网电空间态势感知技术研究

孙亮,武心安,成世文

（中国船舶重工集团第 716 研究所，江苏 连云港 222061）

摘要：网电空间作为一个全新的领域，囊括了所有的电子频谱、电子设备和网络化基础设施。依据网电空间和网电一体战的基本概念，构建网电空间态势感知框架，明确了网电空间态势感知的研究内容，重点介绍了网电空间态势表示技术、生成技术和预测技术以及今后的发展趋势。

关键词：网电空间，网电一体战，态势感知，态势预测

1 网电空间及网电一体战的含义

作为人类开创的第五维空间——网电空间，对其含义的认知经历了计算机网络空间、电磁与网络融合空间、泛在网络电磁空间三个阶段[1]。

计算机网络空间：起始于计算机和网络技术的发展，20 世纪 60 年代末，“互联网传输控制和网际协议”改变了传统通信传输样式，为计算机网络的出现奠定了基础。随即，以有线传输为主的互联网迅速在全球推广并普及，成为人们高度依赖的新平台。在这一阶段，以电磁波为基础的无线电通信技术和雷达技术都得到了长足的进步，但其发展与计算机网络之间相对较为独立[2-3]。

电磁与网络融合空间：随着网络技术的逐渐成熟，以移动通信网络为主的无线电通信技术促进了网络技术与电磁技术之间的快速融合，极大地拓展了人类活动的空间。2006 年新版美军《联合信息作战条令》写道：“由于无线电网络化的不断扩展及计算机与射频通信的整合，使计算机网络战与电子战行动、能力之间已无明确界限。”在这一阶段中，美军提出了网络中心战的作战理念，诠释了传感器网络、指挥控制网络及武器控制网络之间的交融关系，强调了网络在作战指挥体系中的强大作用，但未能全面概括电磁领域作战的特点（如传统的电子对抗等）并体现电磁攻防的重要性[4-5]。

泛在网络电磁空间：随着“网络中心战”“智慧地球”的不断推进，物联网、激光通信、全球信息栅格、云计算技术的发展，使网络与电磁空间融为一体，使网络成为影响社会稳定、国家安全、经济发展和文化传播的重要平台、电磁频谱成为一种重要的作战资源和作战手段。原来提出的网络中心战的作战理念已逐渐被网络和电磁的一体化作战思想所取代。由此，在实现网络信息层与电磁能量层融合的基础上，网络电磁技术逐渐向认知层和社会层发展，形成了涵盖物理、信息、认知和社会四域的第五维空间——泛在的网络电磁空间，并由“赛博空间”一词来描述这种客观存在[6-7]。

网电空间是一个与陆、海、空、天并行存在的域，涵盖涉及电磁频谱的所有领域，包括电磁频谱、嵌入式电子设备和各类网络化基础设施等，使用电子技术完成信息的产生、存储、修改、交换和利用，通过对信息的控制，实现对物理信息系统的操控，从而影响人的认知和活动[5]。网电空间的组成如图所示，由电磁频谱、电子系统和网络化基础设施三部分组成。

在军事领域应用中，随着网络技术和计算机技术在电子对抗作战指挥、武器控制、战斗保障、后勤支援、军事训练、情报侦察、作战管理等方面的不断深入与结合，电子对抗的形态正发生着深刻的变化，它不仅仅是从电磁空间向网络空间的一维延伸，而是呈现出一种以网络为基础，支撑电子对抗全方位发展的模式，全维地改变着战争的各种资源。网络对抗是为破坏敌方信息系统的使用效能和保障己方信息系统正常发挥效能而采取的综合性行动。其与电子对抗的结合具有十分鲜明的系统对扰、体系对抗特征。网电结合、网电一体的发展极大地丰富、创新和发展了电子对抗学科专业知识.全面升华了电子对抗的作战当量。

