doi:10.3969/j.issn.1001-893x.2013.11.017

# 网络空间攻防对抗技术及其系统实现方案*

雷 璟**

(中国电子科学研究院,北京 100041)

**摘 要**:在分析网络空间及对抗特点的基础上,讨论了网络空间攻防对抗的主要技术,即攻防博弈理论、网络攻击行为分析、网络攻击追踪和网络主动防御技术。提出了网络空间攻防对抗系统的实现方案,并分析了其可行性。此技术和系统能够为我国网络空间安全技术体系发展提供技术支撑,保障我国网络空间安全,推动我国网络空间安全产业的发展,对加快我国自主可控安全产品研发和核心技术发展具有重要作用和意义。

**关键词**:网络空间;攻防对抗;攻击追踪;主动防御

**中图分类号**:TN918;TP393.08 **文献标志码**:A **文章编号**:1001-893X(2013)11-1494-06

# Cyberspace Attack and Defense Confrontation Technology and System Realization Scheme

LEI Jing

(China Academy of Electronics and Information Technology, Beijing 100041, China)

**Abstract**: With the analysis of features of cyberspace and confrontation, the cyberspace attack and defense confrontation technology is discussed, including attack and defense fight theory, network attack action analysis, network attack tracing and network active defense technology. The cyberspace attack and defense confrontation system scheme is proposed. The technology and system can provide technology support for China's cyberspace security technology system development, protect China's cyberspace security, promote China's cyberspace security industry development, and also have important effect and meaning on accelerating China's independent, controllable security product exploitation and kernel technology development.

**Key words**: cyberspace; attack and defense confrontation; attack tracing; active defense

## 1 引 言

网络空间是继陆、海、空、天领域之后的第五维空间,它是"以自然存在的电磁能为载体,人工网络为平台,信息控制为目的的空间"[1]。网络空间包括电子系统、计算机、通信网络和其他信息基础设施,通过对"信息"的产生、存储、修改、交换和利用,实现对物理实体的实时控制,以及影响人的认知活动和社会行为。

网络空间已经成为国家最重要的基础设施,网络空间对抗就成为保卫国家安全的重要使命[2]。美国正在利用其信息优势发展全球信息霸权地位,尤其在网络空间安全的"攻击"态势明显,推出了震网、火焰、舒特等典型的网络攻击武器。俄罗斯、日本、英国、以色列等国家也纷纷制定了各自的网络空间安全战略,组建了网络战队伍,研发各类网络攻击武器,加快筹备随时可能会来临的"网络空间战"。

我国在网络空间安全领域已经建立了分级保护体系和信息安全等级保护体系。在网络空间对抗方面,也形成了一些军用和民用的攻防对抗试验床和试验环境。但是由于我国自主可控的基础产品、核心信息技术、各种基础软件和应用软件都比较缺乏,

* 收稿日期:2013-08-07;修回日期:2013-10-22 Received date:2013-08-07;Revised date:2013-10-22
** 通讯作者:leijanet@163.com **Corresponding author**: leijanet@163.com

从应对威胁能力的角度来说,还不足以应对大型跨国集团、国家之间的对抗,对比网络空间霸权国家,基本处于“非对称”的状态。中国要想长久地保证国家安全、社会稳定与经济发展,就必然要能确保自己的网络空间安全,否则其他事情一切免谈[3]。

本文分析了网络空间以及网络空间对抗的特点,对网络空间攻防对抗主要技术进行了分析研究,提出了网络空间攻防对抗系统的具体实现,为我国网络空间安全体系建设提供技术支撑,保障我们国家的网络空间安全,保卫国家核心利益。

## 2　网络空间及对抗特点

### 2.1　网络空间特点

网络空间是第五维作战空间和事关国家利益的重要领域,受到世界各国的重视,推动了信息战新思想、新概念、新战法、新技术的不断涌现,网络空间具有融合性、隐蔽性、无界性、高速性等特点。

