

# 赛博空间指挥控制与态势感知

李冬

(海军航空工程学院指挥系 副教授)

摘要: 指挥控制是赛博空间作战的核心环节,赛博空间态势感知是海上赛博战的重要组成部分,从赛博空间的概念和态势感知的流程出发,构建赛博空间态势感知概念框架,重点研究了赛博态势评估模型。

关键词: 赛博空间; 指挥控制; 态势感知; 效能评估

## 0 引言

20 世纪 90 年代,随着互联网技术的高速发展,美国军事理论界隐约感到:相比于 20 世纪初期无线电技术对军事领域的冲击,20 世纪末期互联网技术带来的信息革命,对军事领域的大规模战争和小规模冲突产生了更大的影响。于是,在以无线电通信和雷达为主要作战对象的传统的“电磁空间”和“电子战”的基础上,出现了“网络空间”和“网络战”。随着无线射频和互联网融为一体的无线宽带互联技术的日趋成熟,应用于军事领域的战场无线互联地位日益凸现,连接着战场上从传感器到火力打击等作战和保障的各种移动平台,主宰着未来战场从“情报获取、作战指挥、武器控制和综合保障”的作战流程,决定着“传感器——射手”的打击链时间,从根本上撼动了以传统“动能+火力”为主要作战方式的军事理念,使未来的作战模式和指挥控制方式发生了革命性的变化。在这样的背景下,就出现了“赛博空间”和“赛博战”。进入 21 世纪以来,美军发布了《赛博空间行动国家军事战略》、《四年防务评估报告》等多个重要文件,对赛博空间的内涵及重要性做了阐述,要求美军夺取赛博空间优势。近来,随着美军组建赛博司令部、扩编赛博空间作战力量、颁布相关政策法规、接连举行赛博空间演习,赛博空间已成为当前世界军事领域的热点、前沿问题。

赛博态势感知是目前需要解决的一项重要挑战。从某种意义上讲,实现有效的态势感知要比主动防御等其他安全措施更加困难。美军赛博司令部司令官基思·B·亚历山大中将认为,赛博态势感知对有效的赛博安全具有致命性的影响,要应对当今的赛博挑战,规划人员必须应用软件可视化能力,洞察赛博空间的各个方面。“我们必须让参与运行和防御赛博空间的人员能够以一种直观的方式来审视赛博空间。”

随着信息技术和网络技术的最新成果不断应用于军事领域,赛博战在海战场上将发挥越来越大的作用。赛博空间态势感知是海上赛博战的重要组成部分,它为指挥员提供完备、准确、及时的赛博空间态势信息,是展开赛博作战行动的最直接依据。因此,认真研究赛博空间指挥控制问题,分析赛博态势感知的概念模型、体系框架、关键技术,对于我海军未来在海上履行多样化使命任务,打赢未来信息化条件下的海上战争具有重要的理论和实际意义。

## 1 赛博空间指挥控制

### 1.1 赛博空间作战

赛博空间(Cyberspace)通常被翻译为网络空间、网电/网络电磁空间、控域等,但其内涵已远远超出了通常意义上的网络空间,我们更倾向于使用其音译词赛博空间。赛博空间作战标志着美军作战发展的新认知。

赛博空间不同于传统的计算机网络,主要由电磁频谱、电子系统和网络化基础设施三部分组成。电磁频谱涵盖现有通信和雷达使用的频率,是计算机网络在无线通信领域和无源探测领域的扩充。电子系统除了传统的计算机系统外,还包括片上微系统和嵌入式系统等,网络化基础设施包括传统的计算机网络,还包括通信网、电力网、指控网、工控网和传感器网等。

赛博空间是以网络系统、电子设备和电磁频谱等物理基础为依托的作战空间,是以网络攻击、信息作

战、电磁频谱争夺等手段，以夺取网络、电磁频谱和信息的控制权，从而影响和主导战争的进程和结局为目标的新型作战领域。赛博空间作战则是指基于电子设备、电磁频谱设施和网络系统组成的广义网络系统和空间实施的信息域的“控制”，其目的一定程度上是实现制信息（包含网络）权和提高赛博空间行动效率，进而为夺取陆、海、空、天等物理空间的优势和实施有效控制创造条件。与传统的陆、海、空、天作战相比，其突出特点表现在作战力量的广泛性、作战空间的广阔性、作战时间的连续性、作战手段的知识化和作战过程的突变性。

