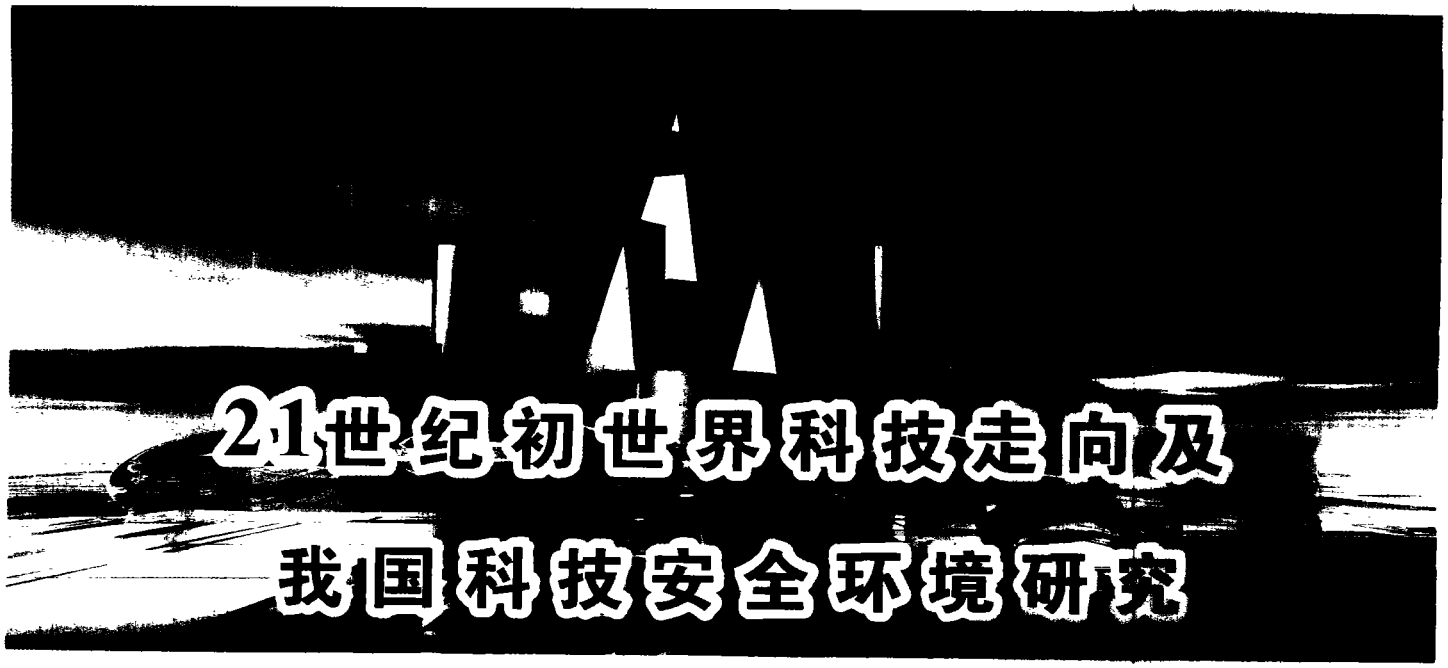


21世纪初世界科技走向及我国科技安全环境研究

张利英，郭建平

（海军军事学术研究所，北京 100841）

摘　要：论述了当今世界科技发展及其对我国科技安全产生的重要影响；阐述了我国科技安全面临的机遇与挑战；提出了我国科技安全的目标及实现这一目标的建议与对策。

关键词：科技发展；国家科技；安全环境；对策

中图分类号：G321　　**文献标识码**：A　　**文章编号**：1001-7348(2004)02-0014-03

1.1　世界科技发展呈加速化

（1）科学技术发展速度越来越快。

（2）科技知识更新速度不断加快。世界科学技术理论成果和实际应用技术呈显著膨胀态势，科技论文、著作和技术发明专利在一定时期内成倍地增长。据估计，目前全世界每天发表科技论文在8000篇以上，全世界全年批准的专利数量达120多万件。科技知识每隔3~5年就要增加1倍，新学科不断涌现。

