

# 美赛博空间作战进展研究

刘建强<sup>1</sup>, 杨作宾<sup>1</sup>, 郭诗军<sup>2</sup>, 肖大海<sup>1</sup>, 孟宪刚<sup>1</sup>

(防空兵学院 郑州 450052; 71521 部队司令部信息化处 453000)

**摘要:** 自美国建立“赛博空间司令部”以来, 在世界范围内掀起了组建网络部队的浪潮。本文分析了赛博空间概念的演化, 对美赛博空间的国家战略和军事战略以及正在进行的武器研究计划进行了分析, 可以为我们做好赛博空间的积极防御提供思路和借鉴。

**关键词:** 赛博空间 作战 进展

## 0. 引言

自美国提出赛博空间<sup>[1]</sup>以来, 赛博空间问题已经引起世界多个国家广泛关注, 成为热议的重点问题。从美国关于赛博空间的理论与实践情况来看, 美军已经着手制定赛博空间及其作战的一系列发展战略。本文试图分析美国相关情况的最新进展, 为我们做好赛博空间的安全提供借鉴。

## 1. 美赛博空间作战概念

所谓赛博空间作战, 是指在赛博空间进行的作战行为。“赛博空间”一词来自英文 Cyberspace, 其译法也有多种, 如“赛博空间”、“网络空间”、“计算机空间”、“计算机网络空间”<sup>[2]</sup>、“控域”等。本文中对上述译法不加区别, 统一称之为赛博空间。其概念也经历了狭义物理域、广义物理域和综合域三个阶段。

**狭义物理域定义:** 在 2003 年的《赛博空间国家战略》中, 将赛博空间定义为“国家关键基础设施的中枢神经, 由成千上万互联的计算机、服务器、路由器、交换机、光纤线路组成, 并使美国的关键基础设施能够正常工作。”将赛博空间界定为物理设施的集合。

**广义物理域定义:** 2006 年的《赛博空间作战国家军事战略》指出:“赛博空间是指利用电子和电磁频谱, 经由网络化系统和相关物理基础设施进行数据储存、处理和交换的域”。认为赛博空间不仅仅包括物理设施, 还包括了依托其运行的电子和电磁频谱领域。

**综合域定义:** 2009 年的《美国赛博空间政策评估》将赛博空间定义为“全球互联的数字信息和通信基础设施, 包括互联网、计算机系统, 以及嵌入其中的处理器和控制设备, 通常还认为其也指信息和人类交互的虚拟环境”。这一最新定义认为赛博空间既包含物理基础设施, 又包含电子系统和电磁频谱, 涵盖承载信息交换的虚拟电磁环境。

随着美对赛博空间内涵的不断扩展, 赛博空间作战的范围也随之扩大。

## 2. 美赛博空间作战战略

美国一直注重赛博空间的战略制定。本世纪以来, 美国发布了多个战略。2011 年, 美国政府相继发布《赛博空间国际战略》、《赛博空间行动战略》、《赛博空间政策报告》等文<sup>[3]</sup>件, 标志着美国赛博空间的国家战略和军队赛博作战战略基本成型。

### 2.1 美国赛博空间国家战略特点

#### 2.1.1. 强调多部门合作

美国政府下属有六大网络安全专职机构, 它们分别隶属于国土安全部、联邦调查局、国家情报总监办公室、国家安全局和国防部。自奥巴马上任以来, 他始终强调网络安全领导机制的集中与全面协调, 坚持“从最高层实施领导”, 2009 年成立了全国通信与网络安全控制联合协调中心。其主要职能是综合分析并上报美国赛博空间的整体运行状况。并于 2011 年在白宫设立了“网络安全办公室”和“网络安全协调官”,

全面统领国家的网络安全事务，欲打破过去各自为政、职能重叠、条块分割严重状况。

### 2.1.2. 将“网络自由”凌驾国家主权之上

新战略首次明确将互联网自由纳入维护网络安全政策体系内。美一直重申，言论自由和信息的自由流动既是美国做出的核心承诺，又是整个战略的基本出发点和目标。在具体政策上，美国要以资助尖端科技的方式为那些受到限制的人提供工具，为民间社会行动者提供可靠、安全的言论自由的平台；加强民间团体和非政府组织合作，制定保障措施保护互联网活动不受非法数字入侵；鼓励有效保护商业数据隐私的国际合作。

