网络空间安全系列教材

网络空间安全学科发展

◎ 邬江兴　王清贤　邹 宏　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列教材

网络空间安全学科发展

邬江兴　王清贤　邹　宏　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

网络空间安全事关经济发展、社会稳定和国家安全，系统梳理国内外建设现状、成果经验、政策法规，准确把握核心内涵、特点规律、基本方法，对于加快学科建设步伐、提升建设质量效益将起到至关重要的作用。本书主要内容包括：学科发展指导思想、学科建设体系架构、人才培养体系模式、一流网络安全学院建设、人才队伍建设、学科领域技术发展、学科竞赛、学科发展趋势，以及创新平台建设情况和学科发展大事记等内容。

本书的读者对象主要为高等院校网络空间安全、信息安全、电子对抗、密码学、计算机等相关专业的学生，以及各网络运营商和网络安全企业、相关行业协会和研究机构的专业人士。

图书在版编目（CIP）数据

网络空间安全学科发展 / 邬江兴，王清贤，邹宏编著. —北京：电子工业出版社，2018.4
ISBN 978-7-121-33926-4

Ⅰ. ① 网… Ⅱ. ① 邬… ② 王… ③ 邹… Ⅲ. ① 计算机网络－网络安全－高等学校－教材
Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字（2018）第 060666 号

策划编辑：章海涛
责任编辑：章海涛　　特约编辑：穆丽丽
印　　刷：湖北画中画印刷有限公司
装　　订：湖北画中画印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　　印张：13.5　　字数：340 千字
版　　次：2018 年 4 月第 1 版
印　　次：2018 年 4 月第 1 次印刷
定　　价：45.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：192910558（QQ 群）。

本书编委会

主　任：

邬江兴

副主任：

王清贤　　邹　宏

编　委：（按姓氏笔画排序）

王天鹏　　王益伟　　刘广华　　刘　勇

朱俊虎　　杨　森　　周天阳　　罗向阳

郭　威　　侯毅刚　　胡宗云　　康　绯

曹路佳　　雷　明　　穆　清

网络空间安全学科的一点认识

网络空间安全作为一个独立一级学科，已经设立近三年时间，期间也是全球网络空间安全技术发生巨大变化的三年，我国在此领域已经出现了由跟跑、并跑到并跑、领跑跨越的势头，正在孕育一些具有颠覆性特征的理论和技术。同样显著的是，学术技术领域异常活跃以及社会关注度与日俱增的同时，对网络空间安全学科本身的认知，仍然处于需要深入研究、凝聚共识、界定内涵的过程中。需要指出的是，编著本书的目的并非只是为了阐述清楚、描述完备网络空间安全学科的内涵特征，作者更愿意结合自身的研究与实践就普遍关注的问题，展开深入细致的探讨。为此，在成稿之际，作者考虑以编著此书的初心展现作为前言，可能是合适的。

本书之所以冠以《网络空间安全学科发展》的大帽子，无非想尽可能得说清两件事。

第一件事，综合表达作者对网络空间安全这个学科的研究体会，这是一个关于学科内涵的问题。我们认为，网络空间安全学科至少存在以下四方面的特点。一是多学科交叉融合。毋容置疑，网络空间安全学科既是特定历史时期创立的一个新兴学科，更是一个交叉融合特点极强的学科，经典意义的学科内涵甚至外延理论都无法覆盖，这是一个基本定位。二是集成创新。这个特点更强调基于跨学科体系间的融合理论和技术创新，融合在字面意义上通常只是一种对形态状态以及演化方式的描述，而网络空间安全学科需要实现有增量意义的“融合”，即在多个学科交叉的基础上创造出有别于其组成学科的知识，乃至出现颠覆性的科学理论或“改变游戏规则”的技术创新。三是“弯道超车”“换道超车”的国家需求驱动。没有网络安全，就没有国家安全。本学科之所以肩负如此沉重之责任、强烈之使命，体现的是国家安全战略的时代需求，标志的是国家科技进步的新高峰，需要通过供给侧（不仅仅是市场）改革方式极大地激发或释放中国人在这一领域的创新活力。四是需要通过行政和学术权力协同用力。不同于传统意义的学科发展，网络空间安全学科必须以强化了行政权力的学术权力才能推动其加速发展，才能超常规地获得包括人力、物力、财力等在内的充沛建设资源，获得足够的发展活力和空间，进而形成可迭代发展的生态环境。正是基于对该学科的总体认识，作者希望做点梳理凝练工作并与大家分享。

