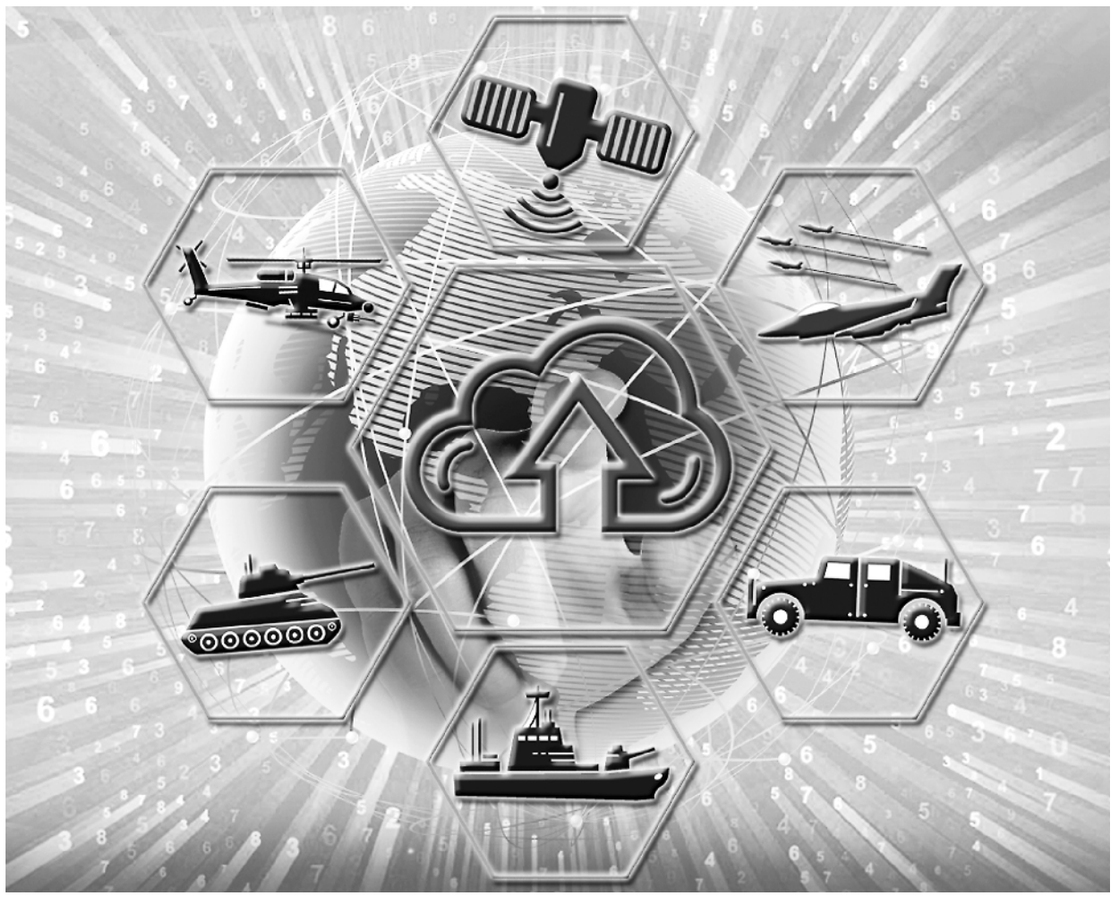
近年来，伴随大数据、“云计算”、物联网等信息技术快速发展，一种被称为“云作战”的全新作战样式应运而生，或将带来信息网络时代作战样式的革命性变化。所谓“云作战”，就是将日益成熟的“云计算”融入网络中心战思想，旨在通过高速、安全的网络连接实现各作战平台的实时交互，提升各军兵种之间的战术信息互联互通能力。未来的“云作战”平台，将最大限度地发挥隐身装备、精确打击武器、先进指挥控制系统和“有人—无人”系统的技术优势，成为制胜信息化战争的关键一招。

未来战争从“云端”打响

■章 敏 玥 凡

高技术前沿



“云端”漫步——未来战场的投资风向标

长期以来，美国国防部一直憧憬着打通战车、舰艇、飞机以及空间卫星数据共享的“任督二脉”。其耗费巨资研制的先进隐身战斗机，竟然不能直接与其他作战平台进行信息交换。即便同是美军，它们之间的“对话”也得需要“战场翻译”才能实现。

