第 1 章 Chapter 1 网络空间安全学科发展指导思想研究

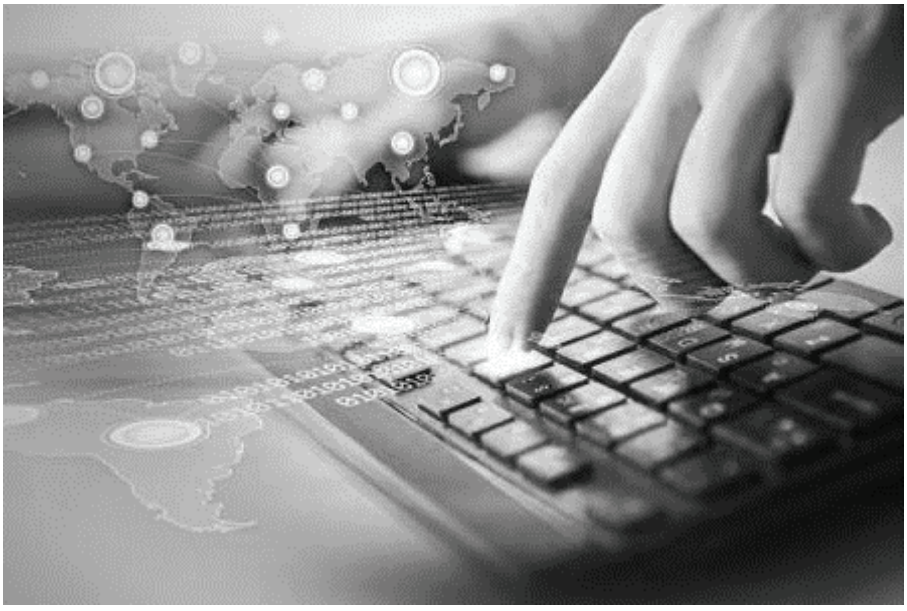
网络空间安全事关经济发展、社会稳定和国家安全，目前已得到了世界各国的高度重视，并纷纷将其提升为国家战略。为加强我国网络空间安全研究和人才培养，教育部批准设立了网络空间安全一级学科，之后国内掀起了开展网络空间安全学科建设和深化研究的热潮。党的十八大以来，习近平总书记高度重视网络安全和信息化建设，作出了一系列重要论述，尤其是在中国共产党第十九次全国代表大会报告中，对加强网络空间建设又提出了新的要求，成为习近平新时代中国特色社会主义思想的重要构成，这为在宏观上把握网络空间安全学科的建设方向提供了根本遵循。

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

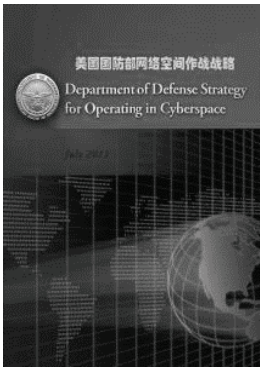


络强国也正是中国梦的题中应有之意。网络空间安全学科的产生，就是源于这个时代大背景之下，就是责任感、使命感、紧迫感的集中体现。尤其是近年来，世界大国都将网络空间建设发展提升到国家战略高度，相继出台战略及战略性文件，全力抢夺网络空间的战略主动，建设网络空间安全学科，更加凸显重大意义。

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 138 178 255 个，发现网站暗链 131 774 248 个，发现国内钓鱼网站数共计 2 803 271 个，木马病毒数共 31 525 452 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

力迸发、活力涌流，是难以成功的。念好了人才经，才能事半功倍。[1]

目前，我国高等学校每年培养的信息安全人才不足 1.5 万人，教育部批准设立的网络空间安全一级学科博士授权单位仅有 29 个，批准全国共 116 所高校设置信息安全类相关本科专业，其中信息安全专业 87 个，信息对抗专业 17 个，保密管理专业 12 个。放眼全球，近两年年平均网络安全人才增量也只有 19 万，网络安全人才荒是个全球性问题，4 年后面临将近 200 万网络安全人才缺口的问题。[5] 据 2015 年全球信息安全人才现状调查显示，62%的受访者认为所在机构急需信息安全专业人才，比上一年度的调查结果上升了 10 个百分点，而且大部分机构都已经提高了信息安全人才的聘用预算，能够雇得起更多人才，而他们所缺少的是合适的候选人适应这些岗位的需要，预计未来 5 年这一人才缺口将达到 150 万人。从目前我国网络空间安全学科、相关专业以及人才培养的总量来看，远远不能满足国家网络空间安全发展的需要。

1.1.6 源自学科自身发展的规律性体现

习近平总书记指出：“‘千军易得、一将难求’，要培养造就世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队。”与美国等发达国家相比，我国的网络空间安全研究和人才培养还比较滞后，原创性研究成果相对较少，核心技术受制于人，安全人才培养也还不能满足国家和社会发展需要。为加强我国网络空间安全研究和人才培养，我国分别在《网络安全法》《关于加强网络安全学科建设和人才培养的意见》和《一流网络安全学院建设示范项目管理办法》等相关文件中明确措施办法。

2014 年 6 月，教育部专门组织专家组来研究论证设立“网络空间安全”一级学科的问题。2015 年 6 月国务院学位委员会在工学门类下增设了“网络空间安全”一级学科（学科代码 0839）[6]，明确了网络空间安全基础、密码学及应用、系统安全、网络安全和应用安全等 5 个学科研究方向，同时将具有“计算机科学与技术”一级学科、“信息与通信工程”一级学科、“数学”一级学科（或“密码学”二级学科）的博士学位授予权作为新增一级学科博士学位授权点的先决条件。随后，清华大学、浙江大学、解放军信息工程大学（现中国人民解放军战略支援部队信息工程大学）等 29 所高校申请并获批成为该学科首批博士学位授权点，并着手制定相应人才培养方案，开启了我国在一级学科目录规范下成体系、全方位的网络空间安全人才培养模式。


中华人民共和国教育部
Ministry of Education of the People's Republic of China

国务院学位委员会 教育部关于增设网络空间安全一级学科的通知

学位[2015]11号

各省、自治区、直辖市学位委员会、教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务院学位委员会批准，决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。请各单位加强“网络空间安全”的学科建设，做好人才培养工作。

国务院学位委员会 教育部

2015年6月11日

1.2 网络空间安全学科建设的基本目标指向

习近平总书记指出：“建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济。”

同时强调，要从国家战略层面整体布局，搞好规划设计，综合施策，发挥集中力量办大事的制度优势，找准差距，加大投入，奋起直追，努力把我国建设成战略清晰、技术先进、产业领先、攻防兼备、制网权尽在手中、网络安全坚不可摧的网络强国。

目前，我国在网络空间安全领域还处于攻防失衡的被动局面，主要表现在：一是核心技术受制于人，高端芯片、操作系统、数据库等长期依赖进口，安全难以保证；二是对抗手段严重不足，从经验看，我方网络对抗意图、手段、技术、人员等核心信息几乎完全暴露于敌方掌控范围，形势非常被动；三是安全态势感知能力薄弱，不知道风险在哪里、是什么、何时来、怎么办；四是信息汇聚能力不强，网络安全数据高度碎片化，开放共享协同不够；五是人才建设滞后，缺少选拔培养使用尖子人才、特殊人才的高效办法，没有形成聚天下英才而用之的良好氛围。时代是行动的基础，问题是行动的导向，网络空间安全学科孕育产生于建设网络强国的战略擘画，那么学科建设的目标指向也必须瞄准服务网络强国这个大目标，有效解决短板问题。

