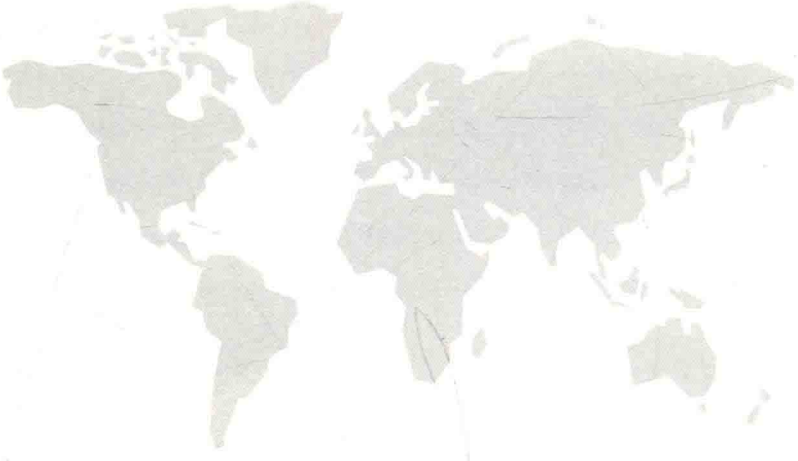
世界国防科技年度发展报告（2016）

网络空间与电子战领域科技发展报告

中国电子科技集团公司发展战略研究中心



国防工业出版社
National Defense Industry Press

世界国防科技年度发展报告（2016）

网络空间与电子战领域科技发展报告

WANG LUO KONG JIAN YU DIAN ZI ZHAN LING YU KE JI FA ZHAN BAO GAO

中国电子科技集团公司发展战略研究中心

国防工业出版社

·北京·

图书在版编目（CIP）数据

网络空间与电子战领域科技发展报告/中国电子科技集团公司发展战略研究中心编. —北京：国防工业出版社，2017.4

（世界国防科技年度发展报告.2016）

ISBN 978-7-118-11278-8

Ⅰ.①网… Ⅱ.①中… Ⅲ.①电子对抗—科技发展—研究报告—世界—2016 Ⅳ.①TN97

中国版本图书馆 CIP 数据核字（2017）第 055326 号

网络空间与电子战领域科技发展报告

编　　者	中国电子科技集团公司发展战略研究中心
责任编辑	汪淳　王鑫
出版发行	国防工业出版社
地　　址	北京市海淀区紫竹院南路 23 号　100048
印　　刷	北京龙世杰印刷有限公司
开　　本	710×1000　1/16
印　　张	12¾
字　　数	145 千字
版 印 次	2017 年 4 月第 1 版第 1 次印刷
定　　价	76.00 元

《世界国防科技年度发展报告》(2016)

编 委 会

主　　任　刘林山

委　　员（按姓氏笔画排序）

卜爱民　王　逢　尹丽波　卢新来
史文洁　吕　彬　朱德成　刘　建
刘秉瑞　杨志军　李　晨　李天春
李邦清　李成刚　李晓东　何　涛
何文忠　谷满仓　宋志国　张英远
陈　余　陈永新　陈军文　陈信平
罗　飞　赵士禄　赵武文　赵相安
赵晓虎　胡仕友　胡明春　胡跃虎
真　溱　夏晓东　原　普　柴小丽
高　原　席　青　景永奇　曾　明
楼财义　熊新平　潘启龙　戴全辉

《网络空间与电子战领域科技发展报告》

编 辑 部

主　　编　李　晨

副 主 编　彭玉婷　李　硕

此为试读,需要完整PDF请访问: www.ertongbook.com

《网络空间与电子战领域科技发展报告》

审稿人员（按姓氏笔画排序）

朱德成　刘　建　关　松　李　晨
陆安南　臧维明

撰稿人员（按姓氏笔画排序）

于晓华　王　浩　王　燕　王龙奇
王晓东　石　杨　石　岚　朱　松
伍尚慧　刘　建　苏建春　李　硕
吴明阁　吴静静　沈　涛　张春磊
陈　越　陈柱文　范振宇　费华莲
常晋聃

编写说明

军事力量的深层次较量是国防科技的博弈，强大的军队必然以强大的科技实力为后盾。纵观当今世界发展态势，新一轮科技革命、产业革命、军事革命加速推进，战略优势地位对技术突破的依赖度明显加深，军事强国着眼争夺未来军事斗争的战略主动权，高度重视推进高投入、高风险、高回报的前沿科技创新。为帮助对国防科技感兴趣的广大读者全面、深入了解世界国防科技发展的最新动向，我们秉承开放、协同、融合、共享的理念，共同编撰了《世界国防科技年度发展报告》(2016)。

《世界国防科技年度发展报告》(2016) 由综合动向分析、重要专题分析和附录三部分构成。旨在通过深入分析国防科技发展重大热点问题，形成一批具有参考使用价值的研究成果，希冀能为促进自身发展、实现创新超越提供借鉴，发挥科技信息工作“服务创新、支撑管理、引领发展”的积极作用。