赛博空间作战，既非传统意义上的常规作战，也不同于电磁空间作战或计算机网络战，它是在虚幻与现实、个体与网络、物理实体与人的行为紧密结合的新的动态空间中的对抗，具有虚拟性、智能性、互动性、流动性、无界性、对抗性等特点，对作战指挥控制提出了新的挑战。

## 1.2 赛博空间指挥控制

赛博空间指挥控制是指赛博空间作战指挥员和指挥机构对赛博空间作战力量的组织、筹备和部署，以及在作战过程中为适应对手、环境、作战节奏和进程变化而实施的调整和控制。显然，赛博空间指挥控制也包含作战之前的筹划部署和作战过程中的协调控制两个环节。赛博空间指挥控制的根本目标，是实现制信息（包含网络）权和赛博空间作战力量作战效能的最大化，最大限度的发挥赛博空间作战力量的战斗力，提高赛博空间行动效率。

指挥控制是赛博空间作战的核心环节，涉及到新型作战样式下指挥控制机理、赛博空间作战力量建设及其作战运用等多个环节多层次因素。赛博空间和赛博空间作战的特点，一定程度上也决定了赛博空间指挥控制的特点，突出体现在赛博空间指挥控制的复杂性。

赛博指挥控制系统主要用于支持赛博空间作战指挥，满足赛博防御和赛博进攻作战需求。按照美国空军设想，该系统应具备完善的赛博态势感知和指挥控制能力，要能够实时监视全球信息栅格空军子网的任何网络活动，一旦探测到受攻击迹象，立即向赛博安全部门发出警报，并自动采取措施减轻网络受损害程度。除了具备传统指控系统的任务排序、战场毁伤效果评估等基本功能外，赛博控制系统还具备实时分析能力，能够根据敌方攻击类型、己方受损害程度等信息进行辅助决策，为赛博作战人员提供最优的响应策略。响应策略不仅包括赛博作战建议，甚至还包括可能的传统作战手段。

## 2 赛博态势感知

赛博态势感知是指由赛博空间中所有电子设备和系统的运行状况、设备行为以及用户行为等因素所构成的整体安全状态和变化趋势，是对在整个赛博空间和电磁频谱内遂行的己方、对手以及其他相关行动信息的即时理解。获得赛博态势感知需要对赛博空间、电磁频谱以及其他领域内的情报和作战行动进行综合分析，对能够引起赛博空间态势发生变化的所有环境要素，进行获取、理解和评估，并预测其发展趋势。

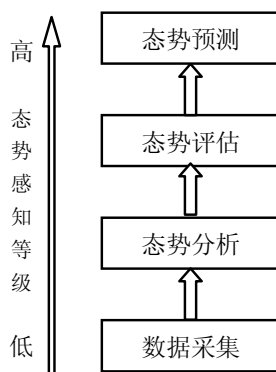


图1 赛博态势感知流程

赛博态势感知是所有赛博空间活动的基础,因此应当优先发展部署赛博态势感知技术和装备,探索发现并智能分析我军敌友赛博空间脆弱点的理论和方法,研究对敌方赛博能力和意向进行分析预测的途径,为我军各级赛博作战提供辅助决策的手段。

在网络安全态势感知的流程的基础上,给出赛博态势感知的概念模型,如图 1 所示赛博态势感知流程包括数据采集、态势分析、态势评估和态势预测四个部分。

数据采集是通过各种检测工具,对影响赛博空间安全的所有要素信息进行采集;态势分析是对各种赛博空间安全要素数据进行处理,分析影响赛博空间的安全事件;态势评估定性定量分析赛博空间当前的安全状态和薄弱环节,并给出相应的解决方案;态势预测预测赛博空间安全状况的发展趋势。

