欺骗谋略在网络空间防御行动中运用

刘小虎[1,*] 张恒巍[1] 张玉臣[1] 吕文雷[1]
(1. 战略支援部队信息工程大学，郑州 450001)

摘 要 军事欺骗是谋略运用的重要内容。结合网络空间攻防行动特点，剖析了网络欺骗的原理；借鉴运用博弈理论，分析了欺骗谋略在网络空间防御行动中的制胜机理；总结了支撑网络欺骗实施的蜜罐蜜网、拟态防御和移动目标防御等 3 种主要技术手段的原理及研究重点；给出了欺骗谋略在网络空间防御行动中的组织运用方法。研究成果对于提升网络空间防御效能具有理论价值和实践指导意义。

关键词 网络空间，防御行动，欺骗谋略，博弈论，制胜机理，组织运用
引用格式 刘小虎，张恒巍，张玉臣，等. 欺骗谋略在网络空间防御行动中运用[J]. 指挥与控制学报，2024，10(1)：117-121
DOI 10.3969/j.issn.2096-0204.2024.01.0117

Deception Strategy in Cyberspace Defense Actions

LIU Xiaohu[1,*] ZHANG Hengwei[1] ZHANG Yuchen[1] LYU Wenlei[1]
(1. *Strategic Support Force Information Engineering University, Zhengzhou* 450001, *China*)

Abstract Military deception is an important part of strategic application. Combined with the characteristics of network attack and defense actions, the principle of network deception is analyzed, the winning mechanism of deception strategy in cyberspace defense actions is analyzed by using game theory for reference, the principles and research focuses of three kinds of main technical means, namely honeypot honey net, micmis defense and mobile target defense, etc. and the organization application method of deception strategy in the cyberspace defense actions are provided. The research results have theoretical value and practical guidance meaning for improving cyberspace defense efficiency.

Key words cyberspace, defensive actions, deception strategy, gaming theory, winning mechanism, organizational application
Citation LIU X H, ZHANG H W, ZHANG Y C, et al. Deception strategy in cyberspace defense actions[J]. Journal of Command and Control, 2024, 10(1): 117-121

“兵者，诡道也”。“诡”指千变万化、出其不意；“道”指计谋、方法和手段。“诡道”指用兵作战要采取诡诈多变的方法或手段。《孙子兵法》中诡道是谋略的核心，实质就是军事欺骗。兵以诈立，军事欺骗是谋略运用的重要内容[1]。

网络空间已成为冲突对抗的最前沿、大国战略博弈的新疆域，“无网不胜”成为现代战争新法则[2]。相比于传统战场，网络战场具有无界性和虚拟性的特点，主要表现为受时间因素和空间因素制约小、作战主体和客体相对宽泛、网络攻防格局不对称等。世界各主要军事大国都成立了专业化的网络部队，不断加强网络空间作战能力建设。网络空间作战正悄悄揭开其神秘面纱，逐渐从后台走向前台。特别是美国明确将网络空间作为“作战域”，强调前向防御理念，出台“进攻优先”的网络空间作战战略。

网络安全的本质是对抗，对抗的本质是攻防两端能力的较量[3]。在网络空间攻防行动中，欺骗谋略广为攻击方采用，而易被防御方忽略，在某种程度上加剧了网络攻防的不对称性，形成了网络空间“易攻难守、矛尖盾薄”的不对称格局。网络欺骗防御为开展网络空间防御行动提供了新思路，成为当前网络安全领域研究热点之一。王硕等基于动态伪装思想，提出了一种欺骗式主动防御方法[4]；贾召鹏等研究了面向防御的网络欺骗防御技术[5]；李阳等采用演化博弈理论对蜜罐欺骗的有效性进行了证明[6]；蒋侣等采用信号博弈理论研究了移动目标防御中最优防御策略选取方法[7]。但是，上述文献侧重于欺骗防御技术的研究，在欺骗谋略的制胜机理和组织运用方法等研究方面还有一定不足。本文结合网络空间攻防行动特点，运用博弈理论分析欺骗谋略在网络空间防御行动中的制胜机理；说明欺骗防御主要技术手段的原理及研究重点；给出欺骗谋略在网络空间防御行动中的组织运用方法。

1 网络空间欺骗谋略的制胜机理

1.1 网络欺骗原理剖析

网络空间之所以不安全，主要可以归类为 3 个原因[8]：1）组成网络信息系统的软硬件以及网络协议存在漏洞和后门。漏洞和后门是网络攻击的起点。网络协议由人设计和实现，初始目的是保证可用性，

