科技战略

“核芯”技术亟需自主掌控

长期以来，我国在微处理器芯片研发领域面临着知识产权、生态体系等诸多问题。尤其是近年来依托ARM构架技术授权，不少国产芯片直接贴上“自主可控”标签，以“安全可信”为由向涉及国家安全的诸多行业渗透。这种自主可控芯片，依然存在知识产权、研发实力、生态体系和利润效益等受制于人的巨大隐患，应当引起高度警惕。

□ 唐　嘉　张乃千　张海波

日前，国产芯片飞腾FT-1500A系列处理器得到人们的广泛关注，将在政府办公和金融、税务等方面得到广泛应用。随着信息技术的飞速发展，信息产业基础性产品直接关系国家信息安全，自主可控的重要性不言而喻。

阵痛隐隐，核心科技尚缺失

在信息时代，一旦发生信息泄露，将造成难以估量的损失。2013年“棱镜门”事件发生后，芯片、操作系统等核心软硬件的自主可控能力再次得到人们的广泛关注。长期以来，我国在微处理器芯片领域受制于人，核心技术缺失，与西方技术强国有较大差距，不少信息技术产品“心脏”之疾“阵痛隐隐”。

知识产权缺失。当前，以美国为首的西方国家在微处理器芯片领域牢牢掌握技术和专利优势。目前市场上x86、ARM、MIPS和POWER四种主流芯片构架，都被外国公司通过专利保护严格控制。除了少数公司外，国产微处理器芯片核心构架尚不能完全自主，好比盖房子用的却是借来的“图纸”。目前ARM公司授权我国的芯片技术并非永久性授权，具有限制性和期限性。国内公司购买的授权，大多不具备自主扩展的指令集，只能在制定好的“游戏规则”中开展设计，更加限制了国产芯片的技术进步和发展。

安全隐患无穷。“棱镜门”事件暴露了美国等西方国家依托高科技产品对其他国家的情报收集工作。在微处理器芯片领域，只有走独立自主发展的道路，才能确保安全可控。国内的ARM构架芯片设计厂商在芯片性能、功耗和安全性上完全不具备话语权。国内公司普遍购买的ARM构架，工艺核心技术还依赖境外提供，大部分核心模块都不可修改。在这种情况下，芯片本身存在的安全和后门问题将难以得到解决，更增加了安全隐忧。

利润受制于人。近年来，由于缺乏自主知识产权、市场竞争激烈，国产芯片虽在国家层面得到了政策和资金支持，但利润受制于人。由于技术上的优势，ARM公司牢牢控制着技术授权的定价权。国内公司购买ARM指令集授权，成本高昂，一旦指令集到期或是更新必须重新购买。此外，每生产一枚芯片，国内公司还要向国外缴纳专利费用。

供血不足，微芯片聚焦国力

在自主可控领域，我们要充分认清“开放授权”与完全自主知识产权的区别，警惕某些拿来主义的“障眼法”。尤其是近几年，国外芯片设计企业采取类似“开放授权”手段，通过技术授权和合资策略加快本土化建设。长期以来，我国在市场拓展、人才储备、技术积累、资金投入等诸多领域存在“供血不足”的严峻问题。把脉宿疾寻找病原，才是解决自主可控芯片发展的一剂“良方”。

专业支持力不足。微处理器芯片和操作系统是信息技术领域的两大复杂性系统工程。目前我国在芯片设计领域的技术储备不足和人才短缺情况较为严重。我国每年出货芯片超过10亿片，但国内自主设计的却为数不多。即使是在获得了ARM公司的技术构架后，我国仍没有完全吃透芯片设计的全部技术，只是在构架的部分可配置开发模块上做些“修修补补”的工作。加大专业支持力度，吸引更多经验丰富的工程人员开展自主可控芯片研发，成为当务之急。

联合挤压成常态。为限制我国自主知识产权的微处理器芯片研发，国外公司“软硬兼施”。一方面，国外公司对高端技术采取严格保密。ARM公司提供的芯片构架，不但价格昂贵、授权期限短，而且被严格限定使用范围。另一方面，为冲击本土企业芯片市场，扼杀国产自主可控芯片，国外厂商释放出多个“糖衣炮弹”。IBM公司在中国成立“POWER技术产业生态联盟”，高通、英特尔公司也相继宣布在国内建立研发基地，对本土企业造成巨大冲击。

