电 光 与 控 制
Electronics Optics & Control
Vol. 21 No. 9
Sep. 2014

doi:10.3969/j.issn.1671 -637X.2014.09.001

赛博空间的战术机动

The Tactical Maneuver in Cyber Space

刘金星[1,2]， 陈哨东[2]， 王 芳[2]

（1.空军第一航空学院航空军械工程系，河南 信阳 464000；
2.光电控制技术重点实验室，河南 洛阳 471009）

刘金星

空军第一航空学院航空军械工程系教授，博士，毕业于西北工业大学系统工程专业。全军院校育才奖金奖获得者，空军教学系列职称评委、空军高层次人才。主持和参研多项国家级、省部级和军内重点科研课题，获军队科技进步奖多项。发表论文40余篇。《电光与控制》期刊编委。主要研究方向为协同空战指挥控制、多智能体系统等。

综合国内外研究现状以及未来作战环境和作战需求，对赛博空间战术机动的概念、分类，以及赛博空间作战力量的特征做相应的概述；针对赛博空间中战术机动的特点，对赛博空间和陆、海、天、空等传统作战空间战术机动的融合难点、可能性做相应分析。

关键词： 赛博空间；战术机动；融合；指挥控制；决策

中图分类号： V271.4 **文章编号：** 1671 -637X(2014)09 -0001 -06

0 引言

进入21世纪，赛博空间逐渐得到美国及世界其他军事强国的认可，赛博空间的定义被不断修订。2008年3月，美国国防部长在《美国国防军事词汇辞典》中给出赛博空间的定义：“Cyberspace是处于信息环境中的一个全球域，由相互依赖的信息技术网络组成，包括互联网、无线电通信网络、计算机系统、嵌入式处理器和控制器”。2008年，美国空军赛博司令部战略构想[1]中指出：“Cyberspace是一个物理域，该域通过相关物理性基础设施，使用电子和电磁频谱来储存、修改和交换数据；并将赛博空间中的作战行动确定为赛博空间作战，包括赛博空间进攻作战和防御作战”。为夺取赛博空间作战优势，美国在战略战术、人员组织和训练、装备研发、军演设施建设等方面致力于备战赛博空间[1-6]。由近年来美军的发展情况可见：在目前及未来的作战中，运用赛博攻击和防御力量以保障多个作战空间中的作战行动是其作战任务目标之一。2007年，以色列成功运用美军的“苏特”电子战系统对叙利亚核反应堆进行袭击[7-9]。该战例一方面展示了美军在赛博作战装备研发进展及作战使用效果，另一方面，以零伤亡战果证明，赛博空间中作战力量是现代及未来战场中的主要作战力量之一，赛博空间的对抗结果将在很大程度上影响战争的结局。因而，如何运用赛博空间的作战力量对敌方进行有效对抗，亦成为指挥控制决策研究的方向之一[2,10-21]。基于战术目标，运用赛博作战力量在赛博空间中实施有效的战术机动，不仅是未来战场中指挥员充分展示其智慧和才华的机会，也将是指控专业科技工作者研究的课题之一。目前，国外相关研究机构和学者已开始这方面的研究[13-15,21]。本文基于未来作战中的需求和特点，对赛博空间战术机动的概念、赛博作战力量的特征和赛博空间战术机动的分类做相应的介绍，并对赛博空间与陆、海、天、空等空间的战术机动相融合的难点、可能性做相应的分析。

基金项目：航空科学基金（20125197001）；光电控制技术重点实验室资助

1 赛博空间战术机动

所谓的机动，即在交战前、或交战中，将作战力量部署于或运动至相关有效作战位置，以获取有效的作战位置优势[16]。作战力量的机动取决于作战力量的性质。在物理空间中，作战力量的运动需要耗费时间，以时间换取空间，作战力量的机动，主要是获取空间位置上或速度上的战术优势。例如，冷兵器时代的骑兵居高临下冲击，格斗空战中获取尾部攻击位置等。赛博空间中的作战力量，其特征与陆、海、天、空等空间中的战术力量有着本质的区别，因此，赛博作战力量的机动与传统作战空间中的战术机动有着截然不同的概念和性质。

