

网电空间与安全

Wangdian Kongjian Yu Anquan

■ 周贤伟 主编

■ 林福宏 王建萍 许海涛 陈月云 刘倩 副主编



国防工业出版社
National Defense Industry Press

网电空间与安全

周贤伟 主编

林福宏 王建萍 许海涛 陈月云 刘倩 副主编

国防工业出版社

· 北京 ·

内 容 简 介

网电空间目前已经发展成为一个从抽象到具体,从单纯虚拟空间到物理、信息、认识、社会多维空间的智慧电磁系统,成为承载科学、经济、艺术、文化的全新空间,成为影响经济发展和文化传播的重要平台。

本书紧紧围绕网电空间的定义、体系架构、网电空间的安全展开,全面介绍了网电空间的安全体制,从用户角度全面解释了网电空间的安全,反映了网电空间的安全研究现状,内容全面。

本书可供从事信息安全研究的技术人员使用,也可供军事爱好者阅读。

图书在版编目(CIP)数据

网电空间与安全 / 周贤伟主编. —北京: 国防工业出版社, 2015. 2

ISBN 978 - 7 - 118 - 08799 - 4

I. ①网… II. ①周… III. ①互联网络 - 安全技术 - 研究 IV. ①TP393.408

中国版本图书馆 CIP 数据核字(2015)第 014482 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

国防工业出版社印刷厂印刷

新华书店经售

*

开本 880 × 1230 1/32 印张 6 $\frac{3}{4}$ 字数 190 千字

2015 年 2 月第 1 版第 1 次印刷 印数 1—3000 册 定价 38.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777

发行邮购:(010)88540776

发行传真:(010)88540755

发行业务:(010)88540717

序

Cyberspace 一词,有译作“赛博空间”者,本书定为“网电空间”。

应该承认,美国人的创新精神强,这是美国科技领先的重要原因之一。除了具体技术,美国人在体系、概念上的新提法也层出不穷,不断地引领潮流,互联网就是一个,几乎改变了科技、产业、媒体、生活等的方方面面。但他们提出的有些概念,以我贫乏之知识,则会感到不得要领,“网电空间”即其一例。近些年,有关网电空间的文章不少,也有少数这方面的书籍出版。其中,以介绍情况、说明理解、联系个别应用者居多。然而,由于此题目的不确定性、不成熟性、理解的差异性,这些讨论还需不断深入,也一定会持续地探讨下去。数年前在会议上与周贤伟教授讨论过“网电空间”,他们团队对于新技术发展较敏感,也投入到网电空间的研究之中。日前,周教授告知其新书《网电空间与安全》一成稿,嘱为之作序,虽感力不从心,仍不揣浅陋而勉为其难,意其作具特色,值得推介。粗略浏览了书稿,尚未能深入理解,但觉此书有数点突出处,值得一读。一、材料丰富,收集、参考了自威廉·吉布森创造“cyber”一词以来大量有关资料,包括技术、管理和哲学,加以综述提炼,方便了读者。二、用4、5、6 三章的篇幅重点讨论了网电空间的安全攻防及管理,是大众关注的热点。安全是双方、多方的博弈,世上原无绝对的安全,但在事关国防军事、国计民生的“网电空间”上人们对安全保密更不敢有半点懈怠。本书对此做了多方面讨论。三、联系应用,8、9 两章从最重要、最为人关注的法律和军事应用开始,讨论了多种最可能应用,能给读者诸多启发。此书适应的读者范围较广,既可作为国防军事领域研究人员学习、了解网电空间的参考读物,也可作为相关领域尤其是高等院校信息、电子、通信和计算机等专业师生的参考用书。总之,本书对关心和研究“网电空间”的各方面读者均值得阅读,不妨

一试。有一点需要提醒注意,由于书中很多材料取自国外资料,加之翻译语言上的差异,有些地方读者需依自己的理解加以体会。

最后,提出常困惑我的一个问题,希望能与看了此书的读者探讨。如一开始所说,美国人善于提出新的概念,那么,这些年来他们将一个科幻小说首先创造的词汇“网电空间”加以提升、扩大,加以“正规化”,所为何来呢?有什么本质的创新呢?与他们一直以来提出的互联网、信息高速公路、C³I、C⁴I、C⁴ISR、C⁴IKSR、全球信息栅格 GIG、信息战、网络战、物联网、虚拟化、云计算等相比增加了什么本质的内容呢?综合了哪些重要元素和系统呢?还成立了“网电空间司令部”,它与以前的网络战“司令部”等相比有何功能、职责上的根本改变吗?多年前,汪成为院士在一次报告中建议,将 Cyberspace 译为“控域”,这是否可视为以上问题的解答呢?我不写微博,有赐教者,请发我电子邮箱:yang_qianli@sina.cn,将不胜感激。