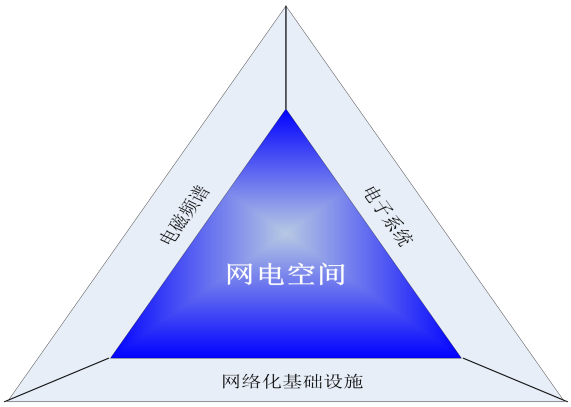

图 1 网电空间的组成

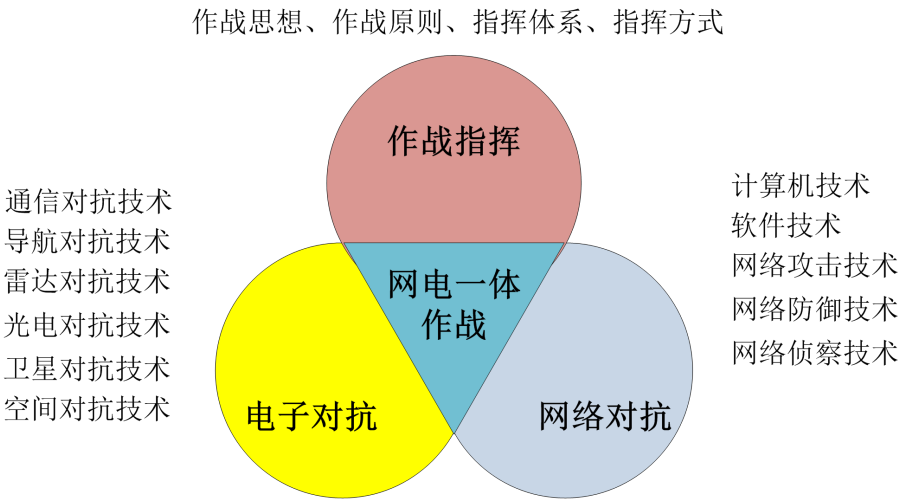

图 2 网电一体战要素结构图

网电一体战是将网络战和电子战这两种手段综合运用，以破坏和控制敌方信息基础和战略命脉，摧毁和瘫痪敌方的作战指挥控制系统为目标而采取的一系列作战行为，最终目的是夺取制信息权。与传统电子战相比，网电一体战不仅是简单的把对抗范畴从带电磁频谱领域扩展到计算机网络领域，而是两者的有机结合，一体作战。

2 网电空间态势感知概述

如上所述，网电作战不仅涉及通信、雷达、光电、隐身、导航、制导等系统, 而且遍及从空间、空中、地面、水面和水下，覆盖了从米波、微波、毫米波、红外和紫外的所有电磁频谱, 涉及各军兵种和各个作战领域。已经由以往单一设备，单项领域的对抗，发展为系统对系统、体系对体系的综合较量。“雷达网、通信网和计算机网”把“指挥控制中心、通信枢纽、雷达站和观通站”构成庞大的侦察预警系统，增加侦察预警的范围，提高侦察预警的快速性和实时性，使全球警戒的作战效能倍增。从图 3 可以看出，网电空间态势感知（Cyberspace Situation Awareness，CSA）正是网电作战能力功能组成图中“全球警戒能力”的重要组成部分

