DOI 10.15302/J-SSCAE-2016.04.006

网络空间安全产业发展研究

安达，梁智昊，许守任

（中国电子科学研究院，北京 100041）

摘要：本文对“十二五”期间我国网络空间安全产业的发展现状、发展经验进行总结，对网络空间安全产业新的发展趋势进行深入剖析，提出了促进产业发展的政策建议，以期对“十三五”期间我国网络空间安全产业的发展提供参考和借鉴。

关键词：网络空间安全；网络空间安全产业；自主可控；标准

中图分类号：F49　　**文献标识码：**A

Study on the Development of Cyberspace Security Industry

An Da, Liang Zhihao, Xu Shouren

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

Abstract: The paper summarizes the development situation and experiences of the Chinese cyberspace security industry during the 12th Five-Year Plan, analyzes its new development trends, and proposes policy suggestions for the industry development to provide a reference for cyberspace security industry during the 13th Five-Year Plan.

Key words: cyberspace security; cyberspace security industry; independent and controllable; standards

一、前言

网络空间建构在由信息技术基础设施构成的相互依赖的网络之上，是在线交流发生的载体，包括在各行业中所使用的互联网、电信网、计算机系统，以及嵌入式的处理器和控制装置等。从更广泛的角度讲，网络空间通常还用于描述信息所处的数字环境，即人、机、物构成的大环境及其中各要素之间的各类交互联系。

网络空间安全是一种确保网络空间能抵御有意或无意的网络威胁，并具备风险管理、应急响应、快速恢复等的安全能力，是一种确保将网络空间风险控制在一个可接受的最小程度的保护状态。网络空间安全涉及的安全要素很广泛，既包括传统信息安全中经典的机密性、认证性、完整性、非否认性、可用性、可控性等技术要素，还包括用以保护网络环境、机构及用户资产的各种工具、安全管理、安全科研教育、法律法规、技术标准、国家战略等要素[1]。

“十二五”期间中华人民共和国工业和信息化

收稿日期：2016-06-15；**修回日期：**2016-06-28

作者简介：安达，中国电子科学研究院，工程师，研究方向为战略管理、网络空间安全、数据科学；E-mail: andadk@163.com

基金项目：中国工程院重大咨询项目“‘十三五’战略性新兴产业培育与发展规划研究”(2014-ZD-7)

本文由《中国战略性新兴产业发展报告》中《网络空间安全产业》改写

本刊网址：www.enginsci.cn

部出台了《信息安全产业“十二五”发展规划》，为我国网络空间安全产业的蓬勃发展奠定了基础，核心技术产品研发取得一定突破，形成一批掌握自主知识产权的龙头企业，自主可控的产业链初具规模[2]。2014 年 9 月，李克强总理在夏季达沃斯论坛上提出“大众创业、万众创新”。在日新月异、极度看重技术价值的网络空间安全领域，这大大激发了企业和从业人员的创新热情。2015 年 6 月“网络空间安全”被列为国家一级学科，我国网络空间安全产业环境进一步完善，同时有望填补我国网络空间安全专业人才的巨大缺口。首部《网络安全法》草案于 2015 年 7 月公布，标志着网络空间安全已上升到国家战略层面[3]。这些政策层面的布局，标志着我国网络空间安全事业迎来了重大历史发展机遇，也为“十三五”期间网络空间安全产业的发展奠定了良好的基础。

二、 网络空间安全产业的概念及范畴

今日世界，网络空间已不再仅仅是虚拟空间，而是人类共同的活动空间。网络空间中发生的一切，与国家、民族和我们每个人，从未如此密切相关。为了认识好、利用好、建设好网络空间，促进其健康有序发展，必须维护网络和平安全。网络空间安全产业是国家网络安全的支撑，可为国家、企业和公共等各类信息系统提供可持续的安全技术、安全产品和安全服务。

