

图书基本信息

书名：<<美军网络战研究-从系统工程学角度探讨美军网络战>>

13位ISBN编号：9787562618119

10位ISBN编号：7562618119

出版时间：2010-7-1

出版时间：国防工业出版社

作者：姚红星,温柏华

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 内容概要

当前一段时间以来，关于美军网络战研究讨论的很多。有的从概念角度分析总结，有的从技术方面探讨学习，更有从美军网络战作战与发展机制层面深入研究讨论。

应该说，相关研究很好的从某个领域对美军网络战做了剖析。

作者认为，从其发展历程的脉络来看，美军网络战发展过程完全体现了战争工程学在信息时代的发展与应用，是信息时代战争工程学的具体体现。

要全面研究美军网络战，必须深刻认识美军网络战发展的信息时代烙印与战争工程学方法论。

### 一、信息技术主导美军网络战发展动力

就美军来说，他们已经解决了网络战发展的所谓思维观念、组织体制、发展机制等等问题。

对他们来说，网络战研究更多的已经属于一种信息技术问题。

当然，这种信息技术也需要在技术发展的理念和创新机制上作出突破。

但这些问题基本上不属于美军军方高层的问题，更多的是底层信息技术创新的核心问题。

1、信息技术不断发展的驱动，导致美军网络战概念的内涵和外延不断变化。

所以，才有了美军提出来的所谓EW电子战、NetOps网络作战、Network-Warfare网络战、Cyber Warfare、Information Operations信息作战等等概念的区分与不断演化，相互渗透。

2、信息技术不断发展的驱动，也直接拓展了美军信息技术作战应用在深入和渗透，直接导致美军网络战相关组织机构与相关力量在军事作战领域地位的转变和提升。

从以往配属型、防御型、支援型走向独立型、作战型、进攻型。

而且，这种转变必将持续下去。

3、信息技术不断发展的驱动，更是直接的导致各型各类信息技术在作战领域的深入应用、在CyberSpace对抗中的手段与方式的不断变化。

不了解信息技术的发展，就不能理解NCCT与link16的区别与联系，就不能看清所谓黑色核心技术到底有什么优势，就不能认识到CyberRange网络靶场建设的可行性与可信性到底该有多少。

### 二、战争工程学创新美军网络战发展机制

战争工程学，也有专家称为战争系统工程学，是系统工程学在军事领域的应用。

作者认为，它应该是军事思想、军事战略、军队建设、作战指挥等等发展的基础方法论，应该是支撑相关领域的科学发展与转型的思想武器。

对于美军来说，战争工程学贯穿美军所有建军发展历程，美军网络战则是战争工程学直接指导下的发展成果。

虽然，美军自己并没有强调战争工程学的指导地位。

1、信息技术在军事领域应用目的是努力解决所谓“战场迷雾”问题。

所谓战场迷雾就是战争复杂性带来的信息缺失（the lost of Information）问题。

信息缺失才给网络战创造了战场空间。

对于复杂战争系统，不说美军现在，就是在可预见的将来，也不肯能彻底解决，只能是有限逼近。

而战争工程学恰是当前有效认识战争复杂性的科学思想。

2、战争工程学所需面对的战争复杂性是战争永恒的本质。

当然也是网络战发展与研究本质课题。

如果不站在这个高度看待美军网络战，就会或者导致对网络战恐慌，或者导致对网络战忽视。更无法深刻看清美军网络战包括本质概念、组织机制和技术创新在内的必然演化方向。

本书作者试图站在美军的角度，参仿美军DoDAF框架的三视图方法，从美军网络战概念——系统视图、美军网络战作战力量体系——作战视图、美军网络战战场空间——技术视图三个角度分析美军网络战。