### 2.1.3. 加强国际合作

新战略的视角把国际合作作为贯彻所有领域的“主线”，换言之，美国认为网络安全所有领域的问题都需要通过国际合作来解决。美国已与澳大利亚、加拿大、新西兰、英同、北约等开展网络安全合作，并将加强与日本、韩同的合作。美国还要与主要战略对手在赛博空间问题上建立互信机制，增加彼此透明和互信，管控危机，防止误判和冲突升级。美国已与俄罗斯在现有战略对话机制下建立网络安全对话机制，并提出与中国建立网络安全对话机制。

尽管该战略在总体是比较温和，但是，美国在该战略中也向外界传达了两个明确信号，一是赛博空间国际规则的制订美国要说了算，二是美国有能力采取所有可能的手段、包括军事打击来应对危及其国家利益的网络攻击。美国在赛博空间的强硬和霸气源自其独一无二的信息优势。

## 2.2 美军赛博空间行动战略

为了完成国家战略赋予军方的任务，美国防部于 2011 年 7 月发布了《赛博空间行动战略》。该战略以五大支柱为核心，也即五大策略。

### 2.2.1. 重视赛博空间作战

美国明确将赛博空间与国防部此前关注的陆地、领空、水域以及太空相提并论，这意味着赛博空间将成为美国军事力量在其中采取“行动”和“防御”的一个领域，国防部以此为基础进行组织、培训和装备，以应对赛博空间存在的复杂挑战和巨大机遇。

### 2.2.2. 积极防御

即变被动防御为主动防御，从而更加有效地阻止、击败针对美军网络系统的入侵和其他敌对行为。根据林恩的解释，这意味着传感器、软件和数字签名等方式在“有害代码对我们的行动造成损害之前”就“侦测”并“阻止”之。这个含糊其辞的“积极防御”涵盖了此前引发争议的两项内容：美国网络司令部有权对境外计算机发动“先发制人的行动”，以及更加具有争议性质的“用炸弹回击黑客袭击”。由于林恩使用的是无法判断其攻击、防御性质的“行动”一词，因此最极端的情况是，美国会在对其他国家采取常规军事打击行动之前，首先通过网络攻击瘫痪对手的网络系统，从而使得对手无法通过攻击美军的指挥通讯控制系统以及美国国内的关键基础设施，来阻滞美国的“行动”。

### 2.2.3. 加强国内合作

加强国防部与国土安全部等其他政府部门及私人部门的合作，在保护军事网络安全的同时，加强重要基础设施的网络安全防护。行动战略强调国防部要与国土安全局等部门合作，要与从事关键基础设施软硬件生产的公司进行兼顾规范性和资源性质的合作。行动战略特别强调指出，由于大量软硬件产品生产过程中存在广泛的“外包”行为，“外包”厂商的安全资质，将构成重要的关注对象。显然今后从事相关生产的企业，无论是美国企业还是非美国企业，恐怕多少都难免以某种方式和国防部打点交道了。。

### 2.2.4. 加强国际合作

加强与美国的盟友及伙伴在赛博空间领域的国际合作。此前林恩也已经在北约峰会等场合演讲过不少次，参考美国冷战时期通过和英国、澳大利亚、新西兰、加拿大签订《五国情报交换协议》组建“梯队系统”的先例，某种覆盖全球赛博空间的新型梯队系统至少已有了一定的基础和雏形。

### 2.2.5. 重视科技创新

重视高科技人才队伍建设并提升技术创新能力，包括强化网络防御人员培训，削弱赛博空间匿名性和网络安全防护普遍松弛给“黑客”攻击带来的便利。

### 3. 美赛博空间作战武器

赛博空间作战武器主要包括：病毒、蠕虫、木马以及相关的平台技术等，主要可以分为侦察预警类、攻击防御类和作战支援类<sup>[4]</sup>，如“逻辑炸弹”、“网络飞行器<sup>[5-7]</sup>”等。美国一直在不断增加投入，2012年5月30日，美国国防部高级防务计划研究局（DARPA）对外宣布将开始一项名为“X计划”（又称“X数据计划”，Plan X）的赛博空间作战武器研发项目。

#### 3.1. 基本情况

“X计划”将赛博战场定义为3个主要概念：网络地图、作战单位和能力集。

网络地图是由点和边构成，显示计算机如何进行连接，协助军事规划者和操作者进行互动。

作战单位是指用于船舶、飞机和装甲战车的平台，是网络拓扑结构的一部分，主要分为两种类型：入口节点和支持平台。入口节点提供了直接的网络物理连接，而支持平台控制不同方面的操作，类似空中作战时军事战斗机、轰炸机、无人机等不同方面的控制。