（3）科学技术的发展周期越来越短。从16世纪中叶到19世纪中叶，人类进入机器时代，大约经历了300多年；从19世纪中叶到20世纪初，人类进入电气时代，经历时间不到100年；第二次世界大战前后，人类进入了原子能时代，时间只有几十年；后来又经历了电子时代、目前正处于信息时代（生命时代，纳米时代）等，其相互交替的间隔越来越短。

1.2　世界科技发展呈综合化

（1）交叉科学的兴起。19世纪中叶以前，科学与技术是分离的，它们各自独立地发挥社会作用。21世纪初，科学技术发展呈现出各门学科之间、各种技术之间的广泛渗透与融合，使各门学科以及科学与技术之间的界限逐渐模糊，从而导致交叉科学、综合学科的兴起，使世界科学技术发展呈现出综合化趋势。

（2）综合技术的应用。随着技术不断向大型化、复杂化方面的发展，技术应用已由过去传统的零散技术向“智能技术”发展，出现了大量复合型的综合技术。

1.3　世界科技发展呈一体化

（1）科技发展的产业化。高新技术的大量引进和跨国传播，使各国经济连成一体，进一步推动了经济全球化和高新技术的产业化。

（2）科技发展的社会化。主要表现在3个方面：①从小科技到大科技是科学技术社会化的重要标志。②科学技术的产业化。一方面，新的科技革命导致新的产业革命，新的科技成果导致新的社会产业；另一方面，科学技术自身的产业化。③是科学技术与教育、经济的一体化。

（3）民用军用的一体化。

随着世界形势的发展变化和各国力量的此消彼长，特别是科技的迅速发展及其在经济发展中作用的不断增大，人们对国家安全的认识也在不断扩展和深化，逐渐从多方面、多角度来探讨和研究国家安全问题。新的国家安全观认为，国家安全不仅是传统意义上的军事和政治安全，而是包括军事、政治、经济、科技、文化等诸方面安全的有机结合。

国家科技安全是国家安全的重要组成部分，它包括科技情报安全、科技人员安全、信息安全和军事科技安全等方面的内容，其目的是争取和保持国家科学技术发展的优势。世界科学技术的飞速发展，对我国未来的科技安全形势和环境将带来重大影响，主要表现在：

2.1　对我国科技安全的影响

收稿日期：2003-06-23

一是面临西方大国科技情报的挑战。在现代科学技术的许多领域，各国之间的竞争十分激烈，谁善于开发利用情报，特别是善于从对方获取有关情报，谁就能迅速赶上或超过对方。冷战结束后，国际间的冲突越来越多地发生在科技领域，因而科技情报的地位正在不断上升。前美国中央情报局局长盖茨说，美国对经济情报的需求比在冷战时期大大增加，为此"中央情报局应把帮助政府确定经济方针、注意新技术的发展和应用的趋势以及经济领域的反情报战，作为自己情报工作的重点"。

二是面临来自企业和事业单位科技情报的挑战。西方国家除了在国家情报机关设立科技情报部门之外，在某些企业和事业单位中，也设有专门的科技情报部门。许多企业设在国外的办事处和分公司，担负着搜集别国科技情报的任务。

三是面临科技情报活动手段多样化和技术高级化的挑战。

四是面临科技人才竞争的挑战。高科技竞争，实质是人才竞争。因为科技人才不仅掌握了一定的科学技术，而且他们还掌握了所从事的科技研究现状、研究成果或科技专利，所以，高科技人员的流动，不仅是某个科研院(所)技术力量的流失，而且也给正处在研究中的科技安全带来了极大威胁。从这个意义上说，科技安全也包括科技人员的安全。

