doi: 10.7690/bgzdh.2016.09.014

网络中心战能力实现方法

戴剑伟[1]，张欣怡[2]
（1. 国防信息学院一系，武汉 430010；2. 武警后勤学院二系，天津 300309）

摘要：为提高网络中心作战能力，对其实现方法进行研究。从技术实现的角度，阐述网络中心战的主要特点，分析网络中心战能力需求，提出实现网络中心战能力的主要方法，包括采用基于利益共同体的信息共享方法、构建基于面向服务架构的信息服务环境和基于云计算的支撑体系等。该研究可为我军信息网络体系建设提供参考。

关键词：网络中心战；能力要求；利益共同体；信息服务环境；支撑体系
中图分类号：TP393.08 **文献标志码**：A

Implementation of Network Centric Warfare Capability

Dai Jianwei[1], Zhang Xinyi[2]
(1. *No*. 1 *Department*, *Academy of National Defense Information*, *Wuhan* 430010, *China*;
2. *No*. 2 *Department*, *Logistics University of PAP*, *Tianjin* 300309, *China*)

Abstract: For improving network centric combat capability, studied the implementation of network centric combat capability. From the view of technical implementation, introduced the characteristics of network centric warfare (NCW) and analyzed the requirements of NCW. Furthermore, proposed the main approaches of NCW capability implementations, which includes the information sharing methods based on community of interest, the information service environments based on services oriented architecture and the supporting system based on cloud computing. The study in this paper can benefit the construction of information network system of our army.

Keywords: network centric warfare; capability requirement; community of interest; information service environment; supporting system

0 引言

网络中心战是信息时代的战争样式，是以网络技术为核心，以信息共享为基础建立信息优势，利用信息优势实现决策优势，从而加快决策和指挥速度，实现作战协同，提高杀伤能力、生存能力、响应能力以及自我协调能力，以极大提高作战效能[1]。

实现网络中心战的主要技术手段包括一系列标准、规范、指南、体系结构、软件基础设施、可重用组件、应用程序接口、运行环境定义和参考工具。推进我军信息化建设，提高网络中心作战能力是我军面临的重要任务；因此，笔者从技术实现的角度，对网络中心战能力实现方法进行研究。

1 网络中心战主要特点及能力需求

1.1 网络中心战主要特点

网络中心战的实质是利用网络实现所有作战要素信息共享，达到实时掌握战场态势，缩短决策时间，提高打击速度与精度的目的。具体体现：通过稳定可靠的网络化能力提升信息的共享程度；通过信息共享来提高信息质量和战场态势感知共享能力；通过战场态势感知共享来促进协同和自我协调能力，提高持续作战能力和决策速度。从技术实现角度来看，网络中心战具体特点包括[1-2]：

1) 采用 Internet 协议。通过采用 Internet 协议标准，针对可靠性和军事特点进行改进，实现各作战要素的物理连接。

2) 安全可靠的信息传输。对核心传输骨干网进行信道加密，以便更好地应对拒绝服务攻击。

3) 确保数据信息的安全。对数据信息进行密级分类和加密处理，确保数据/信息可靠、完整和不可否认。

4) 先投送后处理。对所有信息和数据首先投送，然后再处理，使得数据生产者/发布者无延迟地使信息和数据可见、可访问，确保数据信息用户可以在需要的时候尽快获取相关的数据。

5) 智能拉取。用户可以通过信息共享空间直接查找和拉取数据，订阅或使用增值服务。

6) 以数据信息为中心。将数据信息从应用和服务中分离出来，尽量降低对特定或应用系统的依赖，充分发挥数据和信息的利用效率。

7) 按角色权限访问。建立角色访问控制机制，

收稿日期：2016-05-26；修回日期：2016-06-30
作者简介：戴剑伟(1966—)，男，湖南人，博士，教授，从事信息资源管理研究。

用户根据自己角色权限访问数据信息、应用和服务。

1.2 网络中心战主要能力需求

为了实现各类人员和系统能在任何设备、任何地点和任何时间，安全获取完成任务所需信息的目标，网络中心战需要具备的能力主要包括对各类系统和用户提供数据和服务的能力，以及保证网络中心战体系自身正常运行的支撑能力[3]。