1.2.1 为网络强国建设提供支撑

短短几十年时间，我国从一个后发国家迈入信息化时代，这一过程正蕴含在中国人对现代化国家的追求之中。建设网络强国，离不开政治、经济、社会、文化等领域全面发展的坚实基础；同样，网络空间的拓展与巩固也是国家发展和治理转型的契机。网络空间安全学科建设，首先瞄准的目标就是为建设网络空间的国家级智库服务，为国家网络安全战略的形成、丰富、发展、创新提供有力的智力支撑。坚持国家网络空间安全领域有什么需求，网络空间安全学科建设就在哪里展开、从哪里突破，聚焦网络空间和信息化领域重大问题，组织院士名师积极开展军事战略、安全战略、发展战略的专业化、前沿性对策研究，为服务国家和军队决策需求提供高质量的研究成果。为此，学科建设在战略支撑领域的主要目标是通过学科建设汇聚更多优质力量。

一是进一步形成具有中国特色网络空间发展战略，在网络空间政治、军事、经济、科技、文化、外交以及安全等领域都形成独特的理论体系，跟踪国际国内网络空间安全战略与理论研究前沿，结合网络空间军事斗争实际，开展网络战争形态、网络空间社会学、网络空间主权、网络空间安全战略，以及作战样式、作战指导和技战法等作战理论研究。二是进一步形成具有独特发展路径的网络空间技术战略体系，拥有能够确保我网络空间主权、安全和发展利益，能够为我国充分有效行使网络空间的利用权利提供支持，使我国在网络空间建设、使用、管理、控制等方面，拥有与维护我国国家主权、安全和发展利益相适应的网络空间技术主导权。三是进一步丰富形成网络空间军事发展战略，针对网络意识形态渗透、网络恐怖主义和违法犯罪破坏，以及网络有害信息传播，积极开展网络意识形态领域控制理论、敌对势力和恐怖势力网络渗透破坏防范、网络舆情管控、网络与信息突发安全事件应急响应等研究，能够有效慑止和打赢未来网络战争。四是进一步加强网络空间政策法规研究，研究国家和军队网络空间法律法规与战略政略有关问题，积极开展网络空间国际标准和规则有关问题研究，紧密跟踪开展网络空间国际法适用研究及网络军控等重大基础问题研究。五是进一步形成网络空间国际交流合作战略，能够有效参与和主导网络空间国际规则制定，拥有与我国国际地位相称的话语权、主导权。

1.2.2 为培养新型人才提供支撑

习近平总书记指出，“中国正在积极推进网络建设，让互联网发展成果惠及 13 亿人民。”[8] “网信事业要发展，必须贯彻以人民为中心的发展思想。这是党的十八届五中全会提出的一个重要观点。要适应人民期待和需求，加快信息化服务普及，降低应用成本，为老百姓提供用得上、用得起、用得好的信息服务，让亿万人民在共享互联网发展成果上有更多获得感。”[1] 网络空间安全学科发展也必须致力于贯彻习近平总书记以人民为中心的发展理念。“网络安全为人民，网络安全靠人民”。人永远是最重要的因素，网络安全不是购买并部署一批网络安全设备、堆砌一些产品就能防得住的，还需要大量的专业人员来做分析、研判、响应和处置。网络空间安全学科应把学科建设的首要目标定位在人的全面进步和成长成才，努力在培养更多人才、促进全民网络安全意识普遍提升上下大功夫，确立网络空间人才优先发展的战略布局，健全人才激励机制，加强人才资源管理，拓宽人才生成渠道，突出人才培养重点，优化人才整体结构，培养一大批与网络强国相适应的领军人才、管理人才、骨干人才和基础人才。把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍，培养高水平的创新团队。

一是培养网络空间安全的科技领军人才。网络空间斗争是技术的较量、智慧的博弈，说到底是“高精尖”人才的激烈对抗，支持他们在网络安全和信息技术重点领域取得重大突破，引领网络安全和信息科技发展方向。二是培养网络安全领域的专业技术人才，通过专业化的院校教育和细分的课程学习、实践环节训练，大大提升其服务网络安全和信息化保障各个领域、各个环节的知识能力素质水准。三是培养提升普通网民的网络安全意识，帮助人们掌握维护网络安全的技能和方法，提升抵御和防范网上有害信息的能力。四是推动面向中小学生网络安全教育能力的形成，帮助他们从小就建立网络环境下的信息安全意识，引导他们自觉做有文明网络素养、有守法行为习惯、有必备防护技能的好网民。

1.2.3 为实现“弯道超车”提供支撑

只有把核心技术掌握在自己手中，才能真正掌握竞争和发展的主动权，才能从根本上保障国家经济安全、国防安全和其他安全。技术领先是保持网络空间主动的主要途径，谁掌握了核心技术，谁就掌握了主动权。设立网络空间安全一级学科，一个很重要的任务就是要推动科技创新，实现网络安全技术领域的“弯道超车”，就是要在网络空间先进技术研发、利用和推广方面拥有一席之地，能够实现信息技术和产品安全自主可控，能够掌握网络空间的核心技术、基础技术和前沿技术。

一是解决网络空间核心技术、关键技术、共性技术攻关，支撑网络空间装备、软件、系统研制和自主发展，加快突破核心元器件、基础软件、高端制造工艺等“卡脖子”技术，大力发展软件平滑移植、平台自主适应等配套技术，构建具有自主体制功能的网络系统、软件平台、芯片和元器件，为维护网络空间安全提供基础环境。

二是加强基础技术和前沿技术研究，紧密跟踪量子通信、数据库、云计算、新一代互联网、物联网、人工智能等技术发展，为网络空间发展提供新的动力。

三是加强网络空间预警感知技术研究，着眼提升智能感知、网络实时预警、精确预警、全程预警的能力，加快构建汇集政府、军队、企业、高校、科研院所数据共享资源池，聚力突破大数据挖掘分析、网络漏洞智能识别、精准溯源等主动感知技术，实现对网络安全威胁

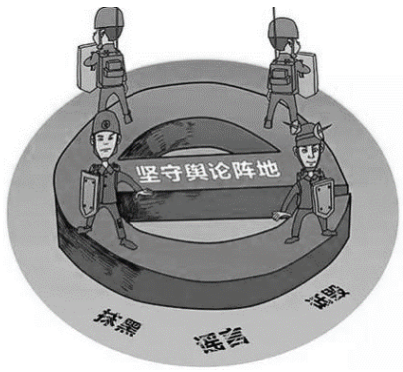
预判在先、料事在先、处置在先、反制在先，构建安全评估、监控跟踪、入侵防御、应急恢复相结合的预警体系，形成全天候全方位感知网络安全态势的能力。

四是争取在网络体系结构上取得突破，瞄准未来绿色、智能、泛在的智慧时代，大力推动软件定义互连技术[9]，更加关注网络结构中的基础物理硬件，更加关注网络体系架构方面的核心技术，将其作为我国在世界竞争舞台上，与对手比拼的新一代信息基础设施和信息系统的崭新“内核”，推动我国提出网信领域“中国方案”、贡献“中国智慧”，形成未来技术先发优势。

