第 43 卷 第 6A 期
2016 年 6 月

计 算 机 科 学
Computer Science

Vol. 43 No. 6A
June 2016

网络作战能力评估指标体系构建问题的研究

申普兵 赵占东 宫强兵
(西安通信学院 西安 710106)

摘 要 网络作战能力评估是一个多指标评估问题。以网络作战任务为牵引,基于“任务_行动_能力”的指标体系构建思路,从面向能力及要素的角度,分别从网络侦察、网络攻击、网络防御、网络保障、指挥控制 5 方面细化网络作战能力评估指标体系,为网络作战能力评估奠定了基础。

关键词 网络作战,指标体系,网络侦察,网络攻击,网络防御
中图法分类号 E211 文献标识码 A

Research on Evaluation of Computer Network Operation Based on Capacity Factor

SHEN Pu-bing ZHAO Zhan-dong GONG Qiang-bing
(Xi'an Communications Institute, Xi'an 710106, China)

Abstract Network operation capability assessment is a multi-index evaluation problem. The paper first analyzed the factors of network operation capabilities, and then built network operational network operational capability evaluation index system from computer network reconnaissance, attack, defense, support and command based on the principles of network operational indicators.

Keywords Computer network operation, Indicator system, Computer network reconnaissance, Computer network attack, Computer network defense

1 引言

网络作战指标体系建设是进行网络作战能力评估的基础和依据,现有的网络作战能力评估指标体系的研究多偏重于某个具体性能指标的分析或某一方面能力建设的改进,很少从整体的角度考虑。

文献[1]首先定义了网络对抗综合效能评估的概念,明确了网络对抗效能评估指标的构建原则及评估模型的选择,借鉴了传统装备效能评估指标构建方法,基于可用性、可信性、机动性、威力和保障力方面构建了网络作战评估指标体系。其主要是以武器装备的工作性能作为研究对象,忽略了作战人员及技术等因素,致使评估具有片面性。文献[2]首先分析了网络作战特点,依据网络作战特点总结了网络作战综合能力的主要因素,即网络侦察、网络攻击、网络防御 3 个子能力,每个子能力同时涵盖了兵力、装备、技术评估指标,指标间相互交叉,容易产生评估的歧义理解。文献[3]从网络攻击实施过程中的信息获取、权限提升、破坏攻击 3 方面出发,构建了网络攻击效能评估指标体系,但没有形成完整的网络作战评估指标体系

网络作战能力评估指标一直没有明确的定义和规范。因此,很有必要建立一套完整、科学、全面的网络作战能力评估指标体系,从而有利于准确、系统地对网络作战能力进行评估,有利于准确找到网络作战能力建设的薄弱环节,有利于网络作战能力建设的优化和发挥。

2 评估指标构建思路

网络作战是一种为了达到作战目的,在网络空间进行的作战活动,主要是为了扩大己方网络空间优势而对网络空间进行的作战,主体是网络空间作战力量,目的是夺取制网络权、保护己方网络空间安全以及控制、干扰或破坏敌实体目标的正常运行。从网络作战的概念描述分析,可以总结出网络作战总体任务主要有两点:1)保卫本国网络空间,使之按照己方的目的运行;2)采用各种手段,能够在需要时使对方的网络空间无法运行或不按照对方的目的运行。

网络作战能力即国家或军队在网络空间遂行作战任务的能力,以网络作战任务为牵引,基于“任务_行动_能力”的指标体系构建思路,深入分析网络作战能力评估指标。网络作战的基本行动主要是指网络侦察、网络攻击和网络防御,每一种作战活动都离不开作战指挥控制及网络作战保障,指挥控制是“倍增器”,网络作战保障是基础。因此,按照面向“能力”类方法,从网络作战样式及构成要素角度构建网络作战能力评估指标体系,可将其一级指标确定为网络侦察能力、网络攻击能力、网络防御能力、指挥控制能力以及网络作战保障能力。