(1)融合性

网络空间强调信息系统和物理系统的深度融合,需要实现计算过程、信息过程和物理过程的高度集成。

(2)隐蔽性

网络空间是变化莫测的,无论是进攻还是防御都可在对方毫无预兆的情况下进行,达到网络空间作战效果。

(3)无界性

网络空间没有地理界限和自然界限,网络空间作战能够在任何地方发生,超越规定的组织和地理界限,可以跨越陆、海、空、天领域,进行全域作战。

(4)高速性

信息在网络空间的移动速度接近光速,利用这种高质量的信息移动速度能够使作战效能倍增。

### 2.2　网络空间对抗特点

基于以上网络空间具备的特点,网络空间主流的对抗方式具备广维度、多目标、高烈度、短猝发等特点,为信息安全防护带来了极大的复杂性和不确定性。我们面临的挑战是如何提高网络的健壮性来防止那些蓄谋已久的攻击[4]。具体网络空间对抗特点如下所述。

(1)广维度

网络空间对抗结合网络战与心理战,可以在物理域、逻辑域、认知域实施,形成监控网络、欺骗网络、瘫痪网络和控制网络的巨大威力。

(2)多目标

网络空间对抗的目标不仅包括军事领域,还涵盖政治、经济、社会等领域,甚至囊括了敌方的军用信息网络、关系到国计民生的信息基础设施。

(3)高烈度

网络空间对抗带来的后果可能直接引发严重的现实空间损害,同时网络空间与人认知交互的复杂性,使得网络空间对抗对社会活动的影响面更大,影响更快速,影响途径更加复杂,引发的后果更加严重,甚至直接威胁国家安全和社会稳定。

(4)短猝发

网络攻击效果不受时间和距离的影响,并具有瞬间到达的特性。当一方成功地对另一方的网络实施攻击后,就会对其社会、政治、经济、科技、军事等系统造成极大的破坏,使整个网络作战态势发生急剧的变化。但整个网络作战过程却往往会在很短的时间内完成。

## 3　网络空间攻防对抗主要技术

网络空间攻防对抗通过配置网络攻防对抗的虚拟试验环境,在虚拟的、高实时、强交互、网络拓扑结构处于高度不稳定状态的网络环境中,对攻防博弈理论、基于过程的网络攻击行为分析技术、网络攻击追踪技术、网络主动防御技术进行研究,实现对网络攻击和网络防御的模拟,再现攻击者与防御者的博弈过程,最终用于评估被测网络的可恢复性、灵活性和安全性。

美国在网络空间安全的“攻击”态势明显,经常进行网电空间战演习,即“网电风暴”,以试验计算机网络的防御能力[5]。俄罗斯、日本、英国、以色列等国网络空间安全战略明确。

### 3.1　攻防博弈理论

博弈论是一套策略选择理论,为应用数学的一个分支[6]。博弈论是研究智能的理性决策者之间冲突与合作的理论,而攻防本身就是一种冲突,攻击与防御在方法和技术上的较量归根到底是攻防双方在决策上的博弈。通过建立和分析博弈模型能够评价攻防双方的既定策略,使得仿真平台的评估不局限于有限次的仿真结果,而是基于攻防双方的驱动与能力,获得纵深的策略集合甚至攻防均衡点,使防御方能够基于最小的代价获得最大的安全收益,为网络空间对抗验证提供理论依据。

美国在长期的网络战理论研究和实践方面已经

初步形成了网络战攻防战略理论,并出台了一系列的网络空间行动战略,统筹谋划网络空间攻防对抗策略。网络已经成为美国必不可少的用于扩展美国价值和思想的工具,正如美国寻求政权扩张一样[7]。俄罗斯、日本、英国、以色列等国也制定了相应的"国家网络空间安全战略"。

### 3.2 网络攻击行为分析技术

攻击行为是测试系统脆弱性和风险的重要手段。从网络攻击操作流程来看,一次网络攻击行为主要由目标分析和攻击实施两部分组成。此外,由于攻击者和攻击目的与网络攻击有着紧密的关联,在对目标分析和攻击实施进行分析的同时,也需要对攻击者与攻击目的分析。