五是加强网络空间先进防御技术研究探索。从 2009 年开始，我国着眼应对漏洞、后门等已知安全威胁和未知安全威胁，积极开展拟态防御技术研究，实现了“改变游戏规则”的颠覆性创新。2015 年，在 21 名院士主持下，汇聚国内 9 家顶级测试团队的 110 余名专家，通过近 6 个月的高强度众测，验证了该技术在主动应对网络安全风险方面的有效性[10]。目前在加快突破网络空间密码防御、可信防御、动态防御、拟态防御、量子技术防御等防御技术的重点难点问题，加快关键领域的新技术应用推广，全面提升国家网络空间的整体防卫水平。

1.2.4 为社会治理能力提供支撑

习近平总书记指出，“网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。”“谁都不愿生活在一个充斥着虚假、诈骗、攻击、谩骂、恐怖、色情、暴力的空间。互联网不是法外之地。利用网络鼓吹推翻国家政权，煽动宗教极端主义，宣扬民族分裂思想，教唆暴力恐怖活动，等等，这样的行为要坚决制止和打击，决不能任其大行其道。”[1] 网络空间安全学科发展遵照党的十九大报告强调的，要实现国家治理体系和治理能力现代化水平明显提高，全社会发展活力和创新活力明显增强，树立为社会服务的建设推进理念。



一是高度重视学科发展对网络斗争的重要支撑作用，网络空间安全的智能化技术突破将改变网络斗争形态，传统“人海战术”将向“人机一体”阶段演化跃升，为防止未来出现“小米加步枪”对抗“飞机加大炮”的局面，应把发展网络意识形态斗争的创新技术提高到战略层面加以重视，尽快抓好战略筹划和顶层设计。

二是加快推动意识形态安全领域关键技术研究。网络空间安全首先是意识形态安全，为更好应对网络斗争的复杂局面，亟需将意识形态安全领域关键技术研究纳入国家科技创新计划重点支持，成体系推动意识形态领域斗争的关键技术创新，为“过网络关”提供支撑。

三是提升新技术的辐射推广作用，充分利用网络搜索引擎、网络论坛、移动多媒体以及即时通信、博客、手机短信等网络技术平台和信息传播载体，培养高度的文化自觉和文化自信，构建面向未来、理念先进、特色鲜明、开放包容的网络空间文化体系，为建设网络强国奠定文化软实力。

四是通过创新网络空间文化推进技术，发展网络文化产业和新技术手段，构建起技术先进、传输快捷、覆盖广泛的网络文化传播体系，加强网络文化管理，弘扬中华优秀传统文化，

发展社会主义先进文化，占领网络空间思想文化阵地，不断扩大中华文化国际影响力，牢牢掌握网络思想文化领域国际斗争主动权，用文化软实力支撑网络强国建设。

1.2.5 为新型安全领域提供支撑

党的十九大报告中明确，要统筹推进传统安全领域和新型安全领域军事斗争准备，发展新型作战力量和保障力量。目前，新型安全领域主要是指网络空间、太空和海洋。[11] 特别是在当前全球经济一体化、专业分工国际化的大环境下，网络空间安全呈现出活动软性化、边境弹性化、手段多样化、范畴全域化和力量多元化的特征，并且日益扩展为国家、军队及各种目的性组织和个人之间的混合复杂对抗，蕴含着毁瘫生产力、文化力、战斗力的混合风险。

对于网络空间，在《国家网络空间安全战略》中明确指出，“网络空间是国家主权的新疆域。建设与我国国际地位相称、与网络强国相适应的网络空间防护力量，大力发展网络安全防御手段，及时发现和抵御网络入侵，铸造维护国家网络安全的坚强后盾。”网络空间安全学科建设，必须致力于维护国家安全，为新型安全领域建设、应对非传统安全挑战提供有力支持。网络空间与陆海空等空间一样，都存在着边界和相关安全问题，并且网络空间边防涉及领域更宽，利害关系更大，建设形势更严峻。当前，我国网络空间边防薄弱，还没有像海防、空防、边防一样形成体系，也没有组建专门的网络空间边防力量，这是影响网络空间安全、制约建设网络强国的一个重大因素。网络空间安全学科建设需要着眼国家安全大局，致力于推进国家级的网络空间安全专业力量的建设和形成，这支力量平时承担组织领导国家信息边防的建设和防护，组织指挥网络空间非战争军事行动，保障网络空间意识形态斗争，支援国家网络空间建设发展，参与国际网络空间活动等职责和任务。

事实上，网络空间安全学科的建设和形成，一定程度上促进了我国在网络空间安全领域国家级专业力量建设的快速发展。

1.3 网络空间安全学科建设的重要指导原则

党的十八届五中全会提出了创新、协调、绿色、开放、共享的新发展理念，这是在深刻总结国内外发展经验教训、深入分析国内外发展大势的基础上提出的，集中反映了我们党对我国经济社会发展规律的新认识。按照新发展理念推动我国经济社会发展，是当前和今后一个时期我国发展的总要求和大趋势。五大发展理念，是习近平总书记从国家建设发展战略全局的高度，科学判断国际国内形势，全面把握当今世界发展趋势，深刻分析我国基本国情和战略任务，对国家建设发展所作出的全面战略部署，体现了解放思想与实事求是的统一，总结历史与规划未来的统一，立足国情与面向世界的统一，奋斗目标与发展路径的统一，战略性、思想性、指导性非常强，充分反映了对国家长远发展和民族最高利益的深谋远虑，是着眼中华民族伟大复

兴作出的重大战略筹划，是统领未来国家建设发展的总纲，是我国网络空间建设发展的重要里程碑。网络空间安全学科的发展，也必须贯彻新发展理念，做到先行一步、走在前列。

1.3.1 坚持创新发展

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。网络信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最大的技术创新领域，是全球技术创新的竞争高地。创新是网络空间安全学科发展的根本动力，网络空间是创新的产物，也是当今社会各个领域创新的新工具、新引擎，这就使得网络空间领域的创新具有十分重要的意义。网络催生了更多的创新载体，大型互联网企业和基础电信企业利用技术优势和产业整合能力，开始向各类小微企业、创新团队和个人开放平台入口、数据信息、计算能力等资源，成为催生创新的母体，创新工场、创客空间、社会实验室、智慧小企业创业基地等各类新型众创空间迅速发展，众包、众筹、O2O、电子商务、分享经济等互联网平台成为催生创新的新型载体。科技创新作为加速实现国家历史性战略转变的强大推动力，是建设网络强国的关键所在。

网络空间安全学科建设与发展必须要瞄准具有独树一帜的创新能力，在技术和手段上技高一筹，才能在科技革命的大浪潮中勇立潮头，不能再按部就班、因循守旧、裹足不前，要紧紧抓住我国仍将处于大有作为的战略机遇期，与前沿科技同行，与超前技术赛跑，做网络强国建设的“急行军”，切实推动跨越式发展。要推进网络空间安全学科发展，必须要为保障国家安全服务，必须勇于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”，在基础技术、通用技术、非对称技术、“杀手锏”技术、前沿技术、颠覆性技术上超前部署、集中攻关，改变技术受制于人的局面，实现网络空间安全可管可控，实现“跟跑并跑”向“并跑领跑”的转变，不断提升网络空间安全学科核心竞争力。

1.3.2 坚持协调发展

网络安全和信息化是事关国家安全和国家发展、事关广大人民群众生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把中国建成网络强国。协调是网络空间安全学科发展的重要使命，网络空间是生产力发展的产物，也是先进生产力的代表。在网络空间安全这个学科平台上要实现不同学科的交叉融合、衍生迭代，一方面要坚持联合协同，促进本学科与计算机科学与技术、信息与通信工程、数学、密码学等强关联学科的共同发展，实现相互促进、良性互动，协同推进学科建设的组织规划、人才交流和科研合作，实现学科建设互补发展，打造形成各具特色、强强联合的学科建设方向。

