方面考虑较少，为发

挥系统的高效率、小体量、实时性优势做出了权衡让步等主观原因，导致操作系统本身在安全防护方面就存在一定漏洞[5]。加之后期在 VxWorks 配置使用中过度依赖较为安全稳定的环境，并且风河公司对早期的系统版本不再进行更新、升级等客观原因，造成当前系统漏洞问题较为突出。通过查询 CNNVD、威努特 IVD 工控漏洞库(ICS-Rader)等权威系统漏洞公布平台，已公布的 VxWorks 的漏洞包括权限许可与访问控制漏洞、数字错误漏洞、输入验证漏洞、缓冲区溢出漏洞以及多种拒绝服务漏洞等。在 ICS-Rader 中最新检索情况显示 VxWorks 系统已知漏洞有 28 条，与武器系统使用版本相关的有 25 条，分布情况如图 3 所示。其中最具有代表性的是编号为 CVE-2010-2965 的 WDB RPC 漏洞，这是一种“权限许可和访问控制”类型漏洞，攻击者可以通过向绑定 UDP17185 端口的目标代理调试接口(WDB RPC)发送请求来直接访问系统的内存，从而可随意读取或修改系统的存储单元，或者执行函数调用，危害巨大。

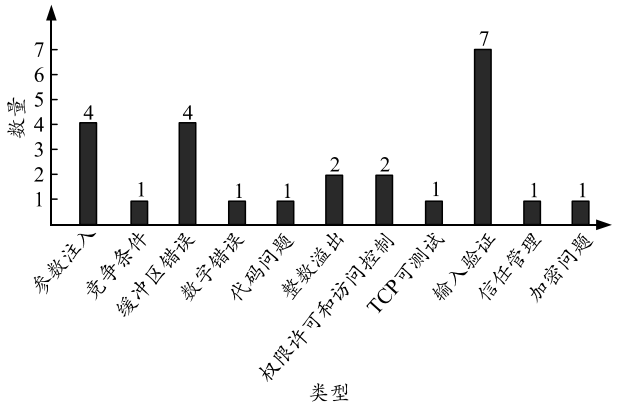

图 3　ICS-Rader 中 Vxworks 系统漏洞分布

3　可能面临威胁

3.1　信息侦测威胁

信息侦测是指使用相应的技术手段，通过对敌方武器系统通信网络电磁信号进行侦查、探测等方式，获取敌方通信参数的活动，主要分为 2 种方式：1) 通过截获、捕捉的方式获取武器系统通信过程中发送的电磁信号，采取相应的技术手段对侦搜到的各种电磁信号进行分析、识别、处理、破译，从而获取电磁频谱参数，侵入敌方武器系统通信网络。也可对上级通信节点电磁信号进行截获和破译，达到接入武器系统网络的目的。2) 在作战过程中，通过窃取敌方网络通信密钥或者缴获、控制通信设备(例如高速电台、通信节点设备等)方式接入武器系统通信网络。

这种信息侦测的手段在空袭作战中得到运用，且达成的作战效果也十分明显。1982 年，贝卡谷地空战中，以色列先是利用无人机来侦测叙利亚防空导弹武器系统的信号，通过技术手段分析、计算相应电磁信号参数，为后续的电磁干扰和反辐射导弹摧毁防空导弹雷达创造了有利的条件。2007 年的“果园行动”中，以色列通过“网电攻击系统”截获叙方防空导弹武器系统电磁信号，采用技术手段侵入叙利亚防空系统通信网络，致使防空系统瘫痪，无法发挥应有的作战效能。2017 年，以色列空袭叙利亚军用机场的一次作战中，通过搭载“舒特”网电攻击系统的 F-16 战机使用逆向分析技术，截获和破译了俄军和叙军防空武器系统电磁信号，侵入其防空系统指挥网络，造成防空系统无法正常工作。从以上作战可以看出，从之前对电磁信号的识别、溯源，实施电磁干扰、反辐射导弹攻击等方式，到现在变更为对电磁信号的截获、分析、破译，实施“以电入网”的网电攻击作战方式，其技术手段在不断革新。

目前，随着大数据、量子计算和人工智能等新兴技术的不断发展，对电磁信号的深度分析、处理、计算将会达到一种新的高度和水平。

3.2　信息窃取威胁

当完成信息侦测活动后，可以顺利与指挥控制系统进行链接，进入到系统内部窃取相关信息，可概括为 2 方面：

1) 网络扫描。

通过采取技术手段，对特定的目标网络进行试探性通信，以获取目标网络信息的活动。利用目前常用的 Nmap、Masscan 等扫描工具，可以实现探知武器系统的网络拓扑结构，内部网络中可以访问的 IP 地址(主机发现)，例如武器系统通信网络终端计算机 IP 地址，探查其操作系统类型、版本(操作系统识别)，检测操作系统开放的端口(端口扫描)以及系统存在的安全漏洞(漏洞扫描)，获取网络的路由表信息等功能[3]。通过以上分析扫描，可以准确地找出武器系统网络中各计算机终端存在的薄弱环节，确定目标主机的攻击点，可探测出进入目标系统的最佳途径。

