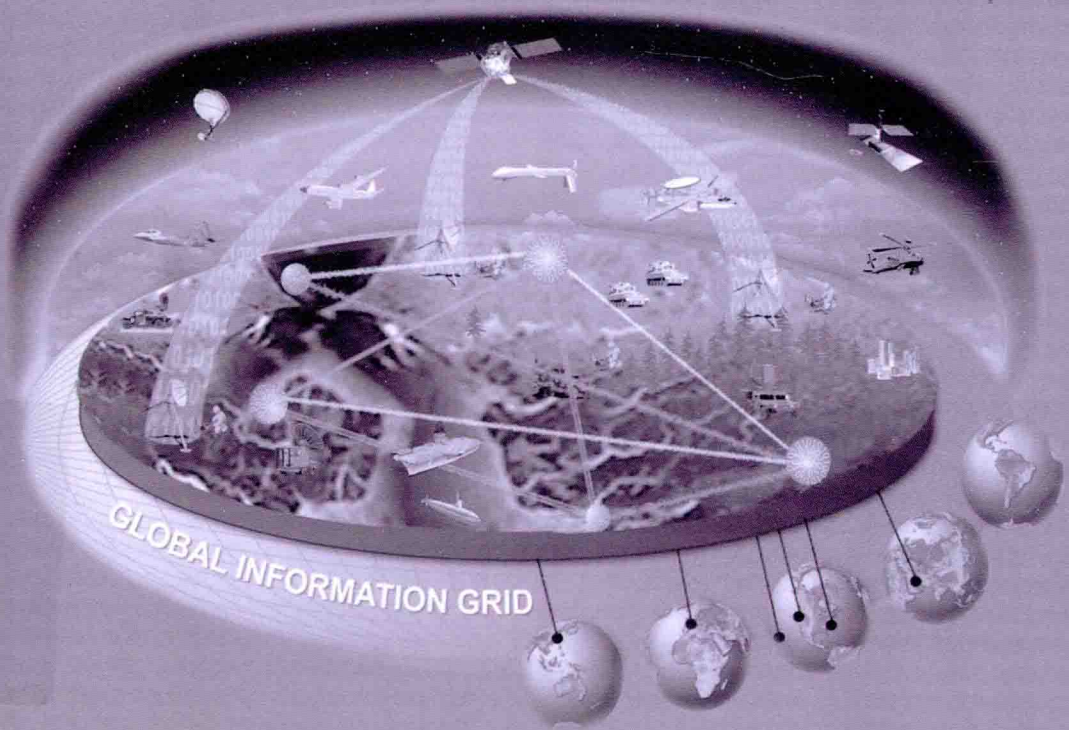
网络空间作战与安全丛书

美国陆军计算机网络作战

蒋豫　沈松　杨秀红　马广兴　李捷　译



网络空间作战与安全丛书

美国陆军计算机网络作战

蒋 豫 沈 松 杨秀红 马广兴 李 捷 译

译　序

美军网络力量主要聚焦于战场环境与武器装备信息化领域，解决了“战场作战”与“业务管理”系统的网络互连、互通与互操作问题。随着技术发展，网络作战的内涵也由计算机网络战（CNO）向计算机网络作战（NetOps）拓展。野战条令 FM6－02．71《计算机网络作战（NetOps）》颁布于2008年11月19日，供美陆军内部使用。该条令主要阐述全球信息栅格的陆军部分（陆战网），计算机网络作战的目标；应用部门的相关作用与组织、装备、领导力、人员及设施所应遵循的陆战网标准，此外还明确了通信、服务及应用的目的。

尽管该条令颁布距今已过数年，且计算机网络作战领域不断发展，组织结构更发生了巨大变化，但其核心内涵并未根本改变，仍具借鉴意义。现将该条令翻译如后，供参考。

译　者

二〇一五年一月

目　录

第一章　计算机网络作战概述

本章主要讨论全球信息栅格（GIG）的陆军组成部分——陆战网，以及那些通过陆战网的指挥与控制来支持战略、战役和战术级指挥员信息需求的计算机网络作战（NETOPS）集成功能。本章重点讨论各组成部分的功能服务、关键能力和效果使能。最后，本章以计算机网络作战有关原则，以及贯穿于全频谱行动过程中利用综合网络的陆军企业化网络基础设施概念作为结束。