另一方面，通过学科交汇，吸纳政治学、法学、管理学、地理学、环境工程、社会学等学科领域的最新建设成果，推进学科建设向更大范围辐射，为促进多学科协调发展提供动力。同时还要推进军民融合、军民共育，创建军队院校和科研体系与国家高等教育体系之间网络安全拔尖人才、特殊人才联合培养、接力培养机制，推进学生访学交流、交换培养、导师互聘、优质课程共享等活动，更大限度地提高学科建设服务国防建设、汇聚优质资源的能力。

1.3.3 坚持绿色发展

党的十八大报告提出，把生态文明建设融入经济建设、政治建设、文化建设、社会建设各方面和全过程。这就意味着，网络空间安全学科发展也必须为生态文明建设的各方面和全过程提供有力支撑，服务于绿色发展。一方面，网络空间是以一定的物质和技术条件为基础的，因此网络空间安全学科要致力于推进支撑网络空间的物质和技术实现绿色发展，在其生产和运营过程中符合绿色健康发展的基本要求。另一方面，网络空间是亿万人民的精神家园，网络空间天朗气清、生态良好，符合人民利益，网络空间学科发展要把营造一个风清气正的网络空间作为重要使命，从根本上推进网络传播内容的绿色、健康、向上。

网络空间领域在经济社会最主要的应用——“互联网+”——通过信息流引领资金流、物质流、人才流、技术流的优化配置与有效利用，为激活绿色经济与低碳生活提供了必需的催化器[13]，推动了传统粗放型经济变轻、变智、变绿色，大数据、云计算、物联网等新一代信息技术在三次产业中的深入应用，推动了过度消费的传统生活方式变省、变少、变低碳，“我占有”式消费逐渐式微，“我分享”式生活正在国内外兴起，这种全新的“我分享”式生活是通过互联网平台，为分散的盈余资源提供供需精准匹配，使资源利用效率最大化，盘活了资源存量，减少了资源浪费，降低了资源环境压力，是绿色发展的最佳体现。

1.3.4 坚持开放发展

互联网让世界变成了地球村，推动国际社会越来越成为你中有我、我中有你的命运共同体。开放是网络空间安全学科发展的必由之路。网络空间，是一个实现人类社会互联互通的载体，开放性是网络空间自身的内在特征，这就决定了网络空间安全学科发展必须具有很强的开放性，其本身具有打破区域壁垒、跨越国境边界、推动开放交流的独特优势，从宏观层面有利于我国拓展网络经济空间、丰富对外合作交流，从微观层面有利于帮助我国各类企业通过互联网平台加快走出去步伐、开展全球化运营。安全可信的信息基础设施互联互通建设为开放发展铺路架桥。目前，“一带一路”的信息基础设施建设正在有序推进，将为我国打造21 世纪的新型开放发展格局提供强大支撑，从建设之初就需要网络安全技术的保驾护航。

另外，信息革命作为继农业革命、工业革命之后的又一次生产力革命，推动和深化信息革命、建设网络空间命运共同体是全人类的共同事业。网络空间安全学科发展进步，要致力于推进高等院校、科研机构、骨干企业之间的联合协作，坚持互利互补，建立健全目标一致、有机协同开放合作机制，探索创办国家网络安全学科联盟，创新网络安全人才培养模式，有效聚合国内优质教育资源为国家经济社会发展服务。要推进学科建设的国际化合作，积极融入“一带一路”和网络“丝绸之路”建设，做到“国家利益拓展到哪里，网络空间安全就保障到哪里。”

1.3.5 坚持共享发展

共享是网络空间安全学科发展的内在追求，网络空间是全人类共有的文明成果。信息技术和产业发展程度决定着信息化发展水平，要加强核心技术自主创新和基础设施建设，提升

信息采集、处理、传播、利用、安全能力，更好惠及民生。我国有 8 亿网民在网络空间中学习、工作，网络正在推动优质公共服务普惠共享，网络课程、远程医疗、慕课等的出现，降低了中西部贫困农村、低收入群体接受优质医疗教育服务的门槛与成本，这是我国网络安全与信息化事业发展了不起的成就。

但是，这种发展也存在不均衡、不充分等矛盾问题，尤其在信息服务、安全保障能力建设上差异化、非均等化的问题更为突出。网络空间安全学科发展，就是要通过学科这个起基础性、牵引性的科学载体，通过学科领域的平台、技术、人才、成果等优质资源共享，推进国家重点实验室、工程中心开放共享，合作建立实装实训基地，联合举办高端论坛，共同打造高端智库，构建高层次创新发展平台，加快推进安全技术、安全知识、安全意识的更广泛普及，更好地服务国家经济社会发展，为推进国家治理体系和治理能力现代化提供更加有力的人才和智力支持。

网络空间安全也要注重军民共享发展，融汇双方的“需求源”，通过军地双方需求信息的对接，把战场“缺什么”与市场“有什么”、军队“需要什么”与地方“能做什么”及时对表，找准同步提升军事和经济效益的增长点、解决制约自主创新和安全发展瓶颈的关键点。共享“大数据”，充分利用测绘、气象、水文、能源、医疗、监测、交通运输、公共安全等领域的既有资源，建立完善信息共享平台，推进作战数据库建设，实现军地信息数据同步更新、互补共用。接通“情报链”。利用军地双方网络资源，及时互通涉及军地的相关信息。共管“频谱源”。目前，我国各省区市均建有无线电管理机构，拥有一定规模的人员和设备，具备覆盖全国、全频管控的能力。可通过网络互联，使军队实时获取电磁环境信息，提升频谱资源统筹、电磁环境感知、用频秩序管控等能力，全面构筑国家信息优势，为网络空间军民融合创造了良好的发展环境。

1.4 网络空间安全学科建设的主要内容构成

习近平总书记指出，建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进。[1] 习近平总书记的重要指示实际上进一步明确了网络空间安全学科研究构成。目前，学科目录规范中将“网络空间安全”一级学科细分为网络空间安全基础、密码学及应用、系统安全、网络安全和应用安全 5 个方向。学习领会习近平总书记重要讲话精神，网络空间安全学科研究方向，还应该更加关注网络空间意识形态安全、数据安全、技术安全、应用安全、资本安全、渠道安全等 6 方面的安全领域，并作为学科的重要构成内容。

1.4.1 网络空间意识形态安全

网络的开放性、多元性以及虚拟性等特点，使当前各种社会思潮都开始借助网络争夺在意识形态领域的话语权，影响人们的思维方式、价值观念，尤其影响青年人对国家、社会、工作、人生的看法。这极大地削弱了马克思主义主流意识形态在我国网络空间的引导力和说服力。由此，保障网络空间意识形态安全日益成为网络空间安全学科建设一个重要领域，如何采取有效措施来优化网络空间意识形态，维护网络空间意识形态的安全，成为互联网时代

下党和国家面临的一个重要课题。

美国著名未来学家阿尔温·托夫勒在《权力的转移》一书中指出：“世界已经离开了暴力与金钱控制的时代，而未来世界政治的魔方将控制在拥有信息强权的人手里，他们会使用手中掌握的网络控制权、信息发布权，利用英语这种强大的文化语言优势，达到暴力、金钱无法征服的目的。”