## 2.1 数据采集

数据采集是态势感知的前提。数据采集的目的是获取态势感知所需的各种数据,包括网络化基础设施的拓扑结构、己方电子系统和设备运行状态、敌方的电磁干扰和各类入侵等数据。安全检测对赛博空间内敌我双方电子系统和设备运行状态、信息资源和设备的薄弱环节、赛博武器和赛博攻击手段等等做详细的侦察和测试,确定赛博空间中有价值的信息和资源的位置,探明己方薄弱环节,检测敌方各类恶意的入侵和攻击。由于传感器的多样性导致检测结果数据量大、结构复杂、差异性大,且存在冗余和错误的数,难以直接用于态势评估,需要运用多源数据融合技术对原始检测数据进行预处理,以得到规范化的检测数据集。

## 2.2 态势分析

态势分析是态势感知的基础,态势分析的目的是获取影响态势的安全事件数据,安全事件是对赛博空间各类攻击的抽象,通过对原始检测数据进行数据级的融合,得到规范化的数据集,然后依据目标、威胁、脆弱性三者之间的关联关系,通过关联分析得到安全事件序列。

攻击归因。由于赛博空间对抗的虚拟性、广泛性,确定赛博攻击发起者是件非常困难的事。为此,美国国防先期研究计划局(DARPA)发布“赛博基因组”计划,拟在赛博空间实现“人为痕迹”的溯源,研究“人为痕迹”与用户/软件的社会关系,分析软件的功能及意图,最终将解决攻击归因这一难题。

脆弱性分析。赛博空间天生具有脆弱性,而脆弱性是赛博空间对抗得以进行的基础。赛博空间脆弱性分析从支持防御和攻击角度出发,分析敌我双方网络及信息系统存在的弱点和漏洞,有针对性地发起攻击,提高攻击效率,同时修补己方漏洞,防止敌方攻击。

## 2.3 态势评估

态势评估是态势感知的核心。态势评估是对赛博空间安全态势的量化描述,目的是根据测试数据,对赛博空间安全态势进行评估。赛博空间的安全度量是通过评估过程从一个偏序集中选择的一个值,描述信息系统安全质量,是一种关于信任程度的描述。安全度量的关键是选取标准、规范而完备的指标体系,在评估赛博空间安全态势时,使用信息保障中的可用性、完整性、保密性、可认证性、不可否认性这五个指标作为指标体系,能够较完备的描述赛博空间安全态势的各个方面。在评估整个安全态势时,以安全态势的五个要素分量评估结果为基础,采用加权模型得到整个安全态势值,根据加权参数的不同,适应不同的应用需求。

## 2.4 态势预测

态势预测是态势感知的最终目标。赛博空间态势预测是基于当前的态势,分析可能的威胁、风险及下一步行动,对未来可能出现的态势情况进行预测。由于赛博空间对抗影响面大、范围广(包括政治、经济、军事和社会等多个方面)、对抗效果多层次(包括性能层、效能层和作战效能层)以及涉及多个域(物理域、信息域、认知域和社会域),只有建立全面、科学和合理的对抗效果评估指标体系和模型,精确预测和评估赛博对抗效果,才能够支持赛博空间对抗的决策及攻防行动的开展。

赛博空间不同时刻的安全态势一般是彼此相关的,态势的变化有一定的规律,利用这种规律可以预测态势的变化趋势,从而有预见性地辅助决策者进行决策,实现动态管理和及时预警,避免预防大规模安全事件的发生造成损失。态势预测是一个重大的技术挑战,以时间序列分析为基础的态势预测方法,可用于对态势感知的变化规律进行分析。

### 3 结束语

态势感知技术对影响赛博空间安全态势的所有环境要素,进行获取、理解、评估以及预测其发展趋势,是实施赛博行动和打赢赛博战的基础,具有重要的作用。赛博空间态势感知是海上赛博战的重要组成部分,研究赛博态势感知问题,对于加强我军新型作战领域的力量建设,推进战斗力生成模式的转变,具有重要的理论价值和应用意义。

#### 参考文献:

- [1] KARMA GABRIELLE. Cyber Vision and Cyber Force Development [EB/OL].[2010-10-02].
- [2] 石荣,李剑.对信息战中赛博空间与赛博战的解析[J].航天电子对抗,2010(4).
- [3] 方正,王刚.对“赛博空间”的再认识[J].空军军事学术,2012,(5).
- [4] 张勇.赛博空间态势感知技术研究[J].信息安全,2012,(3)