第一节　全球信息栅格

联合出版物 JP6.0 把全球信息栅格定义为：由在全球范围内，能够连接到端对端之间的一系列信息系统、相关程序和人员构成的全球连接体系，它根据决策者、作战部队和支援人员的要求，收集、存储、分发、管理和处理信息。全球信息栅格的主要功能包括：所有军种和部队为获取信息优势的一切自有的和租借的计算机系统、通信、软件及应用、数据、安全服务以及其他信息服务；支援所有国防部、国家安全和相关情报界的战略、战役、战术和操作级的任务与功能；扩展所有行动地点的能力（基地、驻地部队、军营、站、设施、一定平台和部署地点等等）；根据需求向多国、盟国、非国防部用户和其他系统提供交互；整

合计算机平台、武器系统和各类传感器以通过全球互联的网络来交换信息。

从以上定义可以看出，全球信息栅格非常类似于万维网（Worldwide Web），它的基本能力是由一系列依赖设施和部门传输的信息和信息服务组成。需要特别指出的是全球信息栅格是网络空间（CYBERSPACE）的一个组成部分。国防部把“网络空间”定义为：“是一个由相互独立的信息技术基础设施构成的全球域，包括互联网、电信网、计算机系统与各类嵌入式处理器和控制器。”全球信息栅格，作为国防部网络空间的一个组成部分，分别与国家和国际网络空间以及国家和国际信息基础设施互联互通。国防部的战略是通过把全球信息栅格的七个组成部分（勇士、全球应用、计算机、通信、计算机网络作战、信息管理，以及图 1－1 所列的基础设施）联合有机整体而建立一个“网以确

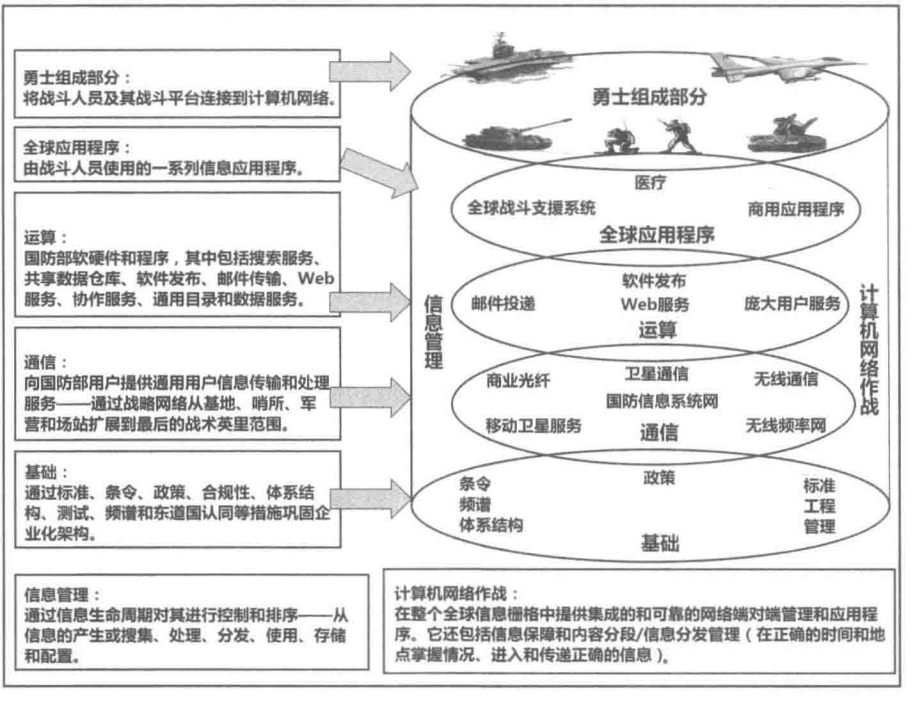


图 1－1　全球信息栅格构成示意图

保联络空间”，合部队获得信息优势，同时在未来必要的时刻，可以用他们来进行攻击性计算机网络作战。授权的用户可以通过军事、商用通信节点甚至敌人的节点来接入全球信息栅格，如标准化战术接入点和电话端口等。这些节点可以连接天基、空中和地面网，为战略、战术、固定资产和其他部署的用户提供信息传输的通路。为信息生产者和使用者之间提供多址连接通路，确保高效顺畅的信息流通。