随着社会的变迁以及互联网的快速发展，人们的思想观念、生产和生活方式发生了深刻的变化。中国于 1994 年正式接入互联网，经过了 20 多年的风雨历程，互联网应用在广度和深度上都得到很大拓展，促进了中国网民数量的增加和网络的繁荣。网络几乎已经成为人们意识形态生产、传播和接受的主要渠道，做好网络意识形态工作有其必要性和紧迫性。现如今，我国的网民数量已达 8 亿人之多，网民已成为当今社会上最大的社会群体。这个群体来自我国社会的不同阶层，其中既有高级知识分子，也有普通群众，他们可以在网络空间获取信息、表达意见、交流信息。虽说网络空间是虚拟的，但它也确是客观存在的。亿万网民正在网络这个虚拟的世界，用各种网络语言和网络形式，反映着现实生活中许多现象。他们参与时事讨论，关注热点问题，创造网络文化，成为现实社会中不可或缺的重要群体。

然而，互联网的快速发展，在给人们的工作和生活带来便利、为主流意识形态的发展和传播提供机遇的同时，也对我国的网络意识形态建设和网络安全提出了更高的要求和更严峻的挑战。网络空间意识形态斗争已逐渐成为意识形态斗争的主战场 [14]。当前，在网络空间意识形态斗争总体上敌强我弱的态势下，设立学科，深入研究和把握网络意识形态斗争的隐蔽性、多元性和现实性等特点 [15]，巧妙利用网络的社会性、娱乐性、交互性和融合性进行意识形态宣传，努力实现意识形态网络空间由“坐而论”向现实社会“起而行”的转化，将有助于提升我们对现实社会意识形态的管控能力。

另外，目前我国之所以在网络意识形态话语权方面时常受到西方意识形态的冲击和挑战，其中一个非常重要的原因是我国在网络核心技术方面与西方网络发达国家还存在很大的差距。因此，维护我国的网络意识形态安全就必须“用实力说话”，通过学科建设不断促进网络核心技术的创新，尽快取得突破。只有掌握了网络空间安全核心技术，才能有能力筑牢我国的网络意识形态防线。

1.4.2 网络空间数据安全

习近平总书记指出：“要深刻认识互联网在国家管理和社会治理中的作用，以推行电子政务、建设新型智慧城市等为抓手，以数据集中和共享为途径，建设全国一体化的国家大数据中心，推进技术融合、业务融合、数据融合，实现跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务。”“要维护网络空间安全以及网络数据的完整性、安全性、可靠性，提高维护网络空间安全能力。”

推进数据建设，首先要保障数据安全，因此数据安全有必要成为网络空间安全学科的重要研究方向。数据安全有两方面的含义：一是数据本身的安全，主要是指采用现代密码算法对数据进行主动保护，如数据保密、数据完整性、双向强身份认证等；二是数据防护的安全，主要是采用现代信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。数据安全是一种主动的包含措施，数据本身的安全必须基于可靠的

加密算法和安全体系，主要有对称算法、公开密钥密码体系两种。数据安全需要重点研究数据的保密性、完整性、可用性，以及数据处理的安全。数据处理的安全是指如何有效防止数据在录入、处理、统计或打印中由于硬件故障、断电、死机、人为误操作、程序缺陷、病毒或黑客等造成的数据损坏或数据丢失现象，某些敏感或保密的数据可能被不具备资格的人员操作员阅读，而造成数据泄密等后果。

美国数据安全政策的发展与互联网、数字技术的发展有着密切的联系，数据安全由克林顿时代的网络基础设施保护、到布什时代的网络反恐、再到奥巴马时代的创建网络司令部，美国的数据安全战略经历了一个“从被动预防到主动出击”的演化过程[16]。而我国在数据安全方面还面临着信息基础设施自主可控程度低、安全防护技术和手段不足等问题，在数据安全与隐私保护技术研究方面还比较落后，有效的防护手段比较缺乏，难以为国民经济和社会发展提供足够的安全保障。

当前，大数据也正在影响着人们的日常生活方式、工作习惯及思考模式。但大数据在收集、存储和使用过程中面临着诸多安全风险，大数据导致的隐私泄露为用户带来严重困扰，对传统网络安全防御体系也提出了挑战，传统体系以数据存储处理节点为中心，从网络边界开始由外向内实施检测、预警、保护和恢复等措施相结合的纵深防御。在大数据背景下，网络结构发生边界模糊、中心离散、分层减少等重大变化，导致原本奏效的安全防护理念，出现了设备位置不确定、检测目标不明确、防护重点不突出、阻断策略不匹配等问题，防护效能严重降低。同时，大数据为解决信息安全问题提供了有效手段，通过对海量信息的关联性分析，从根本上突破了传统“为什么”的逻辑束缚，拓展了“是什么”的预测功能，如基于大数据的威胁发现、基于大数据的认证技术、基于大数据的数据真实性分析等。未来将出现更多的基于大数据的安全保护技术，提供更多、更丰富的安全应用和安全服务。

1.4.3 网络空间技术安全

核心技术是国之重器，最关键最核心的技术要立足自主创新、自立自强。技术安全，主要是指网络空间所有的、具有独立计算能力的、计算机系统安全性设计、实现，以及安全性测试评估的基本原理、方法和技术。重点研究保障芯片，系统软件，计算平台安全的途径、方式、方法与关键技术，并提高计算机系统对恶意代码的防护能力。主要研究内容包括：芯片安全、系统硬件与物理环境安全、系统软件安全、恶意代码分析与防护、可信计算和虚拟化计算安全等。芯片与硬件安全，最早的芯片与硬件安全研究仅限于基于硬件方案实现一些加密、可信认证等安全方案，而随着硬件后门的出现，硬件安全研究开始转向针对硬件本身安全性的分析、检测与防御，具体的研究课题包括：硬件后门检测、形式化验证方法、硬件知识产权保护、可信硬件开发、硬件辅助的计算安全等。

软件安全，包括威胁建模方法、漏洞分析和挖掘技术、脆弱性分析技术、安全防护、检测和恢复技术、安全生命周期过程管理和控制技术[17]，以及安全性评测方法、技术和标准、恶意代码分析与防护等研究方向，其中安全漏洞攻防技术、恶意代码分析与防护是国际上最核心的研究课题。虚拟化计算安全通过计算资源共享，改变了传统的计算模式，提高了资源的利用率、灵活性和可用性，但由于相同硬件资源承载了更多的计算任务，其虚拟化技术自身的安全问题影响也更为突出。虚拟化计算安全主要是保护虚拟机的计算安全，通过分析虚

拟机攻击手段来研究其防御技术。

1.4.4 网络空间应用安全

随着计算机与网络技术的迅猛发展和广泛应用，以网络为基础的应用系统越来越多，工业控制、即时通信、社交网络、电子商务等应用不断创新，各种移动 APP 和应用系统也相继推出，但随之也带来了严重的应用安全问题。特别是，云计算、物联网和大数据等新技术的应用进一步给应用系统带来了新的安全风险。网络空间应用安全，是指为保障各种应用系统在信息的获取、存储、传输和处理各个环节的安全所涉及的相关技术的总称，涉及如何防止未经授权的访问、身份或资源数据的泄露、数据完整性的破坏、系统攻击与入侵、系统可用性的破坏等。