随着网络技术的不断发展，网络空间安全的环境和态势也发生了巨变。一是由于政治、经济和意识形态等因素的影响，网络攻击者的动机发生了变化，由追求技术突破的炫耀，转向基于功利性的目标驱使；二是网络攻击者的目标更加明确、具体，且有从个人的单打独斗逐步发展成有技术、有支撑背景、有经济实力的有组织行为的趋势；三是网络攻击范围的扩展，已由通用网络向专有网络扩展；四是大数据、云计算等新一代信息技术的应用在带来正面效应的同时，也对网络安全提出了新的挑战。面对着内容覆盖广泛、手段复杂多变的网络空间安全形势，网络空间安全产业牵涉极多。底层基础方面，包括元器件提供商、安全芯片提供商、安全系统软件提供商、开发工具提供商；中间一级，包括安全设备提供商、安全应用软件提供商；更高层次上，包括安全集成提供商，以及专业安全服务提供商。目前，软、硬件产品提供商仍是产业链价值最高环节，但随着网络空间安全形势、安全防御理念的变化，网络空间安全产业已经呈现由单一产品向整体安全防御解决方案转变，由软、硬件产品向安全防御应用和服务转变的趋势。

三、 网络空间安全产业发展现状分析

2014 年 2 月，中央网络安全和信息化领导小组正式成立，由习近平总书记亲自担任组长。领导小组统筹协调各个领域网络安全和信息化重大问题，网络空间安全产业的发展得到政策环境的大力支持。全国人民代表大会于 2015 年公布了《中华人民共和国网络安全法（草案）》，我国网络安全法律法规体系进入迅速完善的快车道，产业环境逐步优化，产业规模迅速增长，自主可控技术产品取得一系列突破，市场份额增大，安全体系和标准化方面的工作进步显著。

（一）网络空间安全产业发展总体现状

面对日益严峻的网络空间安全形势，一方面，世界各主要大国纷纷将网络空间安全上升为国家战略，国家间围绕网络空间的角力与博弈呈常态化；另一方面，巨大的经济诱惑使黑客组织产业化，网络入侵规模化。网络空间安全事件频发，国家重要信息系统、企业信息系统以及公众隐私受到严重威胁，这一切都极大地催化了全球网络空间安全产业的发展。2014 年全球信息安全产业规模达到 1 383.08 亿美元，比去年同期增长 9.7 %（见表 1），其中网络监管、信息基础设施安全防护、企业信息安全体系建设、数据安全等成为主要发展推动力[4]。

我国网络空间安全产业起步较晚，但增速可人。2011 年年底，《信息安全产业“十二五”发展规划》印发，国家关键基础设施信息系统、企业信息系统、个人隐私网络安全等方面的需求，为我国网络空间安全产业迅猛发展提供了动力，2014 年产业规模达到 321.28 亿元人民币，比上年增长 21 %（见表 1）[4]。

（二）自主可控产业链发展现状

我国大力推进网络空间安全领域的自主创新发展，2014 年国家颁布了一系列文件。在银行、电信、互联网等行业推进自主可控关键软、硬件应用，建

表 1　2012—2014 年信息安全产业规模及增长率 [4]

	规模及增长率	2012 年	2013 年	2014 年
全球	销售额/亿美元	1 151.92	1 260.78	1 383.08
	增长率/%	9.3	9.5	9.7
中国	销售额/亿元人民币	216.4	265.52	321.28
	增长率/%	20.9	22.7	21

立自主可控信息技术长效机制，提倡政府部门采用国产操作系统，并逐步向商用和民用领域推广 [5,6]。

积极的政策环境促进自主可控产业链日趋完善。在信息基础设施、基础软件、信息安全产品、应用软件、网络安全服务等行业，涌现出一批龙头企业，如龙芯中科技术有限公司、浪潮集团有限公司、中标软件有限公司、启明星辰信息技术有限公司、卫士通信息产业股份有限公司、北京神州绿盟信息安全科技股份有限公司、北京北信源软件股份有限公司等。它们的共同特点是自主知识产权程度较高。虽然其技术和产品与国外同类相比存在一定差距，但基本可以实现对国外产品的替代。企业的发展壮大，较好地带动了产业集群发展，企业自发建立产业联盟，形成联合开发、优势互补、利益共享、风险共担的战略合作组织，打造了良好的自主可控产业生态圈，推动自主可控产业链整体向前持续发展。