随着“云计算”和物联网技术的快速发展，行走在战场上空的“云”，为打破各类作战平台所面临的“信息孤岛”提供了新的技术思路。所谓“云作战”，就是基于“云端”的联合作战信息网络，核心是整合陆、海、空、天、电、网等多维度信息平台，从体系层面实现战场资源的动态高效管控和快速分布式处理。

为了能在未来战场的“云端”漫步，“云作战”早已成为各军事强国投资未来战场的“风向标”。早在2008年，嗅到信息网络技术“火药味”的美国空军就率先提出“在大气层、太空和计算机网络空间飞行与战斗”的全新作战理念。到2012年，美国空军进一步发轫出“作战云”的萌芽。通过整合指挥控制、情报监视和信息网络，快速交换传输来自各平台的信息资源，构建起以全球栅格化信息网络为基础、信息融合作战平台为载体的“云作战”网络平台。此后，“云作战”概念逐渐得到美国国防部的支持，并开始应用到美军作战设计和装备研制之中。

近年来，美军先后出台《网络中心服务策略》《美军联合信息环境》等一系列改革举措，逐渐形成了以云计算为核心的联合信息服务应用能力。在此基础上，美国空军基于“联合信息环境”进一步提出“战斗云”概念，意图通过战术通信网络快速交换作战单元的战场数据，实现信息资源的高度整合。

打通“经络”——建立高度融合作战体系

美国《航空周刊》曾发表过一份描述“空中优势空域云”的发展愿景。在这份“云作战”构想图中，卫星、空中预警机、战斗机、无人机以及远程轰炸机、海上航母战斗群等作战单元通过网络相互连接，在“作战云”的支撑下形成一个高度融合的作战体系。事实上，从早期主要为解决第五代战斗机与第四代战斗机的信息交换问题，到如今成为美军的新型作战理念，战场上空的“云”就是在为打通战场“经络”而穿针引线。

美国空军为实现在阿富汗作战的不同装备互联互通，曾紧急开发出战场机载通信节点载荷。波音公司专门为第五代战斗机和第四代战斗机“通话”而设计的飞行吊舱，能借助数据链把F-22战斗机飞行编队内部数据传送给美国空军的其他作战机群。未来的“云作战”绝不会仅仅把目光停留在机群通信上，势必会形成一个包罗战场万物的数据库。

“云作战”的本质其实在于融合。“云作战”是融合所有作战要素的一体化联合作战体系，通过“跨域协同”打破现有武器系统之间的“硬链接”，建立起一个集“探测—跟踪—决策—打击—评估”于一体的“云杀伤链”，使作战信息流与武器能量流高度融合。同时，“云作战”还将进一步革新战场作战样式，建立集中指挥、分布式控制和分散执行的“蜂群”式作战指挥结构，实现跨代际、跨平台协同作战。

“穿针引线”——激活武器装备作战潜能

作为迄今为止面向商业公司的最大一份军用信息技术类合同，美国国防部抛出的“企业-防务联合基础设施”项目将担负起为美军提供存储和派发任务数据、机密信息的职责。当然，美国国防部的终极目标是通过无形的“数据纤绳”把遍布全球的美军士兵和装备相连接，哪怕是身处地球上最偏远角落的士兵，都能从“云端”获取自己的任务和信息。

事实上，为了更好地决胜“云端”，美军早已开始在战场上对“云作战”进行实战检验。2014年9月，美国空军F-22战斗机首次率领联合空袭机群，对叙利亚境内的“伊斯兰国”极端组织实施空袭作战，标志着美国空军“云作战”实战检验的开端。美军另一款先进战机F-35更是“网络中心战”的概念产物。F-35战斗机能在无线电静默情况下与E-3预警机组成空战机群编队，在超视距对抗中实现“A机+B弹”的完美配合，事实上就是“云作战”的预演。

“云作战”将充分激活信息化装备的作战潜能，是令信息化装备拥有战场“跨代”优势的“保鲜剂”。以战机为例，“云作战”中每一架战机都能实现身份的快速转换，由传统的单一身份变成真正的战场“多面手”。同时，通过与先进战机联网，“云作战”也将使一大批老式战机焕发青春，甚至实现平台无人化和体系无形化，将整个空中作战力量体系“蒸发”进“云端”。