1) 数据和服务能力。

网络中心战支撑体系需要具备向各类终端用户提供连接、访问、共享信息和服务能力。即各类作战人员和任务合作伙伴可以使用各种终端设备在任何时候、任何地点连接到网络，访问信息、服务和其他的信息资源；通过信息共享空间实现信息和服务共享，并确保信息、服务和其他的信息资源是可见、可利用的。具体能力包括：

① 通信服务能力。通信服务能力是通过提供一个稳定的、动态的、逻辑的通信基础设施，实现将信息和服务传输给所有授权的用户。

② 业务应用服务能力。业务应用服务能力为作战、日常事务、情报等领域提供专业应用服务。

③ 核心应用和数据服务能力。核心应用和数据服务能力为各类用户提供通用的、核心数据服务。

④ 信息管理能力。通过对信息资源的有效管理，使各种信息资源能被一个或多个不同的系统、个人、机构按照权限正确访问，同时确保数据和信息在整个生命周期，对所有授权用户来说是可见、可访问、可信和可理解的。

2) 支撑能力。

网络中心战支撑体系需要提供计算存储服务能力，以及保证网络和数据服务等基础设施自身稳定、可靠运行的能力，即：动态分配计算处理、存储等资源；有效管理和监控网络性能；对所有用户和设备实施通用的访问控制；具备跨域安全和主动的网络防护能力；各类用户能有效开发和运用基础设施。具体能力包括：

① 计算和存储服务能力。计算和存储服务能力通过一系列整合的、物理/逻辑互联的各类数据中心集合，为所有用户和系统提供基于云计算、按需的计算处理、存储服务。

② 网络运行维护和监控能力。运维人员能对网络基础设施进行操作，按照用户需要动态配置各种资源；监控和优化网络基础设施运行状态，确保网络基础设施可靠运行。

③ 信息防护能力。确保信息及信息系统的可用性、完整性、可信性、机密性和不可抵赖性，确保信息整个生命周期的安全，确保信息被授权的用户访问。

2 网络中心战能力实现方法

在网络中心战中，信息贯穿于网络中心战的每一个角落，信息共享是网络中心战的基本需求。网络中心战能力实现的方法主要有运用基于利益共同体(community of interest，COI)的信息共享方法、构建基于面向服务架构的信息服务环境和基于云计算的基础设施体系等。

2.1 运用基于利益共同体的信息共享方法[4]

实现信息共享需要代价，实现信息在所有信息系统之间共享相当困难，也不现实。美国国防部在《国防部网络中心数据策略》中提出了利益共同体COI的概念。COI是为了共同的目标、利益、任务或者业务而需要进行信息共享的用户组成的协作组织。COI从本质上来说是一个相互协作、具有相同目的的用户集合，用户之间需要进行信息的交互，这就要求COI内所有用户能发现、访问和理解COI内的信息，COI成员的具体职责包括：

1) COI成员用发现元数据来标记自身的数据，并将元数据发布到可检索的目录中，确保数据在COI成员内部是可见的。

2) 在COI内部需要详细定义相关专业词汇，并按照统一的分类方法，对相关专业词汇进行分类，便于COI成员对业务术语涵义进行一致的理解，同时也支持机器间对数据的理解。

3) 对数据结构、数据定义、数据模型和语义、语法元数据进行注册，使得各类用户可以发现相关的数据。同时实现对已有数据的重用，可以降低数据对仲裁和格式转换的需求。

总之，COI实质是实现适度共享，不追求过度共享，只要各相关实体共同完成某个具体任务或达到某个目标，能进行信息的交换和共享即可，不必要求所有的系统能进行信息共享，从而降低跨业务领域信息系统之间的数据信息共享实施的难度。

2.2 构建基于面向服务架构的信息服务环境

信息服务环境是基于栅格化的信息网络，采用面向服务架构(services oriented architecture，SOA)技术，将拥有数据和信息资源的人和系统与需要数据和信息的人和系统连接起来，实现数据和信息的