（三）网络空间安全技术和产品的发展现状

伴随新一代信息产业的发展，在国家科技专项的持续支持下，在应用需求的牵引下，网络空间安全技术和产品逐步成熟。

近年来，我国在安全芯片、安全操作系统等基础技术的研发和产业应用上取得了一定的突破和进展，尤其是在自主密码技术、安全认证技术以及可信计算技术上进步明显。我国商用密码产品与技术体系已经基本成熟，已拥有自主知识产权和高安全性的全系列商用密码算法。国云科技联合中科院云计算中心研制的面向政府和企业客户的 G-Cloud 云操作系统，拥有自主知识产权，通过了国家信息安全评测中心最高安全级别认证，是近年来我国网络空间安全领域自主、安全、可控技术产品的重大突破。

（四）网络空间安全服务的发展现状

网络空间安全是综合性问题，国家级和企业级用户需求已从单一产品向有针对性的、面向行业的网络空间安全解决方案转变，产业的核心价值正在从“产品和技术”向“应用和服务”转变。安全硬件产业比重逐渐下降，软件与安全服务比重上升，2014 年，全球网络空间安全硬件产业占比下降至 45.4 %（见表 2），安全软件和安全服务产业占比超过一半；同期我国网络空间安全产业中，安全硬件仍占比过半，服务产业占比为 8.7 %。与全球网络安全服务产业占比 20.4 % 的规模相比，还存在很大差距 [4]。

表 2　2014 年信息安全产业产品结构 [4]　/%

	硬件	软件	服务
全球	45.4	34.2	20.4
中国	54.3	37	8.7

（五）网络空间安全标准的发展现状

我国网络空间标准化工作取得显著成效，正在逐步融入国际体系。至 2014 年 10 月，信息安全标准委员会正式发布国家标准 142 项，范围涵盖信息安全基础、安全技术与机制、安全管理、安全评估以及保密、密码和通信安全等多个领域，有力地保障了国家和社会的网络安全。信息安全标准体系的逐步完善，为我国各项信息安全保障工作，例如，云计算服务网络安全管理、政府信息系统安全检查、信息系统安全等级保护、信息安全产品检测与认证及市场准入等，提供了强有力的技术支撑和重要依据 [7]。

四、我国网络空间安全产业发展问题及趋势分析

（一）我国网络空间安全产业发展面临的问题分析

（1）多头管理、职责分散。我国已设立网络安全和信息化领导小组，并下设办公室，但由于网络空间安全领域涉及行业众多，统一协调的工作难度确实较大。此外我国网络空间安全领域存在多头管理现象，多个部门涉及信息安全产业管理，导致决

策权分散、规则冲突、操作效率低、执行难度大，对重大网络空间安全问题、核心安全技术的研究工作难以形成合力，我国网络空间安全产业发展面临瓶颈。

（2）产业发展滞后于需求增长。《信息安全产业“十二五”发展规划》产业目标指出：到“十二五”期末形成 30 家信息安全业务收入过亿元企业，力争培育出信息安全业务收入达 50 亿元的骨干企业。以目前行业内的骨干企业规模来看，这一目标较难达到[2]。目前我国缺乏为国家级客户提供网络空间安全服务、解决国家级网络空间安全问题的专属企业，同时也缺乏提供行业解决方案和完整产品线的专业网络空间安全企业，缺乏可以带动产业集群发展的龙头企业。网络空间安全企业在核心技术、关键产品和服务的创新能力等方面仍存在显著不足，产业链关键环节尚未有效突破。

（3）自主可控普及任重道远。目前我国重点领域信息系统中的大部分高端元器件与核心网络设备仍依赖国外，应用于党政军部门的信息安全管理系统、操作系统、数据库、服务器等设备的国产化率仍然较低，自主可控软、硬件尚未得到广泛的普及和认可，应用推广任重而道远。系统应用核心软、硬件设备的自主化突破已成为必须攻克的战略性课题。同时自主可控软、硬件产品在技术、产品稳定性、兼容性、技术规范、标准化等方面与国外同类产品存在一定差距，以自主可控为基础的国产化替代工作任重道远。