收稿日期 2021-12-03 录用日期 2022-07-03
*通信作者邮箱 ganlanlvliu@163.com

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

难以保证不存在安全逻辑缺陷;软件由数百万行代码组成,漏洞难以完全避免;网络信息产品全球化供应的今天,硬件后门无法保证根除。2)网络运维管理人员可能存在违规或非法操作。网络安全"三分靠技术,七分靠管理"。人是安全尺度,是安全防御链条中最薄弱环节。网络运维管理人员可能无意或者有意地进行了违规,甚至是非法操作。3)网络承载了巨大的政治经济利益,诱发攻击者发动网络攻击。

攻击方采用欺骗谋略实施"挖漏洞、设后门、植病毒和藏木马"等攻击行为,通过多种方法侦察、收集防御方情报信息,多条途径渗透、控制防御方网络。例如,世界著名黑客凯文·米特尼克(Kevin Mitnick),在年仅15岁时就成功侵入北美空中防务指挥系统,此后又分别侵入了美国国防部、五角大楼等重要核心场所网络系统,他撰写的《The Art of Deception》一书总结了黑客利用社会工程学实施欺骗的各种方法[9]。特别是针对重要目标系统,攻击方会遵循"用兵不复"原则,采用高级可持续威胁(advance persisted theater, APT)方法,开展定制化、针对性的网络攻击。以防火墙、入侵检测系统和以病毒软件为代表的传统防御手段,总体上仍停留在"杀毒灭马""封门堵漏"的被动式防御模式。在管理方面,防御系统使用管理人员为方便操作、易于管理、便于维护等原因,静态化甚至是简单化配置防御系统,降低了防御效果。在传统防御模式下,防御方在明处,防御方网络信息、系统信息、用户信息等敏感数据容易暴露;攻击方在暗处,隐蔽性强,攻击方目的、攻击发起时间、攻击手段特征等关键信息很难获取。攻击方在时间、信息和成本等维度上对防御方构成了不对称优势。

网络欺骗(cyber deception)概念最早出现于20世纪80年代,主要是通过设置伪造的账户和文件诱骗攻击方入侵,从而捕获攻击行为,推测攻击目的、方法和工具[10]。近年来,随着蜜罐蜜网、网络空间拟态防御和移动目标防御等新型动态防御技术的出现,为组织和实施网络欺骗提供了技术支撑。在网络空间防御行动中恰当运用军事欺骗谋略,主动为攻击方设置行动障碍和逻辑陷阱,通过增强自身的不确定性布设出"战争迷雾",从而增加攻击成本和攻击复杂度,能够构建起防御方的不对称优势,是一种主动防御思想。一方面可以转移攻击方视线、消耗攻击资源,延缓网络攻击的突然性,为防御方争取反应时间;另一方面,使攻击方在侦察踩点、扫描探测、渗透攻击等过程中留下痕迹,防御方可以根据痕迹信息分析攻击目的、攻击手段、攻击工具、攻击路径、攻击指纹等特征,为有效识别、预警、抵御和反制网络攻击提供信息支持。

网络杀伤链(cyber kill chain)模型由美国洛克希德·马丁(Lockheed Martin)公司提出[11],它将网络攻击的生命周期划分为6个阶段,分别是网络侦察、试探访问、编写代码、发起攻击、控制提权和持续驻守。类比于网络杀伤链,美国网络安全专家SUSHIL等在《cyber deception——building the scientific foundation》一书中提出了网络欺骗链(cyber deception chain)模型[12],将网络欺骗的生命周期划分为8个阶段,分别是制定目标、收集情报、设计故事、筹备工具、准备欺骗、执行欺骗、实施监控、强化效果。通过对比网络杀伤链和网络欺骗链可知,不同于传统的防御思想,在欺骗防御中,防御方通过精心伪装和动态迁移等方法,内生出系统防御能力,形成与网络攻击的整体对抗博弈态势。在对抗过程中,防御方利用欺骗谋略不断增加系统的不确定性、动态性和随机性,迷惑扰乱攻击方认知、增加攻击复杂度,有效减少或者消除网络攻击的生存时间,延缓或者阻断网络杀伤链的形成,使网络攻防态势向着有利于防御方的方向发展。