1.1 赛博空间机动的概念

对于赛博空间中的机动，在美国国防部2011年发布的联合出版物（Joint Publication）JP3-0[5]中是这样描述的：“Cyber Maneuver is the appli-

cation of force to capture, disrupt, deny, degrade, destroy or manipulate computing and information resources in order to achieve a position of advantage in respect to competitors."。这段话的意思是:通过运用己方赛博力量获取、扰乱、拒绝、降低、毁伤敌方计算或者信息资源,以获取对敌方的信息优势。赛博机动的目标就是己方赛博力量到达指定的位置,即在网络这个虚拟空间中的作战位置,以实现与其他作战力量一起进行协同作战,最终实现战役或战术作战目标,如图1所示。

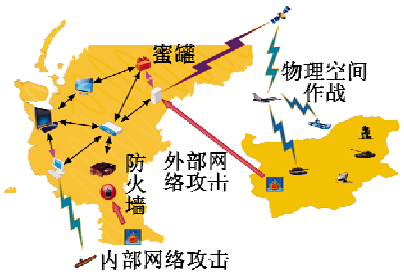

图1 赛博空间及物理空间作战示意图

Fig.1 Combat in Cyber and other spaces

在联合出版物JP3-0中,对于赛博机动目标的另一个解释是:在对手的OODA(Observation-Orientation-Decision-Action)环内,或者在对手意识时间空间内,在精神意识物理层面上摧毁对方,使其与之盟友隔离,并在对手准备抵抗时摧毁之。其做法是,通过产生噪声降低敌方网络侦察能力(Observation),清除敌方入侵(Action),以降低敌方危害;增强我方观察能力(Observation)和对敌方的清除能力(Action),如图2所示。

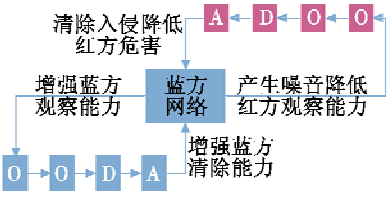

图2 OODA执行过程

Fig.2 Operation process of OODA

与飞机、军舰、坦克等物理空间中的作战实体不同的是,赛博空间作战力量就是特殊的计算机代码,用于实现对敌方指控系统的攻击和对敌方赛博攻击力量的防御;指定位置即特定的时间和虚拟空间中特定的位置。

1.2 赛博作战力量的特征

如前所述,赛博空间中的作战力量主要是计算机程序,驻留于网络这一虚拟空间,因而,在特征上与飞机、坦克、军舰等作战实体截然不同。其差异体现在如下几点[21]。

1)速度。在网络中,信息是以光速进行传播的,因而计算机软件行动执行的快速性致使进攻者和防御者在对方行动执行期间难以调整策略。而在传统空间中,由于作战行动的执行周期和执行速度的原因,当一方开始执行作战行动时,另一方有时间可调整其策略。

2)机动范围。在军事斗争中,机动范围指的是作战力量能够到达和集结的区域、或实施其影响的范围[21]。赛博作战力量的机动范围即攻击者的可达范围,或者是攻击者能够欺骗防御者的观察和探测的范围。具体来说,网络空间的覆盖范围就是赛博作战力量的机动范围。

3)接触与控制。在赛博对抗中,不仅要对敌方、己方的系统进行评估,还要对中立方的系统进行评估,为下一步获取敌方数据、扰乱或控制敌方系统等作战行动提供依据。

4)集结的迅速性。由于信息在网络中传播的高速性,因而,在赛博空间中,可在短时间内实现作战力量的快速集结。

5)广域部署和并行实施。随着网络以及无线网络的普及,赛博空间进一步扩展,为攻击者和防御者提供了广阔的作战空间。攻击者和防御者可在广阔的赛博域内进行部署,并同时发动赛博攻击或赛博防御。

6)攻击的隐蔽性和低可观测性。大多数情况下赛博空间中的攻击行为是不可观测或低可观测的,这是由于赛博空间内攻击力量运动的高速性,使得攻击行为往往瞬间爆发,并且攻击者的攻击目标往往也是不可预测的。

7)技术发展快速。近年来,基于网络的应用正逐步地走向各行业的各个方面,对于军事指挥控制领域同样如此。信息技术的迅猛发展,使得赛博攻防手段随着信息技术的发展日益更新。在今天还发挥作用的技术,在明日可能就会被淘汰。

1.3 赛博空间战术机动的类型

按照作战目的来划分,赛博空间的战术机动可划分为进攻性机动和防御性机动两种类型。其详情如下所述。

1.3.1 进攻性机动

在陆、海、天、空等作战空间中的战术机动主要是获取地理位置上的优势,而赛博空间中的战术机动主要是获取信息优势。因此,赛博空间中的进攻性机动从战术应用的角度可划分为以下几类。