2) 网络嗅探。

通过使用 Wireshark 等流量解析工具，运用流量分析技术，截获武器系统网络通信中终端主机间、

跨车之间发送的数据包，了解其通信控制流程。该方式不会干扰到整体通信的数据流，隐蔽性强，能够做到不被察觉。通过截获发送的数据包，攻击者可通过分析数据包的协议控制部分，获取武器系统内部间正在通信协议实体的地址和身份；通过研究数据包的数据长度和传输频度，了解该数据单元所指示的指控命令；通过分析其数据首部构成，逆向解析数据传送的源端口和目的端口信息，检测其针对数据包传输的安全设计，验证指控指令数据包的伪造以及重放等攻击的可能性[4]。

3.3　网络渗透威胁

基于网络窃取的结果，攻击者将设法进入系统内部，获取系统访问权。结合武器系统终端计算机存在的网络漏洞情况，往往利用缓冲区溢出进行攻击是最为有效的，最容易进入终端系统内部，获取系统权限。网络渗透攻击所获取的权限往往只是普通用户权限，要进行更深层次的渗透攻击，需要进一步提升系统权限，可以利用系统本地漏洞、解密口令文件、安全配置缺陷、猜测和窃听等手段获取系统的管理员或特权用户权限[3]，随后可以展开网络监听、上传恶意程序、木马病毒，下载系统数据进行分析以及清除痕迹等工作，为制造雷达虚假目标、修改作战指令等跨车攻击手段做铺垫。

值得强调的是，一般攻击者在获取系统最高权限，控制系统后，往往首先考虑的就是如何维持这个访问权限，方便下次直接进入系统。就当前技术手段来讲，往往利用木马程序、后门程序、rootkit 等恶意程序或在系统程序中写入恶意代码等方式来实现[3]，这种手段隐蔽，不易被发现，且威胁程度更高。

4　应对措施

4.1　修复存在漏洞

根据现阶段已发现的武器装备网络安全漏洞，应由相关部门牵头、科研院所提供技术支持、部队积极配合，分阶段、分类型及时修补系统软件、网络设备等方面存在的安全漏洞，避免高危漏洞长期存在。对于发现的软件系统漏洞，应由工业部门对现役装备进行更新修复；对于发现的网络设备中存在的安全漏洞，应采用模块更换的方法，及时更换硬件设备模块。对武器装备网络安全漏洞的修补应当慎重，每次修补完后都应进行严格的测试，确保不会带来新的网络安全风险以及对武器装备作战效能的影响。

此外，还应该加强对信息化装备漏洞及修复工作的系统管理，及时记录和统计相应信息，形成对应的武器装备漏洞数据库及修复记录数据库。

4.2　合理配置防火墙

首先，要加强安全策略。对网络通信进行访问控制，利用防火墙屏蔽指控终端计算机的一些不必要的数据端口，降低非法用户访问相应系统服务的风险，使得任何没有得到授权或许可的请求都会受到限制和拦截，在一定程度上可以阻挡病毒或木马的入侵。其次，完善安全规则环境。通过防火墙设定入站规则，创建武器系统指控软件和应用程序安全连接、通信的规则，为武器系统合法的网络通信的链接提供保护。最后，强化身份验证。更改武器系统内网数据交互过程中身份验证的方法，只允许武器系统内网中的指控终端计算机进行通信，降低攻击者采用跳板的方式非法访问武器系统内网的可能性。

4.3　完善异常检测

随着基于网络数据流量的大数据挖掘、分析技术以及计算机智能算法的不断发展，入侵检测技术(IDS)得到不断的完善和广泛应用，能够对网络通信中异常的数据包和流量进行标识和拦截，自动防范、分析、处理各种网络威胁。针对当前地空导弹武器系统面临的网络空间现实威胁，合理运用入侵检测技术，在武器系统通信网络入口和重要设备上部署可以有效地监测异常的网络数据包，过滤网络通信中异常、非专用的数据包，在维持武器系统通信信道畅通的同时，也可以有效地防止数据包劫持、伪造和木马程序的攻击。

可以说，利用入侵检测技术可以实时了解通信网络的安全状况，并能够及时调整安全策略和防护手段，同时改进实时响应和事后恢复的有效性，从而提高地空导弹武器系统网络安全的整体水平。

5　结束语

当前，战场网络环境已不再是一个封闭的空间，信息技术高度集成的武器装备时刻面临网络空间的威胁。加强地空导弹武器系统网络安全研究，积极开展网络安全试验评估活动，不断提升其网络空间下攻防对抗能力，为扎实履行新时代使命任务，建设完备的地面防空体系提供强有力的支撑。

参考文献：

[1] 韩晓明, 张琳, 肖军. 防空导弹概论[M]. 西安: 西北工业大学出版社, 2018: 3-5.