在联合层面，计算机网络作战是美国战略司令部司令实施的系列行动，目的是为操作和防护全球信息栅格而提供的指挥、控制和态势感知。计算机网络作战包括全球信息栅格企业化管理、全球信息栅格网络防护、全球信息栅格内容管理等。计算机网络作战的目的是提供可靠的网络和信息系统以供使用、可靠的信息防护以及信息在战略、战役、战术领域内可靠传输。最终目的是形成全球信息栅格的纵向融合，确保正确的信息在正确的时间、以正确的格式传到正确的位置，以获取信息优势，并最终获得决策优势，保障国防部的全频谱作战职能。计算机网络作战向指挥官提供掌控全球信息栅格的力量并把这种力量应用于战场以塑造和影响行动的能力。

一、全球信息栅格管理机构

全球信息栅格的管理机构是战区联合战术网络结构控制委员会（TJTNCCB）、陆军企业化基础设施技术结构控制委员会（CCB）和陆军企业化计算机网络作战集成体系（AENIA）。这些机构都被授权批准、监管并强制推行标准，以确保设施设备和软件的兼容性来实现网络共享。信息技术标准的新的注册/管理工具是国防部信息系统注册系统。

（一）陆军联合技术企业化

陆军联合技术企业化要求所有的陆军网络都要使用符合全球

信息栅格标准的，且经过证明的工程标准和现代通信设施与技术，以确保美军不同部队之间的兼容性。

（二）联合战术网络结构控制委员会

战区联合战术网络结构控制委员会负责管理战术网络和系统设备标准和能力，这些标准确保整个全球信息栅格战术部分所有设备和软件的通用性。对于非标准化结构，联合战术交换系统网络管理结构控制委员会（JTSSNMCCB）可根据以下情况进行特别规定：

1. 非标准化协议是标准化协议的补充部分。

2. 非标准化能力作为战区联合战术网络结构控制委员会的附件，仅适用于某特定区域并且不作为标准化结构的组成部分。

3. 非标准能力对于某项任务至关重要，并且该标准适用于该特定任务之外的时间和范围。如果该非标准能力慢慢成为一种经常性需要的能力，那么该标准必须以附件的形式或作为标准化结构的一部分来包括在联合战术交换系统网络管理结构控制委员会。

（三）陆军企业化基础设施技术结构控制委员会

陆军企业化基础设施技术结构控制委员会由首席信息官/负责指挥、控制、通信和计算机行动的助理参谋长设立，负责监管陆军陆战网络企业是否使用标准化变更管理程序来处理陆军各机构提出的变更各自陆战网络基础设施的申请。网络企业技术司令部负责结构/变更管理。网络企业技术司令部/陆军第九信号司令部管理和保留“网络调整局”的网络职责，并负责根据陆军野战条令 FM－3.0 第 25－1 条第 2－2a（10）行和第 10－87 条的规定的对陆军所有部门的陆战网运行和维护进行技术监管。

二、陆战网

全球信息栅格企业化管理、全球信息栅格网络防护和全球信

息栅格内容管理三个都是联合及全球网络术语。陆战网各组成部分分别指网络管理/企业化系统管理、信息保障/计算机网络防御、信息分发管理和内容分段。而野战手册，这些术语均代表全球信息栅格和陆战网的计算机网络作战过程，以此建立陆战网计算机网络作战过程和全球信息栅格计算机网络作战过程之间的联系。

陆军计算机网络作战与联合任务具有与生俱来的关系，其目的是提供指挥、控制和态势感知，以操作和防护全球信息栅格的陆军部分——陆战网。陆战网包括所有必需的标准、传输、服务和应用等内容，以使指战员能通过网络从（向）世界任何地方搜集、处理、存储、传输、分发所需信息。能确保陆军高效执行各项作战职能发挥各类设施的作用以取得信息优势，对于确定并执行准确及时的决策非常必要。不像其他任务那样，只需要完成特定数据、操作和防护就可以了，陆战网是连续行动，要持续提供成功、可靠的支援。

陆战网计算机网络作战是三个关键部分的有机组成（网络管理/企业化系统管理、信息保障/计算机网络防御、信息分发管理/内容分段），指导信号机构进行通信网络的设施、管理和防护，并指导信号机构向行动部队提供必要的直接支援。计算机网络作战向用户/系统提供全层次的端对端网络和信息系统、信息防护和实施信息分发。