（4）网络空间安全服务业亟需完善。网络空间安全服务业得到国家的高度重视，传统安全企业结合自身技术特色，加速向安全服务商转型。但我国网络空间安全服务体系不完备、缺乏规范，安全服务业依旧是我国网络空间安全产业的薄弱环节。我国既缺乏相当规模、高质量的专业安全服务提供商，又缺乏大量的相关专业人才，体系化建设的进程缓慢。

（5）产业环境尚需完善。“网络空间安全”获批国家一级学科和《中华人民共和国网络安全法（草案）》的颁布，有望补充我国对高层次、复合型专业安全人才的需求，为网络空间安全实践提供强有力的制度保障。但目前政策法规方面对创新和知识产权保护仍显不足，企业间恶性竞争的情况时有发生，我国网络空间安全产业发展的大环境仍需不断完善。

（二）“十三五”期间网络空间安全产业发展趋势分析

1. 网络空间安全产业总体发展趋势

面对网络空间日益严峻的威胁与挑战，我国政府高度重视网络空间安全产业的发展，不断加大在电信、金融、能源等国家关键基础设施重要信息系统的网络空间安全建设，关键领域网络空间安全产品逐步实现国产化替代，自主创新产品日趋多元化，网络空间安全产业规模逐年递增。据分析，到 2017 年我国网络空间安全产业规模将达 619.87 亿元人民（见表 3），产业结构上仍以网络设备等硬件信息安全基础设施为主，围绕软件、服务的信息安全细分产业将有不同幅度的增长（见表 4）[4]。

2. 网络空间安全与新一代信息技术广泛融合

移动互联网领域成为网络空间安全新战场。移动互联网的安全问题主要涉及移动设备安全、移动应用安全以及移动环境安全三大方面。工业和信息化部颁布的文件特别强调“移动应用商店和应用程序安全管理，督促应用商店建立程序开发者身份信息验证、应用程序安全检查、恶意程序下架、恶意程序黑名单、用户监督举报等制度，建立健全移动应用程序第三方安全检测机制”[5]。移动互联网“云 + 端”的发展模式也为网络空间安全产业的发展带来了新的机遇，一方面是用户海量隐私信息汇聚云端，云安全产品及服务需求显著增长；另一方面移动终端功能（存储、定位、拍摄）日益强大，用户获取共享信息的能力显著增强，导致对用户监管难度增加，因此移动互联网舆情监管产品及服务存在巨大发展机遇。

网络空间安全与大数据互为支撑。大数据技术的广泛应用催生了新类型的网络空间安全产品。其

表 3　2015—2017 年中国信息安全产业规模及增长率预测 [4]

规模及增长率	2015 年	2016 年	2017 年
市场规模/亿元人民币	398.39	503.96	619.87
增长率/%	24.0	26.5	23

表 4　2015—2017 年中国信息安全产业产品比例结构预测 [4]

/%

年度	硬件	软件	服务
2015	53.2	38.4	8.4
2016	52.9	38.6	8.5
2017	51.9	39.1	9.0

中一类是利用大数据技术进行安全防御的产品，主要包括利用大数据技术对网络、终端、数据库、应用和身份与访问管理系统数据进行被动防御，针对潜在攻击的主动防御以及用于发现攻击行为的安全性大数据收集系统等。另外一类是保护大数据应用安全的产品，主要包括开放化数据环境安全、非结构化数据存储安全等。

3. 网络空间安全与“中国制造 2025”

“中国制造 2025”是中国版的“工业 4.0”，以全球制造业格局和我国经济发展环境重大变化为背景，提出我国制造强国建设三个十年的“三步走”战略。第一个十年的行动纲领中，包括提高国家制造业创新能力、推进信息化与工业化深度融合、强化工业基础能力、加强质量品牌建设和全面推行绿色制造五大重点任务 [8]。