第二件事，写写“发展”。对于网络空间安全学科的内涵、边界、外延、特点、规律等苏格拉底式的问题，在学术界存在不同“流派”的认知，相当时期内也无法指望形成主流意识。从某种程度上说，该学科的认知分歧只所以如此之大，很大原因源于对“网络空间”这一概念的不同认识而产生的。为此，作者的基本态度是“搁置争议”。在多方位、各层次的实践过程中再进一步加深对问题本质的理解和把握，同时在理论认知的提升中进一步指导实践。我们的想法是，将一段时间以来网络空间安全学科发展中的一些情况向读者做一个最新介绍，针对一些普遍关注的问题，采用发展的方式、运用发展的眼光、从发展的角度介绍和概括。希望能够为关注这一学科发展的同仁借鉴和参考。

虽然有做好这两件事的激情与愿望，但作者真实感受到当前网络空间安全学科发展面临的不可回避的挑战。一是学科边界存在争议，这个问题不言自明。二是交叉学科处在利益交汇地带，各学科在其中能够配给的资源往往在一所学校的发展过程中被反复“跑马圈地”，新

兴学科要发展无疑会动别人的奶酪，可能还要打破业已形成的格局，甚至需要“拆墙合作”，没有空间就没有起点，这也是新兴学科发展起步阶段的一个“痛点”。三是具备跨学科发展素质的人才培养存在结构性矛盾，网络空间安全学科的发展炙手可热，在热度攀升的同时，带来一个十分严峻的问题，就是学科队伍从何而来，传统学科体系强调人才在本学科内的“专精尖”能力培养，通常不会刻意关注跨学科发展素质的师资队伍建设，对非主流研究人才大多取“自生自灭”的态度。换句话说，现行的人才队伍建设方针和资源拥有模式，很难想象在一个单位内能迅速汇聚起一支具有跨学科发展能力的一流师资队伍。四是没有成熟的参考模式，从分布在若干一级学科领域的二级学科，甚至有些只是在专业方向的基础上，要一跃成为独立的一级学科，全世界没有先例，也无成熟的范式可以参考，只能根据国情从新兴学科自身使命、任务特点出发，从具体承建院校的基础和特色出发的探索发展路子。五是不能承受之重，从我们掌握的相关数据来看，网络空间安全学科专业的人才需求至少在 140 万人，现在的人才保有量不足 40 万人，面对近 100 万人的需求落差，仅仅依靠一个新兴学科或为数不多且大部分是新建的网络空间安全学院的建设去解决问题，挑战态势决不会是短期的。

压力越大越需发展定力。发展的定力来自何处？作者认为，更多地应来自于与包括发展路线在内的一些战略性或关键性问题的缜密思考和清晰认识。我们编写本书的初衷和定位，就是希望从多个角度对网络空间安全学科发展过程中普遍关注的问题进行分析梳理，为高等院校网络空间安全学科的领导者、建设者、研究者提供有益的借鉴。本书试图说明五方面的问题。第一，习近平新时代中国特色社会主义思想对网络空间安全及其学科建设有哪些新的要求，这是我们加强学科建设、培育学科人才的基本遵循。第二，网络空间安全学科的知识体系如何构成，这个问题具有很大的挑战性，作者在分析多种认识流派的基础上，给出了自己的认识，这需要大家广泛讨论，共同研究。第三，网络空间安全学科的“三大支柱”如何加强，也就是师资队伍、科学研究方向、创新平台和环境，本书对这三方面进行了较为全面的分析梳理，提出了一些有益的观点。第四，高水平的网络安全学院如何建设，就是围绕总书记指出的“要下大工夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络安全学院”这个总要求，提出了一些建设的思路和想法。第五，未来网络空间安全学科应该如何发展，时下各方对这一学科的重要意义已经讲得很清晰、很透彻了，说理的任务在一定程度上已经完成，对学界和院校而言，关键在于理清思路、戒除浮躁、抓好落实，避免走原来一些学科短期膨胀、质量下滑以及个别类型学院盲目扩张、空心乏力、不可持续的老路。如果本书能够在这五方面的研究上，有一些让读者受益的观点，或者给大家一些有益的启发，让大家共同思考一些问题，协力推进网络空间安全学科发展，那么本书的作用就达到了。这就是本书作者的初心。