网络化信息管理的目的是使决策者能快速获取信息且信息内容合适，使决策者能做出更好的决策以影响任务完成，并能保护这些决策能安全传达到所属部队并顺利执行。如果决策者不能获取所需的网络服务，陆战网计算机网络作战部门必须共同协作并决定由谁来采取措施且如何对信息流进行优化。计算机网络作战人员需要共享的态势感知/通用作战态势图以及技术、程序和协

同组织机构，来对网络和信息系统的恶化、损坏或行动优先顺序的调整进行快速评估并拿出应对措施。要求要对陆战网进行综合管理，所有部门都要全力保障陆战网，确保各项行动高效实施。

由于整个行动区的各类信息系统都竞相争夺陆战网有限的接入资源和能力，因此计算机网络作战要提供一种方法来操作和防护陆战网，来有序进行传输、服务和应用，以满足指挥员的意图和要求。可通过以下方法来更好地向用户/系统提供支援：

1）确定用户/系统的信息需求（谁、什么时间、什么地点、需要什么内容）。

2）确定何种通信网络和信息资源（硬件和软件）来满足用户/系统的信息需求。

3）确保用户/系统能接入所需的通信网络和信息服务。

4）采取信息保障/计算机网络防御等措施以及使用情报进行基于威胁的危机管理，来保护信息与信息系统的机密性、完整性和可用性。

5）建立信息流和信息处理过程，以确保正确的信息能在正确的时间、以正确的格式分发到正确的地点。

6）确定网络有线、光纤与无线部分的信息源需求。

7）确保信息源高效分配以使用户/系统获得最大限度的带宽。

计算机网络作战的效能是由网络的可用性、可靠性，适用的军种范围、适用的兴趣区以及是否符合所需服务层次等因素决定。网络协同环境中的服务确保方法包括根据服务层次协议，在提供者和使用者之间建立行动起点、共同监控和清晰的能力理解。恰当的陆战网方法手段可以根据各服务层次的协议对所有行动进行监控，同时确保及时决策/执行，对服务先后顺序、资源分配、根源和任务影响进行评估。

计算机网络作战的目的是确保网络和信息系统的可用性，确保可靠的信息防护和可靠的信息分发。所有这些目标都是为了达成和保持行动目标。计算机网络作战要根据所执行的任务和计算机网络作战三个组成部分的重要行动，为指战员提供所需的信息。计算机网络作战的各个组成部分要在战略、战役、战术等各个层次和各项职能实现全面融合。因此，通信部门必须完全指挥和控制行动区内的整个网络，还要了解行动区外那些可能影响指挥员信息需求的陆战网有关部分的表现。

三、计算机网络作战组成与效果

可靠的网络可确保能使用和控制网络与信息系统资源，确保这些资源被有效管理，问题得到预测和减轻。要采取预防性措施来确保网络与信息系统资源的不间断可用，并对网络与信息系统资源加以保护。这些预防性措施包括合适的降级、自我修复、自动切换、多样化以及排除关键节点的失效等等。

可靠的信息防护为信息传输网和信息系统各个环节提供防护，如从信息搜集、存储、处理到发现、分发以及用户、系统、决策者的使用等。信息防护指采取主动或被动方式来保护己方信息和信息系统，以确保己方能及时准确地获取相关信息，同时防止对手利用己方信息和信息系统达到其目的。信息防护包括信息保障、计算机网络防御和电子防护能力（参见 FM3 - 0）。

可靠的信息发送能及时向用户、系统和决策者提供所需信息。要持续监控网络以确保信息在正确的反应时间内传输，信息的产生、可用性及性能满足用户与系统的需求。

计算机网络作战是网络管理/企业化系统管理（NM/ESM）、信息保障/计算机网络防御、信息分发管理/内容分段等组成部分各自能力与结果的有机融合。此外，网络管理/企业化系统管理、信息保障/计算机网络防御、信息分发管理/内容分段等都是信号

团的核心能力。图 1 - 2 描述和构建了产生及维持计算机网络作战效果必须考虑的技术组成。该图的中心是计算机网络作战的三个组成部分、相互关系，也说明了三者一旦有机结合为整体的计算机网络作战能力将产生的巨大效果。计算机网络作战的三个关键组成部分如下图所示。