网络攻击具有一系列的行为特征。攻击者事先经长期的准备,然后在对目标有了清楚的了解之后,再通过各种方法隐藏自己的访问路径、所访问内容,尽力潜藏于目标系统中。网络入侵首先明确攻击的目的,然后寻找漏洞作为突破点,进而逐步扩大访问权限,直至获得最高控制权限。图 1 描述了一种渐进式攻击行为。

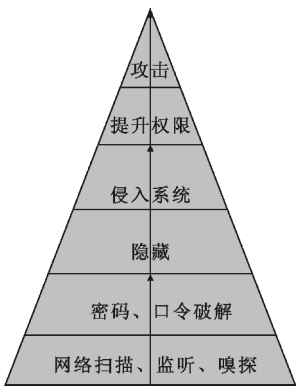



图 1 渐进式攻击行为示意图

Fig. 1 The sketch map of asymptotic expression attack action

美国在网络攻击技术与武器发展方面,除了大力发展恶意代码、网络欺骗以及分布式拒绝服务攻击等常规网络攻击武器以外,具有综合性和定向性的新型网络攻击武器成为其发展的重点。以色列也开始加大对网络作战的研究力度。

### 3.3 网络攻击追踪技术

攻击追踪的最终目标是能够定位攻击源的位置,推断出攻击报文在网络中的穿行路线,从而为入侵检测系统的事件处理、入侵响应决策提供有价值的信息,协助找到攻击者。同时也为网络安全管理员提供情报,指导他们关注入侵行为频繁发生的网段,采取必要的预防措施,以及及时发现成为入侵者"跳板"的主机或路由器。对于网络黑客而言,成熟有效的追踪技术对他们也有威慑作用,迫使他们为了防止被追踪到而减少甚至停止攻击行为。

攻击追踪按照图 1 描述的渐进式攻击层次来进行监测,通过入侵检测系统和在网络中布设的信号采集、分析节点如网络协议分析仪、网络信道检测等设备,结合操作系统、防火墙的日志记录,对攻击者进行识别、锁定,分析攻击者采取了哪个层次的攻击,进一步判断其下一步可能采取的攻击行为,以便在其可能发起攻击的目标上事先做好安全防范和更细致的监测记录,如记录系统所有进程、文件的创建、访问和网络通信数据。系统通过监视网络中的报文,实时发现攻击和非法攻击行为,提供报警信息,与防火墙系统联动,对攻击和非法攻击行为进行及时的阻断。

俄罗斯已经拥有了众多的网络精英,在追踪网络攻击行为与反病毒技术方面更是走在了世界的前列。英国也提出了针对性及操作性都很强的应对网络空间攻击和破坏的有效措施。

### 3.4 网络主动防御技术

主动防御技术是一种新的对抗网络攻击的技术,也是当今网络安全领域新兴的一个热点技术[8]。主动防御是指能够对攻击进行控制和反击,动态地对网络设备进行操作;其特点是能够采取有效的措施避免攻击对系统的破坏,拖住攻击者,侦测或反击攻击行为;它的中心思想是控制和反击。网络主动防御不但对信息系统网络进行保护,同时对恶意进攻进行记录,为必要时进行反击提供信息。

主动防御技术根据使用技术的不同分为初级方式的主动防御、中级方式的主动防御和高级方式的主动防御技术三类。初级方式的主动防御技术可以采用隐患扫描等技术。中级方式的主动防御技术可以采用联动防火墙等技术,如与防病毒、入侵检测、日志处理实现联动。高级方式的主动防御技术可以采用取证、入侵诱骗、自动恢复、主动响应等技术。

美国在安全防护体系方面形成了纵深防御信息安全保障框架、PDRR 动态防御模型,以及国防核心安全服务框架等典型成果。日本设置了专门的"网络空间安全卫队",以应对网络攻击。