对于网络空间安全学科这个本体而言，该学科涉及的领域比较多，学科相关前沿技术更新迭代非常迅速，甚至说学科自身的内涵也处在丰富、完善和拓展阶段，本书的作者只能基于自身的知识领域和认知水平进行一些综合分析和研判，肯定有许多不尽人意的地方，甚至有一些需要争论和研究的地方。对此，衷心希望学界专家、读者朋友不吝赐教，欢迎对书中的内容或观点给予建设性的批评和指正。

目 录

第 1 章 网络空间安全学科发展指导思想研究 …… 1

1.1 学科孕育产生的深刻时代背景 …… 2

1.1.1 源自追赶第三次发展机遇重要判断 …… 2

1.1.2 源自国家安全战略的迫切需求 …… 3

1.1.3 源自科学技术进步的内在紧迫要求 …… 4

1.1.4 源自经济社会发展的巨大需求 …… 5

1.1.5 源自对网络安全人才的强烈需求 …… 5

1.1.6 源自学科自身发展的规律性体现 …… 6

1.2 网络空间安全学科建设的基本目标指向 …… 6

1.2.1 为网络强国建设提供支撑 …… 7

1.2.2 为培养新型人才提供支撑 …… 8

1.2.3 为实现“弯道超车”提供支撑 …… 8

1.2.4 为社会治理能力提供支撑 …… 9

1.2.5 为新型安全领域提供支撑 …… 10

1.3 网络空间安全学科建设的重要指导原则 …… 10

1.3.1 坚持创新发展 …… 11

1.3.2 坚持协调发展 …… 11

1.3.3 坚持绿色发展 …… 12

1.3.4 坚持开放发展 …… 12

1.3.5 坚持共享发展 …… 12

1.4 网络空间安全学科建设的主要内容构成 …… 13

1.4.1 网络空间意识形态安全 …… 13

1.4.2 网络空间数据安全 …… 14

1.4.3 网络空间技术安全 …… 15

1.4.4 网络空间应用安全 …… 16

1.4.5 网络空间资本安全 …… 16

1.4.6 网络空间渠道安全 …… 16

1.5 网络空间安全学科建设的主要支持方式 …… 17

1.5.1 设立博士点、硕士点 …… 17

1.5.2 设立本科专业 …… 18

1.5.3 设立网络空间安全学院 …… 18

1.5.4 设立国家级建设示范项目 …… 19

1.5.5 设立多种奖励激励政策 …… 19

1.6 网络空间安全学科建设的重要改革内容 …… 20

1.6.1 招生考试制度改革 …… 20

1.6.2 学科竞赛方式改革 …… 20
1.6.3 人才奖励激励制度改革 …… 20
1.6.4 科技支持政策改革 …… 21
1.6.5 社会力量参与方式改革 …… 21
1.6.6 国际交流合作改革 …… 21
参考文献 …… 22
第 2 章 网络空间安全学科建设体系架构研究 …… 24
2.1 网络空间安全学科发展历程 …… 25
2.1.1 国外学科发展历程 …… 25
2.1.2 国内外主要大学网络空间安全学科建设情况 …… 27
2.1.3 国内外网络空间安全学科建设的主要规律 …… 31
2.2 网络空间安全学科理论基础 …… 33
2.2.1 数学是一切自然科学的理论基础，也是网络空间安全学科的理论基础 …… 33
2.2.2 信息论、控制论和系统论是现代科学的基础，也是网络空间安全学科的基础理论 …… 34
2.2.3 计算理论是网络空间安全学科的理论基础，包括可计算性理论和计算复杂性理论 …… 35
2.2.4 访问控制理论是网络空间安全学科的理论基础 …… 35
2.2.5 密码学理论是网络空间安全学科的理论基础 …… 36
2.3 网络空间安全学科的方法论基础 …… 36
2.3.1 理论分析 …… 36
2.3.2 逆向分析 …… 37
2.3.3 实验验证 …… 37
2.3.4 工程实现 …… 38
2.4 网络空间安全学科知识体系 …… 38
2.4.1 网络空间安全学科知识体系的五个模块 …… 38
2.4.2 网络空间安全学科知识体系的特色技术 …… 39
2.5 网络空间安全学科与其他学科的关系 …… 39
2.5.1 网络空间安全学科与相邻学科的关系 …… 39
2.5.2 网络空间安全学科与跨领域学科的关系 …… 40
2.5.3 网络空间安全学科与新兴学科的关系 …… 41
2.6 网络空间安全学科的主要研究方向和研究内容 …… 42
参考文献 …… 43
第 3 章 网络空间安全人才培养体系模式研究 …… 45
3.1 国外网络空间安全人才培养现状 …… 46
3.1.1 美国：强调精英人才培养的体系化战略 …… 46
3.1.2 俄罗斯：注重顶尖黑客人才的自主可控体系 …… 47
3.1.3 英国：政府企业高校合作的技能和知识体系 …… 49