共享，其主要功能包括：

1) 提供基于能力的服务架构，便于终端用户能够随时随地地访问及时、安全的各类信息；

2) 使信息提供者能够发布他们所拥有的任何信息；

3) 确保终端用户可以快速准确地发现和获取信息资源，并能为解决某个问题灵活地组成利益共同体；

4) 为网络化的信息资源提供安全保障和配套管理。

信息服务环境的组成主要包括数据资源层、面向服务架构的基础服务层、应用支撑层和应用服务层，如图 1 所示。

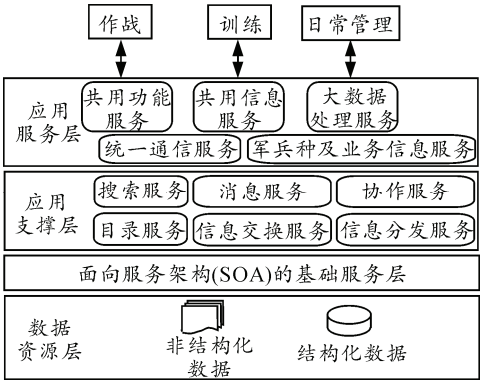

图 1　信息服务环境逻辑

1) 数据资源层。

数据资源层是各业务信息系统中各种类型的数据，主要包括结构化数据和非结构化数据。

结构化数据包括存储在各类关系型数据库管理系统的数据，如 Oracle、Microsoft SQL Server、IBM DB2、MySQL 等数据库管理系统的数据；非结构化数据包括各类文档和多媒体文件。

2) 面向服务架构的基础服务层。

面向服务架构的基础服务的核心是企业服务总线(enterprise service bus，ESB)。企业服务总线是传统消息中间件技术与 Web Service、XML 技术的结合，可以在一个异构的环境中实现信息稳定、可靠的传输，屏蔽了用户实际中的硬件层、操作系统层、网络层等相对复杂、烦琐的接口，为用户提供一个统一、标准的信息通道，保证用户的逻辑应用和这些底层平台无关，从而实现不同操作系统、不同数据库、运行平台和基于这些平台之上开发的应用软件的数据交换、数据共享与应用集成，为网络中心战数据交换与共享提供了有效的手段[5]。

3) 应用支撑层。

应用支撑层主要为应用服务层提供基础服务支撑，由目录、交换、信息分发、搜索、消息和协作等服务构成。

① 目录服务。构建全网目录服务体系，提供全网服务资源和用户的统一命名、名称解析和准确定位等功能，实现基于名称的全网统一寻址和服务，为上层信息服务提供基于目录的寻址服务。

② 信息交换服务。为全网用户和不同业务领域间各类应用提供灵活、可扩展的信息交换功能，支持可定制的数据格式、数据标准和典型报文格式间的交换，为跨部门、跨领域的非预期信息交换提供支撑。

③ 信息分发服务。为结构化、非结构化、流媒体和实时信息等各类信息资源，提供描述、发布、订阅、分发运行环境，实现分布式环境下的信息分发和投递，满足不同信息分发模式和不同信息分发质量要求。

④ 搜索服务。提供分类导航、搜索等多种方式的资源发现功能，支持信息发现、服务发现和用户发现，为用户按需发现和查找资源提供支撑。

⑤ 消息服务。为应用提供多种质量要求的信息传输服务，包括长报文可靠传输服务、短格式传输服务、实时传输服务、流媒体传输服务等；提供 HTTP/HTTPS 传输协议，支持长报文和短报文的适配，支持二进制 XML 编码、解码，提供压缩算法的扩展，实现 SOAP 消息传输性能的优化；基于安全保密体制，提供传输数据的认证和加密，以及加密算法的扩展功能。

⑥ 协作服务。为用户提供在线交流和文件共享，支持一对一、一对多、多对多的语音、文本、视频、文件共享和白板等方式的交互。

4) 应用服务层。

应用服务体系为作战、训练和日常办公提供资源可动态柔性重组、质量可充分保障、服务可即插即用、系统可安全抗毁的信息服务保障体系，各类用户可以通过各种终端随时随地访问信息资源，包括共用功能服务、共用信息服务、军兵种及业务信息服务、统一通信服务和大数据处理服务。

① 共用功能服务。共用功能服务依托各级数据中心，主要提供协同作业、报文处理、软件资源共享、视频服务和语音服务等服务。

② 共用信息服务。共用信息服务依托各级数据中心，为全网用户提供军用基础作业服务、民用

典型信息服务、国防数据词典、频谱信息服务和作战数据基础服务。

③ 统一通信服务。统一通信服务可以为语音、视频、电子邮件、语音邮件和即时消息等多种通信业务提供服务，依托数据中心基础设施，与现有相关通信网系实现互连互通，提供统一通信服务功能。