2.2 对我国信息安全的影响

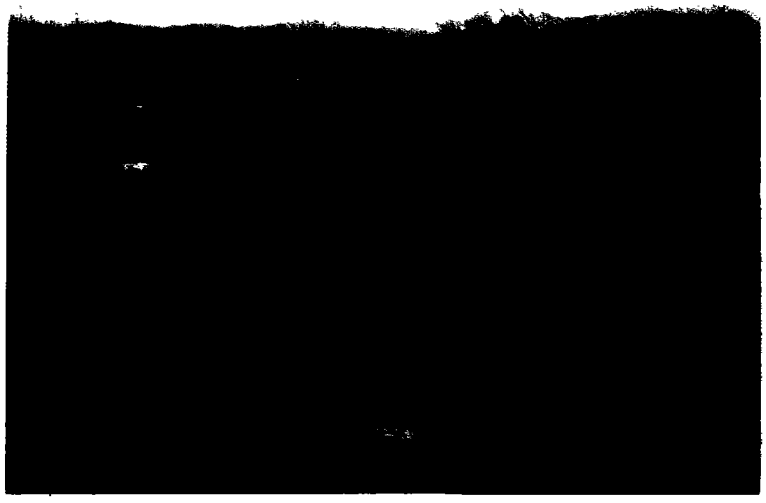
信息安全涵盖国家安全的各个方面，包括政治、军事、经济、科技、社会生活等领域都存在信息安全问题，是一个复杂的大系统。从科技发展上看，国家科技政策制定、发展战略、竞争策略、科技成果转化乃至产品工艺等，都蕴含大量的信息安全问题。

信息安全的威胁来自信息攻击，信息攻击使信息时代的国家安全面临多重威胁，主要有以下几种：一是对某国的信息系统进行攻击性行为。二是利用信息进行欺骗性攻击行动。三是对计算机网络进行攻击行动。四是占位和污染性攻击行动。由此可见，信息安全是科技安全的重要组成部分。只有高度重视信息安全，把安全管理制度与安全管理技术手段结合起来，信息安全才有保证，国家科技安全才有保证。

2.3 对我国军事科技安全的影响

军事科技安全是国家科技安全的重要组成部分，包括军事科技研究安全、军事指挥系统安全和军事科技情报安全等方面的内容，其目的是保障军事科技在安全环境下发展，并始终保持其优势地位，以不断提高我军的军事打击能力和防御能力，维护领土完整和国家安全。

冷战结束后，世界上一些重要的国家在规模裁军的同时加快了军事科技进步的步伐，一个以现代经济实力为基础、在高新技术推动下的新军事变革正在重塑国际军事实力对比，它在很大程度上也决定了未来国家安全的走势。



3 [illegible]安全目标[illegible]建

针对当前和未来世界科技安全环境对我国的重大影响，我们应从我国国情出发，科学地制定我国科技安全的基本目标，即以"科教兴国"和"科技强军"战略为指导，以维护国家安全和国家利益为目的，大力发展科技安全产业，建立健全国家科技安全管理体制，建立完善国家科技安全法律体系，培养壮大科技安全队伍，确保我国科技安全，使我国高新科技在世界占有一席之地。

3.1 增强科技安全的防范意识

一要重视思想建设，确立国家科技安全意识。由于未来科技(信息)环境的特点，决定了我们必须重视思想建设，牢固树立科技安全意识，重视国家科技安全防患工作，特别要下力气抓好军事科技安全工作的落实。二要更新思维方式，开辟科技安全新途径，切实把工作重点从抓一般条件下的常规保密转到抓高技术条件下的科技(信息)安全保密上来。高技术条件下，科技秘密的产生、传递、存储方式发生了根本性变化，窃密的技术、手段有了令人难以置信的发展，保密范围明显扩大，泄密渠道明显增多，保密工作的科技含量明显提高。为适应这种变化，我们应当树立新的思想观念，把工作重点放在抓高技术条件下的科技安全保密上来。三要实现"人—网"结合，提高科技安全防范能力。"人—网"结合是网络时代信息安全的本质特征。因此，要实现科技安全的目标，重要的一条是变革网络技术人员的思维方式，提高攻防谋略能力，实现"人——网"最佳组合，从而达到"趋利避害，为我所用"的目的。