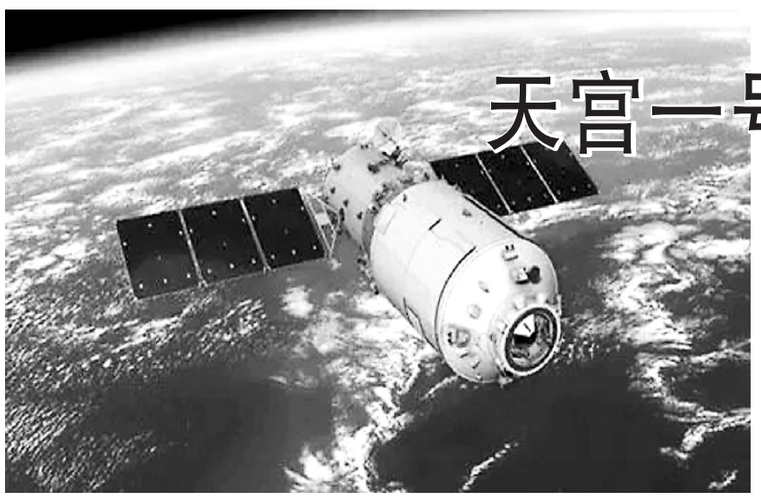
不仅仅是空军装备，美国海军目前正在实施“海军综合火控防空一体化”计划，旨在将舰艇和飞机联网。美国陆军还向着单兵“云作战”平台持续发力。正在研制的新型单兵移动云通信指挥系统，可进一步提升作战自动化和资源共享能力，实现单兵对战场态势的精确感知。

当然，“云作战”也并非“无懈可击”。以F-35战斗机的“战斗云”为例，也存在如何核实不同来源信息可靠性的特殊挑战。此外，在“云作战”环境下如何确保“云端”系统的安全、平台的深度融合和信息的高效提取，都是亟待解决的问题。

制 图：刘 程

天宫一号“回家”为何充满悬念

■翁利斌 张添翼



前段时间，我国第一个空间目标飞行器“天宫一号”在陆续完成既定科学任务后，最终落入被称为“航天器坟场”的南太平洋中部区域。在此之前，国内外许多航天科技工作者曾多次预测“天宫一号”陨落时间和地点，但大都与实际结果相差甚远。那么，究竟是什么力量使得“天宫一号”不断下降直至最后陨落？

我们知道，地球四周环绕着我们赖以生存的大气层，从低到高依次为对流层、平流层、臭氧层、中间层和热层等。由于重力和扩散等作用，大气密度随着高度的上升而迅速下降。我们通常所说的低轨道航天器一般运行在距离地面100—1000千米高度范围，该范围被称为热层区域。研究表明，距离地面200千米高度处的大气密度相当于地面的百亿分之一，400千米高度处仅为地面的千亿分之一。

千万不要小瞧这些不起眼的热层大气。由于低轨道航天器的运动速度一般在每秒7千米以上，加之长时间的累积，大气密度引起的阻力效应，正是低轨道航天器轨道高度逐渐降低的秘密所在。一般而言，距地面400千米处航天器轨道高度每天衰减大约几百米，200千米以下轨道高度每天减少量可达5千米以上。因此，热层大气密度对低轨道航天器轨道预报、姿态控制、空间对接、寿命设计及再入大气层等都有显著影响。

当然，热层大气密度并不是一成不变的，它与地面天气一样随季节和位置等因素变化，还受到太阳辐射和地磁场扰动的显著影响。例如，太阳活动活跃时，增强的紫外波段辐射能量可以使热层大气密度比太阳平静期间增加几十倍，可导致400千米处航天器轨道高度每天的衰减量从几百米增加到几千米。地球磁场扰动时，大量能量会注入到热层区域，大气密度在1至2小时内可增加一倍以上，进而对低轨道航天器的精密定轨和轨道预报产生极大影响。如2000年7月10日至15日，太阳爆发引起的地磁扰动造成国际空间站高度短期内下降了15千米，最终不得不主动变轨，以使其保持在预定轨道高度上。

正是由于热层大气密度自身存在复杂的时空变化，并且受到来自太阳和地磁活动的强烈影响，因此很难对其进行精确预报。大量研究表明，现有的热层大气密度预报误差一般在15%以上，并且这种预报误差会随着时间的推移而不断增大。这也解释了许多航天器的“回家之旅”为何充满了悬念。