前 言

按照术语严格定义来讲,网电空间(Cyberspace)目前并没有一个标准的精确定义,与其意义相近的一些术语有网络世界、网际空间、虚拟空间、数据空间、赛博空间、矩阵、数字领域、电子领域、信息球、虚拟现实、计算机网络、因特网等。网电空间一词最早出现于1982年,吉布森在1989年提出过一些非严谨的定义,如“网电空间是一种合法经营者以及每个国家教以数学概念的孩子们的一致的幻觉经历……”“从银行的每个计算机系统中抽象出数据的图像表示……”如果从人产生的幻想环境看,空间意味着是多维的,并大多与基于计算机的电子空间相关联。因此,网电空间由最初的用于描述计算机虚拟世界,扩展到全球计算机网络,并进一步扩展到更广的系统。

网电空间一词是控制论(Cybernetics)和空间(Space)两个词组合而成,是一个真实和虚拟并存的虚拟现实空间,是哲学和计算机领域中的一个抽象概念。与陆、海、空、天领域一样,网电空间是由电磁频谱、电子系统以及网络化基础设施组成的领域。

网电空间不仅包括因特网,还包括并不直接与因特网相联的军用网络系统或其他系统。因此,网电空间已成为未来战争最重要的作战领域之一,对其研究与控制的主动权很有可能成为决定国家安全的战略因素。

本书共分为9章。第1章概括介绍了网电空间的基础。第2章介绍了网电空间的体系架构。第3章从互联网入手,介绍了网电空间的网络发展演进过程,并较详细地阐述了智慧城市的体系。第4章介绍了网电空间存在的信息安全威胁,对网电空间攻击和漏洞做了分析。第5章针对网电空间存在的安全威胁介绍了安全防御战略。第6章介绍了网络环境的安全,网络安全事故的类型和攻击类型,并针对这些攻

击类型提出了网络安全的技术和非技术措施。还介绍了各种安全技术应对各种攻击类型的优缺点,信息安全保障技术。第7章介绍了态势感知的研究背景及现状,研究范畴和网电空间态势感知模型。第8章主要介绍了网电空间攻击法律。第9章主要介绍了网电空间在军事上的应用。

本书内容翔实,深入浅出,覆盖面广,具有先进性、科学性和实用价值,适合高等院校信息、电子、通信和计算机等专业师生与科研人员、工程技术人员参考,还可作为相关领域人员学习、了解网电空间的参考读物。

北京科技大学计算机与通信工程学院通信工程系的王建萍、陈月云、林福宏、安建伟、杜利平、刘倩和吴华怡老师和曾文璐、张思思、薛培培、谢萍、姚倩燕、王小玲、杨晟淞、史俊杰、王小玲、王亮洁、陈超、白如春、李泽韬、徐湘云等研究生参加了本书的编写工作,吴华怡老师进行了第一稿的统稿工作。在本书编写过程中,获得了北京科技大学研究生教育发展基金项目和教育部科学技术研究重大项目“基于智慧的下一代信息网络体系结构及关键技术研究(No. 311007)”的资助,同时得到了国防工业出版社和北京科技大学计算机与通信工程学院网电空间科学与技术研究所的大力支持、鼓励和帮助,参考或直接引用了国内外许多学者的论文文献和著作,在此一并表示衷心的感谢。

由于水平有限,再加上时间仓促,书中难免存在纰漏之处,恳请专家和读者批评指正。

编著者

目 录

第 1 章 网电空间概述	1
1.1 网电空间的概念和发展	1
1.2 网电空间的意义	4
1.3 网电空间的国内外研究现状	6
1.4 网电空间存在的几个问题	8
1.4.1 网电空间和虚拟现实	8
1.4.2 网电空间的几个误区	10
1.4.3 网电空间安全	11
1.4.4 网电空间知识产权和隐私权的法律问题	13
1.5 美军对网电空间的研究	15
1.6 小结	18
参考文献	19
第 2 章 网电空间的体系架构	21
2.1 网电空间的体系架构	21
2.2 虚拟技术和虚拟架构	26
2.2.1 发展前景	26
2.2.2 虚拟现实技术	27
2.2.3 架构设计原则	28
2.2.4 缺点和不足	30
2.2.5 虚拟架构的未来	31
2.3 数字化架构	32
2.3.1 数字架构	32
2.3.2 应用软件	33
2.3.3 数字架构中的时空关系	34

