战场感知与认知：网络空间安全态势感知的建立方法

尚雅玲[1] 胡昌振[2]
(北京理工大学机电工程学院，博士研究生[1]；教授[2] 北京 100081)

〔摘要〕 实现“积极防御、综合防范”的前提是建立与维持计算机网络空间的信息优势。本文提出了网络信息安全保障模型，探讨了网络信息安全保障体系的组成要素及管理模式，并采用 IPIB 原理与方法，探讨了基于战场感知与认知(DBA/DBK)的网络空间安全态势感知技术的建立途径。
〔关键词〕 IPIB DBA/DBK 网络空间 安全态势 感知 〔中图分类号〕 TN97 TP393 N3
〔文章编号〕 1000-7857(2004)07-0037-03

DOMINANT BATTLESPACE AWARENESS & KNOWLEDGE: THE APPROACH TO CYBERSPACE SITUATION AWARENESS

SHANG Ya-ling HU Chang-zhen
(Beijing Institute of Technology, Beijing 100081, China)

Abstract: Building and maintaining the information superiority is the basis of the principle of "active defense, integrated guarding " in the cyberspace. A model, the composing factors and managing methods on the network information assurance system are brought forward in the paper. According to IPIB, a new approach to build the cyberspace situational awareness is discussed by the principle and means of the DBA/DBK.
Key Words: IPIB, DBA/DBK, cyberspace, situation, awareness

1 前言

“积极防御、综合防范”是我国信息安全保障体系建设必须坚持的原则。实现“积极防御、综合防范”的前提是建立与维持计算机网络空间的信息优势。从技术本质上讲，基于信息优势所建立的网络信息安全保障体系，应该是一种能实时、有效地感知网络空间安全态势，并根据网络空间安全态势的变化制定应变策略，协调各种防范技术的人-机结合智能系统。

网络空间安全态势感知包括网络风险状态评估、网络毁损态势评估和网络防范效用评估等内容，它是网络信息安全保障体系建立的一项核心关键技术。战场感知与认知(DBA/DBK)主要指根据传感器的观测和人类的信息源，通过数据融合或模拟对指定作战空间中所有与决策有关的因素的综合感知，从而实现对战场当前形势及其内涵的了解，及对敌人近期行动和战斗结果的可信预测能力。它对拨开“战争迷雾”，使指挥官获得主宰性作战空间感知具有重要意义。

本文探讨了基于 DBA/DBK 的原理与方法，建立了网络空间安全态势感知的技术途径与方法。

2 网络信息安全保障体系组成

2.1 网络信息安全保障模型 网络信息安全保障模型如图 1 所示。

网络空间即为信息域，是信息优势的争夺焦点。在网络信息安全保障体系中，应该在信息域建立信息收集、保护和协同等能力，并以此为基础取得相对攻击的信息有利地位。认知域是知觉、感知、理解、信仰和价值观并通过推理做出决策的领域，存在于人的思想中。在网络信息安全保障体系中，应该在认知域建立、产生和共享高质量态势感知、共同了解攻防意图和攻防过程自我同步等能力。网络信息安全保障体系主要通过改善网络空间同步效果、加快响应速度和提高防范效能、生存能力和响应能力等行为，提高整体保障效能。

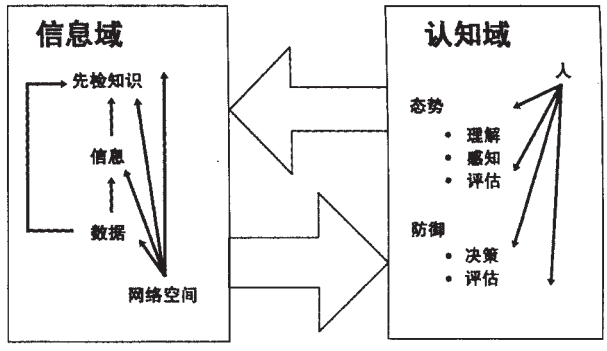

图 1 网络信息安全保障模型

2.2 网络信息安全保障体系的组成要素 基于图 1 模型，网络信息安全保障体系的组成包括 3 种基本要素：组织要素、内容要素和技术要素(如图 2 所示)。

组织要素包括网络信息安全保障思想理论基础、主客体、法

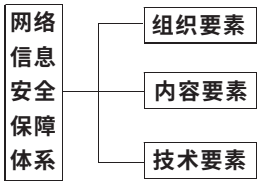

图 2 网络信息安全体系的基本要素

律基础和管理协调机构;内容要素包括网络所有领域的现实和潜在风险以及相对应的具体安全类型;技术要素是保障网络信息安全,实现风险的描述、管理与控制的所有技术手段与因素的总和。