## 4 网络空间攻防对抗系统实现

网络空间攻防对抗系统由网络防御模块、网络

攻击模块、攻击追踪与主动防御模块 3 个部分组成。网络防御模块实现对系统进行保护,同时对恶意进攻进行记录,为必要时进行反击提供信息。网络攻击模块通过对网络防御模块进行探测、扫描的信息进行分析,利用对方系统开放的相关服务及存在的漏洞,根据攻击库相应攻击策略进行有针对性的攻击并报告攻击进展情况。攻击追踪与主动防御模块依托网络防御模块和网络攻击模块对实施的各种攻击行为进行追踪,通过追踪攻击来源、推测攻击目的来建立攻击行为规则,从而识别出所采取的攻击手段,在入侵网络进入系统内部时进行主动防卫,阻止入侵数据的传输,从而抵制入侵者的入侵,这种机制就称为主动防御[9]。

### 4.1　网络防御模块

防御子系统从网络结构、操作系统、应用程序、数据、人员 5 个方面进行全面防御,并利用网络入侵检测和网络入侵欺骗进行积极防御。

防御子系统的功能框图如图 2 所示。

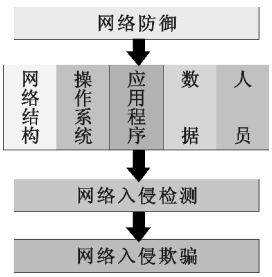



图 2　防御子系统功能框图

Fig. 2 The functional framework of defense subsystem

### 4.2　网络攻击模块

攻击子系统从信息收集、网络侦察、实施攻击、攻击后处理到攻击效果评估来实现整个攻击过程,具体攻击过程如下所述。

(1)信息收集:信息收集是一个综合过程,包括使用者信息、网络开放时间等信息采集功能。

(2)网络侦察:网络侦查是指在对目标进行全面了解的基础上,使用一定的技术手段和策略,依托智能攻击库支持,确定攻击目标的攻击点,生成网络攻击方案,为攻击做好准备。

(3)实施攻击:使用系统集成的工具包,按照生成攻击方案实施网络攻击,攻击目标包括使目标不能有效工作、获取目标有价值数据、破坏目标有价值数据、控制目标部分或全部功能等多种效果。

(4)攻击后处理:实现消除痕迹、再次攻击、间接攻击等。

(5)效果评估:实现系统攻击效果自动评估功能。

攻击子系统的功能框图如图 3 所示。

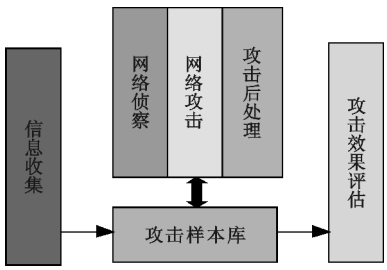



图 3　攻击子系统功能框图

Fig. 3 The functional framework of attack subsystem

### 4.3　攻击追踪与主动防御模块

攻击追踪与主动防御模块以攻防对抗网络为依托,对网络攻击数据进行采集,提取攻击行为规则和相应的特征码为攻击样本库提供数据源,采集到的攻击数据将提交给攻击行为识别子模块,攻击行为识别子模块也将利用攻击样本库对攻击进行识别,同时提交结果由攻击行为预测子模块来对下一步攻击进行预测,以便为攻击主动防御提供支持,在攻击的下一节点和方向进行有目的地防范。攻击追踪与主动防御模块组成结构图如图 4 所示。

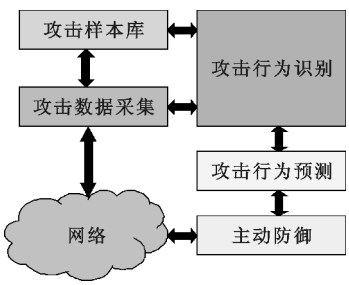



图 4　攻击追踪与主动防御模块组成结构图

Fig. 4 The composition of attack tracing and active defense module

### 4.4　攻防对抗系统实现

攻防对抗系统实现集成各种网络攻击技术为一体的网络攻击系统和集成各类网络防护技术为一体的网络防御系统之间的对抗[10]。在虚拟的、动态变化的网络空间环境中的攻防对抗系统包括网络防御模块、网络攻击模块和攻击追踪与主动防御模块。防御模块提供各类网络安全防护手段,对被保护的系统进行防护。攻击模块提供多种攻击工具,针对被攻击的系统存在的漏洞和缺陷进行攻击。攻击追