1)侦察性机动。侦察性机动是一个信息获取的过程,即通过网络侦察或入侵敌指控网络以获取敌方信息资源,进而获取在战役、战术和交战层面上的优势。类似于地形优势,在赛博空间中获取信息情报优势,可对作战结果起到决定性的影响。

2)定向攻击机动。所谓的定向攻击机动即通过获取敌方信息环境中的物理和逻辑节点信息,选取敌方指控网络中的脆弱节点或重要节点进行定向攻击,最终实现对敌方信息、指控系统进行控制或摧毁,为作战提供支持。

定向攻击机动的典型战例就是2007年以色列空袭叙利亚核反应堆[7]。2007年9月6日晚,以色列空军第69战斗机中队18架F-16I战斗机,沿着叙利亚的海岸线超低空飞行,成功躲过叙利亚军队的防空体系,对叙方纵深100 km内的所谓"核设施"目标实施了毁灭性突击,如图3所示。

图3　2007年以色列空袭叙利亚核反应堆

Fig. 3　Combat process of Israeli attack on Syria nuclear reactor in 2007

在此次战斗中，以军以F-16I等非隐身飞机突破道尔-M1等俄制先进防空武器系统的严密防护，正是由于使用了美军的“苏特”攻击系统[7]，对叙利亚防空武器系统进行了网络攻击。在攻击前，以方分析和破解了俄制“道尔”防空武器系统的脆弱点，进而向叙利亚防空武器系统中的脆弱处理节点植入定制的信号，包括专业算法和恶意程序。巧妙渗入其防空雷达网络，或窥测敌方雷达屏幕信息，或实施干扰和欺骗，或冒充敌方网络管理员身份接管系统，操纵雷达天线转向，使其无法发现来袭目标。

3）袭扰机动。袭扰性机动的目的是对敌方指控网络的正常工作进行袭扰，使其无法实施正常指挥控制，其主要做法是渗入到敌方指挥控制环节中，以改变敌方指挥控制决策，最终误导或者改变敌方交战行为。袭扰性机动以直接或非直接的形式对敌方的指挥控制决策进行影响，以实现对己方作战行动的保障。所谓直接的形式，即渗入敌方指控系统中，破坏、误导、中断敌方指控系统的决策；而非直接的形式，则是以提供虚假数据、篡改敌指控系统数据等形式，使敌指控系统根据虚假情报制定出错误决策。

1.3.2　防御性机动

防御性机动主要是用于保护自身信息系统的安全以及网络系统的正常运转。防御性机动从防御思想的角度，可划分为如下几类。

1）纵深防御。

目前，为抵御网络入侵，常用的网络安全防护措施，是将防火墙、杀毒软件在计算机网络相关节点上进行部署，构成环形防御，以保护信息资产的安全，如图4所示。由于网络攻击的隐蔽性和不确定性，采用单层环形防御的方法难以抵御多次网络攻击，为此，纵深网络防御思想随之而产生。

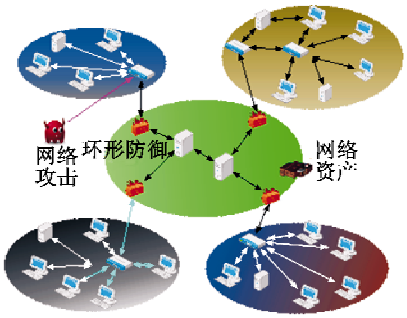

图4　网络安全环形防御

Fig. 4　Perimeter defense of network security

纵深防御思想首先在美国信息保障技术框架（IATF）中提出，并应用于美国国防部（DoD）的《全球信息栅格（GIG）信息保障政策与实施指南》中，以指导美军GIG的建设[22]。纵深防御的基本思想是采用多重防护，以防范信息网络威胁，使能够攻破一层或一类保护的攻击行为无法破坏整个信息基础设施和应用系统，如图5所示。