3.2 网络空间安全人才培养体系 …… 51
3.2.1 学历教育体系：大规模人才培养的主要渠道 …… 51
3.2.2 资格认证体系：标准化人才培养的关键支撑 …… 51
3.2.3 职业培训体系：专业化人才培养的核心环节 …… 51
3.2.4 基础教育体系：普及化人才培养的重要途径 …… 52
3.2.5 特殊人才选拔：体系化人才培养的必要补充 …… 52
3.2.6 领军人才培养：高水平人才队伍的核心标志 …… 52
3.3 优秀人才超常规培养模式 …… 52
3.3.1 优秀运动员培养模式 …… 53
3.3.2 飞行员培养模式 …… 54
3.3.3 医学院培养模式 …… 55
3.4 高等院校实验班人才培养模式 …… 55
3.4.1 学科综合：中国科学技术大学少年班 …… 56
3.4.2 文科大类：北京大学元培班 …… 56
3.4.3 理科大类：南京大学匡亚明班 …… 57
3.4.4 工科大类：浙江大学竺可桢班 …… 58
3.5 网络空间安全人才特点分析 …… 59
3.5.1 知识体系的复合性 …… 59
3.5.2 实践要求的对抗性 …… 59
3.5.3 思维方式的双向性 …… 60
3.5.4 成长渠道的多元性 …… 60
3.6 高校网络空间安全人才培养路径选择 …… 60
3.6.1 拓宽生源渠道，建立特殊人才选录机制 …… 60
3.6.2 打破学科边界，实施交叉融合培养模式 …… 61
3.6.3 完善培养机制，实行主辅结合专业培养 …… 61
3.6.4 抓好整体设计，建立本硕贯通知识体系 …… 61
3.6.5 注重四堂联动，构建体系多元培养环境 …… 62
3.6.6 强化网络实训，注重实践对抗能力培养 …… 62
3.6.7 探索军民融合，搭建产学结合桥梁纽带 …… 62
3.6.8 加强国际交流，提升教师学生学术水平 …… 62
参考文献 …… 63
第 4 章 一流网络空间学院建设情况研究 …… 64
4.1 一流网络安全学院建设的缘起 …… 65
4.2 一流网络安全学院建设的前期探索与准备 …… 66
4.2.1 设立网络安全人才培养基地试点示范 …… 66
4.2.2 建设网络空间安全一级学科 …… 66
4.2.3 建立国家网络安全人才与创新基地 …… 68
4.3 组织实施一流网络安全学院建设计划 …… 68
4.4 一流网络安全学院建设的评价标准 …… 70