2.4	流畅型架构	35
2.4.1	流畅型架构介绍	36
2.4.2	流畅型架构的表示形式	36
2.4.3	流畅型架构的组成	37
2.5	虚拟架构体系的演变	39
2.5.1	重要性质	39
2.5.2	发展历史	40
2.5.3	系统的生成	40
2.5.4	工具	41
2.5.5	演化模式	42
2.6	小结	43
	参考文献	44
第3章	网络的演进	45
3.1	互联网的重要性	45
3.2	互联网的发展历程	46
3.2.1	互联网的起源	46
3.2.2	万维网起源	47
3.2.3	互联网上人数统计	48
3.2.4	网络带宽作用	48
3.2.5	互联网协议起源	49
3.2.6	智慧网络概览	49
3.3	超文本概述	56
3.3.1	网电空间的导览	56
3.3.2	超文本的含义	58
3.4	虚拟社区	59
3.4.1	网电城市构想	59
3.4.2	网电空间的软件建设	59
3.4.3	多用户体验	60
3.4.4	“人居”简介	63
3.5	网电城市化	66
3.5.1	虚拟城市	67

3.5.2 数字城市	69
3.5.3 智慧城市	70
3.6 网电空间无处不在	72
3.7 小结	74
参考文献	74
第4章 网电空间信息安全威胁	78
4.1 网电空间攻击影响	78
4.1.1 网电空间攻击起因	79
4.1.2 可视化网络攻击	81
4.2 网电空间安全和保障	81
4.2.1 攻击保护、预防和先发制人	82
4.2.2 自主攻击检测、警告和响应	83
4.2.3 检测和消除内部威胁	84
4.3 网电空间攻击分析	84
4.4 网电空间存在的安全漏洞	87
4.4.1 漏洞——图结构	87
4.4.2 图表类型的漏洞	88
4.4.3 网电空间攻击恢复时间常数	89
4.5 主动网电空间攻击模型	89
4.5.1 相关知识	90
4.5.2 主动网电攻击模型	90
4.5.3 网电空间攻击管理模型	92
4.5.4 行为控制器和攻击损失评估器	94
4.6 小结	95
参考文献	95
第5章 网电空间安全防御战略	98
5.1 网电空间安全防御面临的问题	98
5.2 网电空间的免疫系统	99
5.2.1 先天免疫系统	99
5.2.2 自适应免疫系统	101
5.3 安全防御的国家战略	106

5.3.1	概述	106
5.3.2	保障网电空间的国家战略	107
5.3.3	美国国防部和国土安全部防御策略	110
5.3.4	网络事件的影响	113
5.3.5	友好征服	114
5.3.6	TCP/IP 安全	115
5.4	安全防御的实现	115
5.4.1	我们都是网电战士	116
5.4.2	成功是建立在平衡的基础上	116
5.4.3	有效平衡网络的安全和访问	116
5.5	安全防御的未来发展趋势	117
5.5.1	新技术	117
5.5.2	云计算	118
5.5.3	信息管理	119
5.5.4	国际合作	119
5.5.5	封闭式小区	120
5.5.6	更多的预测	120
5.5.7	智慧安全	121
5.6	小结	122
	参考文献	122
第6章	网电空间的安全管理	124
6.1	网络环境的安全	124
6.1.1	网电空间的参与者	124
6.1.2	网络事故的类型	126
6.2	网电空间的攻击类型	128
6.3	网络安全技术	129
6.3.1	网电空间安全的技术措施	129
6.3.2	网络安全技术的比较	131
6.4	网电空间信息安全保障技术	133
6.4.1	认证、授权和信任管理	133
6.4.2	访问控制和权限管理	135

6.4.3	大规模网电态势感知	137
6.4.4	自主的攻击检测、警告和响应	138
6.4.5	内部威胁的检测和消除	140
6.4.6	检测隐藏的信息和隐蔽信息流	141
6.4.7	恢复与重建	142
6.4.8	取证、追踪和归类	144
6.5	小结	146
	参考文献	147
第7章	态势感知	148
7.1	态势感知概述	148
7.2	态势感知研究背景及现状	150
7.3	态势感知的研究范畴	153
7.4	网电空间态势感知模型	154
7.4.1	态势感知参考模型	155
7.4.2	态势感知过程模型	160
7.4.3	态势可视化	162
7.4.4	网电空间领域应用	164
7.4.5	性能和效力的衡量	165
7.5	小结	170
	参考文献	170
第8章	网电空间法律维度	173
8.1	网电空间带来的机遇与挑战	173
8.2	现有管辖网电攻击的法律制度	175
8.2.1	国际网电攻击法律的发展	175
8.2.2	国内网电攻击法律的发展	179
8.3	网电攻击法律的发展趋势	181
8.4	小结	181
	参考文献	182
第9章	网电空间在军事上的应用	184
9.1	网电空间领域	184
9.1.1	网电空间在军事上的定义	185