踪与主动防御模块在网络防御模块和网络攻击模块的基础上,监测、记录、分析网络、主机、网络设备状态和日志,实现对入侵识别、追踪,并确定适当时机进行反击。

网络空间环境中的攻防对抗系统实现示意图如图 5 所示。

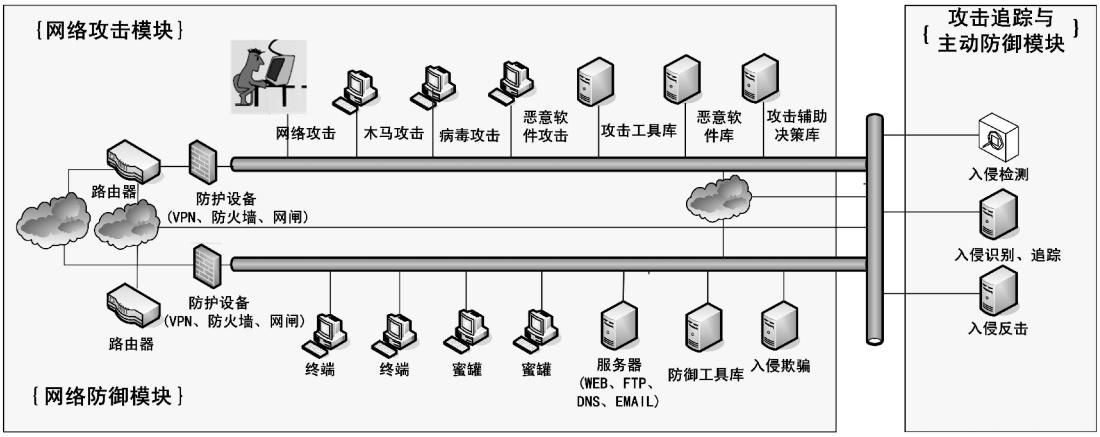



图 5 网络空间攻防对抗系统实现示意图

Fig. 5 The sketch map of cyberspace attack and defense confrontation system realization

### 4.5 系统可行性例证

攻防对抗系统实现的关键是需要对网络攻防博弈理论、攻击建模、主动防御等理论和技术进行研究,实现对网络攻击和网络防御的模拟,再现攻击者与防御者的博弈过程。其中,网络攻击模块需要实现对典型网络攻击手段和攻击效果的模拟,可提供模拟入侵攻击、流量攻击、病毒攻击等攻击手段的工具集。网络防御模块需要实现对典型网络防御手段和防护效果的模拟,可提供模拟网络入侵检测、防病毒网关等防御手段的工具集。

目前,攻防对抗系统已经在实验室通过现实、仿真相结合的方式,搭建了一个网络攻防对抗演练平台,包括攻防软件和攻防演练网站两部分,实现了对各种网络攻防手段进行演练、测试与验证的功能。在网络攻防对抗演练平台中集成、开发了大量的网络攻防工具,实现了多种特殊的攻击方法,包括网络扫描类、监听嗅探类、口令破解类和网络攻击类攻击手段。攻防演练网站为网络攻防演练搭建所需的网站环境,提供邮箱破解、论坛漏洞入侵、网页木马传播和脚本破解等测试环境。攻击方通过夺取网站的控制权,并利用网站扩散病毒、木马来对被攻击方实施攻击。防御方则要对入侵进行告警,追踪其来源,并分析其后续破坏目标,从而启动防护系统。攻击追踪与主动防御模块通过追踪攻击来源、推测攻击目的来建立攻击行为规则,从而为防御设备对特殊攻击的识别提供参数以便识别出所采取的攻击手段。