体系建设任务重。生态体系才是微处理器芯片竞争的“选票”。国产芯片起步晚，在工艺和技术性能上存在一定劣势，整个行业体系发展还面临诸多障碍。国外主流微处理器芯片经过几十年的发展，已经建立了成熟的生态体系。而国产软件行业和信息厂商对自主芯片配合失误，更加限制了国产芯片的推广发展之路。

牵线搭桥，精雕细琢出精品

在信息产业领域，俄罗斯与我国有着相似的国情。经过快速技术消化吸收，目前俄罗斯已独立研发出“厄尔布鲁士”（Elbrus）微处理器芯片，并配套开发了相关操作系统和应用软件。他山之石可以攻玉。治愈信息产业的“芯脏病”，仍需我们从国家层面牵线搭桥，对自主可控芯片精雕细琢出精品。

可以充分借鉴吸收。学习国外技术成果，迅速提升自主设计和研发实力，不失为提高芯片自主可控的“捷径”。高通公司就是在获得ARM构架许可后，研发定义新指令集，加以知识产权保护，逐步摆脱了对ARM构架的依赖。近年来，国外主流微处理器芯片厂商纷纷加紧高价值专利收储和专利产出，我国可充分利用这一机遇，通过国家层面建立专门的专利运营与收储机构，对核心技术予以收购吸收，增强我国芯片产业的风险防控能力和谈判话语权。

要学会借力打力。信息产业领域市场竞争激烈，国外公司形成的“芯片技术联盟”并非牢不可破。除单纯依靠ARM构架外，我们还可以充分利用MIPS和POWER构架，争取可持续授权，在短时间内提升芯片研发和设计实力。近年来，IBM公司为了抗衡英特尔X86构架在CPU市场上的垄断地位，正逐步提升POWER构架的开放程度。短时间内我国利用POWER构架开展微处理器芯片自主设计，不存在知识产权壁垒，可有效提升我国自主可控芯片的整体性能。

当然不可操之过急。“冰冻三尺，非一日之寒。”龙芯在获得了MIPS公司永久授权后，经过长期自主扩展指令集和软件系统配套建设，才逐步形成具有自主话语权的生态体系。提升国产芯片独立、安全、可控的技术实力，是一项长期而艰苦的斗争，必须做好充分准备。我们应当加快专利许可与反垄断制度的研究，避免国外芯片厂商利用过期专利再包装、公知技术专利化建立起“技术恐吓”。在技术层面上我们要集思广益，拿出完整的体系解决方案以吸引开发者，培育自主可控芯片的产业生态。

完全自主可控是关键。我国自主微处理器芯片面临着“兼容”与“可控”同时并举的现状，但如果不能完全自主可控，势必对国家信息安全构成巨大威胁。在芯片设计和研发上，我国决不能始终做他国技术的“追随者”，要加速形成芯片生态体系的持续改进、螺旋上升的研发态势，着力将投资集中在自主可控芯片的产业化以及工艺设备的自主化升级方面。我们必须以应用需求为牵引，以市场选择为导向，通过软硬件领域整体优化，精雕细琢，逐步建立具有我国国情的自主可控微处理器芯片体系。

美军人事体制改革新动向

□ 付征南

近年来，美军为顺应信息化时代的新趋势，不断加大人事体制改革的力度，特别是在国防部长卡特的强力主导下，以“未来部队”计划为核心，连续出台了多项人事制度改革方案。综合来看，这些改革举措体现出四大新动向，将对美军的未来产生极为深远的影响。