网络空间安全产业是“中国制造 2025”大力推动的新一代信息技术产业，既是建设“中国制造 2025”的重要任务之一，也是实现这一战略的重要保障，具体表现在以下几个方面。

（1）网络空间安全是实现自主可控的关键环节。当前国内自主可控信息系统在处理器、操作系统、数据库、中间件等关键领域取得了技术突破。软、硬件间兼容适配、测试验证等工作也全面展开，在一定范围内进行了规模化应用。然而，目前自主可控信息系统“标准化、系列化、通用化”发展滞后，行业内缺乏自主可控产业标准和规范支撑；自主软件和硬件相对独立开发，相互间的技术协同和融合不够，导致从底层硬件到上层软件之间的整合优化不够。这些问题导致应用自主可控信息产品的系统存在脆弱点与较高的安全风险。一方面需要大力开展网络空间安全核心技术产品的自主研发工作，加强系统安全一体化设计；另一方面应大力发展网络空间安全服务业，开展自主可控信息系统的测试评估、监测预警、安全维护等高质量专业服务。

（2）网络空间安全是强化工业基础能力的重要保障。信息化与工业化深度融合是发展的大方向，其中智能制造是“两化”融合的主攻方向之一。新型生产方式将逐步实现生产过程智能化，随之而来的网络空间安全问题也更加严峻，已全面融入企业研发、生产、管理和服务各个环节；另一方面互联网在制造领域应用的深化也使得网络空间威胁常态化。“中国制造 2025”为强化工业基础能力，提出统筹核心基础零部件、先进基础工艺、关键基础材料和产业技术基础“四基”发展，突破国外垄断。但是目前很多核心元器件，如芯片制造等，高水平的生产线还建在国外，在生产过程中存在被植入后门，遭受网络空间攻击的风险。我国在推进“四基”发展建设中，应统筹考虑与网络空间安全的一体化设计。

（3）提升我国网络空间安全企业品牌。“中国制造 2025”战略鼓励我国企业追求卓越品质，形成具有自主知识产权的名牌产品，不断提升企业品牌价值和中国制造整体形象。近年来，网络空间安全产业逐步呈现繁荣景象，在市场竞争机制下，相关企业逐步分化，掌握核心技术产品和服务的网络空间安全企业在市场竞争中占据主导地位，不良企业被淘汰，产业格局逐渐明朗；另一方面创新创业的热潮带来更广阔的互联网发展空间，也为网络空间安全提供了更多的产业机会。近些年，传统互联网巨头企业如腾讯计算机系统有限公司、阿里巴巴网络技术有限公司、百度等公司通过入股或收购中小信息安全企业布局网络空间安全产业。华为技术有限公司等设备提供商也利用其在网络设备、软硬件产品的技术研发优势，不断开发相关网络安全产品。这些龙头企业的品牌效应以及市场容量有助于其网络空间安全产品的推广，不失为快速树立我国网络空间安全产业品牌的一条途径。

五、促进网络空间安全产业发展的政策建议

（一）统一国家产业战略规划，建立强大网络空间安全产业基础

国家需要统一产业战略规划，统筹考虑我国具有高水平、自主可控、科学规划的强大网络空间安全产业基础。通过政府的力量，扶持国家网络空间安全的产业国家队发展。首先，必须在关键、核心信息技术和产品上实现突破，提高网络空间安全保障能力水平，逐步摆脱受制于人的被动局面；其次，政府要加强对自主可控产业的扶植政策。在事关国家安全的核心领域，不能单靠市场，也需要政府的宏观调控，甚至是阶段性的直接支持，要重点扶持有实力的国内龙头企业，提高中国网络空间安全市场的战略性地位，使得中国网络空间安全企业可以立足中国市场向国际市场迈进。

（二）设立网络空间首席安全官，落实网络空间安全产业政策与措施

“责任落实”是网络空间安全产业政策和措施得以落地的先决条件，如《中华人民共和国网络安全法（草案）》中规定设立网络安全责任人及责任制等。要重视网络空间首席安全官等网络安全责任人的设立，并以此明确安全责任制度，使网络空间安全产业政策和措施能“落实到岗、责任到人”。

