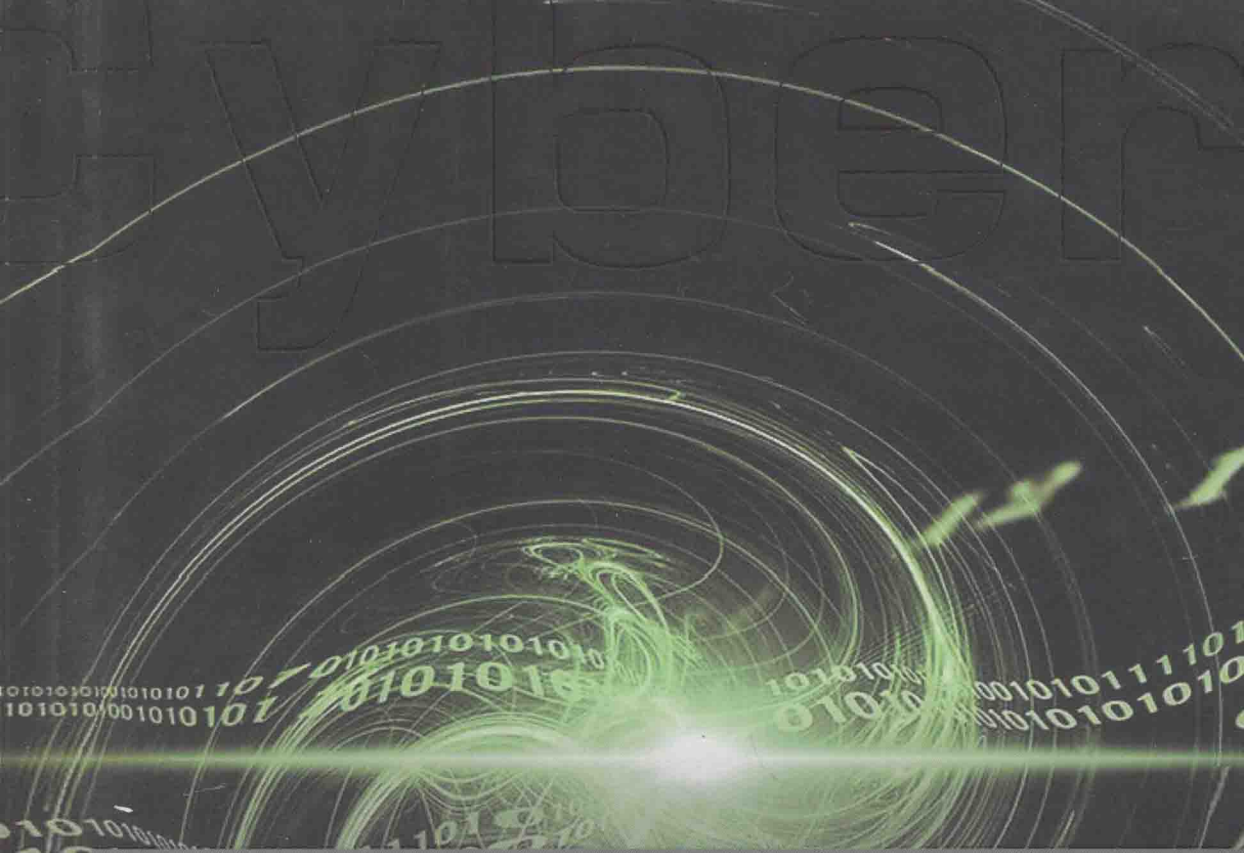

Foreign Armed Force Cyber Operations
Present and Future

外军网电空间战
——现状与发展

马林立 编著

国防工业出版社
National Defense Industry Press

外军网电空间战
——现状与发展

马林立　编著

国防工业出版社
·北京·

内 容 简 介

随着网络技术的发展，网电空间已成为继陆、海、空、天之后又一新的作战领域。世界各国纷纷加强网电空间领域的发展与建设，以期在网电空间的军事竞争中占有一席之地。本书针对这一新领域主要介绍了网电空间及网电空间战的基本概念；论述了近年来各国就网电空间领域发布的相关政策法规与战略；阐述了各国网电空间指挥机构的建设，尤其是美国网电空间相关机构的发展与建设；涉及各国网电部队特别是美军网电部队的建设情况；分析了美军和俄罗斯网电空间能力的现状与发展；讲述了美国网电武器装备的发展与建设；最后介绍了各国在网电测试、训练与演习方面的情况。