3.2 健全科技安全的管理机制

一是建立健全国家科技安全体制。首先，要从有利于实施统一领导的实际需要出发，建立权威性强主管国家科技安全的职能部门。其次，要按照归口管理、分级负责的原则，明确各部门在科技安全工作中的权力与职责，做到密切配合，通力协作，军地互融，形成合力，使科技安全落到实处。再次，要坚持以我为主，构建科学合理的科技安全防护体系；要尽快建立与我国科技安全发展相适应的科技安全技术发展体制，形成研究、开发、应用一条龙式的技术保障体系。

二是构建科技安全技术管理机制。为了更有效地贯彻安全措施，发挥安全功能，要尽快构建安全技术管理机制。其主要内容：第一，加强资源管理。这里主要是指设备和用户。为了搞好资源管理，要建立网络安全管理中心，负责对网络的构造和性能进行管理。第二，进行鉴别管理。主要是指对要求使用信息系统的用户与身份进行确认。从贯穿分配描述性的信息、口令或密钥到要求服务的实体的全过程。第三，实施运行监视。主要是监视系统的运行，记录成功和非成功的连接及其连接用户的姓名、地址和现行状态等；记录网上出现的错误，监测系统

状态的变化，对非法用户的访问要报警。第四，开展访问控制管理。它是指利用访问控制权限表、通行字、持续访问时间等，对用户的权限和访问时间进行限制。也可包括通信实体间协议的使用和提供访问控制服务的其他实体。

3.3 完善科技安全的法律法规

我国对科技（信息）安全的立法建设一直十分重视。1997年修订的《中华人民共和国刑法》首次规定了计算机犯罪，标志着我国信息社会安全保护的规范化、法制化、科学化迈上了一个新台阶。1994年国务院令发布的《中华人民共和国计算机信息系统安全保护条例》是我国第一部计算机安全法规，它强调在计算机信息系统安全保护方面，不仅要保障信息的完整性、可用性、保密性和可控性，还要保障信息系统的正常运行。此后还发布了《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《计算机病毒防治管理办法》等。

除了法规，还需要制定操作性强的科技（信息）安全保密技术检查标准和便于检查的制度。信息安全保密技术标准的制定，为安全保密的量化管理提供了依据。由公安部主持制定、国家技术标准局发布的中华人民共和国国家标准GB17895—1999《计算机信息系统安全保护等级划分准则》已正式颁布，并于2001年1月1日起实施。

虽然我国在信息安全保密法规制度的建设方面，已经做了大量工作，但从迅猛发展的信息化进程来看，已有的这些法规制度，尚不足以覆盖科技安全的方方面面，尚难完全满足新形势下科技信息安全工作的客观需求。因此，应当进一步加强科技安全法规制度的建设。一是加快立法进程。凡属科技安全所需要的法规制度，应当按照急事急办的原则，抓紧研究拟制，不断建立和完善法规制度。二是提高立法质量。主要是增强法规制度的科学性、针对性和可操作性。三是加大执法力度。就是严格按照法规的要求约束、规范人们的保密行为。按法规要求规范科技安全工作，纠正各种违反法规的事项和行为，做到有法必依，执法必严，违法必纠。

3.4 提高科技安全的防御能力

第一，发展有我国特色的科技安全技术和产品。①发展密码技术和产品。加快研究和发展网络加密技术，研究密码算法体制、算法分割、密钥体制、密钥分割，统一加密标准，提高密码强度，以确保我国我军秘密信息的安全。同时，要跟踪研究基于物理的量子密码和基于生物的DNA基因密码。②发展防御信息攻击技术和产品。面对网络受到的种种威胁，应当大力发展计算机网络系统的早期预防技术，如发现信息武器攻击的技术，病毒认证技术，“黑客”的发现跟踪技术等，形成防御信息攻击、非法入侵的早期预警系统，防止重要信息被破坏、删除、歪曲和拦截。要充分利用这些高技术，开发出相应的科技安全产品。③发展计算机网络的安全保护技术和产品。④发展秘密信息防护技术和产品。为对付敌方的信息侦察技术，我们要大力发展秘密信息防护技术。要积极研制新的隐身材料，吸收雷达波、红外线、紫外线和微波的材料，使雷达、声纳和红外探测仪等侦察设备变成“瞎子”和“聋子”。就电磁波安全防范技术而言，要采取包括屏蔽、滤波、接地和噪音调制等技术。⑤建立我军统一的信息安全平台。我军信息安全基础包括安全产品测评认证、病毒检测和防治、国际出入口监控、关键网络系统灾难恢复、系统攻击与反攻击、信息安全紧急处置、密钥恢复监管、公钥基础设施与监管、信息战防御与遏制等。应尽快建立一套科学的标准和一组可以被调用的安全函数，为互联网中的各种应用提供统一的安全接口，为用户提供简捷安全的应用支持，以满足各种应用的安全需要。