2.3 网络信息安全保障体系的管理模式 网络信息安全保障体系所面对的是开放的复杂巨系统环境,该环境具有高速、高度变化和高度不确定性,处理网络信息安全保障问题时,应该将持续变化当作通用准则,首先承认不确定性和变化的存在,因此管理协调机构对网络信息安全保障体系的有效运转具有重要的作用。

在网络信息安全保障体系中,由于环境变化特性的存在,不能试图利用精确的预测和死板的控制策略来实现管理目标,而应该依赖策略与协作,采用如图 3 所示的管理模式。

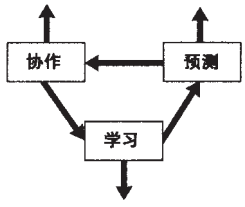

图 3 网络信息安全保障体系的管理模式

预测–协作–学习这 3 个活动构成的循环,存在明显的重叠,其目的是为了强调体系管理不确定的能力。"人"是网络信息安全保障体系的核心,如果"人"作为循环体系中的一个重要环节,参与到所有的预测–协作–学习活动中去,则必须建立在网络空间安全态势的感知基础上。DBA/DBK 的原理与方法,为网络空间安全态势感知的建立提供了可资借鉴的技术途径。

3 基于 DBA/DBK 的网络空间安全态势感知原理

3.1 基于 DBA/DBK 的网络空间安全态势感知原理 基于信息的战争,其中心目标是夺取信息优势或控制信息权。信息优势包括如图 3 所示的 DBA/DBK 和信息作战两个方面。

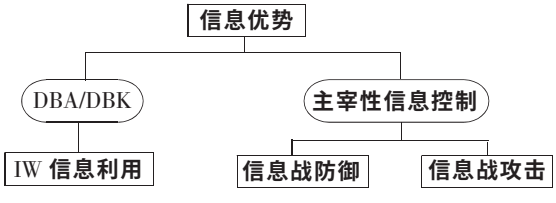

图 4 信息优势的内容

所谓 DBA/DBK 是指对给定作战空间中所有与决策有关因素的综合感知,及对敌近期行动和战斗结果的可信预测能力;所谓信息作战是指对敌信息和信息系统施加影响,同时使我方信息和信息系统免遭敌方影响的行动。DBA/DBK 依赖于对当前态势含义的理解,及对适当数据的获取和分析能力。它既是一种能产生将来可能行动方案的能力,也是一种能把握何时取得预警而实施行动的智能。通过 DBA/DBK 所得到的信息优势,对作战空间准备、作战空间的监视与分析、作战空间可视化和作战空间态势感知分发等 4 种作战行动均能产生影响。DBA/DBK 对作战空间提供统一的观察,并将结果分发给所有的部队。DBK 建立在 DBA 的基础上,而 DBA 又依赖于对作战空间观察所得到的数据。对信息优势,两者都是至关重要的。DBA/DBK 的核心能力是收集相关的资料并及时准确地产生情报知识,因此,作战空间情报准备(即 IPB)是 DBA/DBK 的核心技术。

3.2 IPB 的原理与方法 IPB 是对指定战场空间的环境和威胁进行分析的连续系统过程,用于支持战场人员估计及战场态势决策。应用 IPB,可帮助指挥官在战场时空的关键点选择和优化使用战斗力。IPB 的主要功能为:确定威胁的最可能行动路线(即 COA);描述部队环境,并确定影响环境的行为。IPB 由如图 4 所示的 4 个步骤组成。