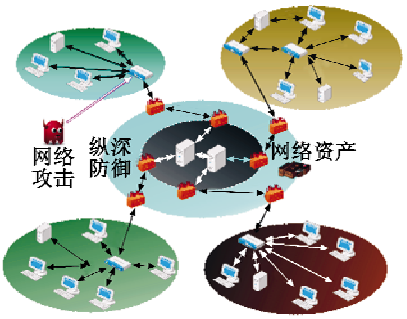

图5　计算机网络纵深防御

Fig. 5　Defense in depth of network security

2）运动防御机动。

前述“纵深防御”是在网络中固定位置上的特定类型和数量的网络防御力量，以抵御来自外部和内部的网络攻击。随着网络攻击数量的加大，这种防御总有捉襟见肘之时。文献[12]提到的“Moving target defense”，在本文中冠以“运动防御机动”之称。这种防御思想是：通过转移和变更受保护系统的某些方面，以加大攻击者识别被攻击系统的难度，从而降低攻击者攻击成功的概率。运动防御机动的主要模式包括地址空间布局随机化、指令集随机化和数据随机化3种[12]。

3）欺骗性防御机动。

欺骗性防御机动即在网络上部署“蜜罐”等欺骗性设施[23-25]，为攻击者展示一个虚假的网络脆弱环节，通过吸引引诱网络攻击来保护重要信息资产的安全。在赛博防御中实施欺骗性机动，必须基于防御的对象和重点，以及攻击者特性的要素部署“蜜罐”等诱骗设施。

4）反击性防御机动。

在军事斗争中，最好的防御就是进攻，在赛博空间同样如此。采用赛博攻击行动对敌方的指控系统或其他设施进行攻击[26]，迫使敌方无法对己方指控网络实施有效攻击。相对于其他防御行动而言，这种反击性防御机动所需成本小、隐蔽性强、防御效果好，但须对敌方指控系统实施有效的网络侦察，获取有效的情报，以保证攻击性防御机动的有效执行。

2　赛博空间战术机动与其他空间战术机动的融合

在军事斗争中，赛博空间的作战行动是整个作战规划中的一部分，或以实现赛博作战目标为意图；或以保障其他空间中的战术作战任务为意图。因此，赛博空间中的战术机动必须与其他空间中的战术机动相融合，保障各种作战力量作战效能的有效

综合与发挥。而赛博空间中作战力量的性质与其他空间中的性质截然不同,因此,二者在融合上具有相应的难度,必须针对二者各自的特点进行规划,以实现赛博和其他空间上战术机动的融合。

2.1 融合的难点

根据上文分析可见,两个空间中作战力量的运动特征存在着巨大差异,导致融合难以实现。主要差异如表1所示。

表1 赛博空间和其他空间的差异

Table 1 The difference between the Cyber and other spaces

度量内容	陆、海、天、空	赛博空间
作战单元	实体作战单元	计算机代码
时间	天(d)、小时(h)、分(min)、秒(s)	微秒(μs)、毫秒(ms)
距离	千米(km)、米(m)	接近于零
执行效率	存在人为差错、疲劳、迟钝	无疲劳、无差错
与敌同等力量遭遇交火	不可避免与敌遭遇交火	很难与敌遭遇交火

从表1所列举的两个空间作战力量之间的差异可见,实现二者之间的融合具有相应的难度。具体体现在如下几点。

1)作战时间协调。

由于二者在执行时间上存在的巨大差异,在作战中将二者的发起战斗时间、退出战斗时间以及作战的节奏进行统一、或在作战中交替穿插使用是不现实的。

2)空间部署协调。

赛博空间和其他空间作战力量运行速度上的巨大差异,使得二者在空间上的部署协调具有一定的难度。在作战中,不可能将赛博空间和其他空间中作战力量的兵力部署位置、行军路线、行动节奏等进行统一规划。

3)难以评估攻击效果。

在作战中,各方作战力量的作战效果评估是作战按计划执行以及指挥员调整部署、改变作战决心的依据。然而,赛博空间的作战效果却存在着一定的不确定性。例如,入侵失败或入侵时间增加、敌方的"蜜罐"引诱,遭受攻击后的"灾备恢复"等都会影响己方对赛博攻击效果的正确评估,而陆、海、天、空等空间的打击效果则具有较高的可观测性,因而,赛博空间中作战行动效果的评估会影响作战计划的正常执行和调整。

2.2 融合的可能性

虽然赛博空间和其他空间作战力量在时间和速度上的巨大差异,导致二者之间的协调和融合具有一定的难度,但在实际中,充分分析各自的特点,还是可以将二者进行有效融合,以充分发挥和利用各自的作战效能。具体可行途径分析如下。