9.1.2	网电空间“领域”的军事含义	186
9.1.3	网电空间的互联性	189
9.1.4	网电空间战场的国际认可	190
9.2	网电空间战场	190
9.2.1	网电空间中的攻击	190
9.2.2	网电空间的物理基础设施	192
9.2.3	网电空间的公私协作关系	192
9.2.4	网电空间的作战武器	193
9.2.5	网电空间的战术行动	193
9.2.6	网电空间战场的漏洞	194
9.2.7	网电攻击造成的影响	195
9.3	美国空军与网电空间	195
9.3.1	美军一个全新的军种——网络部队	196
9.3.2	美军成立新军种所遭遇的问题	198
9.4	美军设立联合部队网络指挥官	199
9.5	小结	202
	参考文献	202

第 1 章 网电空间概述

本章简要介绍网电空间 (Cyberspace, 网络电磁空间的简称) 的基本概念、国内外研究发展现状及美军对网电空间的军事战略构想。尽管网电空间这个词早在 20 世纪就已经存在, 同时在人类的许多研究领域也发挥着重要作用, 但是实际上它所带来的相关内涵思想与理论却一直没有为人们所接受和重视。本章通过网电朋克 (Cyberpunk) 运动和美国科幻小说作家、网电空间之父威廉·吉布森 (William Gibson) 的描述来阐述网电空间的起源。

1.1 网电空间的概念和发展

网电空间 (Cyberspace) 一词是控制论 (Cybernetics) 和空间 (Space) 两个词的组合, 是由居住在加拿大的科幻小说作家威廉·吉布森在 1982 年发表于杂志的短篇小说《融化的铬合金 (Burning Chrome)》中首次创造出来, 并在后来的小说《神经漫游者》中被普及。

目前对 Cyberspace 的叫法繁多, 如网络世界 (Cyberria)、网际空间 (Cyburbia)、虚拟空间 (Virtual world)、数据空间 (Dataspace)、矩阵 (The Matrix)、数字领域 (The digital doman)、电子领域 (The Electronic Realm)、信息球 (The Information Sphere)、虚拟现实 (Virtual Reality)、计算机网络 (Computer Networking)、因特网 (The Internet)、……但是确切意思是什么呢? 目前并没有一个确切的定义来描述它。

在《神经漫游者》中, 吉布森对网电空间的定义是: 它与“一个由计算机控制台控制的, 有关计算机网络的, 适于航行的和数字化的空间”相关; 它是一种可视的、有色彩的、电子的、笛卡儿式的数据景观。

维基百科中对网电空间的解释是: 网电空间是可以通过电子技术

和电磁能量调制来访问与开发电磁域空间,并借助此空间以实现更广泛的通信与控制能力。网电空间集结了大量的实体,包括传感器、信号、连接线、传输线、处理器、控制器,不在乎实际的地理位置,以通信与控制为目的,形成一个虚拟集成的世界。在现实中,网电空间构建了相互依赖的信息技术基础设施网络与电信传输网络,如因特网、计算机系统、综合传感器、系统控制网络、嵌入式处理器、通用控制器等。从社会的角度讲,可以通过网电空间实现思想的交流、信息的分享、服务的提供、活动的组织等。

美国一直是在该领域内处于研究的最前沿,即使是这样,对于网电空间的概念也没有达成最终的一致。美国总统国家安全令中对于网电空间给出的定义如下:“网电空间是一个相关联的信息技术基础设施的网络,包括互联网、电信网、计算机系统以及关键产业中的嵌入式处理器和控制器。通常在使用该术语时,也代表信息虚拟环境,以及人们之间的相互影响。”

在美军参联会 2006 年出台的《网电空间国家军事战略》中则认为,“网电空间是一个作战域,其特征是通过互连的、因特网上的信息系统和相关的基础设施,应用电子技术和电磁频谱产生、存储、修改、交换和利用数据”。