4.5 一流网络安全学院的主要改革推进内容 …… 71
4.6 一流网络安全学院建设的社会反映 …… 71
4.6.1 建设一流网络安全学院意义重大 …… 71
4.6.2 获评并不意味着已是一流网络安全学院 …… 72
4.6.3 一流网络安全学院怎么建 …… 72
4.6.4 网络安全人才缺口大 …… 73
4.6.5 网络安全人才怎么培养 …… 74
4.7 一流网络安全学院建设的前景和对策分析 …… 75
4.7.1 要下大功夫 …… 76
4.7.2 要下大本钱 …… 76
4.7.3 要请优秀的老师 …… 77
4.7.4 要编写优秀教材 …… 77
4.7.5 要招优秀的学生 …… 77
4.7.6 要推动学院和学科两个一流协调并进 …… 78
4.7.7 要着力推进中国特色一流网络安全学院制度建设 …… 78
4.7.8 要形成中国特色的评价体系 …… 79
4.7.9 要始终坚持动态管理模式 …… 79
参考文献 …… 80
第 5 章 网络空间安全人才队伍建设研究 …… 82
5.1 网络安全人才队伍建设的重要性 …… 83
5.2 网络安全领域人才队伍建设面临的困境 …… 83
5.2.1 专业人员严重不足 …… 84
5.2.2 技术水平参差不齐 …… 84
5.2.3 对从业人员的要求越来越高 …… 85
5.2.4 人才流动性强 …… 85
5.3 美国网络安全人才队伍建设情况 …… 85
5.3.1 美国国家安全人才培养战略 …… 85
5.3.2 美国高校网络安全人才队伍建设情况 …… 87
5.3.3 美国高校的网络安全师资队伍特点 …… 89
5.4 我国网络安全人才队伍建设现状 …… 91
5.4.1 高校师资队伍建设 …… 91
5.4.2 网安企业人才队伍 …… 93
5.4.3 网络安全人才的薪资与福利 …… 94
5.5 对网络安全人才队伍建设的几点思考 …… 95
参考文献 …… 97
第 6 章 网络空间安全学科领域技术发展概述 …… 99
6.1 基本概念 …… 100
6.1.1 网络空间 …… 100

6.1.2 网络空间安全……101
6.1.3 网络空间安全技术……101
6.2 网络空间安全技术发展历程……105
6.2.1 密码技术……105
6.2.2 网络和系统防护技术……107
6.2.3 移动安全技术……110
6.3 网络空间安全技术发展趋势……114
6.3.1 新型防御技术……114
6.3.2 新型网络安全技术……120
6.3.3 新型密码技术……125
参考文献……129
第 7 章 网络空间安全学科竞赛情况研究……132
7.1 国际竞赛情况……133
7.1.1 美国……133
7.1.2 日本……134
7.1.3 韩国……135
7.1.4 俄罗斯……135
7.1.5 印度……136
7.1.6 竞赛层次分析……136
7.1.7 竞赛特点……137
7.2 国内竞赛情况……138
7.2.1 发展历程……138
7.2.2 国家级赛事……139
7.2.3 省市级赛事……141
7.2.4 企业、院校级竞赛……142
7.2.5 网络空间安全相关领域竞赛……143
7.2.6 比赛平台……144
7.3 网络安全竞赛类型特点及层次水平……145
7.3.1 CTF 类……146
7.3.2 漏洞挖掘类……147
7.3.3 认证类……148
7.4 分析及启示……148
7.4.1 比赛背景……149
7.4.2 主要作用……149
7.4.3 比赛公平性……150
7.4.4 非 CTF 类形式竞赛与 CTF 竞赛的关系……151
7.4.5 下一步策略……151
参考文献……152

第 8 章　网络空间安全学科发展趋势研究 …… 155
8.1　星火燎原：网络空间安全学科建设方式发展趋势 …… 156
8.2　交叉融合：网络空间安全学科知识体系发展趋势 …… 157
8.3　新工科建设：网络空间安全学科人才培养模式发展趋势 …… 158
8.4　积极主动防御：网络空间安全学科技术研究发展趋势 …… 160
8.5　重点投入：网络空间安全学科创新平台建设发展趋势 …… 163
8.6　先行一步：网络空间安全学科军民深度融合发展趋势 …… 165
8.7　持续深入务实：网络空间安全学科社会支持发展态势 …… 167
8.8　行稳致远：网络空间安全学科发展的冷思考 …… 169
附录 A　网络空间创新平台建设概览 …… 172
A.1　国外网络空间科研力量现状研究 …… 173
A.1.1　美国网络空间科研力量建设 …… 173
A.1.2　欧盟网络空间科研力量研究 …… 180
A.2　我国各类网络空间领域重点实验室现状研究 …… 182
A.2.1　国家重点实验室 …… 182
A.2.2　国家工程实验室 …… 183
A.2.3　企业重点实验室 …… 183
A.2.4　网络安全相关学科国家重点实验室情况 …… 184
A.2.5　国家科技创新平台政策解读 …… 186
参考文献 …… 193
附录 B　网络空间安全学科发展大事记 …… 194
后记 …… 201