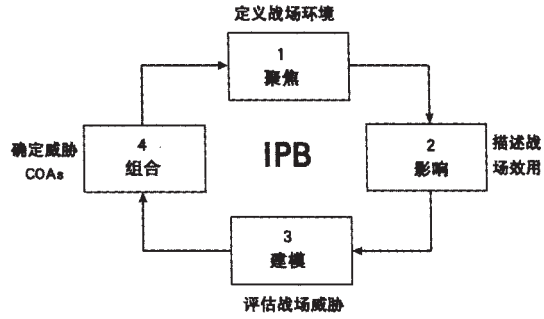

图 5 IPB 的 4 个步骤

步骤 1 主要确定 IPB 的分析对象、需要识别的战场特性及对敌方部队作战效果进行分析的内容;步骤 2 主要评价影响敌方作战的环境效用,包括战场环境分析及有关敌方一般军事能力和广义 COA 的战场效用描述等内容;步骤 3 主要检查敌方参与作战的部队组织模式,包括建立或更新威胁模型、识别敌方广义 COA 等内容;步骤 4 主要集成前述步骤的结果,并形成有意义的结论。

从本质上讲,IPB 的目标是分解和关联与敌方有关的"5W1H"(即 who、what、和 where、when、why 和 how),以发现在作战过程中敌方的 COA 和企图。

4 基于 IPIB 的网络空间安全态势感知方法

IPB 的原理与方法在网络空间安全态势感知分析中的应用称为 IPIB。应用 IPIB 的方法和工具具有如下价值:可应用于网络信息安全保障的各层面;能帮助定义不同层面的计算机威胁,并对国家信息基础设施的多种威胁予以特征化和确定优先级。

4.1 IPIB 的分析内容与能力 IPIB 的分析内容如图 6 所示。

网络空间的破坏性攻击一般发生在微秒或纳秒级,应该在攻击发生前对其实施有效预测并制定可靠的预防措施,否则就只能选择恢复响应。实施有效预测和制定可靠预防措施的前提就是准确感知网络空间安全态势,IPIB 则是网络空间安全态势感知的重要方法与工具。IPIB 可为网络空间安全态势感知提供如下能力:对网络攻击与威胁的预测能力;对网络空间安全态势的智能分析能力;对战场环境及我方信息系统的威胁作出假设和判断并进行识别的能力;对敌方信息攻击方式和 COA 进行识别的能力;对己方网络防御措施和敌方网络脆弱性进行威胁的评价能力。

4.2 IPIB 在网络信息安全保障中的应用 网络信息安全保障的生命周期包括准备、配置、使用、维护和重构等 5 个阶段。IPIB 在这 5 个阶段中均可得到有效应用。

4.2.1 准备阶段 IPIB 具有很高的杠杆作用,可应用于对原始数据提供索引方式、增添新的数据源和对各种数据提供智能分析等。

(下转第 7 页)

来难以承受的、不可逆转的、持久的严重影响。但是迄今为止，我国还未把适应与减缓气候变化影响的问题提上议事日程，就连这方面的研究都十分薄弱和不足；因此，需要全面深入研究气候变化对我国自然生态系统和国民经济各部门的影响后果、可采取的适应与减缓措施，并在对其进行成本效益分析的基础上，提出我国适应与减缓气候变化影响的规划和行动计划。

5 结论与建议

全球变暖是不争的事实，只是在变暖的幅度、原因和区域分布，特别是未来气候变化预估方面，还有不少的不确定性。气候变化对自然生态系统、国民经济和国家安全将产生诸多影响，有些影响可能是不可逆和灾难性的。及早研究、及时采取适应气候变化的措施，可以减少气候变化的不利影响。气候变化问题的重要性与复杂性，决定了气候变化公约谈判的难度将不亚于入世谈判。目前国内外没有低排放、高经济增长的发展模式可供采用。承担控制温室气体排放的义务应与经济发展水平相适应，否则可能对我国经济发展、能源供应和人民生活产生相当的影响。

为了应对气候变化问题，我们提出以下一些对策建议。

5.1 继续加强气候变化研究，提高我国气候变化研究的水平

目前我国的气候变化研究工作，由于组织不力和经费不足，远不能满足国家可持续发展的需求，也难以为气候变化谈判提供强有力的科技支持。

建议国家加强对气候变化研究的组织和协调，并给予长期、稳定的经费支持，以便紧紧围绕国家需求开展相关研究，特别是在气候变化对我国自然生态系统和社会经济系统的影响与适应对策方面，进行有针对性的研究。