3 网络作战能力评估指标构建

从网络作战能力构成出发,依据网络作战指标体系构建原则,运用指标分析法[4],选定 5 个指标作为能力评估的一级

本文受国家社科基金:我军网络作战基础问题研究(13GJ003-032)资助。
申普兵(1964—),男,教授,硕士生导师,主要研究方向为信息安全、网络对抗、军队指挥学;赵占东(1987—),男,硕士,主要研究方向为网络作战、效能评估,E-mail:aifhqai@tom.com(通信作者);宫强兵(1991—),男,硕士,主要研究方向为栅格化信息网络业务网系。

指标，并对其再进行层层分解，逐步形成合理、完备的综合评估指标体系。建立的指标体系如图 1 所示。

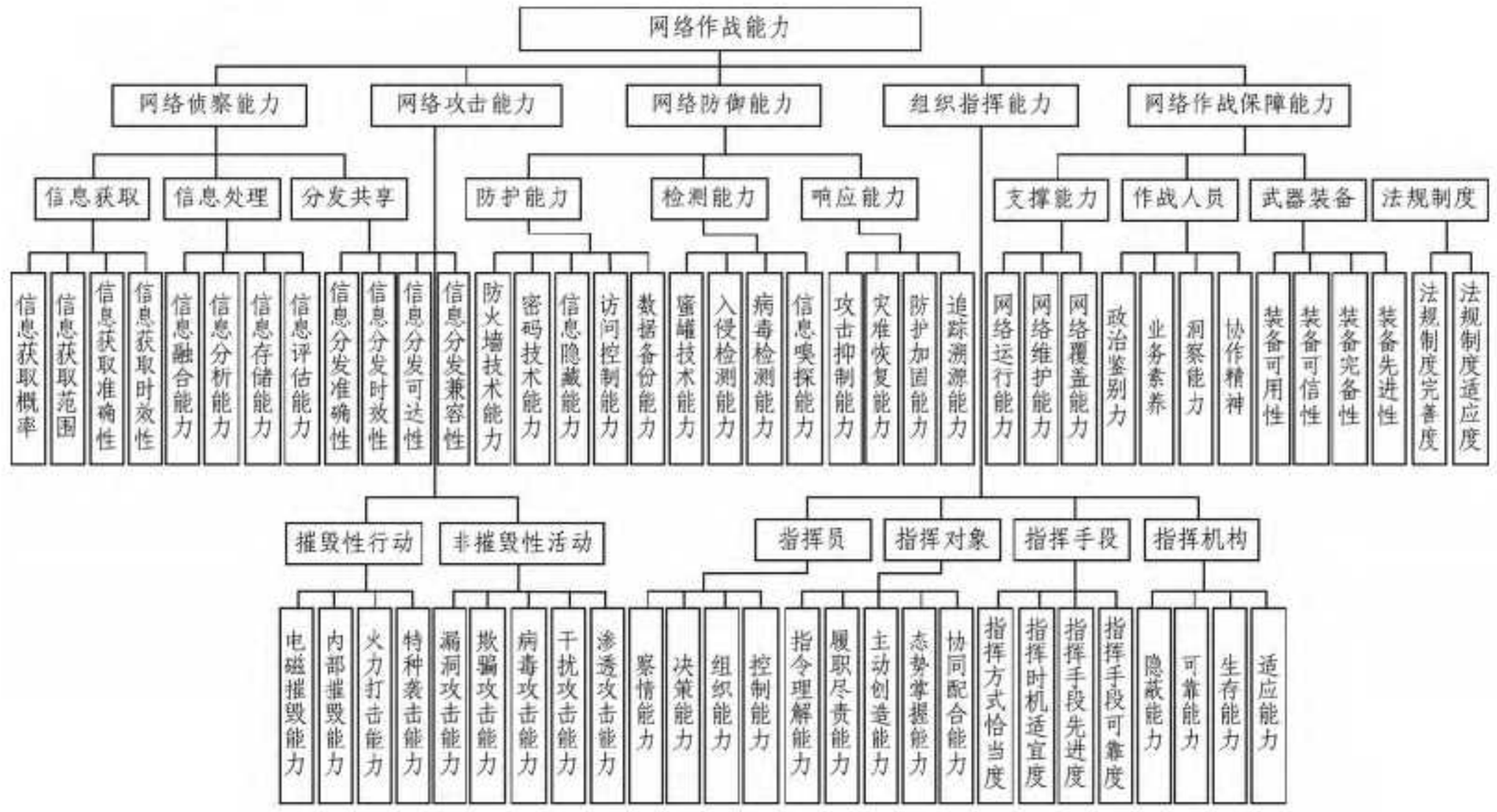

图 1　网络作战能力评估指标体系

3.1　网络侦察能力

网络侦察，是指利用网络专用软硬件工具及其他方法，从敌网络中获取信息情报的一系列活动的总称。它为网络攻击寻找敌网络系统的安全漏洞，并获取各种情报信息，为各级指挥员作战决策提供情报依据。基于网络侦察的任务以及信息流程角度，基于信息获取能力、信息处理能力及信息分发共享能力 3 个指标评判网络侦察能力。

信息获取能力是指利用各种网络侦察武器装备对敌网络空间的情报信息进行收集获取。按照面向效果的角度，可以采用获取概率、获取范围、准确性和时效性 4 个指标进行描述。获取概率，是指系统在一定范围内能够获取目标信息的概率。获取范围，是指系统能够获取信息的范围。准确性，是指系统获取到的信息与战场客观情况相符的程度。时效性，是指系统快速、及时获取信息的能力[5]。