第1章 Chapter 1 网络空间安全学科发展指导思想研究

网络空间安全事关经济发展、社会稳定和国家安全，目前已得到了世界各国的高度重视，并纷纷将其提升为国家战略。为加强我国网络空间安全研究和人才培养，教育部批准设立了网络空间安全一级学科，之后国内掀起了开展网络空间安全学科建设和深化研究的热潮。党的十八大以来，习近平总书记高度重视网络安全和信息化建设，作出了一系列重要论述，尤其是在中国共产党第十九次全国代表大会报告中，对加强网络空间建设又提出了新的要求，成为习近平新时代中国特色社会主义思想的重要构成，这为在宏观上把握网络空间安全学科的建设方向提供了根本遵循。

1.1 学科孕育产生的深刻时代背景

学科一词译自英文 discipline，最初是指知识和学习，随后经历了从早期古拉丁文的 disciplina（知识与权力）到乔塞时代的 discipline（多层概念体系）等变化，并在时代演变和人们认识深化的过程中逐渐衍生为多样化的概念体系，有着学术领域、制度、组织、训练、规范等丰富内涵。对于如何理解学科，还有明显的中外差异。如今，随着人类认识的深化，学科已从最初的单纯知识领域或教学科目到大学中的组织建制，再到知识和组织双重作用下形成学科文化以及以后扩展的学科制度、学科共同体、学科规范等，但是不论如何变化，学科从本源意义上讲，仍旧是指知识的分类体系。对于网络空间安全学科而言，能够成为人类知识集合中的一个独立类别，有着深刻的时代背景。

1.1.1 源自追赶第三次发展机遇重要判断

习近平总书记指出："从社会发展史看，人类经历了农业革命、工业革命，正在经历信息革命。"[1]农业革命增强了人类生存能力，使人类从采食捕猎走向栽种蓄养，从野蛮时代走向文明社会。工业革命拓展了人类体力，以机器取代了人力，以大规模工厂化生产取代了个体工场手工生产。而信息革命则增强了人类脑力，带来了生产力又一次质的飞跃，对国际政治、经济、文化、社会、生态、军事等领域发展产生了深刻影响。我国曾是世界上的经济强国，后来在欧洲发生工业革命、世界发生深刻变革的时期，丧失了与世界同进步的历史机遇，逐渐落到了被动挨打的境地。特别是鸦片战争之后，中华民族更是陷入积贫积弱、任人宰割的悲惨状况。想起这段历史，我们心中都有刻骨铭心的痛。经过几代人的努力，我们从来没有像今天这样离实现中华民族伟大复兴的目标如此之近，也从来没有像今天这样更有信心、更有能力实现中华民族伟大复兴。这是中华民族的一个重要历史机遇，我们必须牢牢地抓住，决不能与这样的历史机遇失之交臂。习近平总书记心中始终装着"两个一百年"奋斗目标，顺应当代中国发展大势，顺应人民过上更好生活的热切期盼，顺应世界发展进步的时代潮流，鲜明提出了要实现中华民族伟大复兴的中国梦，建设网

络强国也正是中国梦的题中应有之意。网络空间安全学科的产生，就是源于这个时代大背景之下，就是责任感、使命感、紧迫感的集中体现。尤其是近年来，世界大国都将网络空间建设发展提升到国家战略高度，相继出台战略及战略性文件，全力抢夺网络空间的战略主动，建设网络空间安全学科，更加凸显重大意义。

1.1.2 源自国家安全战略的迫切需求

习近平总书记指出，“我们一定要认识到，古往今来，很多技术都是‘双刃剑’，一方面可以造福社会、造福人民，另一方面也可以被一些人用来损害社会公共利益和民众利益。从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。特别是国家关键信息基础设施面临较大风险隐患，网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击。这对世界各国都是一个难题，我们当然也不例外。”[1]