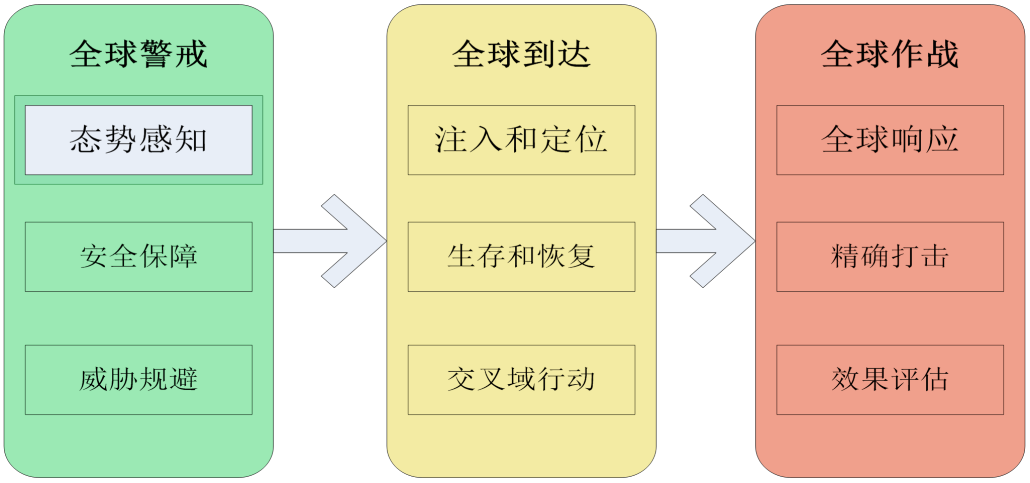

图 3 网电作战功能组成图

网电空间态势感知是指对网电空间中所有网络系统、电子对抗状况、设备行为以及用户行为等因素所构成的整体状态感知和变化趋势预测。通过多传感器多手段协同侦察的方式，对能够引起网电空间态势发生变化的所有要素，进行获取、理解、评估和预测，是来自网电空间内的关于己方、敌方及其他相关信息活动的直接知识，是夺取制信息权的重要基础。

与传统的态势感知相比，网电空间态势感知具有范围广(网电空间没有物理的、地理的和组织上的边界)、对象多(如互联网、电信网、电力控制网和信息基础设施等) 以及作战行动快(近光速)等特点。针对上述特点，态势感知正在由现有的“攻击后响应式”感知方式向“攻击前预防”方式转变，根据网电空间监测状态预测未来可能的攻击类型、时间和位置。这对未来应对突发性网电攻击将起到重要作用。

3 网电空间态势感知技术研究

3.1 网电空间态势感知框架研究

网电空间态势感知（CSA）提供的态势信息，用于威胁分析和决策支持，而且与信息域、认知域和决策域关系紧密，层与层之间不仅数据通信频繁，而且方法相近，作为一个整体而存在。因此，CSA 研究包括多方面内容，其总体研究框架如图 4 所示。