信息处理能力是指将收集到的原始信息消除冗余，确立置信度，再将信息转化成便于分析、观察和传输的形式。从信息处理的一般过程分析，可以采用信息融合、信息分析、信息存储、信息评估 4 个指标进行描述。信息融合是指将侦察获取的情报信息进行分类综合后存放到相应的数据库中。信息分析是指分析情报信息所含内容，进一步判断情报的可靠度、重要程度、紧急程度和价值。信息存储是指将分析判断的结果进行筛选，将有价值的情报信息根据不同用户的需求，以相应格式进行存储。信息评估是指把敌方重要目标的情报信息进行综合处理，并结合网络战场的实际情况，对整个网络战场的威胁和敌方意图做出评估，进而得出相关结论[6]。

信息分发共享服务能力是指将战场信息正确地建立索引、存储和传输，并在最终的用户处正常展现的水平，从面向效果的角度，可以采用准确性、时效性、可达性、兼容性 4 个指标进行描述。准确性，是指信息在共享过程中不发生错误、保持原义的程度。时效性，是指共享信息的寿命周期，适用于任务周期的程度。可达性，是指信息共享的广度和深度。兼容性，是指信息在共享过程中，在不同平台、不同场合以及不同应用环境下能够保持可用的程度[7]。

3.2　网络攻击能力

网络攻击是指通过使用网络攻击武器装备、技术手段等方法破坏、压制和消除敌方网络空间中信息的行动，或针对敌方网络空间本身的行动[8]。网络进攻的主要目的是“破网”。从网络作战进攻的基本手段方面，可以采用摧毁性网络进攻能力与非摧毁性网络作战进攻能力两个指标评判网络作战进攻能力。

摧毁性行动攻击，是以“硬摧毁”为主要手段，对构成敌方各种网络基础设施的硬件以及网络运行的物理实体进行摧毁和破坏，使其丧失网络进攻的能力[9]。从实施摧毁性行动所使用的主要手段评估其能力，主要涉及电磁摧毁能力、内部摧毁能力、活力打击能力以及特种袭击能力 4 个指标。