（三）加速网络空间安全标准化工作

结合当前和未来的网络空间安全发展形势，尽快制定网络空间安全标准，进一步提高标准质量，积极应对新的突出问题和共性问题。各级政府应积极研究改进标准化工作，加强对标准研制过程的管理，加大对重点标准的支持力度，确保标准质量。建立标准评价机制，将公众和同行的参与度作为标准评价依据，提高中国标准的被接受程度和影响力。

参考文献

[1] 刘助仁. 信息安全产业是数字信息社会可持续发展的保障[J]. 信息安全与通信保密, 2002(7): 15–18.
Liu Z R. Information security industry is the guarantee of sustainable development of digital intelligence society [J]. Information Security and Communication Privacy, 2002(7): 15–18.

[2] 工业和信息化部信息化和软件服务业司. 促进产业创新发展，提升信息安全保障能力——《信息安全产业“十二五”发展规划》解读[N/OL]. 中国电子报, (2012-02-24) [2016-06-15]. http://epaper.cena.com.cn/content/2012-02/24/content_233661.htm.
Information Technology and Software Service Division of the Ministry of Industry and Information Technology of the People’s Republic of China. Promote the innovation and development of the industry, enhance the ability of information security—interpretation of *the development plan for information security industry during the 12th Five-Year Plan* [N/OL]. China Electronics News, (2012-02-24) [2016-06-15]. http://epaper.cena.com.cn/content/2012-02/24/content_233661.htm.

[3] 全国人大常委会法制工作委员会. 中华人民共和国网络安全法（草案）[EB/OL]. (2015-07-06) [2016-06-15]. http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.
Legislative Affairs Committee of the Standing Committee of the National People’s Congress. Cyber Security Law of People’s Republic of China (Draft) [EB/OL]. (2015-07-06) [2016-06-15]. http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.

[4] 中国电子信息产业发展研究院. 2014—2015中国信息安全产业发展研究年度报告[R/OL]. (2015-02-10) [2016-06-15]. http://www.ccidreport.com/report/content/6/201502/679308.html.
China Center for Information Industry Development. Annual report on the development of information security industry in China (2014—2015) [R/OL]. (2015-02-10) [2016-06-15]. http://www.ccidreport.com/report/content/6/201502/679308.html.

[5] 中华人民共和国工业和信息化部. 关于加强电信和互联网行业网络安全工作的指导意见[EB/OL]. (2014-08-29) [2016-06-15]. http://www.gov.cn/xinwen/2014-08/29/content_2742159.htm.
The Ministry of Industry and Information Technology of the People’s Republic of China. Guidance on strengthening cyberspace security in the telecommunications and internet industries [EB/OL]. (2014-08-29) [2016-06-15]. http://www.gov.cn/xinwen/2014-08/29/content_2742159.htm.

[6] 中国银行业监督管理委员会. 关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见[EB/OL]. (2014-09-03) [2016-06-15]. http://www.cbrc.gov.cn/govView_115696B8621049099A0B880DAB133A33.html.
China Banking Regulatory Commission. Guidance on strengthening the construction of cyberspace and informationization in banking industry by applying safe and controllable information technologies [EB/OL]. (2014-09-03) [2016-06-15]. http://www.cbrc.gov.cn/govView_115696B8621049099A0B880DAB133A33.html.

[7] 高林. 标准化工作有力支撑网络安全保障[J]. 信息安全与通信保密, 2014(12): 49–50.
Gao L. Standardization supports cyberspace security assurance vigorously [J]. Information Security and Communication Privacy, 2014(12): 49–50.

[8] 中华人民共和国国务院. 国务院关于印发《中国制造2025》的通知[EB/OL]. (2015-05-19) [2016-06-15]. http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.
The State Council of the People’s Republic of China. Notice of the State Council on issuing “Made in China 2025” [EB/OL]. (2015-05-19) [2016-06-15]. http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.