1.2 网络欺骗博弈机制分析

博弈论为研究冲突对抗环境下最优策略选取问题提供了有力工具[13]。网络攻防与博弈论在3个本质特征方面十分契合[14]:1)网络攻防双方目标完全对立。攻击方意图攻破目标系统的机密性、完整性和可用性,防御方保护己方目标系统不被破坏。攻防双方目标完全对立、矛盾不可调和。2)网络攻防双方策略相互依存。网络攻防双方行动彼此制约、相互影响,网络攻防态势由双方策略共同决定。防御行动效果不仅取决于防御策略本身,还依赖于攻击方所采用的攻击行动。3)网络攻防双方具有信息有限性。网络攻防双方存在着非合作对抗关系,不可能事先将自身决策信息告诉对方。攻击方和防御方一般仅能了解己方信息和部分对方信息,所掌握的信息是有限和不完备的。但是,在动态对抗过程中,攻防双方均可根据历史数据和专家经验,在分析判断的基础上,对对方决策信息进行预测和推理。因此,借鉴博弈理论研究网络攻防行为,分析网络欺骗的博弈对抗机制,具有重要的理论指导价值。

通过构建网络攻防博弈模型,在分析攻防对抗过程和计算博弈均衡的基础上,可以有效提升攻击预测预警的时效性和准确性,以及防御行动决策规划的针对性和效能,指导网络防御行动。信号博弈理论是典型的不完全信息动态博弈[15]。它通过信号传递描述局中人策略对抗过程,适用于研究欺骗谋略下防御行动组织与实施问题。基于信号博弈理论,将防御方建模为信号发送者,攻击方建模为信号接收者,可对欺骗谋略的制胜机理加以分析[16]。例如,在网络攻防对抗的初始阶段,防御方部署网络信息系统,

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

配置网络拓扑结构、IP 地址和划分网段等。由于网络要对外界提供服务，具有开放共享、互联互通的特点，以及网络信息产品所具有的“同源、同构、同质”等特性，攻击方可通过社会工程学、扫描渗透探测、公开情报获取等多种途径收集防御方初始配置信息。此类信息是攻击方发动网络攻击的基础，可将其视为防御方释放信号。网络杀伤链模型第一阶段“网络侦察”即为攻击方对防御方进行探测、扫描等情报收集活动，可视为接收防御方所释放信号。攻击方接收防御方信号，形成对防御方类型的先验判断，通过综合分析比较，选择对应的攻击策略。在持续动态对抗过程中，攻击方可根据收到的防御方信号，利用贝叶斯法则，动态形成对防御方的后验概率，不断修正对网络防御体系的认知，进而针对性调整攻击行动。

1.3　欺骗信号作用机理分析

根据攻防双方的不完全信息特点，防御方作为信号发送者，可采用欺骗谋略，通过释放欺骗信号，达到误导对方判断，扩大己方收益的目的。但是，由于攻防对抗具有动态多阶段的特点，攻击方作为信号接收方，可以基于专家经验和历史数据，利用贝叶斯法则不断修改对所接收信号的先验判断。因此，应从有效性和局限性两个方面对欺骗谋略的作用机理进行分析。

1）欺骗谋略的有效性。在攻防博弈初期阶段，防御方可通过释放欺骗信号，迷惑和误导攻击方，扰乱攻击方认知，延缓网络杀伤链形成，降低网络攻击速度和减弱攻击突然性，能够为防御方赢得反应时间，部分抵消攻击方拥有的时间不对称优势和先发优势，这是欺骗信号的有效性。因此，防御方在组织和实施网络空间防御行动时，应充分利用欺骗信号的有效性，主动释放欺骗信号。同时，为防止攻击方运用欺骗谋略，应提高对攻击方欺骗信号的甄别能力，尽早识别攻击方动机和行为偏好，从而实施针对性主动防御策略。

2）欺骗谋略的局限性。随着博弈进程推进，攻防双方对对手都逐渐了解，欺骗信号作用会逐渐衰减，低质量的欺骗信号作用甚至可能完全消失。因此，在组织和实施防御行动时，应避免自身欺骗信号的局限性，通过提高欺骗信号质量延缓其衰减过程。同时，注意收集威胁情报，放大攻击方欺骗信号的局限性。

2　网络空间欺骗谋略的主要支撑技术

网络空间是以技术为基础的空间，网络空间作战谋略的设计必须考虑技术手段的支撑。实施欺骗谋略所需的技术手段主要有蜜罐蜜网、网络空间拟态防御和移动目标防御等 3 种支撑技术。