非摧毁性行动，是指通过截取、篡改、控制、破坏敌方信息网络，使其丧失信息能力，进而夺取和保持网络控制优势的一种网络进攻[9]。从实施行动所采取的技术手段评估其能力。根据美国 Intelomics 等 3 个智库最近联合公布的《网络武器威胁矩阵报告》，目前世界上有 18 种常见的网络战攻击手段。通过对 18 种手段进行深入研究，可以概括出以下几类方法手段：漏洞攻击、欺骗攻击、病毒攻击、干扰性攻击、渗透性攻击。

3.3　网络防御能力

网络防御是指在网络作战中运用网络防御手段，抵御敌网络侦察和攻击，保护己方信息网络安全的一系列活动的总称。从网络防御任务角度及基本流程出发，以常用的技术手段评估网络防御能力，即防护能力、检测能力和响应能力。

防护能力是整个网络防御的基础，也是最为关键的一个环节，用作抵御各类攻击，通常指拒绝进攻方使用目标信息资源。以其手段及技术为主要指标，包括：防火墙技术能力、密码技术能力、信息隐藏能力、访问控制能力、数据备份能力等。

检测能力是指当己方网络受到入侵时，对入侵行为进行检测识别的能力，其主要技术手段包括：蜜罐技术能力、入侵检测能力、病毒检测能力、信息嗅探能力等。

响应能力是指攻击发生后对敌方攻击所采取的措施，其技术手段包括：攻击抑制能力、灾难恢复能力、防御加固能力、追踪溯源能力等。

3.4　组织指挥能力

网络作战组织是指作战人员及指挥机构获取分析处理信

息、制定行动方案并组织实施控制的周而复始的过程[10]。网络作战组织指挥能力包含了3个基本要素:指挥主体、指挥客体和指挥手段。指挥主体主要指指挥员及指挥机构;指挥客体是指网络作战战士。指挥主体通过一定的指挥手段来对指挥客体的作战活动进行组织指挥控制。从面向要素角度评估网络作战组织指挥能力,主要涉及指挥人员、指挥对象、指挥手段及指挥机构。

指挥人员指挥能力评估是指在指挥活动履行职责和发挥作用程度的评估。其能力素质主要包含察情能力、决策能力、组织能力和控制能力。

指挥对象操作能力、网络作战能力的发挥,最终是通过指挥对象的具体操作实现的,指挥对象既要服从指挥,又要适应网络空间环境的变化,协调一致,灵活对抗。其业务能力主要包含指令理解能力、履职尽责能力、主动创造能力、态势掌握能力和协同配合能力。

指挥机构战(技)术能力中指挥机构是实施指挥控制的基本条件。评估指挥机构主要从其隐蔽性、可靠性、适应性及生存能力4个方面考虑。

指挥方式与手段是主体与客体的一种媒介。网络作战指挥中,指挥方式是否恰当,以及指挥手段的功能和作用发挥的程度,都直接影响网络作战指挥控制效能的高低。在指挥方式方面,主要从指挥方式在网络作战过程中的转换条件和时机是否适宜,以及其发挥作用的程度、即方式适当度评估,时机适宜度;在指挥手段方面,主要从指挥手段在网络作战过程中的先进性及可靠程度评估。

3.5 网络作战保障能力

网络作战保障是指网络作战顺利开展的基础网络环境以及参与网络作战的作战力量,是实施网络作战的重要基础,形成网络作战能力的重要保证和条件。从其构成要素角度,基于基础网络支撑能力、作战人员能力素质、武器装备、法规制度4个方面对网络保障能力进行评估。

网络支撑能力是展开网络作战的基础,保证网络作战武器装备实现互联、互通、互操作的关键部分,是各种作战能力实现的物质基础。评估支撑能力主要从网络运行能力、网络维护能力、网络覆盖能力3个方面考虑。