本书适合网电空间、网络安全、信息安全专业的技术人员及高等院校有关专业师生阅读参考；也可供军事爱好者作为科普图书阅读。

图书在版编目（CIP）数据

外军网电空间战：现状与发展/马林立编著. —北京：国防工业出版社，2012.9

ISBN 978-7-118-08096-4

Ⅰ. ①外… Ⅱ. ①马… Ⅲ. ①互联网络—应用—信息战—研究—美国 Ⅳ. ①E869

中国版本图书馆 CIP 数据核字（2012）第 103170 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号 邮政编码 100048）

北京嘉恒彩色印刷有限责任公司

新华书店经售

*

开本 710×960 1/16 **印张** 13 **字数** 227 千字

2012 年 9 月第 1 版第 1 次印刷 **印数** 1—4000 册 **定价** 46.00 元

（本书如有印装错误，我社负责调换）

国防书店：（010）88540777 发行邮购：（010）88540776

发行传真：（010）88540755 发行业务：（010）88540717

前　言

随着现代技术的发展，网络正以超乎想象的速度在全球扩张，成为承载政治、军事、经济、文化的全新空间，成为影响社会稳定、国家安全、经济发展和文化传播的无形力量。网络及信息技术以指数速度渗透到社会生活的各个角落，并创造出人类活动的第五维空间——网电空间。网电空间并不等同于计算机网络或互联网，它是“信息环境中的一个全球域，由相互关联的信息技术基础设施网络构成，这些网络包括国际互联网、电信网、计算机系统以及嵌入式处理器和控制器”。

一位美国学者曾指出：“21 世纪掌握制网络权与 19 世纪掌握制海权、20 世纪掌握制空权一样具有决定意义。”世人在对网电空间依赖快步攀升的同时，网电空间给社会和国家安全造成的威胁和风险也日益加剧，已经成为继陆、海、空、天之后又一新的作战领域。

2008 年，“俄格冲突”期间，格鲁吉亚政府网络遭受“蜂群”式网络拒绝服务攻击，造成长时间的网络瘫痪，开创了国家间网络攻防的先河。面对数以万计“蜂群”的狂轰滥炸，能否保持信息基础设施的正常运行，将是网电空间安全防护面临的重大挑战。

2010 年，以西门子数据采集与监控系统为攻击目标的“震网”病毒神秘出现，伊朗境内包括布什尔核电站在内的 5 个工业基础设施遭到攻击，成为运用网络手段攻击国家电力能源等重要关键基础设施的先例。能够“震颤”攻击伊朗核设施的病毒，同样也可以“震颤”攻击这些国家工业系统中的相关控制与采集系统，国家重要的战略网络将面临着平时被控、战时被瘫的巨大风险。

2010 年，传奇人物阿桑奇的“维基揭秘”网站公开了 25 万份美国外交文件，美国陷入“外交 9·11”的恐怖泥潭。随后，“维基揭秘”又成了中东、北非政局动荡的导火索。据悉，一些大国以本土为中心，依托海外基地和太空卫星等，大力构建全球组网、远程操控的网电空间作战体系，以有关国家军政主要网络为目标，大肆进行窃密活动，致使网络环境面临越来越严重的安全挑战。