能力集涉及赛博战场控制技术，可分为三大类：接入、功能和通信。接入技术使用户能够运行程序或有效载荷。功能技术涉及影响计算机和网络的其他技术，如网络扫描、拒绝服务（denial-of-service）、防御规避、网络和主机的侦察以及操作系统控制。通信技术将帮助入口节点、支持平台和功能系统之间进行信息交换。

#### 3.2. 主要研究内容

“X计划”寻求将这3个赛博战场概念整合到军事赛博操作中，开发一种整合政府和行业技术的开放式平台架构。该计划主要包括三个研究项目。

##### 3.2.1. 建立一个整体赛博空间态势图。

该图将以国际互联网为基础，把整个赛博空间由计算机、智能手机、服务器、路由器及其他相关设施组成的上百亿个节点尽收其中，从而保证网络战计划者可实时感知赛博空间敌我态势。虽然美国相关报道就此使用了Map一词，但不应将它简单理解为“数字化地图”。根据研发要求，这一赛博空间态势图系统将具有以下功能：其一，标定赛博空间每个节点的敌我属性。其二，网络态势图也要实时自我更新。其三，确定赛博空间每个节点的功能属性，特别是那些各国用以控制信息基础设施的重要节点。其四，分析和掌握赛博空间每条网路容量大小，能否承载网络武器，这将有助于美军网络战指挥员根据流量大小决定网络作战时的目标、网路和手段选择。最后，在人力等其他情报手段的支持下，确定赛博空间态势图中重要节点在地理空间的对应关系。

##### 3.2.2. 开发一个实时、灵敏、快速、精确的网络战指挥控制系统。

为适应赛博空间作战的高度复杂性和多变性，DARPA的“X计划”研发的这一多任务指挥控制系统系统具有以下功能和特点：其一，反应速度快。它使网络战指挥员可根据预先设定的想定预案，对所遭受的网络攻击源以光速发动反击，从而避免使用缓慢的人工输入代码方式。其二，精确、实时的态势评估和结果预测。借助网络态势图实时掌握网络战态势变化，该系统可对网络进攻结果自动进行量化的精确预测。其三，实时调整网络战的强度、进程和节奏。在网络攻击时，美军网络战指挥员可根据需要控制敌方关键基础设施的计算机系统，关闭或重新开启，还可随时根据态势评估改变网络武器的攻击路径，或根据后果预测，在其对非计划目标造成损害前令其停止攻击。

##### 3.2.3. 研发一套拥有强大网络战攻防能力的操作系统。

这种新的操作系统最大的特点就是强大：可对敌方发动强大的网络攻击，同时可承受对方的强力反击。现有操作系统虽然很好用，但不抗打。犹如一辆SUV运动越野车，在高速公路上可以跑得很快，但却上不了战场。与之相比，新的操作系统就是“网络坦克”。美军前参联会副主席詹姆斯·卡特莱特将军提出：不应幻想能找到某个完美目标，一击便可结束战争。这种目标不存在。美军需要的是可在尽可能短的时间内干掉上千目标的手段。

美国推进以维护霸权为目的的赛博空间战略，将改变国际赛博空间的现有格局，使各国在赛博空间中的安全与处境面临新的挑战。美军在赛博空间的扩张可能导致赛博空间军事化，我们必须早做应对。

参考文献:

1. 赵捷,赵宝献,王世忠.关于赛博空间与赛博空间作战问题的思考[J].中国电子科学研究院学报.2011 (6) 3: 235-239
2. General Dynamics Computer Network Defense:Protecting net-centric information systems[D-CND-1-0406]
3. 郝叶力. 美国网络空间安全战略发展脉络[M].北京: 国防大学出版社.2012.01
4. 王源 张博. 赛博武器的现状与发展[J]. 中国电子科学研究院学报. 2011 06(3) : 221—226
- 5.DANITL KARRELS.White Paper:CyberCraft C3 Architectrue[R].2008
- 6.刘红军. 赛博空间武器——赛博飞机[J]. 中国电子科学研究院学报. 2011 06(3) : 248—251
- 7.MICHAEL STEVENS,PAUL D. Williams.Integrating Trust into the CyberCraft Initiative via the Trust Vectors Model[R].2008