1)利用赛博攻击起效时间和效果持续时间规划作战行动。

从时间上来说,赛博攻击具有时间短、执行迅速的特点,但是赛博攻击需要对敌方网络进行有效侦察和入侵,才能有效地攻击敌方网络,进而影响敌方指控系统,如图6所示。

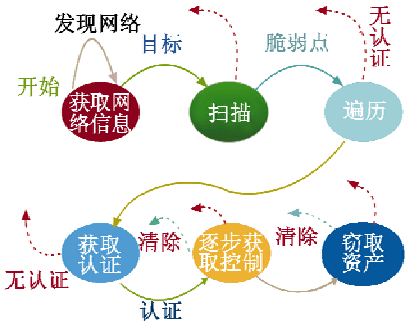

图6 攻击生效时间

Fig. 6 The effective time of the Cyber attack

因此,赛博攻击由开始到生效存在着一个生效时间。而赛博攻击生效后,在一定的时间内,敌方发现被攻击,并采取恢复系统等行动,因而,赛博攻击效果又有一个持续的时间。基于这两个时间来规划其他作战实体的作战行动,可有效实现赛博空间和其他空间中战术机动的融合。

2)空间部署上的伴随行动。

对于赛博作战力量而言,其作战行动需要在网络覆盖范围内才能执行,作战行动需要物理载体的支持,例如,战场电子战飞机。而目前的战场网络大多是无线网络,赛博攻击力量必须借助于物理载体到达敌方网络覆盖范围内才能进行攻击。基于这一特点,飞机、坦克、军舰等作战实体和赛博空间作战力量在空间上的部署可采用伴随保障的模式,以实现二者之间攻击行动的协调。所谓的伴随保障,即赛博攻击载体(电子战飞机)在战线边界附近盘旋飞行,接收敌方网络信号,入侵和控制敌方指控网络,而攻击实体(战斗机)则根据赛博攻击的起效和持续时间执行其战术任务。

3)基于敌方电磁辐射确定赛博攻击效果。

赛博攻击效果的评估取决于敌方指控系统的工作情况,而敌方指控系统的工作情况分析需要情报数据的支持,但战场上的情报数据往往不能做到实时提供。因此,基于敌方电磁辐射(包括传感器辐射、通信信号辐射)来分析赛博攻击效果,可为火力打击作战实体的作战行动提供支持。

根据不同类型信号的频段,可分析出敌方的传感器辐射信号以及通信辐射信号。

基于敌方传感器辐射方向和辐射量来分析赛博攻击对敌方传感器工作情况的影响;基于敌方各作战节点之间的通信交互辐射量,来判断敌方指控网络的连接情况。从这两方面出发,可实现对赛博攻击效果的间接评估,为赛博空间和其他空间作战行动的协调提供评估依据。

3 结束语

综合指控网络的发展以及赛博空间攻防技术的研究发展可见,在未来,赛博空间和陆、海、天、空等作战空间的综合攻防是未来战场的主

要作战模式。实现赛博空间和其他空间作战行动的统一与协调，不仅需要在网络侦察、网络攻防等赛博作战手段上取得进展，而且要在相应的效能评估技术和决策技术上取得进展。因而，网络攻防技术等新兴学科的研究方向应与智能控制、智能决策等控制学科中的研究方向进行有机融合，实现互相支撑联合发展，为我国的国防事业发展提供技术储备和支持。

参考文献

[1] Air Force Cyber Command. Air force Cyber command strategies version [M]. Barksdale: AAAFB, LA, 2008.

[2] FORSYTH M H, GENERAL M. "Cyberspace operations", air force doctrine document 3-12 [R]. Air Force, Washington D. C., 2010.

[3] Chairman of the Joint Chiefs of Staff. National military strategy for cyberspace operations [R]. Washington D. C. December, 2006.

[4] TYUGU E. Command and control of Cyber weapons [C]//The 4th International Conference on Cyber Conflict, 2012:1-11.

[5] Joint Chiefs of Staff. Joint publication 3-0:Joint operations, JP 3-0[R]. United States Department of Defense, Washington D. C., 2011:III-27.

[6] PARKS R C, DUGGAN D P. Principles of Cyber warfare[C]//Proceedings of the IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001:122-125.

[7] FULGHUM D A, WALL R. U. S. electronic surveillance monitored israeli attack on Syria[EB/OL]. 2007-11-14 [2014-01-01]. http://www. aviationweek. com/aw/generic/story_generic. jsp? channel = defense&id = news/ISRA112107. xml&headline = U. S. % 20Electronic % 20 Surveillance % 20 Monitored % 20 Israeli % 20 Attack % 20 On % 20 Syria.