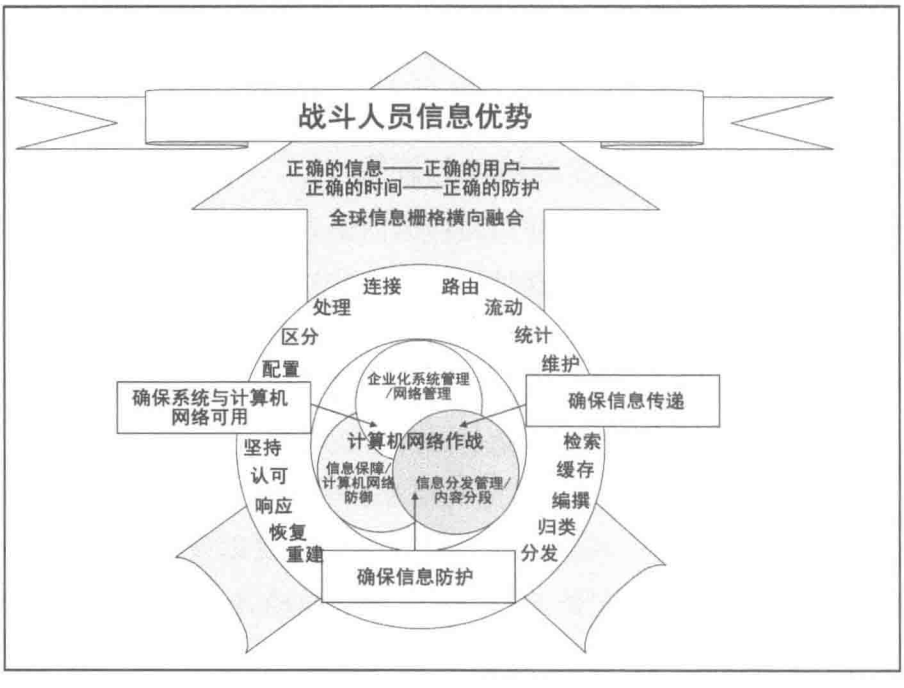


图 1 - 2　计算机网络作战组件、效果和目标

（一）网络管理/企业化系统管理

网络管理/企业化系统管理指为了高效设计、安装、运行、管理、优化、存储陆战网各类通信网、信息系统及其他应用程序所必需的技术、程序和政策。这是使信息技术服务与计算机网络作战三大关键能力有机融合的重要部分。

网络管理指的是为运行、管理、维护、补充网络系统，使之安全可靠并提供所需的服务质量，而采取的行动、方法、程序和工具。

企业化系统管理指的是通过性能监控、结构管理、问题诊测/解决等方法对全网分发的信息系统进行管理，企业化系统管理很大程度上受通信网络管理的自主性所影响。

1. 功能服务

网络管理/企业化系统管理有五种主要功能服务，分别用于通信网络和信息服务技术的设计、安装、操作、管理、优化和恢复，以确保信息与信息系统的高效操作、运行、安全、可用。为此，这些必须服务必须在战略、战役、战术层次的所有陆军作战功能中得到 应用。这五种服务分别是：

1）企业化服务的可用性指的是最终用户/系统应用，侧重于企业化服务能力的可访问性、可接入性、可使用是、性能及反应能力等。此处的“企业”指一系列形式多样、物理隔离但又紧密联系的组成部分，这些组成部分共同协作以达到一个共同的功能目标。企业化服务指提供协作、软件分发、讯息、发现、存储、用户/系统协助及安全功能。

2）系统可用性指对电脑系统和系统构成元素进行日复一日地管理，向主机和最终用户提供软件应用、操作系统和数据库服务等。系统管理包括为确保地面作战系统与系统和服务高效运行而采取的一切必要措施。

3）网络可用性指确保网络基础设施能提供所需的网络质量和可靠的服务。网络管理/企业化系统管理所指的网络分布于通信的所有三个层次（地面、空中和卫星通信），包括所有用有线、无线、光纤传播媒体服务的回路交换网、信息包交换网和单元交换网。

4）卫星通信可用性指对所有分配和未分配的卫星通信资源进行日复一日地操作管理，包括当服务中断时提供合适的支援，提供卫星通信系统情况，保持组织机构当前行动和计划行动的空