为应对日益严峻的网络空间安全问题，近年来世界各国开始逐渐加大网络空间战略部署，

纷纷将网络空间安全提升为国家战略，抢夺网络空间的“制高点”和“制网权”。2011 年 7 月，美国国防部发布《网络空间行动战略》，将网络空间列为与陆、海、空、太空并列的“行动领域”，并提出加强美军及重要基础设施的网络安全保护；2013 年 2 月，奥巴马签署行政命令《增强关键基础设施网络安全》，要求加强“关键基础设施”部门的网络安全管理与风险应对能力；2015 年 4 月，美国又发布最新的《网络空间安全战略》，用于指导国防部发展网络力量，同时明确提出要提高美军在网络空间的威慑和进攻能力；2016 年 2 月，美国政府发布《网络安全国家行动计划》，将从加强网络基础设施建设、加强专业人才队伍建设、加强与企业的合作、加强民众网络安全意识宣传以及寻求长期解决方案 5 方面入手，全面提高美国在数字空间的安全。2013 年，欧盟发布《欧盟网络安全战略》。2014 年 11 月，日本通过了《网络安全基本法》，并设立了由内阁成员组成的“网络安全战略部”。据不完全统计，全球已有超过 50 个国家发布了相应的网络空间安全战略或成立了相应的安全机构。

我国已经成为名副其实的网络大国。数据显示，截至 2017 年上半年，我国网民规模达 7.51 亿，互联网普及率达 54.3%[2]。经过 20 多年的发展，互联网已经不再是一个行业，它与整个社会的结合越来越紧密。加上现在物联网、车联网、工业互联网的发展，真实物理世界和网络虚拟世界的界限被打破，线上线下连成一体，在这样的背景下，网络世界的攻击开始蔓延到我们的真实世界。也就是说，当互联网的规模越来越大，网络安全面临的挑战也日趋严峻。

从全球角度来看，网络攻击威胁正向工业互联网领域渗透，工业互联网安全事件频发。2015 年 12 月，乌克兰发生了一次影响巨大的有组织、有预谋的定向网络攻击，致使其境内

近三分之一的地区持续断电。目前，各国的关键基础设施已成为网络攻击对象，一旦被攻击导致瘫痪，将给国家安全、社会稳定造成不可估量的伤害。

根据中国信息安全测评中心（CNITSEC）统计，2015 年全国共发现恶意网站 138178255 个，发现网站暗链 131774248 个，发现国内钓鱼网站数共计 2803271 个，木马病毒数共 31525452 个。根据国家漏洞库（CNNVD）统计，截至 2015 年年底，CNNVD 漏洞总量已达到 80300 个，新增漏洞数量持续增长，安全威胁加剧[3]。目前，我国也是遭受网络安全攻击最严重的国家。2015 年 5 月 29 日，360 公司“天眼实验室”发布报告，曝光专门攻击中国政府的境外黑客组织“海莲花”（Ocean Lotus）。该组织自 2012 年 4 月以来，针对中国政府、海事机构、海域建设部门、科研院所等展开了长时间的高级持续性威胁（APT）攻击。360 安全中心发布的《2015 中国互联网安全报告》显示，2015 年移动端监测到 Android 用户感染恶意程序达 3.7 亿人次。另外，网络窃听、网络欺诈、账号盗取等网络犯罪日益猖獗，给广大网民和众多企业造成了巨大的经济损失。

2016 年 12 月 7 日，我国发布《国家网络空间安全战略》，明确指出中国致力于维护国家网络空间主权、安全、发展利益，坚定捍卫网络空间主权、坚决维护国家安全、保护关键信息基础设施、加强网络文化建设、打击网络恐怖和违法犯罪、完善网络治理体系、夯实网络安全基础、提升网络空间防护能力、强化网络空间国际合作。网络空间安全上升为国家战略、体现国家意志，是网络空间安全学科形成发展的一个重要支撑，也是网络空间安全学科发展的重要任务。

1.1.3 源自科学技术进步的内在紧迫要求

习近平总书记指出：“互联网核心技术是我们的最大‘命门’，核心技术受制于人是我们的最大隐患。一个互联网企业即使规模再大、市值再高，如果核心元器件严重依赖外国，供应链的‘命门’掌握在别人手里，那就好比在别人的墙上砌房子，再大再漂亮也可能经不起风雨，甚至会不堪一击。我们要掌握我国互联网发展主动权，保障互联网安全、国家安全，就必须突破核心技术这个难题，争取在某些领域、某些方面实现‘弯道超车’。”[1] 同时，习近平总书记还指出，要以技术对技术，以技术管技术，做到魔高一尺、道高一丈。