网络作战人员是网络作战评估最为活跃的因素,也是网络作战保障能力重要的构成要素。网络作战人员主要涉及指挥人员与指挥对象,根据其担负的不同职责,要求具备相应的能力素质。有关能力的评估已经在网络作战指挥控制中进行了讨论,此处主要从网络作战特点角度出发对作战人员特定素质进行讨论,从敏锐的政治鉴别力、极高的业务素养、极强的问题洞察力、良好的协作精神和团队意识4个方面进行评估。

网络作战武器装备是网络作战的构成要素和物化形式,是网络作战赖以进行的物质基础以及网络作战能力的载体。参照美国工业界系统效能咨询委员会评价武器系统用的模型——ADC模型[11],主要根据武器装备的可用性、可信性和固有能力3大要素对武器装备进行评估。网络作战侦察、攻击、防御能力,是武器装备及其他网络作战力量共同作用的集中体现。因此,依据指标构建独立性原则,武器装备的固有能力这里不再讨论。将武器装备的可用性、可信性作为评估武器装备的两个指标,考虑到网络作战武器装备的复杂性和多样性,同时将武器装备的完备性及先进性作为另外两个评估指标。

法规制度是合法开展网络作战活动的依据,是执行网络作战的准绳,必须具备相对完善的法规制度。对法规制度的评估主要围绕法规制度的完善程度和法规制度对任务的适应程度两方面进行评估。

结束语 通过对网络作战能力评估指标体系的研究和确立,为有效地评估网络作战能力提供了参考和依据。确立指标体系化,下一步的工作就是对各项指标数据的获取及评估模型的选择,由于篇幅所限,这些问题不再论述。

参 考 文 献

[1] 徐志明,卢昱,邹利鹏,等. 空间信息网络对抗效能评估指标体系研究[J]. 计测技术,2005,25(2):11-13

[2] 贾珺,战晓苏,程文俊. 基于灰色关联分析的网络战综合能力评估[J]. 系统仿真仿报,2012,24(6):1185-1188

[3] 彭子枚. 网络攻击效能评估若干关键技术研究[D]. 长沙:国防科技大学,2011

[4] 贾爱国,王新辉. 信息优势的度量与效能评估[M]. 北京:军事科学出版社,2006

[5] 么健石,郑美,谭越郡. 空间信息对抗作战效能评估内容与指标体系[J]. 信息对抗学术,2014(1):37-41

[6] 任海泉. 军队指挥学[M]. 北京:国防大学出版社,2007

[7] 董亚卓,詹武,常歌,等. 指挥信息系统指标体系划分方法综述[J]. 电光与控制,2014,12(1):50-54

[8] 李大光,李万顺. 基于信息系统的网络作战[M]. 北京:解放军出版社,2010

[9] 徐小岩. 计算机网络战[M]. 北京:解放军出版社,2003

[10] 智韬. 编队级网络对抗效能评估研究[D]. 郑州:解放军信息工程大学,2009

[11] 陈健,滕克难,杨春周. 基于ADC法防卫装备体系打击效能评估模型研究[J]. 舰船电子工程,2014(3):32-35

(上接第470页)

[12] Ertl M A. Stack caching for interpreters[J]. SIGPLAN Not., 1995,30(6):315-327

[13] Komondoor R, Horwitz S. Using slicing to identify duplication in source code[C]// Proceedings of the 8th International Symposium on Static Analysis. 2001:40-56

[14] Liu Chao, Chen Chen, Han Jia-wei, et al. Gplag: detection of software plagiarism by program dependence graph analysis[C]// KDD'06. ACM, 2006:872-881

[15] Myles G. Software Theft Detection Through Program Identification[M]. University of Arizona, 2006

[16] Myles G, Collberg C. Detecting software theft via whole program path birthmarks[C]// 7th International Conference Information Security. 2004

[17] Kontogiannis K. Evaluation experiments on the detection of programming patterns using software metrics[C]// Working Conference on reverse Engineering. 1997:1-44

[18] Krsul I, Spafford E. Authorship analysis: Identifying the author of a program: CSD-TR-94-030[R]. Computer Science Deparment, Purdue University, 1994