[2] 杨建军. 地空导弹武器系统概论[M]. 北京: 国防工业出版社, 2006: 3-7.

[3] 吴礼发, 洪征, 李华波. 网络攻防原理与技术[M]. 2 版. 北京: 机械工业出版社, 2019: 19-20.

[4] 谢希仁. 计算机网络 [M]. 7 版. 北京: 电子工业出版社, 2017: 324-326.

[5] 任秋洁, 韩英. 面向 VxWorks 系统的嵌入式安全研究[J]. 电脑知识与技术(学术版), 2020, 16(22): 26-27.

[6] 袁书杰, 张庆生, 伍飞. TBR171-2 型背负式超短波电台网络模式及设置[J]. 石家庄机械化步兵学院学报, 2016(5): 81-82.

****

（上接第 5 页）

4.3 评估分析

由计算结果可知，利用基于直觉梯形模糊多属性决策评估方法进行评估得到的 4 型传输装备在役综合能力评估结果排序为：$T_3 > T_1 > T_4 > T_2$，针对评估背景，建议选取传输装备 3 作为该固定通信台站扩容备选装备，装备 3 部队适用性及任务效能相比其他 3 型装备更加优秀，无明显较弱的在役考核指标，该型传输装备在役综合能力最好，易于维护，运行稳定，能够满足任务部队对当前通信保障业务的扩展需求。

5 结束语

笔者采取 5W1H 方法对在役考核概念模型进行设计和阐述，介绍在役考核相关概念内容，构建在役综合能力评估属性指标。分析利用直觉模糊 TOPSIS 理论与进行在役综合能力评估的可能性与合理性，构建了基于直觉模糊 TOPSIS 的在役综合能力评估模型；以固定台站通信保障装备为研究对象，以固定通信台站扩容改造中装备选型需求为在役考核任务背景，进行在役综合能力评估的仿真应用。通过对比评估结果确定装备扩容对象，证实了笔者所提方法的适用性及有效性，可为装备在役综合能力评估提供方法借鉴。

参考文献：

[1] 孟庆均, 曹玉坤, 张宏江. 装备在役考核的内涵与工作方法[J]. 装甲兵工程学院学报, 2017, 31(5): 18-22.

[2] 孟庆均, 郭齐胜, 曹玉坤, 等. 装备在役考核评估指标体系[J]. 装甲兵工程学院学报, 2018, 32(1): 18-24.

[3] 朱闽, 杨清文. 主战装备在役考核指标体系的构建及评价[J]. 指挥控制与仿真, 2020, 42(5): 61-65.

[4] 张宏江, 罗建华, 郭英, 等. 装备在役考核[M]. 北京: 国防工业出版社, 2020: 44-62.

[5] 李赫才, 韦国军. 基于深度置信网络的装甲装备在役考核评估研究[J]. 指挥控制与仿真, 2021, 43(6): 66-70.

[6] 周泽云, 王斌, 孙剑桥, 等. 基于 TOPSIS 法的装备综合水平评估研究[J]. 兵器装备工程学报, 2016(6): 102-106.

[7] 徐海波, 邹建华, 汪彩玲, 等. 一种装备体系作战试验综合能力评估方法[J]. 火力与指挥控制, 2018, 43(7): 157-159.

[8] 杨罗章, 胡生亮, 冯士民. 基于 Entropy-TOPSIS 方法的目标威胁动态评估与仿真[J]. 兵工自动化, 2020, 39(3): 53-56, 60.

[9] 甘佳霖. 基于模糊多属性决策的干扰效果评估[D]. 西安: 西安电子科技大学, 2021.

[10] 季晓晓. 武器装备作战试验概念模型及评估方法研究[D]. 长沙: 国防科技大学, 2018.

[11] 陈晓红, 李喜华. 基于直觉梯形模糊 TOPSIS 的多属性群决策方法[J]. 控制与决策, 2013, 28(9): 1377-1381, 1388.

[12] 朱学耕, 王作根, 麻勇, 等. 基于组合赋权和直觉模糊集的合成营作战能力评估[J]. 火力与指挥控制, 2021, 46(9): 62-67, 71.

[13] 谭跃进, 陈英武, 罗鹏程, 等. 系统工程原理[M]. 北京: 科学出版社, 2017: 208-212.

[14] 杨宇晨. 基于层次分析法和熵权的后方指挥所选址决策评价[J]. 兵工自动化, 2020, 39(10): 48-51, 61.

[15] LIN L, YUAN X H, XIA Z Q. Multicriteria fuzzy decision-making method based on mtuitionistic fuzzy sets[J]. European Journal of Operational Research, 2007, 179(1): 220-233.