希望能够尽最大能力，透视美军网络战。

特别需要声明的是，本书内容的三分之一属美军原版资料翻译、三分之一属作者观点、三分之一收集、整理、并借鉴了很多学者的已有研究成果。

对于借鉴其他学者的研究成果，作者深表感谢，因部分内容无法找到原始来源，顾没有全部标识出处。

我们认为，本书的成型离不开相关学术前辈的多年努力，也希望得到学术前辈能够支持，对相关问题的研究，促进军事理论的研究与发展，是我们共同的目标。

## 书籍目录

- 第1章 网络战概念框架（系统视图） 1
  - 1.1 网络战相关概念 1
    - 1.1.1 电子战——Electronic Warfare 1
      - 1.1.1.1 EW电子战三领域 1
      - 1.1.1.2 联合电子战的机构组成情况 4
      - 1.1.1.3 电子战计划需要考虑的因素 6
      - 1.1.1.4 联合电子战计划过程 7
      - 1.1.1.5 协调联合电子战 7
    - 1.1.2 网络战——Network Warfare 9
      - 1.1.2.1 Network 的内涵 9
      - 1.1.2.2 Network Warfare的误区 10
    - 1.1.3 网络作战——NetOps 11
      - 1.1.3.1 Netops基本概念 11
      - 1.1.3.2 全球网络作战特遣部队（JTF-GNO） 13
      - 1.1.3.3 Netops的指挥控制 16
    - 1.1.4 网络战——Cyber Warfare 30
      - 1.1.4.1 Cyber Space 30
      - 1.1.4.2 Cyber Conflict 域 31
      - 1.1.4.3 美空军最早开始Cyber Warfare研究 32
      - 1.1.4.4 DOD和美国的關鍵基础设施 33
      - 1.1.4.5 Cyber warfare的作战问题 34
      - 1.1.4.6 Cyber Warfare法律和Proportionality问题 38
    - 1.1.5 信息战——Information Warfare 38
    - 1.1.6 信息作战——Information Operations 39
      - 1.1.6.1 心理战PSYOP 39
      - 1.1.6.2 军事欺骗（Military Deception MILDEC） 40
      - 1.1.6.3 作战安全（Operational Security） 40
      - 1.1.6.4 计算机网络作战Computer network operation 40
      - 1.1.6.5 EW电子战 47
    - 1.1.7 指挥控制战——C2（Command and Control）Warfare 47
      - 1.1.7.1 C2（指挥与控制）系统 47
      - 1.1.7.2 C3（指挥、控制与通信）系统 48
      - 1.1.7.3 C3I（指挥、控制、通信与情报）系统 48
      - 1.1.7.4 C4I（指挥、控制、通信、计算机与情报）系统 48
      - 1.1.7.5 C4ISR（指挥、控制、通信、计算机、情报、监视与侦察）系统 48
      - 1.1.7.6 C4IKSR（指挥、控制、通信、计算机、情报、杀伤、监视与侦察）系统 49
    - 1.1.8 网络中心战——Network - Centric Warfare 50
      - 1.1.8.1 NCW与《2020年联合构想》 50
      - 1.1.8.2 NCW与GIG 51
      - 1.1.8.3 NCW与国防部军事转型 51
  - 1.2 网络战相关基本概念分析 52
    - 1.2.1 Electronic与Electromagnetic 52
    - 1.2.2 Network 对Cyber 55
      - 1.2.2.1 Network 55
      - 1.2.2.2 Cyber 59

- 1.2.3 Operation对Warfare 64
- 1.2.4 Information warfare 对 network centric warfare 65
- 1.3 美军的网络战概念框架 65
  - 1.3.1 美军“大网络战概念” 66
    - 1.3.1.1 美军“大网络战概念”实质性内容 66
    - 1.3.1.2 美军“大网络战”相关概念分析 68
  - 1.3.2 美军“小网络战概念” 71
    - 1.3.2.1 EW概念内容 71
    - 1.3.2.2 Computer Network Operation概念内容 72
    - 1.3.2.3 Cyber Warfare概念内容 72
    - 1.3.2.4 Information Operation概念内容 72
- 第2章 网络战力量体系（作战视图） 73
  - 2.1 美军高层指挥控制关系 73
    - 2.1.1 美军指挥关系相关概念 74
    - 2.1.2 四种指挥关系 75
  - 2.2 国防部信息系统局DISA 77
    - 2.2.1 使命任务 77
      - 2.2.1.1 指挥与控制C2（Command and control）：77
      - 2.2.1.2 计算服务和应用托管（computing/application Hosting） 78
      - 2.2.1.3 合同和采购（Contracting and Procurement） 79
      - 2.2.1.4 GIG工程 79
      - 2.2.1.5 信息安全IA（Information Assurance） 80
      - 2.2.1.6 MNIS（Multinational Information Sharing） 81
      - 2.2.1.7 网络中心企业服务（Net-Centric Enterprise Services） 81
      - 2.2.1.8 卫星通信服务（Satellite Communications (SATCOM) Services） 81
      - 2.2.1.9 频谱管理 82
      - 2.2.1.10 兼容性测试 82
      - 2.2.1.11 语音、视频和数据服务 83
    - 2.2.2 DISA的发展历程 83
      - 2.2.2.1 国防通信局（Defense Communications Agency）阶段 83
      - 2.2.2.2 DISA阶段 83
      - 2.2.2.3 当前的革新 84
      - 2.2.2.4 未来展望 84
    - 2.2.3 DISA组织结构 85
      - 2.2.3.1 战略事务分部 85
      - 2.2.3.2 共享服务分部 85
      - 2.2.3.3 特殊使命 86
      - 2.2.3.4 特殊顾问 86
      - 2.2.3.5 作战司令部野战局（Combatant Command Field Offices） 86
    - 2.2.4 DISA的战略：SURETY, REACH, SPEED 87
  - 2.3 美战略司令部网络战职能 88
    - 2.3.1 基本情况 88
    - 2.3.2 组成结构 89
      - 2.3.2.1 全球打击联合职能组成司令部 89
      - 2.3.2.2 航天作战联合职能组成司令部 90
      - 2.3.2.3 全球网络作战联合特遣部队 90
      - 2.3.2.4 网络战职能组成司令部 92