由此可见，当前网电战场全球化、网电攻防常态化、网电攻心白热化等突出特点，使得如何科学高效地管控网络空间、如何占领第五维空间战略博弈的

制高点等，成为亟待解决的重大课题。

为了在网电空间博弈中获得优势，美国率先采取了一系列措施，如颁布网电空间相关战略，创建网电空间指挥机构，成立网电空间特种部队，加速研发网电空间攻防武器，开展各种网电空间对抗演习等。俄罗斯、德国、法国、日本等主要国家也不甘落后，纷纷将发展网电空间能力提高到了一个新的高度。俄罗斯提出“网络军控”力图遏制美国网电空间能力的发展。北约成立网电防御中心，出台新的网电防御政策，成立网电快速反应部队。德国组建网电空间战部队。法国为加强网电空间作战能力，成立新的信息系统安全局，专门负责预防和应对网电攻击。另外，英国政府发布了首版国家网电安全战略，宣布成立网电安全办公室和网电安全行动中心。印度组建了陆海空三军联合计算机应急分队，日本组建了一支主要由计算机专家组成的网电部队。世界各国网电空间军备竞赛正在如火如荼地进行着。

本书由马林立担任主编，参加编写的有马林立、赵静、邹祝、方志英、贺玉寅、杨茜、李妍、李瑛、何重德、张海翔等。在本书的编写过程中，相关领导和专家给予了大力的支持，科技处田旭等同志也给予了很多帮助，在此向所有为本书做出贡献的同志致以衷心的感谢！

由于本书涉及面较广，要求编写者具有广博的外军网电空间战方面的知识以及深厚的学术与研究积累，而我们的能力和水平与这些要求尚有很大差距。加之经验不足，纰漏在所难免，衷心恳请专家和广大读者批评指正。

编著者

2012.3.1

目　录

第1章 概 述

1.1 网电空间

网电技术的发展，催生了“第五个作战域”——网电空间。这是一个全新的领域，也是“最后的边疆”。未来战争，越来越可能首先在网电空间打响。世界各国纷纷意识到，“网电空间第一战”绝对不能输，否则很难像传统战争那样，“以空间换时间”，东山再起。因此，在依赖网电的21世纪夺取“制网权”，可能与20世纪掌握制空权一样，具有决定性意义。

1.1.1 网电空间的定义及内涵

网电空间一词来自英文“Cyberspace”，关于“Cyberspace”的起源有两种观点，一种认为其由 cybernetics（控制论）和 space 组合而成，另一种认为其由 cyber（网电的、计算机的）和 space 组合而成。其译法也有多种，如“网络空间”、“赛博空间”、“计算机空间”、“网电电磁空间”、“计算机网电空间”、“控域”等。本书将“Cyberspace”一词统称为网电空间。

20世纪90年代，这一概念被引入学术界，当时对赛博的定义与互联网的定义基本相同。进入21世纪以后，随着网电空间对国家政治、经济、社会发展的重要性日益提升，对其认识也不断深化。美国政府和军方多次在重要文件中定义网电空间的概念与内涵。

2001年初美国国防部的“官方词典”——《联合出版物 JP1-02》将网电空间定义为数字化信息在计算机网电中通信时的一种抽象环境。这个定义虽很简洁，但有一定的模糊性。

2003年2月，美国布什政府发布了《保卫网电空间的国家安全战略》，其中将网电空间比喻为“国家中枢神经系统”，它是用光导纤维将成千上万的计算机、服务器、路由器、交换机互联在一起，并支持关键基础设施运行的网电。

2006年12月，美国参谋长联席会议主席签署了《网电空间行动的国家军事战略》，并将网电空间定义为一种“域”，其特征是：使用电子技术和电磁频谱存储、修改和交换信息，并通过网电化的信息系统和物理基础设施达此目的。

该定义重在强调支撑网电空间的技术基础，即电子技术和电磁频谱。

2008 年 1 月，布什卸任前夕签署了两份网电安全的文件，其中对网电空间的定义是：由众多相互依存的 IT 基础设施网电组成，包括互联网、电信网、计算机系统和用于关键工业部门的嵌入式处理器、控制器。这个定义首次明确指出网电空间的范围不限于互联网或计算机网电，还包括了各种军事网电和商用网电。