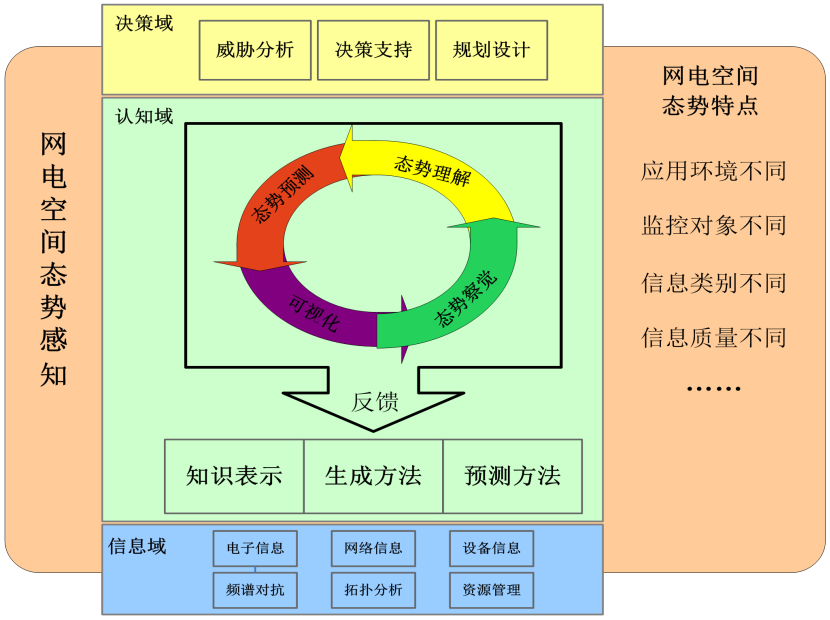

图 4 网电空间态势感知研究框架

从图 4 可以看出，网电空间态势感知研究框架概括了 CSA 研究内容,体现了 closing-the-loop 理念,突出动态循环、不断细化的本质,强调反馈的重要作用。研究内容广泛,包括自身功能细化、关键技术的理论方法、与其他域的通信与交互.目前的研究主要集中在 3 个方面:CSA 知识表示方法、CSA 生成方法和 CSA 预测方法。另外，网电空间态势感知采用的技术理论与传统作战领域的态势感知存在很大不同，表现为：①应用环境不同：传统领域态势感知的应用环境大多是真实的战场环境，而网电态势感知则针对网络(有线与无线)、电磁和电子设备三大跨维度环境。②监控的对象不同：传统领域的监控对象大多是现实环境中的作战实体、电磁辐射源等等；而网电领域则关注的范围广泛，包含网络、电磁、电子结构信息、电磁频谱信息、电子系统设备信息、电子系统参数信息等等。③需要收集的信息类别不同：在传统领域，信息基本是各类底层传感器上报的电磁辐射等数据；而网电领域则还要关注关键的服务设备，链接设备和安全设备等产生的数据和特种信息。④对信息的质量需求不同：传统的态势感知更多地关注运动平台的运动信息、关联关系、威胁以及这些行为的目的和造成的影响。网电态势更关注跨多维空间的网电协同数据和电子设备数据。其信息往往具备海量、高速、指向性流动、突发性等特点。

3.2 网电空间态势表示方法研究

网电空间的态势表示主要解决两个问题:其一是对不确定信息的表示，信息包括网络数据流、电磁场强频谱数据以及电子设备资源数据等。其二是对复杂系统的表示，这也是网电空间态势表式的挑战之一。

为了改变当前各作战单元独立工作的状况,建立真正意义上的统一的网电空间态势感知,在很大程度上依赖统一的系统表示方法。能够对网电空间各要素做出准确、全面、详尽的描述,是进行态势感知的前提[13-15]。同时，网电空间作为复杂巨系统,面对纷繁丰富的内容和错综复杂的关系,对其进行描述的能力很弱,而相关的研究又很少。本体论是其中的重要方法，指对共享概念模型所作的明确而规范的形式化说明,强调领域中的本质概念,同时也强调这些本质概念之间的关联[16-18]。Eric 使用本体论建立态势视图,从时空两方面分析给出形式化结构[19],能够将该领域中的各种概念及概念之间的关系形式化地表达出来,从而表达出概念中包含的语义,增强对复杂系统的表示能力。不足之处是过于具体，起到的层次化作用更多一些[20-23]。

从以上分析可以看出,目前有关网电空间态势表示的研究还存在很多不足:(1)作为态势感知的关键问题,对多维信息的表示研究不足。尽管对不确定性信息的表示有一些方法，但是对于高速、复杂、异类的电子对抗、网络和设备信息无合适的表示方式。(2)缺乏对复杂关系和复杂系统的表示方法，无法表现复杂的关系和内容，不能满足态势感知的需要。

3.3 网电空间态势生成方法研究

网电空间态势感知的生成，核心就是将网络、电磁和系统三大信息载体产生的各种基于数据的对抗行为、突发事件、能力变化、影响结果有效关联，形成及时、有针对性、符合作战指挥需求的态势感知视图。其中“综合”是网电空间态势感知生成方法的本质，具有两层含义：其一是将网络要素、电磁要素和电子设备要素有效综合；其二是将各种突发、高速信息与特定战场环境和指挥需求有效综合。目前可采用的理论方法有以下几种：

基于粗集理论的态势生成，兼具表达、学习与分类能力，突出的特点在于学习能力强,具有从海量网电数据中发现隐含信息、生成与规律相符态势的能力，且无须提供所需处理数据集合之外的任何先验信息[31, 32]。其难点在于设计网络、电子对抗（雷达、通信、导航、光电等）行为的关联模式以及对网电空间大量欺骗、干扰、压制数据的精简规则(求核与约简)。由于算法计算量大，在非实时环境中有很好的效果，但在实时环境中可能无法满足要求，成为粗集理论研究的焦点问题.随着研究的深入和理论突破,基于粗集理论的态势生成方法也将不断完善,更适合应用在网电空间态势感知生成领域。

网电空间中的态势要素聚合技术是指在事实关系或对额外隐性需求的基础上将原始数据与感兴趣的行为或数据进行相关。形成的集合可以描述当前的环境状态，并高度依赖环境。网电空间，是对具有内在关联的网络信息层与电磁能量层的有效聚合。聚合技术主要因解决以下两个方面的问题：①支持不同类型、不同规模数据之间及其与相关行为之间的关联；②在适当的级别为适当的操作人员提供适当的态势，同时保持关于相似态势不同视图的一致性。