- 2.3.2.5 集成导弹防御联合职能组成司令部 94
  - 2.3.2.6 ISR职能组成司令部 94
  - 2.3.2.7 联合信息作战战争司令部 95
  - 2.3.2.8 大规模杀伤性武器作战中心 97
  - 2.4 美国陆军网络战力量 97
    - 2.4.1 陆军网络战力量构成 97
      - 2.4.1.1 网络战司令部/9th 信号司令部 (NETCOM/9th SC(A)) 97
      - 2.4.1.2 陆军情报和安全司令部(INSCOM) 99
      - 2.4.1.3 陆军通讯电子战生命周期管理司令部 101
      - 2.4.1.4 美陆军航天和导弹防御司令部(SMDC)/陆军战略司令部 102
      - 2.4.1.5 陆军计算机网络作战-电子战支持局USACEWP 103
    - 2.4.2 与其他部队的关系 103
    - 2.4.3 陆军网络战的指挥与控制 104
    - 2.4.4 陆军网络基础设施 105
  - 2.5 美国空军网络战力量 106
    - 2.5.1 空军网络战相关部队 106
    - 2.5.2 空军野战局中其他网络战力量 108
    - 2.5.3 空军NETOPS业务处理模式 113
  - 2.6 美国海军网络战力量 115
    - 2.6.1 海军网络战司令部 115
      - 2.6.1.1 NAVSOC海军卫星作战中心 117
      - 2.6.1.2 NCTAMS海军计算机和通讯地面 (Area) 主站 118
      - 2.6.1.3 舰队信息战中心与海军信息作战司令部 118
      - 2.6.1.4 海军战术系统交互能力中心 (OPNAV39) 119
      - 2.6.1.5 通信安全物资系统主任办公室 119
      - 2.6.1.6 舰队侦察支援司令部 120
      - 2.6.1.7 海军安全司令部 120
      - 2.6.1.8 海军计算机特遣部队计算机网络防御司令部 120
      - 2.6.1.9 海军信息作战司令部 121
      - 2.6.1.10 海军网络与空间司令部 (NNSOC) 121
      - 2.6.1.11 第十舰队 (Navy Tenth Fleet) 122
    - 2.6.2 海军网络战司令部基本情况 124
      - 2.6.2.1 美海军网络战司令部下属网络与空间作战司令部的基本情况 124
      - 2.6.2.2 海军GNOSC在NETOPS业务领域基本情况 124
    - 2.6.3 海军全球NNSOC的部署情况 126
  - 2.7 美军拟建的网络战司令部 126
  - 2.8 美国政府网络安全相关机构 129
    - 2.8.1 国家安全局 (NSA) 130
    - 2.8.2 国土安全部 (DHS) 131
    - 2.8.3 与军事系统相关领域机构的关系 133
    - 2.8.4 国家安全令2008 133
  - 2.9 美民间网络安全力量 135
- 第3章 网络战战场空间 (技术视图) 137
- 3.1 GIG相关情况介绍 137
    - 3.1.1 GIG的核心通信链路 139
    - 3.1.2 GIG建设过程中的重要计划 140
      - 3.1.2.1 全球信息栅带宽扩展计划(GIG-BE) 140