2008 年 5 月 12 日，美国国防部副部长戈登·英格兰签署的一份名为“网电空间定义”的备忘录指出：网电空间是信息环境中的一个全球域，信息环境是由包括互联网、电信网、计算机系统以及嵌入式处理器和控制器在内的相互依赖的信息技术基础设施组成的。

2009 年，奥巴马上任不久，美国白宫发布了《网电空间政策评审》报告，援引第 54 号国家安全总统令/第 23 号国土安全总统令中的网电空间定义，指出网电空间是由各种信息技术基础设施组成的一个彼此相互依存的网电，包括了互联网、电信网、计算机系统和关键行业中的嵌入式处理机及控制器。

2009 年 4 月，美国国防大学根据美国国防部负责政策的副部长的指示，组织专家学者编写出版了《网电空间能力和国家安全》一书，书中对网电空间的定义作了全面的阐述：

（1）它是一个可运作的空间领域，虽然是人造的，但不是某一个组织或个人所能控制的，这个空间是全人类的宝贵资源，不仅仅是用于作战，还可用于政治、经济、外交等活动，例如，在这个空间中虽然没有一枚硬币流动，但每天都有成千上万美元的交易。

（2）与陆、海、空、天等物理空间相比，人类依赖电子技术和电磁频谱等手段才能进入网电空间，才能更好地开发和利用该空间资源，正如人类需要借助车、船、飞机、飞船才能进入陆、海、空、天空间一样。

（3）开发网电空间的目的是创建、存储、修改、交换和利用信息，网电空间中如果没有信息的流通，就好比电网中没有电流，公路网上没有汽车一样，虽然信息的流动是不可见的，但信息交换的效果是不言自明的。

（4）构建网电空间的物质基础是网电化的、基于信息通信技术的基础设施，包括联网的各种信息系统和信息设备，所以网电化是网电空间的基本特征和必要前提。

2010 年 2 月，美国国防部发布了最新《四年一度防务评审》报告，该报告将网电空间定义为：一个包括互联网和各类电信网电在内的、涵盖所有相互依赖的信息技术基础设施网电的全球域。报告还指出，尽管网电空间是一个人造域，但对美国国防部而言，已是一个与陆、海、空、天四大自然域并列的重要

领域。美军的指挥控制、情报、监视与侦查、后勤保障、武器技术研发与部署无不依赖与网电。

2011 年 7 月 14 日，美国发布《网电空间行动战略》，首次将网电空间列为与陆、海、空、天并列的“行动领域”，美国国防部以此为基础进行组织、培训和装备，以应对网电空间存在的复杂挑战和巨大机遇。这意味着，网电空间将成为美军未来作战的一个重要领域。

从上述概念可以看出，虽然目前理论界在网电空间的概念和内涵上还有不同认识，但是在以下两点看法基本一致：一是网电空间构成要素是网电化的信息基础设施；二是网电空间是完成各种信息活动的主要载体。

尽管从提出至今，关于网电空间的定义表述方式有多种，但是通过对其概念的内涵进行剖析可以发现，网电空间本质上属于环境、域、空间的范畴，并且日益成为与陆、海、空、天同样重要的作战领域。全球网电示意图如图 1-1 所示。