由于编写时间仓促，且受信息来源、研究经验和编写能力所限，疏漏和不当之处在所难免，敬请广大读者批评指正。

中国国防科技信息中心

2017 年 3 月

前　言

随着无线技术与万物互联技术的飞速发展，网络空间与电磁频谱空间逐渐成为陆、海、空、天、水下以外的独立作战空间，成为国际战略新的竞争制高点，主要军事大国围绕网络空间与电子战领域的战略博弈日趋激烈。为此，密切跟踪分析世界范围内网络空间与电子战领域科技发展，掌握评估国际网络空间和电子战战略态势，应对网络空间安全和电磁频谱安全威胁与挑战，维护国家安全，推动我国网络空间和电子战领域建设与发展，具有重要意义。

本书系统梳理了2016年网络空间与电子战领域科技发展的基本情况，目的是供领导机关及科研一线人员及时准确、系统全面地掌握国外网络空间与电子战领域的发展动向。本书内容包括综合动向分析、重要专题分析和附录三部分：综合动向分析主要对2016年网络空间与电子战整个领域及各分领域发展情况进行系统梳理；重要专题分析针对重点问题、热点技术展开深入研究；附录则对2016年网络空间与电子战领域发生的大事进行了简要记录。

本书由中国电子科技集团公司发展战略研究中心牵头，在统一编撰思想的指导下，以“小核心、大外围”的组织方式，由中国电子科技集团公司第二十七研究所、第二十九研究所、第三十六研究所、第五十一研究所、第五十三研究所等相关单位的专家共同完成。

由于时间仓促，编者水平有限，难免存在错误和疏漏之处，敬请领导、专家和广大读者批评指正。

编者

2017年3月

目　录

综合动向分析

重要专题分析

附录

ZONGHE

DONGXIANGFENXI

综合动向分析

此为试读，需要完整PDF请访问：www.ertongbook.com

2016 年网络空间与电子战领域科技发展综述

2016 年，网络空间与电子战继续成为全球军事重点发展领域，在战略、技术和应用上呈现活跃态势。

在网络空间领域，2016 年网络空间安全重大事故频发，网络攻击、网络勒索持续升级，针对关键信息基础设施和工业系统的攻击影响巨大，黑客攻击事件密集发生且成为大国博弈的新形式。军事大国纷纷加快在网络空间的军事部署，积极推进网络空间作战装备技术发展。

在电子战领域，随着电磁频谱作战域的逐步确立，电磁频谱正成为与陆、海、空、天和网络空间并列的独立作战域。2016 年，全球电子战持续发展。美国高度重视电磁频谱优势，俄罗斯研发并装备了大量电子战新装备，全球电子战进入新一轮高速发展期。

一、网络空间

2016 年，在大数据、云计算、人工智能等技术的驱动下，网络空间态势感知、防御和攻击技术都在蓬勃发展，未来更多学科的技术融合或将为

网络空间技术带来一次“革命性”的发展。特别的，在军事应用方面，美军已经在战场态势感知和防御方面拥有了一定技术优势，未来网络空间与电子战在技术战术的进一步融合或将真正实现全频谱的“网络空间电磁行动”。

（一）基于大数据、可视化等技术的网络空间态势感知趋向成熟

在大数据、云计算、可视化技术的助推下，在网络空间态势感知技术与传统电子侦察、定位技术越发紧密地结合下，美国当前已具备相当成熟的网络空间态势感知能力，未来或将具备覆盖网络空间及电磁频谱的全局、多维态势感知能力。

一是利用大数据和云计算技术提升网络空间态势感知能力。2016 年 5 月，美国国防信息系统局（DISA）公布了一整套基于云的“网络分析态势感知能力”（CSAAC）方案，可对国防部信息网络（DoDIN）中的海量数据进行收集、分析、可视化处理，为网络分析人员及作战人员提供一种审视 DoDIN 活动的全新综合性视角。

二是利用可视化技术提升网络空间态势感知能力。可视化技术作为一项提升作战人员直观认知网络空间、简化作战操作流程的技术，也已通过美军近几年着重打造的网络空间基础性研发项目“X 计划”日趋成熟。“X 计划”能够从技术上完成对战场网络空间的基础建构，使作战人员能够在直观界面上应对敌方网络空间攻击，达到降低网络空间作战门槛的效果。2016 年 6 月，“X 计划”首次走出实验室进入实战应用阶段，如后续进展顺利并按既定时间交付军方，必将对未来美军战场的网络空间攻防能力带来不可估量的提升。

三是打造网络空间和电磁频谱共享的态势感知能力。2016 年，美国陆军推出开发基于软件的网络空间态势感知样机项目，旨在获得包括己方、

友方、敌方在内的完整战场网络空间态势感知图，为旅级指挥官提供量身定做的、及时的态势感知数据，简化基于风险的决策过程。雷声公司也推出可提供电子战、电磁频谱、网络空间共享态势感知的网络空间及电磁战场管理（CEMBM）系统。

（二）针对军用系统及网络的网络空间防御技术发展迅猛

与态势感知技术一样，军用系统及网络的网络空间防御也是美军当前发展的重点之一，美军正在针对己方军用系统和网络开展大规模的网络空间防御技术和系统研发，提升作战中的网络空间安全性，确保作战胜利。