3.4 网电空间态势预测方法研究

态势预测基于过去和当前生成的态势结果，对网电空间整体或局部的态势在未来某个时间点或一段时间的发展趋势进行预测。根据网电空间应用的环境、监控对象、收集的信息以及不同的需求，可依据实际情况选择以下两大类技术开展研究：基于知识推理的方法和和时间序列分析方法。基于知识推理方法充分利用经验知识建立态势预测模型,通过逻辑推理判断态势完成预测.其目标是处理多源多属性信息。恰好可以满足网电空间网络信息、电磁信息和电子系统信息多类信息源、多属性信息数据的特点。知识推理又可以进一步细分为基于产生式规则的推理、基于图模型的推理和基于证据理论的推理等。时间序列分析是根据系统观到的时间序列数据，通过曲线拟合和参数估计来建立数学模型的理论和方法。网电空间不同时刻的态势彼此相关，态势的变化有一定的规律，利用这种规律可以预测网电空间相关事件、行动及结果的变化趋势，从而有预见性地辅助决策者进行决策，避免大规模高威胁事件发生造成的损失。时间序列分析的方法能够很好的刻画随时间变化顺序取得的一系列评估值之间的前后依赖关系，适合用于对网电空间态势的变化规律进行分析。

4 未来研究趋势

在详细讨论了网电空间态势感知概念和关键技术的基础上我们发现,对能够引起网电空间态势发生变化的所有要素，进行获取、理解和预测和评估，是夺取制赛博权的重要基础。根据以上分析我们认为,未来研究趋势重点在以下几个方面:

(1)评价体系的研究

明确统一的评价标准是开展网电空间态势感知研究的前提,也是研究走向成熟的标志。建立评价体系至少要完成以下 3 个阶段的任务:其一,明确网电空间态势的定义,达成对态势状态进行划分、定级的共识，建立形式化描述；其二,制定评价态势评估方法准确性的度量标准,选择具体的度量指标,建立规范的准确性度量方法；其三,以准确性为中心,综合其他系统评价指标,建立系统评价标准。

(2) 人机交互机制的研究

人在态势感知中始终是一个重要环节,尤其在评估阶段,很少有一种方法能够独立完成评估任务。即使像聚类这种无监督学习方法,也只能依据“异常事件很少发生,正常行为占大部分”这一假设对态势进行简单划分。建立人机交互机制,包括以下工作:①提供友好的人机交互界面;②随时接收领域知识和专家建议,并及时对模型进行修改;③实现从自然语言到计算机能够处理的数学表达式的转换;④将数据挖掘技术与领域知识相结合,实现用户细化。

5 小结

网电空间作为一个全新的领域，囊括了所有的电子频谱、电子设备和网络化基础设施，随着信息技术和电子设备的快速发展和广泛应用，网电空间在生产、生活和战争中的地位逐渐凸显，成为各国争夺的热点。态势感知技术对影响网电空间的所有环境要素，进行获取、理解、评估以及预测，是实施电子战行动和网络战行动的基础，具有重要的作用。本文在大量研究国内外相关工作的基础上，明确了网电空间态势感知的研究内容，以网电空间的概念和态势感知的框架为基础，重点介绍了网电空间态势表示技术、生成技术和预测技术。

参考文献：

[1] 维基百科[EB/OL]. http://en.wikipedia.org/wiki/Cyberspace, September 2011.

[2] 戴清民 信息作战概论[M] 北京: 解放军出版社, 1999

[3] 郑连清 等 战场网络战[M] 北京: 军事科学出版社, 2001

[4] Department of Defense. National Military Strategy for Cyberspace Operations[M]. December 2006.

[5] 戴清民 网电一体战引论[M] 北京: 解放军出版社, 2002

[6] Franklin D. Karmer, Stuart H. Starr, Larry Wentz. Cyberpower and National Security[M]. National Defense University Press, April 2009.

[7] 石荣，李剑，黄鹏滔，李昊，贺岷珏. 对信息战中赛博空间与赛博战的解析[J]. 航天电子对抗，2010，26（04）：44-46.