- 3.1.2.2 联合战术无线电系统(JTRS) 141
- 3.1.2.3 转型卫星(TSAT) 142
- 3.1.2.4 网络中心企业业务(NCES) 142
- 3.1.2.5 水平融合(HF) 143
- 3.1.2.6 加密转型 143
- 3.1.3 GIG各军种组成部分 143
  - 3.1.3.1 海军部队网 ( FORCENet ) 143
  - 3.1.3.2 陆军LandWarNet陆战网 145
  - 3.1.3.3 空军C2星座网 146
- 3.2 GIG网络集成方式 149
  - 3.2.1 硬件集成—网络互联技术 149
    - 3.2.1.1 IPV6 149
    - 3.2.1.2 MPLS 151
    - 3.2.1.3 黑色核心网络技术 159
  - 3.2.2 软件架构---服务集成方式 164
    - 3.2.2.1 采用COTS方式采购通用商用软件 164
    - 3.2.2.2 采用SOA构架做软件应用集成 164
  - 3.2.3 作战层面上的集成方式 165
  - 3.2.4 DOD业务方面的集成方式 165
  - 3.2.5 战略层面集成框架 166
- 3.3 基于GIG的作战应用 170
  - 3.3.1 CEC协同作战能力 170
    - 3.3.1.1 CEC网络系统具有以下三大功能 172
    - 3.3.1.2 CEC的组成与操作 172
  - 3.3.2 FCS未来作战系统 173
    - 3.3.2.1 完成目标 173
    - 3.3.2.2 技术上的实现方式 174
    - 3.3.2.3 主要技术挑战 174
  - 3.3.3 TTNT战术目标网络瞄准与NCCT网络中心协同瞄准技术 175
    - 3.3.3.1 TTNT战术目标网络瞄准技术 176
    - 3.3.3.2 网络中心协同目标瞄准(NCCT) 技术 178
- 3.4 GIG的信息保障 ( IA ) 180
  - 3.4.1 IA信息 ( 安全 ) 保障 181
    - 3.4.1.1 IA信息 ( 安全 ) 保障战略规划 181
    - 3.4.1.2 美国国防部GIG IA Architecture 183
    - 3.4.1.3 IA战略转型 184
  - 3.4.2 美国国防部DMZ ( De-Militarized Zone ) 187
    - 3.4.2.1 CSD DMZ 基本情况 187
    - 3.4.2.2 DOD DMZ 基本情况 189
  - 3.4.3 AdHoc网络及其安全 191
    - 3.4.3.1 Ad Hoc网络 191
    - 3.4.3.2 Ad Hoc网络安全 197
- 3.5 美军NCR项目 202
  - 3.5.1 项目背景 202
    - 3.5.1.1 颁布网络安全法律, 制定国家安全战略 203
    - 3.5.1.2 健全组织机构, 实施全面统筹 203
    - 3.5.1.3 增加投入加强管理, 确保信息系统安全 204



3.5.2 建设目标	204
3.5.3 建设内容	206
3.5.4 建设计划	206
3.6 SUTER计划	208
3.6.1 Suter计划的背景和现状	208
3.6.1.1 开发历程	208
3.6.1.2 Suter 3概况	209
3.6.1.3 Suter 5 演习情况	210
3.6.2 Suter计划的能力	211
3.6.2.1 能力概述	211
3.6.2.2 能力总结	211
3.6.3 Suter计划的实施细节	211
3.6.3.1 Suter 1计划细节分析	212
3.6.3.2 Suter 2计划细节分析	213
3.6.4 NCCT网络	214
3.6.4.1 概述	215
3.6.4.2 演习情况	215
3.6.4.3 NCCT系统的组成	217
3.6.4.4 NCCT工作原理	218
3.6.4.5 Suter能力在NCCT网络中的实现	218
第4章 经典网络战案例分析	220
4.1 俄罗斯攻击爱沙尼亚---因特网网络战	220
4.2 以色列“电子攻击”叙利亚—战场网络战	223



版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>