2.1　蜜罐蜜网

蜜罐（honeypot）是最早被防御方所采用的欺骗防御技术[17]。防御方在防御系统中设置诱饵（假目标），诱骗攻击方发动攻击。一方面利用蜜罐收集攻击方手段、特征、路径等信息；另一方面消耗攻击方资源，转移攻击方视线，迟滞攻击方行动。蜜网（honeynet）在蜜罐基础上发展而来，本质上是一种分布式蜜罐。相对而言，蜜罐蜜网方法属于“被动式”欺骗，在应初级的或者自动化的网络攻击时，能够取得较好效果。但是，蜜罐蜜网具有无法实时感知网络状态、可能会被攻击方识破和发现等缺点。在利用该技术组织实施网络空间防御行动时，应着重设计具有交互性好、欺骗性强特点的蜜罐蜜网系统。

2.2　网络空间拟态防御

网络空间拟态防御（cyber mimic defense，CMD）是中国工程院邬江兴院士团队于 2013 年提出的防御技术[18]。受生物界“拟态”现象启迪，邬院士先后提出了“结构适应应用”的拟态计算技术和“结构决定安全”的拟态防御技术。拟态防御通过动态、随机地执行硬件和软件的变体，构建出具有动态、冗余、异构等随机性特点的防御系统，增加攻击方攻击难度，以应对具有不确定性的未知威胁。该防御技术下，基于软硬件漏洞和后门等“暗功能”的攻击方法不再有效。拟态防御属于主动欺骗，软硬件的动态、冗余、异构增强了系统的安全性，但同时也会造成防御成本、系统功耗和复杂度的增加。在利用该技术组织实施网络空间防御行动时，应着重平衡安全性与防御成本的关系，以最小防御代价取得最佳的防御效果。

2.3　移动目标防御

移动目标防御（moving target defense，MTD）是美国国家科学技术委员会于 2011 年提出的 “改变游戏规则”的防御技术[19]。它通过构建、部署动态可变的机制和策略，快速迁移系统攻击面，降低系统脆弱性暴露时间，增加攻击方攻击难度，内生出系统防御能力。作为网络空间安全领域的新思路，移动目标防御反映了未来网络防御将“死”网络变成“活”网络的技术发展趋势。移动目标防御模式下，防御系统“移动” 频率低，则系统安全性无法保证，防御系统“移动”频率高，则可能影响系统性能。在利用该技术组织实施网络空间防御行动时，应着重判断“移动时机”，并变换到系统最佳的状态，平衡由于“移动”所带来的安全性，与由于“移动”所造成系统可用性降低之间的关系，以最大程度地增强防御效果。

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

3 网络空间欺骗谋略的组织运用方法

3.1 技术层面的智能动态欺骗

随着智能指挥与控制广泛应用，需要在网络空间防御中灵活实施智能动态欺骗[20]。技术方面综合运用主动、被动欺骗防御支撑技术，通过设置假目标和动态迁移，使攻击者收集到虚假信息或者失效信息，增大攻击方成本，延缓或阻断网络攻击杀伤链的形成，降低网络攻击的成功率。通过冗余路径、多态服务、动态跳变等多种手段，增加防御系统的随机性和不确定性，增大攻击方通过探测扫描获取防御方信息的工作量和实施攻击的复杂度，消耗其精力和资源。利用人工智能技术和博弈论方法实施智能动态欺骗，解决欺骗过程中“欺骗什么-欺骗方式”和“何时欺骗-欺骗时机”问题。根据不同的网络攻防场景，分别建立智能动态欺骗博弈模型，量化计算欺骗成本和收益，利用 Q-learning、深度 Q 网络（deep Q-learning，DQN）等智能强化学习算法求解博弈均衡，在此基础上给出最优欺骗防御策略，指导防御行动。同时，利用大数据技术，深入挖掘痕迹信息，准确分析攻击手段、攻击工具、攻击路径等特征，为有效识别和抵御网络攻击提供信息支持，设计更有针对性的欺骗策略。

3.2 谋略层面的虚实结合欺骗

在实体空间战争实践中，运用欺骗谋略往往要遵循真真假假、虚虚实实、隐真示假、虚张声势的原则。在网络空间防御行动中，同样需要进行虚实结合欺骗。“能而示之不能，用而示之不用”。为扰乱对方认知决策过程，在网络对抗过程中，根据信号博弈理论，防御方应释放真假参杂、虚实结合的信号，最大限度发挥欺骗信号的有效性。例如，可在蜜罐蜜网的基础上布设动态伪装网络。动态伪装网络包括真实网络和伪装网络两个部分。真实网络为合法用户提供正常服务，并不可避免地释放出真实信号。在伪装网络中设置“高价值”诱饵文件、模拟真实业务流量，并主动释放虚假的防御配置信息，例如，网络拓扑结构、IP 地址、网段划分、服务器开放端口和远程访问点、系统漏洞等，诱骗攻击方渗透和攻击。