④ 业务信息服务。各军兵种专业数据中心发布联合海情服务、预警空情服务等军兵种信息服务，各业务部门专业数据中心发布情报侦察、技术侦察、气象水文、测绘导航、动员、后勤和装备等业务部门信息服务。

⑤ 大数据处理服务。大数据处理服务主要实现情报信息、态势信息的融合处理、挖掘分析和可视化展现，最大限度地将数据和信息转化为指挥员决策的知识。

2.3 构建基于云计算的网络中心战支撑体系

基于云计算的网络中心战支撑体系包括基于云计算的基础设施体系、安全防护体系和运维管理体系，如图2所示。

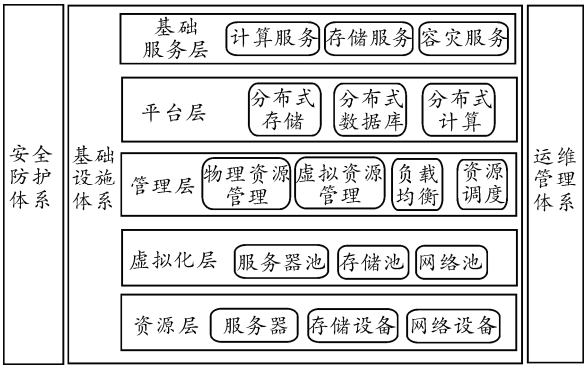

图2 基于云计算的网络中心战支撑体系

1) 基础设施体系。

基础设施体系指信息资源开发应用所需要的软/硬件设施。主要包括栅格化信息网络、虚拟化的存储与计算基础设施，实现信息资源的采集、存储、传输和处理设施。栅格化信息网络主要包括光缆网、卫星网、短波网和移动网等基础网系；存储与计算基础设施主要包括各类数据中心和容灾备份中心。

① 基础服务层。提供计算和存储资源的按需、动态分配及无缝扩展功能，提供资源负载管理、动态迁移等策略，构建全网一体的计算环境和存储环境，为用户获取虚拟计算和存储环境提供支撑；通过双机热备、服务迁移等方式，提供数据中心内各类信息服务系统数据、业务的容灾保护；根据用户需求构建异地容灾备份机制，实现用户信息系统数据的快速恢复、业务的快速接替。

② 基础承载层。基础承载层包括资源层、虚拟化层、管理层和平台层，通过将资源层的服务器网络、业务网络、存储网络等异构资源网络集中整合，形成高性能、低延迟、无阻塞的统一网络交换平台，为各类信息系统提供高效可靠的运行承载环境。虚拟化层将计算资源、存储资源、网络资源等物理资源抽象为虚拟资源，形成逻辑的服务器池、存储池、网络池；管理层提供对虚拟化和物理资源的管理能力以及负载均衡等网络服务能力。

2) 安全防护体系。

安全防护体系由基础承载平台安全、安全支撑服务、应用服务安全和安全管理构成。

① 基础承载平台安全。从网络安全防护、虚拟计算安全、存储系统安全和信道传输安全等方面，保护支撑体系网络边界安全，保证计算、存储资源受控使用，提供对虚拟环境、资源调度、网络架构的安全防护，为用户访问虚拟环境下的业务资源提供安全防护[6]。

② 安全支撑服务。安全支撑服务系统提供认证、授权、单点登录和审计日志等安全服务，采取网络拓扑屏蔽、网间接入认证、业务服务鉴权、传输协议控制等安全机制和策略，提供网间交换安全保护，为应用服务提供安全支撑。

③ 应用服务安全。应用服务安全系统采取服务代码安全性审核、服务软件注册认证和数据服务发布授权，恶意攻击识别与阻断、交互消息加密与签名/验证，用户身份验证、授权控制等策略，提供服务注册认证、服务运行安全和用户受控访问功能，保障应用服务注册、发布、执行过程的安全可信。

④ 安全管理。安全管理系统提供安全策略动态调整、安全设备管理和安全事件管理功能，支持运维管理员操作全程审计、用户访问关键操作审计、核心数据访问全程审计、服务交互安全审计等，提升支撑体系安全运维管理效能。