1.4.5 网络空间资本安全

网络空间资本安全的核心是金融安全，这一学科研究方向应重点关注三个方面的风险问题。首先是安全风险，如互联网账户泄露、资金被盗、资金被骗等。这些问题都是因为没有采用必要的安全技术和手段而导致的。因此，互联网金融系统建设工作最好邀请专业的信息安全机构提供专业安全咨询服务，协助规划安全体系建设，包括：操作系统、网络、应用层面的安全设计，引入必要的安全产品，如防火墙、入侵检测设备、SSL 网关、签名服务器、服务器证书等。黑客技术是不断在发展的，因此在互联网金融系统运行过程中，也应该定期邀请专业的信息安全机构对系统进行安全检测，对于存在的漏洞及时进行修补。

其次是法律风险。互联网金融的交易通常依托互联网在线完成，交易过程中涉及的身份确认、电子合同、电子发票等如果没有按照相关法律法规的要求采用电子签名技术就可能导致交易没有法律保证，存在法律风险。因此在互联网金融系统中应该引入可靠的身份认证服务和电子签名服务，其中电子签名服务一定要选择国家认可的合法的电子签名服务提供商。

最后是信用风险。互联网金融使跨空间、跨地区的交易成为现实，为人们在海量的人群找到了合适的交易伙伴，但是这种通过网络发生联系，使得交易双方在信用评价方面的信息不对称，信用评价不准确，增加了交易者不能如约履行其义务的风险。因此在互联网金融系统中应该引入可靠的信用服务，包括个人信用服务和企业信用服务。

1.4.6 网络空间渠道安全

网络空间渠道安全，核心是研究网络空间的供应链安全。国家高度重视，专门作出部署安排，要求以提高经济发展质量和效益为中心，以供应链与互联网深度融合为根本路径，以信息化、标准化、信用体系建设和人才培养为支撑，创新发展供应链新理念、新技术、新模式，高效整合各类资源和要素，提升产业集成和协作水平，打造大数据支撑、网络化共享、智能化协作的智慧供应链体系。美国非常注重 ICT（Information Communication Technology，信息通信技术）供应链安全。2008 年布什政府提出国家网络安全综合计划（CNCI），提出建立全方位的措施来实施全球供应链风险管理。在此基础上，2009 年奥巴马政府指出不应局限于只是谴责国外产品和服务供应商，同时提出了新的供应链风险管理方法。2011 年美国在发

布的《网络空间国际战略》中将“与工业部门磋商，加强高科技供应链的安全性”作为保护网络空间安全的优先政策[18]，该项政策将 ICT 供应链安全提升至保障网络空间安全的高度。

欧盟、俄罗斯和中国同样将 ICT 供应链安全上升到国家安全的战略高度。欧盟的《供应链完整性》报告指出，ICT 供应链完整性是国家经济发展的关键因素，提高供应链完整度对公共和私营部门意义重大。中俄共同提交给联合国的《信息安全国际行为准则》强调，应当努力确保信息技术产品和服务供应链的安全，防止他国利用自身资源、关键设施、核心技术及其他优势，削弱落后国家对信息技术的自主控制权，或威胁落后国家的政治、经济和社会安全。

华为美国网络安全官及白皮书的作者 Andy Purdy 称：“供应链风险是日益蔓延的网络安全风险的一个关键要素。一个组织要想成功，必须了解并管理好供应链风险。这绝不仅是确保按时交付产品和服务，还包括在产品整个生命周期内确保风险最小化。我们应基于现有的工作成果，提升大家对供应链风险的意识，共同努力，一起采取行动，更好地应对这些风险。”

1.5 网络空间安全学科建设的主要支持方式

习近平总书记强调，顶层设计要有世界眼光，找准世界科技发展趋势，找准我国科技发展现状和应走的路径，把发展需要和现实能力、长远目标和近期工作统筹起来考虑，有所为有所不为，提出切合实际的发展方向、目标、工作重点[19]。当前，网络空间安全学科建设作为我国乃至世界范围内新兴技术领域的基础工程，没有成型的经验可以借鉴、没有固定的路径可以套用。站在国家“双一流”建设的高度，推进网络安全学科建设要在国家整体学科规划的顶层设计中进行，加强顶层设计要在网络安全学科试验推进的阶段性成果基础上来谋划，既需要有广大高等院校和机构摸着石头过河，更需要加强国家在政策支持和指导方面的顶层设计，要注重加强整体推进的系统性、整体性、协同性，创造良好的试点改革政策、制度环境，不断带动网络安全学科建设单位的大胆试验与突破，推动学科建设质量持续跃升。

1.5.1 设立博士点、硕士点

学科建设是研究生教育的存在基础，研究生教育是学科建设的强大动力。2016 年，为了加快网络空间安全高层次人才培养，国务院学位委员会批准，在“工学”门类下增设“网络空间安全”一级学科，为我国做好网络安全人才培养工作提供了制度基础。从此，网络空间安全学科建设形势呈破竹之势、方兴未艾，但是相关人才数量和结构与其学科地位还不匹配，高端人才、专业型人才、复合型人才、领军型人才明显短缺，严重影响学科发展建设，严重制约我国网信事业发展进程。

网络空间安全学科应坚持学科建设与学位点的布局发展相结合，将研究生的培养教育作为一级学科建设的重要抓手大力发展，论证和设立一批博士与硕士授权点，全面启动网络安全研究生培养工程，结合各授权点优势，建设齐全配套的研究生培养体系，制定人才培养方案、条件建设规划、导师队伍遴选方案，做好过程质量评估与监控工程，按照“厚基础、宽口径、强能力、高素质”的创新人才培养目标，加强研究生的素质教育和创新能力培养。

1.5.2 设立本科专业

据有关资料显示，当前我国重要行业信息系统和信息基础设施需要各类网络空间安全人才 70 万，预计到 2020 年需要各类网络空间人才约 140 万人，而我国高等学校每年培养的信息安全相关人才不足 1.5 万人[20]，远远不能满足网络空间安全的需要。为建立大规模、多层次的网络安全学科专业人才培养格局，适应未来发展需要，应在有条件、有基础的院校广泛设立网络空间安全本科专业，以此为牵引带动教学资源整合、课程体系建设、教材体系建设和创新能力培养等工程实施，加强学科建设所需的资源统筹。要推动相关本科专业与教育部“卓越工程师教育培养计划”主动对接，促进网络空间安全人才培养与国家网络安全事业发展紧密结合，培养更多卓越网络空间安全人才。鼓励学生在校阶段积极参与创新创业，形成网络安全人才培养、技术创新、产业发展的良好生态链。要认真分析网络空间安全学科特点，突出学科特色，建立科学合理的评价体系，尤其要在教学管理中实施细粒度量化评价指标，准确、科学地对教学工作质量进行评判，不断总结经验，提高教育教学质量，尽快制定网络空间安全类专业人才培养标准和教学质量国家标准。要强化网络空间安全实战技能培养和实习实训，在国家和省区市网信办牵头下，组织规划建设一批网络空间安全实习实训基地，统筹安排网络空间安全类专业学生到国内信息安全企业参加实践锻炼，提高学生在网络空间对抗中的实践能力。

1.5.3 设立网络空间安全学院

设立网络空间安全学院是推动网络空间安全学科，带动和促进更多的高校、企业和社会各方面都来关心和参与网络安全人才培养工作的一个有效手段。2017 年 9 月，中央网信办、教育部决定在 2017 年至 2027 年期间实施一流网络安全学院建设示范项目，共 7 所高校，分别为：西安电子科技大学、东南大学、武汉大学、北京航空航天大学、四川大学、中国科学技术大学、战略支援部队信息工程大学[21]。