[8] 刘兴，赵敏. 网络战攻击和防御技术——对苏特计划的分析[J]. 指挥信息系统与技术，2011，2(4):1-9.
LIU X, ZHAO M. Offense and defense technology in Cyberwar—analysis on project Suter[J]. Command Information System and Technology 2011, 2(4):1-9.

[9] 杨曼，沈阳. 美军空中电子攻击体系研究[J]. 电子信息对抗技术，2010, 5(4):12-16.
YANG M, SHEN Y. The overview of US AEA system[J]. Electronic Information Warfare Technology, 2010, 5(4):12-16.

[10] HEW P, LEWIS E. Situation awareness for supervisory control: Two fratricide cases revisited[C]// International Command and Control Research and Technology Symposium, Santa Monica, California, 2010: 1-20.

[11] U. S. Department of Defense. Department of defense strategy for operating in Cyberspace [R]. Washington D. C., Jul. 2011.

[12] JAJODIA S, GHOSH A K, SUBRAHMANIAN V S. Moving target defense Ⅱ: Application of game theory and adversarial modeling advances in information security [M]. New York: Springer Science Business Media, 2013.

[13] LORD W T. Cyberspace operations: Air force space command takes the lead[J]. High Frontier, 2009, 5 (3): 3-5.

[14] BERAUD P, CRUZ A, HASELL S, et al. Using Cyber maneuver to improve network resiliency[C]//Military Comm unications Comference, 2011: 1121-1126.

[15] BERAUD P, CRUZ A, HASSELL S, et al. Cyber defense network maneuver commander[C]//IEEE International Carnahan Conference on Security Technology (ICCST), 2010:112-120.

[16] U. S. Department of Defense. JP 1-02 DOD dictionary of military and associated terms [R]. Washington D. C., Oct. 17, 2008.

[17] HUANG N F, KAO C N, HUN H W, et al. Apply data mining to defense-in-depth network security system [C]//The 19th International Conference on Advanced Information Networking and Applications, AINA 2005, 2005:159-162.

[18] GROAT S, TRONT J, MARCHANY R. Advancing the defense in depth model [C]//The 7th International Conference on System of Systems Engineering (SoSE), 2012: 285-290.

[19] SLIPPER D, MCEWAN A A, IFILL W. Modelling and analyzing defense-in-depth in arming systems [C]// International Conference on System Science and Engineering (ICSSE), 2013:303-308.

[20] EOM J H, KIM N U, KIM S H, et al. Cyber military strategy for Cyberspace superiority in Cyber warfare [C]//International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012:295-299.

[21] Joint Chiefs of Staff. Joint publication: 3-0 joint operations, JP 3-0[R]. United States Department of Defense Washington D. C., 2001, 3-28.

[22] WELLS Ⅱ L. Maneuver in the global commons——the Cyber dimension [EB/OL]. 2010-10-01 [2014-01-01]. http://www. afcea. org/signal/articles/templates/Signal _ Article _ Template. asp? articleid = 2472 & zoneid = 306.

[23] 黄仁全，李为民，张荣江，等. 防空信息网络纵深防御体系研究[J]. 计算机科学，2011，38(10A):53-55, 58.

HUANG R Q, LI W M, ZHANG R J, et al. Research on the defense in depth system in air defense information network[J]. Computer Science, 2011, 38(10A):53-55, 58.

[24] SPITZNER L. Problem and challenges with honey pots [EB/OL]. 2004-01-14 [2014-01-01]. http://www.security focus. Com/infocus/1757, 2004.

[25] 姚兰,王新梅. 基于欺骗的网络主动防御技术研究[J]. 国防科学技术大学学报,2008,30(3):65-69.
YAO L, WANG X M. A study on the network active defense technology based on deception[J]. Journal of National University of Defense Technology, 2008, 30(3):65-69.

[26] 吴烨虹. 基于移动代理的入侵检测及反击技术研究[D]. 南京:南京邮电学院,2005.
WU Y H. Study on the intrusion detection and counter attack technology based on the mobile agent[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2005.

Abstract: In this paper, the concept and classification of the Cyber maneuver and the features of the Cyber combat unit, are introduced based on the existing research results and the environment and requirements of the future warfare. According to the features of the tactical maneuver in Cyber space, the difficulties and possibility of fusing the tactic maneuvers of Cyber space with that of the other spaces are discussed.

Key words: Cyber space; tactical maneuver; fusing; command control; decision making