3.3 能力层面的显隐结合威慑

类似于“核威慑”战略[21]，在组织实施网络空间防御行动时，应结合欺骗谋略实施“显隐结合”的网络空间威慑行动。“显”，即一方面通过一系列网络空间作战演习、演练等活动，充分展示己方具备瘫痪敌方网络空间的能力。例如，美国自 2006 年以来持续开展两年一度的“网络风暴”演习，展示其网络战能力；另一方面通过官方渠道公开表明维护己方网络空间安全的决心意志，释放出强烈信号，有力震慑攻击方。同时，也可借助地方网络安全企业的技术优势，实施攻击溯源和反制。例如，2020 年 3 月 3 日，360 安全大脑曝光了美国中央情报局对我国发起的网络渗透攻击行动，公布了 APT 行动组织、攻击武器样本文件和部分从事武器研发制作的人员信息等证据材料。“隐”，即通过系统的、专业化的网络预攻击行动，提前在敌方网络空间预置漏洞后门、埋设逻辑炸弹、隐藏病毒木马，研发“杀手锏”武器，确保己方具备毁瘫敌方网络空间的能力，形成可信威慑。在“显”和“隐”的过程中，再综合运用欺骗谋略，真真假假、显隐结合，增强威慑效果，达到不战而屈人之兵的目的。

4 结论

兵不厌诈，欺骗谋略在网络空间防御行动中具有重要应用价值。本文结合网络空间攻防行动特点，剖析了网络欺骗的原理；借鉴运用博弈理论，分析了欺骗谋略在网络空间防御行动中的制胜机理；给出蜜罐蜜网、网络空间拟态防御和移动目标防御等 3 种主要支撑技术的原理及研究重点；从技术层、谋略层和能力层给出了 3 种网络空间欺骗谋略的组织运用方法。研究成果是对欺骗谋略在网络空间防御行动中运用的探索，对于增强网络空间防御效能具有借鉴意义。

References

[1] 高金虎, 张佳瑜. 战略欺骗 [M]. 北京: 金城出版社, 2015: 1-7.
GAO J H, ZHANG J Y. Strategic deception[M]. Beijing: Jincheng Publishing House, 2015: 1-7. (in Chinese)

[2] 敖志刚. 网络空间作战: 机理与筹划 [M]. 北京: 电子工业出版社, 2018: 1-10.
AO Z G. Cyberspace operation: mechanism and planning[M]. Beijing: Electronic Industry Press, 2018: 1-10. (in Chinese)

[3] 习近平. 在网络安全和信息化工作座谈会上的讲话 [N/OL]. (2017-01-29)[2016-04-26]. http://cpc.people.com.cn/n1/2016/0426/c64094-28303771.html.
XI J P. Speech at the Forum network security and information[N/OL]. (2017-01-29)[2016-04-26]. http://cpc.people.com.cn/n1/2016/0426/c64094-28303771.html. (in Chinese)

[4] 王硕, 王建华, 裴庆祺, 等. 基于动态伪装网络的主动欺骗防御方法 [J]. 通信学报, 2020, 41(2): 97-111.
WANG S, WANG J H, PEI Q Q, et al. Active deception defense method based on dynamic camouflage network[J].

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Journal on Communications, 2020, 41(2): 97–111. (in Chinese)

[5] 贾召鹏. 面向防御的网络欺骗技术研究 [D]. 北京: 北京邮电大学, 2018.
JIA Z P. Research on defensive cyber deception technology [D]. Beijing : Beijing University of Posts and Telecommunications, 2018. (in Chinese)

[6] 李阳, 赵俊楠, 石乐义. 基于演化博弈的蜜罐有效性机理证明 [J]. 计算机技术与发展, 2020, 30(4): 105–109.
LI Y, ZHAO J N, SHI L Y. The mechanism of honeypot effectiveness based on evolutionary game[J]. Computer Technology and Development, 2020, 30(4): 105–109. (in Chinese)

[7] 蒋侣, 张恒巍, 王晋东. 基于信号博弈的移动目标防御最优策略选取方法 [J]. 通信学报, 2019, 40(6): 128–137.
JIANG L, ZHANG H W, WANG J D. Optimal strategy selection method for moving target defense based on signaling game[J]. Journal on Communications, 2019, 40(6): 128–137. (in Chinese)