在此基础上，应鼓励其他有条件的高等院校，根据自身实际，在已有的计算机学院、信息与通信工程学院、数理学院等基础上，可通过整合、新建等方式自建网络安全学院，拓展网络安全专业方向，合理调整和扩大网络安全专业招生规模，建设跨理学、工学、法学、管理学等门类的网络安全人才综合培养平台。加强学科专业建设，开展高水平科学研究，完善本科、研究生教育和网络安全人才培养体系。适当增加相关专业推荐应届本科毕业生免试攻读研究生名额，探索开设网络安全相关专业少年班、特长班。积极创造条件，吸引和鼓励专业知识好、富有网络安全工作和教学经验的人员从事网络安全教学工作。聘请经验丰富的网络安全技术和管理专家、特殊人才担任兼职教师。推动网络安全学院与企业、科研单位联合建设一流网络安全实验室，开展网络安全科研教学活动，主动申请承担国家下达的重点和专项研究任务。以时不我待的精神瞄准建设世界一流网络安全学院目标，汇众智探索网络安全人才培养新思路、新体制、新机制，培养更多梯次合理、创新能力强的网络安全人才队伍。

1.5.4 设立国家级建设示范项目

网络空间安全学科是综合了计算机、数学、通信、电子、物理、管理、法律等学科，而发展形成的新兴交叉学科。它与其他学科既有紧密的联系和渊源，又具有本质的不同。研究对象上，具有一般工科所不具备的特殊性，从知识体系上看，具有多学科交叉融合的特点；从作用地位上看，具有军地一体、军民融合特点；从技术特点上看，具有攻防兼备、网密一体的特点。推动网络空间安全学科的建设发展，其实也是在落实创新驱动发展战略，需要有精确的试点和强有力的示范带动作用。要在中央网信办和教育部统筹下，设立一批国家级的网络安全学院、网络安全专业、网络安全实验室、网络安全综合实践基地试点和示范项目，与企业、科研单位联合建设一流网络安全实验室，开展网络安全科研教学活动，承担国家下达的重点和专项研究任务。有计划组织网络安全专业教师赴网信企业、科研机构和国家机关合作科研或挂职。从培养目标、课程设置、教材编制、实践教学、课题研究等多个环节与企业加强合作。着力开展学科建设和人才培养的改革创新，先行先试，从政策、投入等多方面采取措施，总结归纳出我国网络安全特色的内涵、特点、理论、技术体系，形成各自可推广、可复制的经验做法，带动全国的科研院所和企业参与其中，形成“众人拾柴火焰高”的生动局面。

1.5.5 设立多种奖励激励政策

对于网络空间安全学科来讲，奖励与激励政策同样重要。以美国为代表的发达国家建立了适合网络安全人才培养的激励政策。美国于 2012 年发布了国家网络空间安全教育战略计划激励机制[22]，该计划建立了从小学到高等院校的学生培养、从业人员培训及普通民众教育的人才培养体系，对全体网民进行网络安全意识培训，对专业人员进行系统的知识技能教育。网络空间安全学科涉及知识面广、难度大、学科交叉、知识更新快等特点，人才难以培养、培养出来难以保留等问题，较其他学科会更加突出，亟需各类奖励激励机制加以促进。要在人才培养体系上建设“绿色通道”，探索开设网络安全相关专业少年班、特长班与本硕博连读等多种模式，做到按需培养、精准培养；在师资队伍组建上，要吸引和鼓励专业知识好、富有网络安全工作和教学经验的人员从事网络安全教学工作，高薪聘请经验丰富的网络安全技术和管理专家、特殊人才担任兼职教师；在人才考核上，要坚持“英雄不问出处”，突出专业性、创新性、实用性，不唯学历，不唯论文，不唯资历，以实际能力为衡量标准；在资金支持上，要在网络空间安全重点项目、拔尖人才科研基金上加大力度，促进学术、人才、科研三者均衡发展，相互倚重、相互促进；要探索网信领域科研成果、知识产权归属、利益分配机制，在人才入股、技术入股以及税收方面制定专门政策。

1.6 网络空间安全学科建设的重要改革内容

网络空间安全作为当前社会先进生产力的代表和科技前沿，在推动相关学科建设发展过程中，贯彻改革创新思想尤为重要。目前，网络空间安全学科建设刚刚起步，政府的“政策链”、高校的“建设链”和社会的“支持链”，这三条“关系链”仍未形成高度耦合和高效联动。需要围绕一流学科建设的总体目标，在从学科建设之初开展网络空间安全领域改革，破坚冰、拆藩篱，走出一条具有中国特色的网络空间安全学科改革发展之路。

1.6.1 招生考试制度改革

互联网领域的人才，不少是怪才、奇才，他们往往不走一般套路，有很多奇思妙想。对待特殊人才要有特殊政策，不要求全责备，不要论资排辈，不要都用一把尺子衡量。网络空间安全学科的招生，也要突破当前的高考制度，把真正的网络安全人才苗子选进来。要加大自主招生力度，主要选拔具有计算机、网络攻防特长和创新潜质的优秀学生；要改进录取方式，创造条件逐步取消高校招生录取批次，改进投档录取模式，推进并完善平行志愿投档方式，增加高校和学生的双向选择机会，把真正有从事网络空间安全志趣的学生放入相应的专业中去学习深造；要加大从社会上延揽优秀人才的力度，通过组织竞赛等活动，发掘在相关企业、其他行业和自由职业者中的年轻“民间高手”，将其进行能力测评后，录取为本、硕、博相应等级的学生，按照专业化模式进行系统培养。

1.6.2 学科竞赛方式改革

网络空间安全时时存在着攻击与防护，处处可能带有漏洞和后门。网络空间安全是一个集操作性、经验性和应变性于一体的专业，对该领域人才要求十分苛刻。学科竞赛作为促进交流、提升能力的重要途径，在网络空间安全学科领域，也需要进行相应改革。要改革竞赛以客观题为主的模式，加大应用类型和主观题比重，与网络上的真实对抗看齐对标；要改革竞赛的组织模式，网络空间安全学科竞赛可以在网络上展开，利用网络开展竞赛成绩评定；要改革竞赛的参与范围，改变以往专业领域相关院校为主的人员构成模式，公开竞赛信息，采用竞赛者匿名等方式，吸引国内外的网络安全从业者、爱好者参与其中，打破院校围墙，提高环境真实度；要改革竞赛的竞争模式，赋予参赛选手更多自主权，可以自由组队、可以采取“独狼”模式，既鼓励团队协作，又鼓励冒尖挑战，激发学生学习知识的原动力、能力增长的内动力、荣誉激励的推动力，从中选拔相应的人才苗子。

1.6.3 人才奖励激励制度改革

网络空间安全领域学科建设应与人才奖励激励制度改革一道，先行先试，抓紧推进，形成系列的吸引人才、培养人才、留住人才办法。要设立高端人才引进专项奖励，设立与其水平相称的科研基金、安家费和薪酬体系；要鼓励网络空间安全人才创新创业，在人才入股、技术入股以及税收方面制定专门政策，予以支持和优惠；要尊重网络空间安全人才的创新创

造，及时对其科研成果、知识产权归属、利益分配机制等进行明确；要放眼全球，开放视野，不管是哪个国家、哪个地区的，只要是优秀人才，都可以为我所用，加大对网络安全领域海外人才的奖励力度，不断提高全球配置人才资源能力；要对重大成果和突破进行单项奖励，特别是对国计民生和国家网络安全有突出贡献的，要有相应的奖励和荣誉体系对其进行认可和表彰。