实施“数据化”考评机制。作为工业化时代军队人事制度的产物，美军现行军官晋升考评制度最早源于20世纪初的“鲁特改革”，而后经过1947年《军官人事法》、1954年《军官等级限制法》和1980年《国防军官人事管理法》等数次调整，逐步形成了较为完善的人才选拔机制，其核心是依靠严格透明的考评标准，来规范选人用人程序，以扭转此前长期存在的超常提拔、违规用人的“政治将军”现象。在此制度下，上尉到少将军官晋升采取“集中选拔制度”，由各军种临时组建的集中选拔委员会进行评定；中将以上军官晋升则采取“提名审批制度”，候选人须经国防部长推荐、总统提名和参议院审批三道环节，才能履新就任。这一制度最大的优点，是通过严格的考评标准，避免人事政策出现“劣币驱逐良币”的“逆淘汰”现象，并依托透明的晋升程序，杜绝人事腐败问题。但其最大的弊端则在于考评标准过于单一僵化，不仅导致某些高级岗位长期为某一军种或兵种垄断，从而形成尾大不掉的利益集团和任人唯亲的“裙带”现象，而且也难以做到与时俱进，将符合时代特点的优秀人才选拔出来，导致约翰·博伊德等一大批顶级战略人才，只能在中校或上校岗位被迫退役，进而成为美军人才流失问题的主要根源。例如，美空军一份调查报告显示，空军参谋长人选自1982年以来长期为战斗机飞行员“垄断”，导致67%的上将和63%的一级司令部司令职位都由其把持，因此“他们构成一个上层精英群体，即使不是彻底控制，至少也影响空军体制的方方面面”。为扭转这一现象，卡特于去年11月推出了“未来部队”计划，力求通过新组建的“人力分析办公室”，利用大数据等先进数据分析手段，更为精确地反映军官潜力、贡献和能力等隐性指标，以最大化地排除选人用人过程中的主观人为因素，并使人才考评标准能够随着时代的发展而不断升级演进，同时效仿“LinkedIn”的运行机制，试行“基于网络的人才管理制度”，将官兵的个人档案全部入网入库，使各军种和各作战司令部等用户单位能够通过网上数据库，根据岗位动态需求，及时发现所需人才，从而最大限度地做到人职匹配、人尽其才。

推广“弹性化”服役制度。长期以来，美军一直秉承“终身教育”和“教育是最大福利”的基本理念，依托传统的岗位轮换和职业教育制度，使军官的学历、阅历和能力等“人力资本”能够随着服役时间的延长而实现“阶梯化”的“增值”效应，确保了军官即便退出现役也会成为整个社会的精英阶层，从而有效解决了年轻军官的保留和中高级军官的退役安置问题。然而，这一制度当前存在轮换渠道封闭、教育机会失衡等严重问题，相关政策的灵活度和竞争力无法与地方企业相比，难以适应信息化时代人才知识结构和培养管理模式发展的新特点。为解决这一难题，美军准备全面推行“职业间歇计划”，允许官兵服役期内拥有3年可自由支配的假期，使其能够赴地方求学、政府工作或进入谷歌等顶级企业任职而后再重返部队服役，进而加大军队与政府和地方企业之间的人事互动，使官兵人力资本能够通过这种“旋转门”式的弹性服役制度，实现最大化的增值效应，同时也让社会最新管理理念和技术创新成果无缝融入军队实践，进而促进技术和思维创新。

深化“多元化”人事政策。过去，美军高层人事结构长期由白人男性主导，用人政策方面普遍存在性别歧视和种族歧视的“潜规则”，不能反映当前女性和少数族裔兵源比重和地位作用不断上升的主流趋势，也与国家社会的整体发展潮流相互脱节，难以调动相关群体安心服役的积极性。为此，美军“未来部队”计划，提出全面拓展“多元化”人事政策，力求通过选拔和培养女性和少数族裔优秀军官，特别是增加其在高层人事结构中的比例，并向女性官兵全面开放任职岗位，来拓展相关群体的职业发展路径，提升相关群体官兵的向心力和凝聚力。在此政策下，美军近年来将多位优秀女性和少数族裔军官，选拔到高级指挥岗位，有力地促进了部队思维方式、决策模式和行动样式的“多元化”。正如美国国防部题为《“多元化”与“包容性”战略计划——2012—2017》所言，“多元化的身份背景和个人经历，将会带来不同的思想观点和思维模式，对于组织创新至关重要……利用各类人员的多样化特性，营造一个包容性的环境，进而让每名成员都能得到重视和鼓励，为我们提供组织创新、资源优化和任务成功所必需的思想，是我们的一大战略优势。”