第二，警惕技术设备引进中的科技安全风险。由于技术水平等条件的制约，我国相当一部分重要的信息处理设施及办公自动化、指挥自动化设备还不可避免地从国外引进，这就带来风险。发达国家在制造这些产品时，可能会嵌入窃密元件或埋下逻辑炸弹。在设备引进中如果放松警惕，不加检测，盲目引进，就可能造成信息泄露、系统瘫痪、指挥失灵等无可挽回的损失。因此，凡党、政、军、科研机关及涉及到国家秘密的单位，在配置自动化设备时，要优先选用我国产品；核心秘密的处理设备（如密码机等）必须选用经国家有关部门批准的产品。必须使用进口产品的，应在启用前请有关部门进行检查、测试，特别是通讯设备和计算机系统设备应列入必检之列，以防别有用心之人在原机上埋设窃密元件。

第三，采用独立的先进安全技术，增强科技安全措施。为保证网络正常运行，在网络自身安全方面亦应采取相应的技术措施，尽量采用我方自行研制的性能可靠、稳定的网络连接设备及自主的网络操作系统，加强网络防护措施，避免防护设施中“后门”现象的出现。一是研制和使用我国自主研制的防火墙技术，加强对外界人员访问网络的限制和监测。二是利用代理服务器加强对内部网络人员访问外部网络的统一管理，预防无意泄露秘密信息和地址信息行为的发生。三是对网络核心设备如路由器和域名服务器等采取双备份工作，如确有必要可建立堡垒机的安全体系，确保网络受到攻击时能正常运行。四是对网络重要资源服务器和备份系统加强管理，采用安全稳定的网络操作系统，及时发现系统存在的隐患，尽早加以解决，尽量减少“后门”现象所带来的损失。五是加强加（解）密技术的研究，寻找出更多更安全的加密技术。

第四，尊重科技安全人才，确立人才安全观念。在科技安全技术的运用和创造中，最关键的因素不是物理的设施和工具，而是掌握知识、善于创造的科技人才。因此，搞好科技安全工作，必须确立人才安全观念。首先，要高度重视运用技术性力量和手段，要充分利用和发挥科技人员特别是计算机技术人员的优势。其次，国家应当在高科技领域的人才安全方面专门立法，以保护人力资源，防止人才的不正常流失。据有关人士介绍，截至目前，我国尚没有任何一部专门的人力资源法。而在有些国家，人才安全早已是立法保障的重要对象。在经济条件尚不足以与发达国家和跨国集团对垒的今天，又有不断健全和完善立法保障措施，才是防止人才不正常流失的变革之举。

参考文献：

[1]刘鸿基，范震江，罗海曦.邓小平国防建设思想研究[M].北京：国防大学出版社，1997.

[2]丛友贵.信息安全保密概论[M].北京：金城出版社，2001.

[3]迈克尔·皮尔斯伯里.美国学者解读中国安全[M].北京：新华出版社，2001.

[4]中共中央党校教务部.五个当代讲稿选编[M].北京：中共中央出版社，2000.

[5]张召忠.网络战争[M].北京：解放军文艺出版社，2001.

[6]李大光.中国安全决策[M].北京：石油工业出版社，2002.