[8] 刘小虎, 张玉臣. 网络空间安全保密困境与移动目标防御 [J]. 保密工作, 2019, 35(2): 71–72.
LIU X H, ZHANG Y C. Cyberspace security dilemma and mobile target defense[J]. Confidentiality Job, 2019, 35(2): 71–72. (in Chinese)

[9] 凯文·米特尼克, 威廉母·西蒙. 入侵的艺术 [M]. 潘爱民, 译. 北京: 清华大学出版社, 2014: 15–26.
KEVIN M, WILLIAM S. The art of deception[M]. PAN A M, translation. Beijing: Tsinghua University Press, 2014: 15–26. (in Chinese)

[10] 胡永进, 马骏, 郭渊博. 基于博弈论的网络欺骗研究 [J]. 通信学报, 2018, 39(2): 9–18.
HU Y J, MA J, GUO Y B. Research on cyber deception based on game theory[J]. Journal on Communications, 2018, 39(2): 9–18. (in Chinese)

[11] BRYANT B, SAIEDIAN H. A novel kill–chain framework for remote security log analysis with SIEM software[J]. Computers & Security, 2017(67): 198–210.

[12] SUSHIL J, SUBRAHMANIAN V S, VIPIN S, 等. 网络空间欺骗——构筑欺骗防御的科学基石 [M]. 马多贺, 雷程, 译. 北京：机械工业出版社，2017: 1–11.
SUSHIL J, SUBRAHMANIAN V S, VIPIN S,et al. Cyber deception–building the scientific foundation of deception defense[M]. MA D H, LEI C, translation. Beijing: China Machine Press, 2017: 1–11. (in Chinese)

[13] 王震, 袁勇, 安波, 等. 安全博弈论研究综述 [J]. 指挥与控制学报, 2015, 1(2): 121–149.
WANG Z, YUAN Y, AN B, et al. An overview of security games[J]. Journal of Command and Control, 2015, 1(2): 121–149. (in Chinese)

[14] ZHANG H W, WANG J D, YU D K, et al. Security defense policy selection method using the game theory of incomplete information[J]. China Communications, 2015(12): 123–131.

[15] 张恒巍, 余定坤. 基于攻防信号博弈模型的防御策略选取方法 [J]. 通信学报, 2018, 37(5): 51–61.
ZHANG H W, YU D K. Defense policies selection method based on attack–defense signaling game model[J]. Journal on Communications, 2018, 37(5): 51–61. (in Chinese)

[16] LIU X H, ZHANG H W, ZHANG Y C, et al. Active defense strategy selection method based on two–way signaling game [J]. Security and Communication Networks, 2019(1362): 1–14.

[17] 诸葛建伟, 唐勇, 韩心慧, 等. 蜜罐技术研究与应用进展 [J]. 软件学报, 2013, 24(4): 825–842.
ZHUGE J W, TANG Y, HAN X H, et al. Honeypot technology research and application[J]. Journal of Software, 2013, 24(4): 825–842. (in Chinese)

[18] 邬江兴. 网络空间拟态防御原理 [M]. 北京: 科学出版社, 2019: 1–5.
WU J X. The principle of mimicry defense in cyberspace [M]. Beijing: Science Press, 2019: 1–5. (in Chinese)

[19] 蔡桂林, 王宝生, 王天佐, 等. 移动目标防御技术研究进展 [J]. 计算机研究与发展, 2016, 53(5): 968–987.
CAI G L, WANG B S, WANG T Z, et al. Research and development of moving target defense technology[J]. Computer Research and Development, 2016, 53(5): 968–987. (in Chinese)

[20] 王飞跃, 刘玉超, 秦继荣, 等. C2M 和 5G: 新时代的智能指挥与控制 [J]. 指挥与控制学报, 2019, 5(2): 79–81.
WANG F Y, LIU Y C, QIN J R, et al. C2M and 5G: intelligent command and control in the connected and smart age [J]. Journal of Command and Control, 2019, 5 (2): 79–81. (in Chinese)

[21] 张小娟, 向钢华. 基于信号博弈的“显隐结合”战略威慑分析 [J]. 兵工自动化, 2018, 37(2): 54–57.
ZHANG X J, XIANG G H. Analysis of strategy deterrence combining with evident and recessive ways based on signal game theory[J]. Ordnance Industry Automation, 2018, 37(2): 54–57. (in Chinese)

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net