“一体化”的用人机制。美军通过1986年《戈德华特-尼科尔斯法》和2007年《约翰·华纳法》逐步构建起了一套相对完善的联合军官培养、选拔、晋升和任用管理机制，规定联合军官晋升比例不得低于军种同级军官，不经联合培训和联合岗位任职不得晋升为将军等，进而确立了“联合优先”的用人导向。然而，这套制度在联合军官认证机制的设计方面过于僵化封闭，只把政策计划和指挥控制等岗位军官列为联合军官，但却把情报、火力、运输、后勤、预备役等其他岗位排除在外，从而导致作战部队与情报部队、常规部队与特种部队、现役部队与预备役部队军官岗位类别出现了明显的等级化差异。例如，在传统联合军官制度下，美军军官晋升任用比例严重失衡，常规部队与作战部队军官晋升机会较多，属于“主流派”军官，掌握重大的话语权，但是情报等专业密集型部队、特种作战部队以及预备役部队军官只能在有限领域任职，军衔晋升空间受限，属于典型的“非主流派”军官，难以反映信息化时代作战空间多维化、平战界限模糊化、力量使用无缝化的新趋势。为此，卡特4月5日在“战略与国际问题研究中心”的讲话中，提出全面拓展联合军官的概念，并将联合军官必要任职年限由3年压缩为2年，从而全面拓宽情报、后勤等岗位军官的职业发展路径。在此机制下，美军诞生了首位空军武器控制员出身的战区司令——罗丽·鲁滨逊（北方司令部）和首位特种作战出身的中央司令部司令约瑟夫·沃特尔。这些举措将使美军各类部队之间的任职界限和岗位差异日益淡化，也使美军“主流”与“非主流”军官的职业定位发生历史性转变。

外军动态

何为网络战

□ 王永华　姜连举

面对踏着信息时代鼓点而来的网络战，人们既熟悉又陌生，说熟悉是因为网络战早已在视听之中，说陌生是源于对网络战的庐山真面并非完全认知。

网络战是个多维的概念，不仅网络空间具有多维性，而且网络战的“战”字也有多层内涵。日常所说的网络战包括政治、经济和军事网络战，政治和经济网络战的“战”，并不是真正意义上的战争，准确地讲是带引号的战，这个“战”非真刀真枪之战，是通过网络空间开展的政治和经济博弈对抗，打的是政治仗和经济仗，称其为网络战是因为其目的和意义不亚于战争。军事网络战是真正的战，打的是军事仗，是围绕军事目的在网络系统空间开展的作战。目前世界上发生的网络战多是政治和经济网络战，真正意义上的军事网络战还没有发生，但已经和战争如影随形，时刻都会发生。

政治网络战、经济网络战和军事网络战，三者相互交织，既有联系又有区别。各种网络战相互浸透，有的通过政治网络战达到经济与军事目的，或通过经济和军事网络战实现政治目的，有的采取经济网络战达到军事目的。2008年爆发的俄格冲突，是世界上首次与军事作战同时发生的网络攻击。俄出兵前就对格鲁吉亚政府网站进行了协同攻击，导致互联网瘫痪，幸运的是，格当时经济领域对网络依赖程度低，网络攻击只是给格网民造成了不便，而没有造成电力、金融等经济领域灾难性后果。政治、经济和军事网络战亦有区别，政治网络战主要目的是冲击和影响社会各个层面，破坏对手国家政治安全和稳定，近年来世界范围的“颜色革命”背后，都不同程度存在利用网络推波助澜的影子，可称为政治网络战的现实版。经济网络战是通过网络攻击摧毁对方的金融、商贸、交通、电力等经济中枢，令其经济体系陷于瘫痪。军事网络战则是通过破坏对手战场网络的核心属性，降低网络对联合作战的支撑保障作用，实现对战场网络系统的体系破袭，抢占军事体系对抗的先机与优势，赢得作战的胜利。