对于网电空间有很多可能的解释,但是网电空间到底是什么一直没有阐述清楚。但是可以找到网电空间的一些主要特点。

(1) 它是一个虚拟的空间,像是一种精神状态,一个真实和虚拟并存的地方,因此根据定义它没有一个实际的物理位置。它好比是一种当人们被视觉或言语上的沟通所吸引的状态,如阅读、写作、观察和研究图片、观看视频或艺术品以及认真听音乐或演讲等。这样,网电空间可以看作是我们的原子世界的一个数字化补充。

(2) 可以通过一些带有人工处理机制的物理接入设备来进入网电空间,如在网络上具有数字运算能力的接入设备。这些辅助设备可以看作是网电空间的边界,也可以说是进入网电空间的窗口。

(3) 它使个人和群体之间进行互动和沟通,这种互动很大程度上独立于时间和空间。网电空间里面的事物因为完全独立于实际生活中的时间和空间概念,导致人们觉得这样的一种互动并不如现实般真实,

总觉得缺少些许东西。这种相互作用与通常意义上所讲的不同,它可能稍微有点间接性、延迟时间或者间隔距离。

通常,计算机屏幕可以看作是物理接入设备。作为一个连接电子设备和现实生活的窗口,计算机屏幕把人类和硬件设备联系起来,创造了一个替代的现实,即虚拟空间。万维网(WWW)的迅猛发展,使得网电空间增加了越来越多的图片、声音与视频。可以断定,在不久的将来,这些连接会越来越真实,越来越能让人感觉到“身临其境”,因此会越来越接近“虚拟现实”。最终,技术的发展会使最接近未来幻想的情景出现,虽然现在还只能存在于想象中。

网电空间有许多表现形式,下述列表简要概述了网电空间用到的在线活动表现形式:

- (1) 电话交谈;
- (2) 电子邮件(E-mail);
- (3) 电话答录机;
- (4) 新闻组和论坛;
- (5) 邮件列表;
- (6) 聊天室;
- (7) 远程登录;
- (8) 网站;
- (9) 电子图书馆;
- (10) 电子会议;
- (11) 电话会议;
- (12) 多用户域(MUD);
- (13) 虚拟现实;
- (14) 各种形式的互动电视,包括可视电话。

其他一些人们日常所熟知的网电空间的应用还有观看一部计费点播的电影、通过一个特殊的消费号码提交商品订单或游戏订阅或者是在自动取款机(ATM)上取钱等。

据此,我们可以认为,网电空间是指由因特网、电信网、传感器、武器平台、计算机系统及嵌入式处理器和控制器等各种信息技术基础设施网络构成的智慧电磁空间,是一个通过网络化系统及相关的物理基

基础设施,利用电子和电磁频谱存储、修改并交换数据的智慧电磁空间,具有时域、空域、频域和能域特征。

1.2 网电空间的意义

网电空间通过吉布森的书而流行起来。在将来它必然会对人类身份和文化产生重要的影响。人类学家 David Tmos 认为吉布森给人们传达了迄今为止最成熟和精细化的网电空间的人类学情景,即它的科技与经济方面,还有先进的后工业化时代形式的轮廓。从这个观点来看,吉布森的描述在以下三个方面具有重要的意义。

(1) 科幻小说被认为是一个可以使我们理解一个飞速发展的后工业化时代的文化的重要手段。它就像是一个通过现在来连接过去和未来的空间操作员。

(2) 它使我们能够理解先进信息科技有能够颠覆人类身体的感知结构的能力,这是通过在强大的计算机生成的数字化的空间中重新定格人体的有机边界而实现的。

(3) 先进的数字化技术。网电空间由于通过后工业化时代的人类学而概念化,可以作为一个后仪式化的理论和实践的测试平台。

一些作家争辩吉布森能成功地想象出网电空间并不是真为了突出某些技术发展的优点,而是因为他想描述一个新的吸引人的社交社区。对社会研究者 Allucqu re Stone 而言,《神经漫游者》衍生出了黑客、技术上的学者和社会的敌对者。这本书提供给他们可以想象的公众范围和重新描述的社区,而这个社区能够推出一种新的社会相互作用的基础。在这种情况下,20 世纪 80 年代其他文学出版物中大量引用本书内容,部分内容还出现在了科技出版物、会议主题、硬件设计和科学与技术演讲中。

但是,网电空间是与虚拟现实、数据可视化、图像用户界面、网络、多媒体、高级制图学以及其他众多由计算机技术产业产生的词联系在一起的,所以说网电空间作为一个工程和概念,已经将这些离散的项目集中到一个目标上。它促使这个概念整合,并吸引了许多学科和企业。吉布森的描述对虚拟现实产生了巨大的影响,网电空间的研究者们已