[8] 丁建林，张勇, 赛博空间的结构和攻防研究[J],技术研究，2012 年 4 期

[9] 阎宗广, 电子对抗概论[M] 北京: 解放军出版社, 1999

[10] Franklin D. Karmer, Stuart H. Starr, Larry Wentz. Cyberpower and National Security[M]. National Defense University Press, April 2009.

[11] 纪凯 赵文祥. 网电一体战在现代海上作战中的应用[J]. 舰船电子工程，2009 42（05）

[12] 张奎新.“网电一体战”指挥体系构想[J] 电子对抗学术，2001（4）.

[13] Zhang Y, Ji Q, Loonet C. Active information fusion for decision making under uncertainty. In: Proc. of the ISIF. 2002. 643−650. http://www.ecse.rpi.edu/homepages/qji/Papers/fusion02_zhang.pdf

[14] Mirmoeini F, Krishnamurthy V. Reconfigurable Bayesian networks for hierarchical multi-stage situation assessment in battlespace. In: Proc. of the 39th Asilomar Conf. on Signals, Systems and Computers. 2005. 104−108. http://ieeexplore.ieee.org/

[15] Klir G, Yuan B. Fuzzy Sets and Fuzzy Logic. New York: Prentice Hall, 1995.

[16] Xu XH, Liu ZL. A method for situation assessment based on D-S evidence theory. Electronics Optics &Control, 2005,12(5):36−37 (in Chinese with English abstract).

[17] Wei SZ, Zhao H, Wang G, Zhang XD. Situation assessment model of complex system and its implementation method based on ontology. Journal of System Simulation, 2005,17(5):1200−1202 (in Chinese with English abstract).

[18] Li WS, Wang BS. A synthetic method for situation assessment based on fuzzy logic and D-S evidential theory. Systems Engineering and Electronics, 2003,25(10):1278−1280 (in Chinese with English abstract).

[19] Little E, Rogova G. Ontology meta-model for building a situational picture of catastrophic events. In: Proc. of the FUSION. 2005.796−803. http://ieeexplore.ieee.org/

[20] 聂 忠，黄高明，李仙茂 海战场赛博空间态势感知能力定量分析[J], 舰船电子对抗,2011 年 12 月

[21] 周光霞，孙欣 赛博空间对抗[J], 指挥信息系统与技术,2012 年 4 月

[22] 龚正虎, 卓 莹 网络态势感知研究[J],软件学报，Vol.21, No.7, July 2010, pp.1605−1619

[23] 平殿发，刘峰 电子战与网络战的一体化[J],现代电子技术，2003 年，第 18 期

concept capabilit y pla n 2016—2028[R] . Washingto n,D. C. : US DoD, 2010.

[24] LeMay Center f or Doctr ine Development and Educatio n. Cyber space o per atio ns [R] . Washingto n,D. C.T he United St ates Air For ce, 2010.

[25] US DoD. JP1-02: depart ment of defense dictio nary of militar y and associated terms [M] . Washingto n,D.C. US DoD, 2011.

[26] Zhu L, Wang HQ, Zheng LJ. Survey of network security situation visualizations. 2006. http://www.paper.edu.cn

[27] Lau S. The spinning cube of potential doom. 2003. http://www.nersc.gov/nusers/security/TheSpinningCube.php

[28] Yang YH, Li XD. The study of a framework for IP network performance metrics. Journal on Communications, 2002,23(11):1−7 (in Chinese with English abstract).

[29] Zhuo Y, Zhang Q, Gong ZH. Research and implementation of network transmission situation awareness. In: Proc. of the CSIE. Los Angeles, 2009. 210−214. http://ieeexplore.ieee.org/

[30] Deng JL. Gray Control System. Wuhan: Publishing House of Center-China University of Technology, 1985 (in Chinese).

[31] Pawlak Z. Rough Sets: Theoretical Aspects of Reasoning about Data. Boston: Kluwer Academic Publishers, 1991. 1−10.

[32] Wei SZ, Jin ND, Hui XJ, Liu H, Zhang XD. A situation assessment model and its application based on data mining. In: Proc. of the FUSION. 2006. 1−7. http://ieee-aess.org/isif/sites/default/files/proceedings/fusion06CD/Papers/322.pdf