5.2 制定我国应对气候变化问题的总体规划

我们还没有一个总揽国际谈判对策和国内应对行动的总体规划。目前气候变化谈判的重点已转向确定发达国家在第二个承诺期(2012 年以后)的减排义务。届时，要求我国承担实质性限排或减排义务的压力将更大。我国必须从现在开始认真研究制定我国应对气候变化的总体规划，统一规划外交、经济、能源等方面的应对策略和行动，使应对气候变化问题成为促进我国可持续发展的动力之一。

5.3 建设中国气候系统观测网

我国现有的气象观测网主要针对天气预报的需要。气候预测和气候变化研究需要把观测范围扩大到整个气候系统，既观测它的各种物理过程、化学过程、生物地球化学过程，也监测人类活动的影响。有鉴于此，国际上已实施全球气候观测系统(GCOS)项目，我国也急需建设中国气候系统观测网(CCOS)，获取长序列、高精度的观测资料，并实现真正意义上的共享，以满足我国气候预测和气候变化研究工作的需求。

参 考 文 献

[1] 秦大河. 中国西部环境演变评估——综合卷[M]. 北京: 科学出版社, 2002. 80
[2] 施雅风, 孔昭宸. 中国全新世大暖期气候与环境 [M]. 北京: 海洋出版社, 1992. 212
[3] 王苏民, 林而达, 佘之祥. 环境演变对中国西部发展的影响及对策[M]. 北京: 科学出版社, 2002. 187
[4] 王绍武, 董光荣. 中国西部环境特征及其演变 [M]. 北京: 科学出版社, 2002. 242
[5] 丁一汇. 中国西部环境变化的预测 [M]. 北京: 科学出版社, 2002. 231
[6] 王苏民, 施雅. 晚第四纪青海湖演化研究析视与讨论[J], 湖泊科学, 1992. 4(3): 1~9
[7] 冯松, 汤懋苍, 周陆生. 青海湖近 600 年来的水位变化[J]. 湖泊科学, 2000, 12(3): 205~210
[8] IPCC. Climate change 2001: the science basis. Contribution of Working Group I to the Third Assessment Report of the Intergovernmental Panel on Climate Change [M]. Cambridge, United Kingdom and New York, NY. USA: Cambridge University Press, 2001. 881

(责任编辑 苏 青)

(上接第 38 页)

图 6 IPIB 的主要分析内容

4.2.2 配置阶段 IPIB 可用于建立态势知识库，以及在网络空间安全态势感知与评估中应用态势知识库，并为网络空间安全防御行为(如防御 COA 的连续、动态再规划，高价值入侵检测器与相关处理器的配置、应用与对抗措施的制定等)的确定提供决策支持。

4.2.3 使用阶段 IPIB 用于对网络安全保障体系的应用状况进行评价，并对更新提供决策支持。评价与更新依据观察和预测的风险状况、新的网络攻击事件的突发能力和网络信息安全保障体系的对抗能力等内容进行。

4.2.4 维护阶段 IPIB 将用于入侵检测器的布置和应用、法律措施的使用、防御措施的使用、计算机攻击行为的应用和命令的 COA 等内容的优化。

4.2.5 重构阶段 IPIB 将用于对准备、配置、使用和维护等 4 个阶段进行评估，并为重构的网络信息安全保障方案的建立提供决策支持。

参 考 文 献

[1] 胡昌振. 把握我国信息安全技术跨越式发展机遇[J]. 计算机安全, 2003, 31(9)
[2] 约翰·H·霍兰著. 隐秩序——适应性造就复杂性 [M]. 上海: 上海科技教育出版社, 2000
[3] 钱学森著. 创建系统学[M]. 山西: 山西科技出版社, 2002
[4] Edward Waltz 著. 信息战原理与实战[M]. 北京: 电子工业出版社, 2004
[5] Tim Bass. Cyberspace Situational Awareness Demands Mimic Traditional Command Requirements. In Proceedings of the 30th Symposium on the Interface: Computing Science, 1998

(责任编辑 王宏章)