全面认知网络战，还有一个问号要拉直，黑客行为等于网络战吗？答案：否。由于网络战平战界限模糊，加之网络技术先天不足，黑客获取网络攻击的工具和手段易得，且手法卑劣，具有偷梁换柱、栽赃他人、异地作案、暗下黑手等特点，使得黑客“黑”你不商量的“网患”天天有，难免让人把黑客行为理解成“战”。一般而言，网络上黑客所干的“黑事儿”，多是谋取私利的“非战”行为，并未升级到战的层面，有些群体和企业采取黑客行动也多是以获取经济利益为目的，也不能同网络战画等号。当然，如果黑客变成实现某些政治、经济和军事目的工具，实施网络黑客行动时，其黑客行为就发生了质变，披上了网络战的“战袍”。网络的复杂性使得网络战具有多重性，这就需要以多维的视角全面审视，认清网络战的真面目，寻求有效应对之策。

军事理论

无人化武器推动战法创新

□ 张　翟　张小龙

俄罗斯媒体曝光了2015年底，叙利亚政府军在俄罗斯战斗机器人的支援下强攻伊斯兰极端势力据点的战斗，宣称这是世界上第一场以机器人为主的攻坚战。俄罗斯投入了4台履带式“平台”-M战斗机器人、2台轮式“阿尔戈”战斗机器人和至少一架无人机。这些机器人和无人机由俄军遥控指挥，与叙利亚军队配合作战，围攻拉塔基亚省一处由伊斯兰极端势力据守的754.5高地。

战斗打响后，无人机首先升空，将战场情况实时传送到俄军指挥系统。操作员操纵战斗机器人抵近武装分子据点100～120米，用机枪和反坦克导弹进行攻击，叙利亚政府军则在机器人后150～200米相对安全的距离上肃清武装分子。遇到坚固火力点时，己方阵地上的2S3式152毫米自行榴弹炮根据无人机和机器人传回的画面，实施精确炮击，彻底摧毁目标。战斗持续了20分钟，一边倒的猛烈打击令极端势力武装分子毫无还手之力，约70名武装分子被击毙，而参战的叙利亚政府军只有4人受伤，显示出战斗机器人的巨大优势。俄军总参谋长格拉西莫夫不久前表示，俄罗斯正在试图建立全自动化战斗系统，“我们将很快见证机器人军队独立进行战斗”！

战争面貌的刷新，不仅不以人的意志为转移，而且比我们想象的快得多。美国已将“捕食者”“全球鹰”“死神”等无人机，及“利剑”机器人等智能化无人装备投入阿富汗和伊拉克战场。截至2013年，美军已列装约8700架无人机和1.5万个机器人，无人系统成为美军行动不可或缺的重要力量。英、法、德、日、韩等国对智能化武器的关注和投入也呈加速上升态势。目前，70多个国家拥有军用机器人计划，4000种无人机在全球市场上销售。俄罗斯战斗机器人精彩的实战表现启示我们：科幻电影里的“终结者”军团正迅速走进现实。一线无人化作战已成为信息化战争新特点，其比例也在实战中不断上升。未来作战必须对无人作战平台高度重视，将其作为一种首选或必选的作战力量使用，同时列为指挥控制的重点要素。

技术决定战术。备战智能化战争首先要明确无人化作战需求，完善无人化装备体系。目前，我军各类无人作战系统仍主要遂行侦察监视、扫雷破障或电子干扰等保障性任务，直接作战能力有限，应瞄准世界无人武器发展潮流，加紧研发直接用于作战的无人攻击机、无人战斗机、无人潜艇等，同时注重发展“察打一体”“察扰一体”等多功能无人武器，力求形成大、中、小、微型，远、中、近程，太空、空中、地面、水面、水下，战略、战役、战术级衔接配套、系列化、标准化、模块化的无人化装备体系。在此基础上，积极组建无人化作战力量，创新无人化作战理论，组织无人化作战训练，加快无人化作战力量融入当前的联合作战体系，不断提高无人化作战能力。

除了运用无人化力量实施进攻迫在眉睫，还有无人武器的战斗防御问题同样不可忽视。特别是随着纳米技术的日臻成熟，各种微型机器人发展迅猛且成本骤降。未来对抗强敌铺天盖地蜂拥而至的机器人军团，擅长“点杀伤”的各类精确制导武器容易应接不暇且效费比太低，使用具有大规模毁伤效应的“面杀伤”武器可能是更好的选择。人工智能的快速发展，无人武器的大量使用，使战法创新进入了新的历史轮回，呈现出新技术推动下的螺旋式上升，对这一趋势必须充分认识、未雨绸缪。

军事战略