一是强化作战平台信息系统的网络空间安全。重点从日常操作规程和填补信息系统漏洞方面确保武器系统满足网络空间安全要求，为此美军发起了“网络卫生”“武器系统弹性网络战能力”等项目。

二是开发针对军用系统及网络的网络空间防御系统。例如，美国国防高级研究计划局（DARPA）持续推进的“高保证网络空间军用系统”（HACMS）项目，通过系统各层的重新架构、设计和安全软件加载等生成开源、高保证、网络使能的军用航空器平台，从而抵御包括针对加密和认证、利用软件漏洞、利用无人机外部通信接口等发起的各种网络空间攻击。此外，美国海军“武器系统弹性网络战能力”项目和美国空军“红旗”军演中“决战”公司的网络运作平台，都侧重实现军用系统及网络的恶意软件检测、保护、响应和恢复能力。

三是发布被视为“网络武器”的网络空间防御系统。2016 年，美国空军先后发布了两款被视为“网络武器”的系统，即“美国空军内联网控制”（AFINC）和“网络空间脆弱性评估/猎人”（CVA/H）。虽然这是两款被美国空军作为“武器”推出的网络系统，但两者都是网络空间防御系统，前者作为空军内联网最顶层防御边界及接入美国空军内联网的所有数据入口，

后者可执行美国空军信息网的脆弱性评估、威胁探测和合法性评估等。

（三）人工智能或为网络空间攻防带来突破性能力

人工智能技术的发展在2016年引起了全球的高度关注，其在网络空间攻防领域的应用同样值得关注。人工智能在网络空间攻防领域已经具备了一定的技术积累，技术的进一步成熟或将给未来网络空间攻防两端都带来突破性的能力，打破传统的网络空间攻防模式，改变整个网络空间的存在样式。

一是自主加密。谷歌公司的“谷歌大脑”团队2016年10月成功通过三个神经网络的相互攻击，让系统创建属于自己的算法。名为“鲍勃”（Bob）和“爱丽丝”（Alice）的两个神经系统自行开发出共享的安全密钥并彼此收发消息，而第三个名为“夏娃”（Eve）的神经系统试图窃取并解码消息，但最终没能成功窃取信息，证明了机器学习与神经网络实现自主加密的可行性。

二是自动漏洞检测及修复。2016年8月，在DARPA举行的“网络空间大挑战”中，诸多“机器人黑客”都在一定程度上展现了使用不同人工智能方法自动检测软件漏洞并自行修复漏洞的能力，但实际操作中出现了长时间处于休眠或不小心破坏所保护系统的情况。

三是自动漏洞利用及攻击。在上述“网络空间大挑战”中，“机器人黑客”也展现出了一定程度的利用漏洞进行攻击的能力，这种基于人工智能技术的网络空间攻击或将大大提升网络空间攻击的效率以及多手段综合攻击的能力。

四是恶意软件行为学习。2016年8月举行的“黑帽”大会上，“火花认知”安全公司发布的杀毒软件“深度装甲”，利用自动建模算法等人工智能技术不断了解新恶意软件的行为，可识别病毒发生变异以尝试绕过安全系

统的过程。

五是物联网安全。2016 年 7 月，PFP 网络安全公司推出了基于电力使用分析、机器学习和云技术，可探测供应链、内部篡改、持续攻击等各种异常的方案，用于防护任何连接物联网的设备（数据中心、电网、移动/智能设备等）。

（四）美军发展用于体系对抗的网络空间攻击能力

从早前揭露的“舒特”计划至今，美军虽然一直对其拥有的具体网络空间攻击技术或系统讳莫如深，但根据美军 2016 年诸多表述和项目可以看出，美军已具备并正在加速开发可用于战场体系对抗的网络空间攻击能力。

2016 年 2 月，时任美国国防部长卡特和参谋长联席会议主席邓福德在国会证词中称，美国在对叙利亚境内极端恐怖组织“伊斯兰国”的军事打击行动中，运用网络战武器破坏敌方的指挥控制与通信系统。此外，美国国防部据称还在开发在敌方导弹系统发射前施行非动能攻击的网络空间武器，攻击敌导弹系统的计算机、传感器和网络。2016 年 7 月，美国海军官员表示，潜艇也是美国网络战略的重要组成部分，或将把潜艇用作水下无人潜航器母舰，利用后者机动抵近近岸处执行干扰和网络空间攻击行动。2016 年 10 月，美国海军空中系统司令部（NAVAIR）网络战特遣部队授予麦考利·布朗公司合同，为美国海军飞机、武器和相关航空系统及子系统提供网络战能力，其中就包括网络渗透工具开发、全频谱的作战级网络战支持等。

从美军透露的以上消息来看，美军或已具备破坏敌方通信、指挥控制系统的网络空间攻击能力，而且正在发展空中、水面、水下的网络空间攻击技术，以实现体系化的战场打击。从技术上看，美军的战场网络空间攻击能力与电子战联系紧密，无论是“全频谱作战”的表述，还是从对“伊

此为试读，需要完整PDF请访问：www.ertongbook.com