1.6.4 科技支持政策改革

由于我国在计算机网络技术方面的后发地位，网络空间安全领域的技术水平也处于“跟跑并跑”到“并跑领跑”的转变阶段，稍不留神，就会被对手挤在身后。因此，网络空间科技支持政策方面需要改革的形势更加迫切，以适应发展迅猛的网络空间安全形势。要在国家重点项目和基金中设立专项，将网络空间安全作为与生物工程、人工智能等同等重要的技术领域，分配专门经费进行支持；要贯彻军民融合战略加强科技攻关的总体效益，推动网络空间安全领域前沿技术从统筹规划、研发试验，到成果应用的全过程中，兼顾军民需求，协调军民力量，推动军民共用[24]；要加快科技创新成果的应用步伐，利用国家重点实验室、自主创新示范区等孵化器，开展政产学研用于一体的产业化模式，减少中间环节，缩短科技成果向网络空间安全防护能力转化的周期。

1.6.5 社会力量参与方式改革

在建设网络空间安全学科过程中，要高度关注以互联网企业为代表的社会力量，改革参与方式，让他们发挥出更大的作用和影响。要促进社会力量参与人才培养，遵循市场化、公益性原则，适当降低教育准入门槛，激发企业、科研院所、社会组织等多元社会力量参与人才培养的积极性，促进企业和高校、科研院所联合建立人才双向流动的体制和机制。积极推动企业与高等院校、科研院所在人才培养体制、机制、政策、资金、服务等方面形成“人才+项目+产品”的产学研用模式；要积极推动高校资源社会化、社会资源教育化，实现学校教育资源和社会教育资源的共享，加大网络实验室、研发基地等各类公共社会教育资源的共享与共建，强化服务能力；要推动与社会力量人才交叉聘用的共享机制，促进人才培养的互联互通，建构学生学习与实习的合作机制，提倡学生社会调研与发明创新的学分社会化，积极推动人才培养的互联互通，共同推动社会力量参加人才培养的新局面。

1.6.6 国际交流合作改革

开展广泛的国际交流合作也是一流网络空间安全学科建设的必由之路，互联网已经让世界变成了地球村，学科建设过程中要注重国际交流，注重世界范围内的新技术发布与协作开发，只要有利于提高我们的水平和能力，都不应该拒绝。要不断拓展国际交流合作范围，下放审批权限，推动国内高校与国际网络空间安全优势高校或企业进行双向沟通，建立双发认可的学分制度、考核制度等，互派学生交流培养，互派教师交流访学；要积极与国外大学、企业、科研机构在网络安全人才培养方面开展合作，引进国外网络安全领域高端人才，支持网络安全学科青年骨干教师出国培训进修、参加国际学术交流活动；要积极引进国外优质教

育资源和课程体系，推动学科建设与国际接轨，培养具有世界眼光、熟悉国际互联网事务规则、掌握学科前沿的国际型人才；要增强学科建设的国际化观念，防止自说自话，把学科的建设水平放到国际参照系中进行比较和检验，争取早日形成一批世界一流的网络空间安全学科建设示范点。

参考文献

[1] 习近平．在网络安全和信息化工作座谈会上的讲话[R/OL]．(2016-04-19)．https://www.zhihu.com/question/68010990.

[2] 中国互联网络信息中心．中国互联网络发展状况统计报告[R/OL]．(2017-08-04)．http://www.cac.gov.cn/2017-08/04/c_1121427672.htm.

[3] 中国信息安全测评中心．2015 年国家信息安全态势[R/OL]．(2016-01-06)．http://www.doc88.com/p-9903152412824.html.

[4] 中国网络空间研究院．中国互联网二十年发展报告[R/OL]．(2015-12-16)．http://www.cac.gov.cn/2016-01/21/c_1117850404.htm.

[5] 新华社．我国网络安全人才培养缺口巨大[N/OL]．(2016-09-23)．http://www.xinhuanet.com/legal/2016-09/23/c_1119614489.htm.

[6] 国务院学位委员会　教育部．关于增设网络空间安全一级学科的通知：学位〔2015〕11 号[A/OL]．(2015-06-11)．http://www.moe.edu.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221423.html.

[7] 习近平．总体布局统筹各方创新发展　努力把我国建设成为网络强国[R/OL]．(2014-02-17)．http://www.cac.gov.cn/2014-02/27/c_133148354.htm.

[8] 新华社．让互联网发展成果惠及 13 亿中国人民[N/OL]．(2014-11-20)．http://politics.people.com.cn/n/2014/1120/c70731-26057575.html.

[9] 新华社．我国首个网信领域软件定义互连技术与产业联盟在天津成立[N/OL]．(2017-11-25)．http://news.xinhuanet.com/2017-11/25/c_1122010442.htm.

[10] 新华社．我国网络空间防御技术取得重大突破　将改变网络安全游戏规则[N/OL]．(2016-11-13)．http://news.xinhuanet.com/2016-11/13/c_1119901058.htm.

[11] 新华社．习近平主持召开中央军民融合发展委员会第一次全体会议[N/OL]．(2017-06-20)．http://news.xinhuanet.com/politics/2017-06/20/c_1121179676.htm.

[12] 新华社．习近平在中共中央政治局第三十六次集体学习时强调：加快推进网络信息技术自主创新朝着建设网络强国目标不懈努力[N/OL]．(2016-10-09)．http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm.

[13] 胡拥军．“互联网+”对践行五大发展理念大有可为[N/OL]．(2016-04-21)．http://theory.gmw.cn/2016-04/21/content_19797363.htm.

[14] 习近平．胸怀大局把握大势着眼大势　努力把宣传思想工作做得更好[N/OL]．(2013-08-20)．http://politics.people.com.cn/n/2013/0821/c1024-22635998.html.

[15] 朱东来．网络空间意识形态斗争的特征分析[J]．南京政治学院学报，2015，31(01)：38-40.

[16] 马海群，王茜茹．美国数据安全政策的演化路径、特征及启示[J]．现代情报，2016，36(01)：11-14.

[17] 詹姆斯·兰萨姆．软件安全从源头开始[M]．北京：机械工业出版社，2016.

[18] 倪光南，陈晓桦，尚燕敏，王海龙，徐克付．国外 ICT 供应链安全管理研究及建议[J]．中国工程科学，2016, 18(06):104-109.
[19] 新华社．习近平在中共中央政治局第九次集体学习时强调：敏锐把握世界科技创新发展趋势　切实把创新驱动发展战略实施好[N/OL]．(2013-10-01)．http://www.gov.cn/ldhd/2013-10/01/content_2499370.htm.
[20] 中国网信网. 积极构建网络空间安全创新人才培养体系[N/OL]. (2015-06-04). http://www.cac.gov.cn/2015-06/04/c_1115514398.htm.
[21] 新华网．首批一流网络安全学院建设示范项目高校名单公布[N/OL]．(2017-09-16)．http://news.xinhuanet.com/2017-09/16/c_1121675194.htm.
[22] 美国网络空间安全教育计划[R]．中国教育网络，2014-09-43.
[23] 新华网．习近平在亚太经合组织工商领导人峰会上的主旨演讲[N/OL]．(2015-11-18)．http://news.xinhuanet.com/world/2015-11/18/c_1117186815.htm.
[24] 解放军报．维护网络安全，打响第五空间人民战争[N/OL]．(2017-11-29)．http://military.people.com.cn/n1/2017/1129/c1011-29675113-2.html.
[25] 新华社．习近平在第二届世界互联网大会上的讲话[N/OL]．(2015-12-16)．http://politics.people.com.cn/n1/2015/1216/c1024-27936712.html