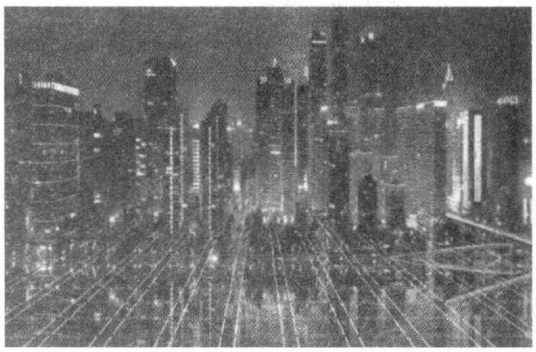
当今世界正处在深度调整期，科学技术日新月异，政治经济文化等交流交融交锋不断向深度、广度拓展，新一轮科技革命的先兆已在一些重要领域显现。21 世纪上半叶发生科技革命的可能性很大，而这一革命性变革有可能在网络空间安全领域最先打响。网络空间安全就拿软件开发行业举例，有个名词叫“千行代码缺陷率”，意思是一千行代码中的漏洞率。绝大部分软件公司的每一千行代码就有可能存在一个漏洞。据计算，Windows 操作系统的代码量是 5000 万行左右，安卓系统大概是 1200 万行，其中的漏洞可想而知。

学科建设在科学技术发展中有着基础和先导的作用，网络空间的规模和复杂度都远超传统计算机网络，网络空间安全的影响跨越物理域、逻辑域、社会域和认知域，研究网络空间中的安全威胁和防护问题，即在有敌手的对抗环境下，研究信息在产生、传输、存储、处理

的各个环节中所面临的威胁和防御措施，网络和系统本身的威胁和防护机制，包括传统信息安全所研究的信息保密性、完整性、可用性、真实性和可控性，以及网络空间的基础设施、信息系统的安全性和可信性。而传统的网络安全、信息安全理论和方法学无法满足发展需求，我们需要新的网络空间安全知识体系和理论体系。

1.1.4 源自经济社会发展的巨大需求

习近平总书记指出："我国经济发展进入新常态，新常态要有新动力，互联网在这方面可以大有作为。我们实施'互联网+'行动计划，带动全社会兴起了创新创业热潮，信息经济在我国国内生产总值中的占比不断攀升。"[1] "党的十八届五中全会、'十三五'规划纲要都对实施网络强国战略、'互联网+'行动计划、大数据战略等作了部署，要切实贯彻好落实好，着力推动互联网和实体经济深度融合发展，以信息流带动技术流、资金流、人才流、物资流，促进资源配置优化，促进全要素生产率提升，为推动创新发展、转变经济发展方式、调整经济结构发挥作用。"党的十九大报告指出，要加强应用基础研究，拓展实施国家重大科技项目，突出关键共性技术、前沿引领技术、现代工程技术、颠覆性技术创新，为建设科技强国、质量强国、航天强国、网络强国、交通强国、数字中国、智慧社会提供有力支撑。"加快建设制造强国，加快发展先进制造业，推动互联网、大数据、人工智能和实体经济深度融合，在中高端消费、创新引领、绿色低碳、共享经济、现代供应链、人力资本服务等领域培育新增长点、形成新动能。"



事实表明，我国信息经济的发展速度越来越快，我国互联网经济规模在 GDP 中占比持续攀升，2016 年达到 10%，网络零售交易规模跃居全球第一，2017 年的网络零售总额达到 67100 亿元。互联网企业市值规模迅速扩大，互联网相关上市企业 328 家，其中在美国上市 61 家，沪深上市 209 家，香港上市 55 家，市值规模达 7.85 万亿元，相当于中国股市总市值的 25.6%。[4] 目前，阿里巴巴、腾讯、百度、京东 4 家公司进入全球互联网公司市值排名前 10；华为、蚂蚁金服、小米等非上市公司估值也进入全球前 20 名。互联网经济的发展，越发需要网络空间安全保驾护航，这是网络空间安全学科发展的重要社会基础。

1.1.5 源自对网络安全人才的强烈需求

习近平总书记指出："人才是第一资源。古往今来，人才都是富国之本、兴邦大计。我说过，要把我们的事业发展好，就要聚天下英才而用之。要干一番大事业，就要有这种眼界、这种魄力、这种气度。'得人者兴，失人者崩。'" 网络空间的竞争，归根结底是人才的竞争。党的十九大报告中也强调，要培养造就一大批具有国际水平的战略科技人才、科技领军人才、青年科技人才和高水平创新团队。建设网络强国，没有一支优秀的人才队伍，没有人才创造