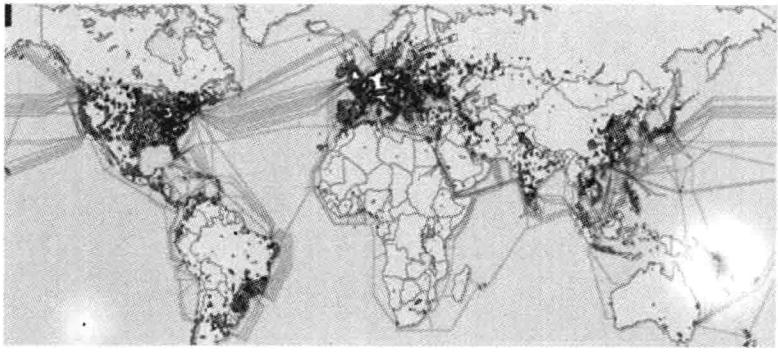

图 1-1　全球网路示意图

1.1.2　网电空间的特征与特点

1. 特征

作为一种域，网电空间具有以下特征：

（1）由公共部门、私有部门以及政府各方创造、保持、拥有和运行，并且全球存在。

（2）随技术、体系结构、流程以及知识技能的共同发展而变化，将产生新的能力和作战结构。

（3）受电磁频谱可用性的影响。

（4）允许进行高速的作战机动，特点是决策信息以接近光速的速度进行移动。

（5）实现跨陆、海、空、天各个域的行动。

（6）超越了传统意义的组织和地理边界。

（7）形成所需要的信息和数据传输系统、支撑关键基础设施、数据存储/处理/传输设备的相互连接以及软件、硬件、应用程序的利用。

（8）包括“静止”和“运动”的数据、语音和视频。

（9）其他国家、组织、伙伴、私营部门以及敌人都能够不同程度地进入这个域。

（10）构成了信息环境的基础。

2. 特点

网电空间具有一些与陆、海、空、天领域所不同的特点，主要包括以下几个方面：

（1）技术创新性。网电空间是唯一能够动态配置基础设施和设备操作要求的领域，将随着技术的创新而发展，从而产生新的能力和作战概念，便于作战效果在整个网电空间作战中的应用。

（2）不稳定性。网电空间是不断变化的，某些目标仅在短暂时间内存在，这对进攻和防御作战是一项挑战。敌方可在毫无预兆的情况下，将先前易受攻击的目标进行替换或采取新的防御措施，这将降低己方的网电空间作战效果。同时，对己方网电空间基础设施的调整或改变也可能会暴露或带来新的薄弱环节。

（3）无界性。由于电磁频谱缺乏地理界限和自然界限，这使得网电空间作战几乎能够在任何地方发生，可以超越通常规定的组织和地理界限，可以跨越陆、海、空、天全领域作战。

（4）高速性。信息在网电空间内的移动速度接近光速。作战速度是战斗力的一种来源，充分利用这种近光速的高质量信息移动速度，就会产生倍增的作战效力和速率。网电空间能够提供快速决策、指导作战和实现预期作战效果的能力。此外，提高制定政策和决策的速度将有可能产生更大的网电空间作战能力。

1.2 网电空间战

1.2.1 网电空间战的定义与内涵

1. 美国对网电空间战的定义

美国国家安全策略第 54 号指令对网电空间战的定义是：网电空间战是基于数字化的作战，旨在对网电空间和其中的数据进行攻击、防御、开发和维护。

根据《联合出版物 JP1-02》，网电空间战是网电能力的运用，主要目的是在网电空间内或通过网电空间实现军事目标或军事效果，包括支持全球信息栅格运行和防御的计算机网络作战和行动。网电空间提供从频谱管理到计算机网络利用、电子战支持、信号情报和网电管理等多种功能，其不断发展的核心能力有5种，即网电空间作战、电磁频谱作战、电子战、计算机网络作战和空间优势。

网电空间战可分为4个任务区域，即网电态势感知、网电维护和防御、网电攻击、网电支持。网电态势感知是核心，也是作战模式从传统指挥向网电领域的延伸。网电攻击包括计算机攻击和通信网电攻击，它是一种攻击作战。而防御不仅仅是保护网电空间，确保己方安全使用网电空间资源，同时要阻止敌方对网电的侵入、破坏和利用。防御与攻击都离不开网电支持，支持行动包括脆弱性评估、安全评估和法律强制等。

网电空间战主要在以下4个层面展开：①信息基础设施，也就是计算机和通信设施的联网，包括有线、无线通信设施，通信卫星，计算机等硬件设备；②基础软件系统，包括操作系统、网络协议、域名解析等；③应用软件系统，包括金融、电力、交通、行政、军事等方面的软件系统；④信息本身，针对在网电中流动的所有信息。严格来说，对信息基础设施的打击应归为广义上的网电空间战，它针对的是网电运行的基础。各个国家和地区在定义网电空间战概念时，并没有将信息基础设施完全纳入网电空间战的范畴，但是，现代战争一旦打响，对信息基础设施的打击却是第一位的。