## 5 结束语

本文针对网络空间对抗的特点,在攻防博弈理论研究的基础上,通过网络攻击行为分析技术、网络攻击追踪技术和网络主动防御技术而实现的网络空间攻防对抗系统,已经列入我国网络空间安全技术体系发展建议。同时,该系统能够模拟真实的网络作战环境,针对各种作战手段进行试验,以实现网络战能力的重大变革,打赢网络战争,最终为保护国家网络空间安全、保卫国家核心利益提供有效的技术保障手段。下一步的工作重点是深入网络空间安全技术体系研究和网络攻击、主动防御等关键技术攻关,研发攻防兼备的网络空间攻防对抗工具和系统。同时提高系统的攻防对抗试验与验证能力,提升对网络空间攻防对抗机理与技术发展方向的认知,支撑网络空间对抗策略制定、技术验证和自主安全研发,促进我国由信息安全产业大国向信息安全产业强国转型。

**参考文献:**

[1] 孙柏林. 网络空间病毒猖獗,工业安全形势严峻[J]. 自动化技术与应用,2012,31(10):1-2.
SUN Bo-lin. Cyberspace virus rampancy, industry security situation grimness[J]. Techniques of Automation & Applications, 2012, 31(10): 1-2. (in Chinese)

[2] 曲成义. 网络空间安全保密对抗态势和应对策略[J].

保密科学技术,2012(4):6-7.
QU Cheng-yi. Cyberspace securityrivalry situation and reply policy[J]. Secrecy Science and Technology, 2012(4):6-7. (in Chinese)

[3] 董淑英,林克成,郑雨昊. 物联网与网络空间安全[J]. 河北省科学院学报,2011,28(3):81-82.
DONG Shu-ying, LIN Ke-cheng, ZHENG Yu-hao. Internet of Things and cyberspace safety[J]. Journal of the Hebei Academy of Sciences, 2011, 28(3): 81-82. (in Chinese)

[4] Qu Zehui, Wang Pu, Song Chaoming, et al. Enhancement of scale-free network attack tolerance[J]. Chinese Physics B, 2010, 19(11): 110504-1.

[5] Clarke R A, Knake R K. 网电空间战[M]. 刘晓雯,陈茂贤,李博恺,等,译. 北京:国防工业出版社,2012:26-27.
Clarke R A, Knake R K. Cyber War[M]. Translated by LIU Xiao-wen, CHEN Mao-xian, LI Bo-kai, et al. Beijing: National Defense Industry Press, 2012: 26-27. (in Chinese)

[6] 牛通,田志宏. 基于博弈论和网络弱点分析的网络主动防御技术研究[J]. 智能计算机与应用,2012,2(3):57-58.
NIU Tong, TIAN Zhi-hong. The Network Active Defense Research based on the Game Theory and the Analysis of Network Vulnerabilities[J]. Intelligent Computer and Applications, 2012, 2(3): 57-58. (in Chinese)

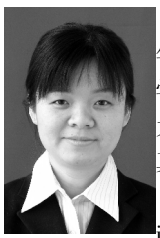
[7] Yi Wenli, Xing Haibing. Divergence and Co-operation between China and the U. S. on the Cyberspace Issue[J]. Contemporary International Relations, 2012, 22(4): 124-141.

[8] 王朝阳. 基于主动防御的网络安全攻防实验平台设计[J]. 电脑知识与技术,2010,20(6):5442-5443.
WANG Chao-yang. Design of Network Safety Attack and Defense Test Platform based on Active Defense[J]. Computer Knowledge and Technology, 2010, 20(6): 5442-5443. (in Chinese)

[9] 刘彦玲. 基于主动防御的网络安全防范技术研究[J]. 无线互联科技,2013(3):15-16.
LIU Yan-ling. The network security keep watch technology research based on Active Defense[J]. Wireless Internet technology, 2013(3): 15-16. (in Chinese)

[10] ZHANG Xian, YAO Shupin, TANG Chenghua. Assessing the Risk Situation of Network Security for Active Defense[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6): 1718-1719.

## 作者简介:



**雷　璟**(1977—),女,湖北武汉人,2003年于华中科技大学获计算机应用技术专业工学硕士学位,现为高级工程师,主要研究方向为信息安全、信息网络安全建设、网络安全仿真评估。

LEI Jing was born in Wuhan, Hubei Province, in 1977. She received the M. S. degree form Huazhong University of Science and Technology in 2003. She is now a senior engineer. Her research interests include information security, information network security construction, network security simulation and evaluation.

Email: leijanet@163.com