3) 运维管理体系。

运维管理体系包括基础运维、服务管理和服务保障等内容。

① 基础运维。基础运维包括支撑体系运行监控、资源管理调度、故障处置以及服务质量保证。

② 服务管理。服务管理主要提供服务运行监控、应用服务器监控和关键业务操作审计等功能，实现信息服务和应用软件的“状态可视、行为可管、

日志可查、操作可审”，保障信息服务的高效可靠运行和服务质量的持续改善。

③ 服务保障。通过部署人工服务席、工单系统、服务查询和分析系统等，受理语音和报表形式的服务业务申请和故障申告处理，确保能实时处理和响应故障及问题。

3　结论

网络中心战的核心是通过战场信息的高度共享，形成高效、统一的作战体系，最大限度地将信息优势转化为决策优势。实现战场信息共享的主要方法包括采用基于利益共同体的信息共享方法，构建基于面向服务架构的信息服务环境和基于云计算的支撑体系。

参考文献：

[1] 何风. 实施网络中心战的军事需求工程研究[D]. 长沙: 国防科技大学, 2009: 1-2.

[2] DISA. NCES Capabilities Overview[EB/OL]. www.dodcio.defense.gov/Portals/0/.../DT-07-NCES-Capabilities.ppt, 2013-10-8.

[3] 戴剑伟, 张育军, 王强. 美军信息体体系架构研究[J]. 指挥控制与仿真, 2014, 36(6): 1-4.

[4] 徐飞, 戴剑伟. 美军 COI 与信息共享研究[J]. 指挥控制与仿真, 2011, 33(5): 114-118.

[5] 戴剑伟, 王刚. 基于 ESB 的指挥信息系统数据交换与共享平台[J]. 通信指挥学院学报, 2012, 32(2): 65-67.

[6] 包林波, 季新源, 陈希林, 等. 空中异常情况网络计划处置方法[J]. 兵工自动化, 2015, 34(7): 24-27.

****

（上接第 56 页）

3　应用效果分析

新研制的程序从 2014 年 3 月起陆续投入应用，截止到 2015 年 10 月，已完成 5 000 余次吹风试验。从程序改造前后的控制曲线对比来看，程序的控制精度完全满足需求。图 5 是 *Ma*=0.9 的实际控制曲线。流场稳定后，马赫数控制精度都在±0.002 以内，完全满足国军标的精度要求，也优于原来程序的马赫数控制精度。限于篇幅，其他马赫数的精度曲线就不在此一一列举。

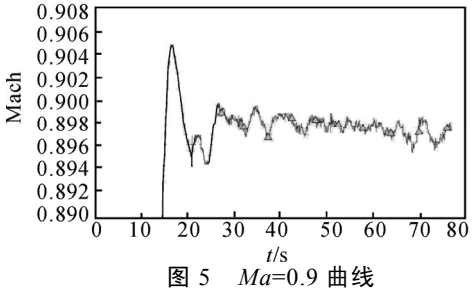

图 5　*Ma*=0.9 曲线

4　结束语

笔者以软件逆向工程技术为主要手段，重新研制了 2.4 m 风洞 PLC 核心控制系统中存在的无源代码模块，解决了今后系统升级面临的技术障碍，消除了存在的隐患。新软件投入应用后的试验数据表明，软件研制是成功的。

参考文献：

[1] 饶正周, 马永一, 杨兴锐, 等. 基于知识规则的 2.4 m 风洞控制开车参数自动生成专家系统[J]. 兵工自动化, 2015, 34(6): 94-95.

[2] 张晓峰. 软件逆向工程技术相关研究与实现[D]. 成都: 电子科技大学, 2007: 8-39.

[3] 王茹. 基于软件逆向工程技术和系统研究[J]. 煤炭技术, 2012, 31(9): 183-184.

[4] 肖仕红, 沈亚坤, 刘立新, 等. 水下液压控制系统浅水测试专用仿真测试软件[J]. 机电工程, 2015, 32(10): 1385-1389.

[5] 李伟华, 李由. 实时软件逆向工程技术研究[J]. 西北工业大学学报, 2003, 21(4): 391-393.

[6] 马金鑫, 忽朝俭, 李舟军, 等. 基于控制流精化的反汇编方法[J]. 清华大学学报, 2011, 51(10): 1345-1347.

[7] 张龙杰, 谢晓方, 袁胜智, 等. 跟踪式智能反汇编算法研究[J]. 计算机应用, 2009, 29(1): 242-244.