人类传统的战场是陆、海、空、天，如今，网电空间俨然成了“第五战场”（图1-2）。

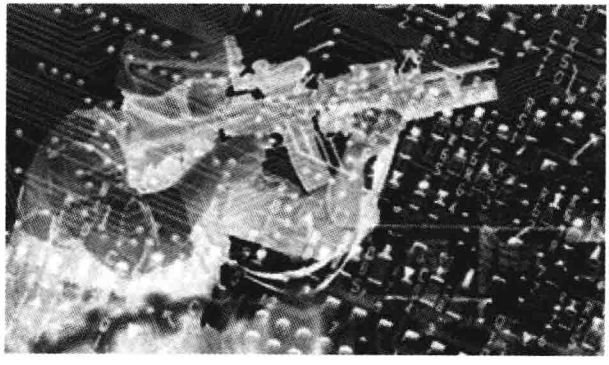

图1-2 网电空间——“第五战场”

2. 俄罗斯对网电空间战的定义

俄罗斯军事学术界认为，网电空间战主要包括在发动传统军事行动之前能

扰乱金融市场、军事和民用通信能力以及敌方其他关键基础设施的战略。它们还包括削弱敌方的经济以便进一步降低敌方对联合威胁的反应能力。进攻性网电武器在俄罗斯网电空间战纲要中受到特别的重视。先进的研发能力使俄罗斯在网电空间战中处于领先地位。俄罗斯网电空间战能力要成为更多传统军事行动包括大规模杀伤性武器攻击的力量倍增器。

虽然美国在网电空间战方面比较积极，但俄罗斯则更加重视电子信息战方面，这点与美国非常不同。俄罗斯所强调的信息战其实是一个更大的范畴，它既涵盖了网电空间战，也包括电子干扰、舆论信息战、太空武器等诸多方面。不过由于美俄在战略问题上还存在着竞争的问题，目前俄罗斯也在紧跟美国的步伐，不排除俄罗斯会形成一个新的网电军事学说，最终把网电空间战从电子信息战中单独规划出来。

1.2.2 网电空间战的特点

网电空间战是信息化条件下以计算机及其网电为基本工具、以网电攻击与防护为基本手段的一种全新的作战样式。网电空间战是在看不见的战场上进行的“软”较量，它充分利用计算机网络的开放性、便捷性和即时性等特点实施网电攻防，具有平时和战时一体化的特点，不仅战时是配合陆、海、空、天各个领域作战的重要作战手段，在平时也可独立实施并可随时发动网电攻击。

网电空间战是一种非常规的作战形式，与传统作战样式相比，网电空间战最大的特点就是“界限模糊”。具体可分成以下 4 个方面：

（1）作战疆域界限模糊。传统战争离不开陆地、海洋、空中和太空等有形空间，而网电空间战是在无形的网电空间进行。

（2）进攻防守等战役战术界限模糊。网电空间成为战场，消除了地理空间的界限，使得前方、后方、前沿、纵深的传统战争概念变得模糊，同时，由于网电技术本身的属性，没有进攻和防守之分，因此攻防界限很难划分。加上网电空间战的战略性、战役性和战术性信息在集成化网电环境中有序流动，呈现出紧密互连、相互融合的特点。这势必使得网电空间战的战略、战役、战术界限模糊，日益融为一体。

（3）参战“兵”“民”界限模糊。与传统战争中的部队、老百姓界限分明不一样，网电空间战中，专职网电部队官兵、民间黑客、学界专家等各类人群可能混在一场网电空间战中，就是美国的网电部队，也并非全部都是现役军人，还包括中情局特工、民间招募的黑客等人群。

（4）国家网站实力界限模糊。传统战争中，国家与国家之间，一般实力比较分明，可以分析得很透彻。这是因为传统战争的实力，是靠综合国力以及多