论 见

夯实网络安全的「地基」

■李 杨 许妍敏

习主席在全国网络安全和信息化工作会议上对加强网络安全和信息化工作作出重要战略部署。俗话说，基础不牢，地动山摇。网络安全和信息化建设同样如此。2018年相继爆发的诸多与处理器芯片有关的安全事件，更为我们加强网络安全敲响了警钟。

当今世界，随着以互联网为代表的新技术、新应用不断推广，现实世界与信息技术的融合日益紧密。然而，“棱镜门”“黑屏门”等网络安全事件时刻警醒着我们，网络安全不容小觑。芯片、路由器、操作系统等网络关键设施如果受制于人，就如同在别人打好的地基上盖房子，修葺得再漂亮也不堪一击。实现国防信息系统与信息化装备的自主可控，是确保国家网络安全的“命门”。这就要求我们必须抓紧在网络关键设施领域掌握“话语权”，为网络建设夯实坚固的“地基”。

自主可控、安全可信是网络安全的基石和保障。可控就是实现信息与信息系统的安全监管，自主可控则需要我们全面掌握网络关键基础软硬件设施的核心技术，实现网络系统的自主研发、生产、升级与维护的全程可控。唯有这样，才能彻底打破网络关键基础软硬件“看他人脸色”的局面，有力保障国防信息化建设。

网络建设必须从“芯”出发。网络关键设施的核心器件就是处理器芯片，发展自主可控的处理器芯片是实现网络安全的重要前提。为网络关键设施装上“中国芯”，抓紧提升国产处理器性能，补足生态体系上的断层，逐步实现国产芯片和硬件设备的推广应用，才能确保网络基础设施的安全可靠。

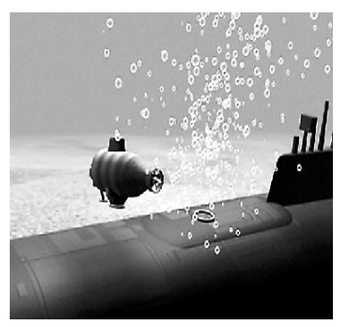
网络建设更要“软硬兼施”。如果把处理器芯片比作信息设备的“心”，操作系统就是它的“大脑”。除提升处理器芯片等硬件设施的安全应用水平外，操作系统无疑也是解决自主可控问题的关键要素。操作系统是管理计算机硬件与软件资源的程序，不仅是用户与计算机的接口，更是信息系统的内核与基石。如果操作系统存在“后门”或安全隐患，再坚固的“防火墙”也将形同虚设。据悉，俄罗斯军方和政府采购的电脑、手机等设备都将逐步抛弃微软、英特尔、谷歌等公司的产品，俄国防部还计划为所有的办公电脑都安装本土研发的Astra Linux操作系统。这启示我们，自主可控软硬件产品的推广应用，必须注重“软硬兼施”，着力提升国产网络关键设备的整体安全性。

网络建设也要留给自己“打补丁”的机会。实现网络关键设施自主可控是一个庞大的系统工程，不可能一蹴而就。一方面，处理器芯片等硬件设施设计制作复杂，操作系统等应用软件开发工作量大，不可能在短时间内完全达到西方发达国家几十年的发展水平。另一方面，由于计算机体系结构的固有特点，电子元器件和系统软件制作复杂，即便是在自主可控平台下研发，依旧存在各类不可避免的未知漏洞。加快网络关键基础设施研发，本身就是一个创新与提升的过程。我们要允许自主可控设备存在一些小瑕疵，留给国产设备厂商“打补丁”的机会，这样才能在不断试错中前进，推动网络基础设施建设快速健康发展。

新成果速递

双曲调频信号技术

为水下作战精准导航



前不久，韩国釜山大学研究人员开发出一种可实时精准定位无人潜航器的双曲调频信号技术。主要是通过结合双曲调频信号和具有高时间相关性的频分多址技术，将来自锚节点的多个信号传输到同一接收机，再用一组滤波器进行分离。这样，多个锚节点能够在不冲突的情况下同时向无人潜航器传输数据，进而消除介质访问控制延迟，提高定位精度。（郭淑军）

新型水下潜艇

可变身人形机器人

据英国《每日邮报》报道，美国军方资助的一家公司近日研发出“可变形”水下潜艇，可在潜艇与人形机器人模式间自由转换。这种新型潜艇被誉为“多功能水下机器人”，可在“潜艇”模式下潜行数百英里，亦可“变形”为能进行精准操作的机器人。它摆脱了对母舰和操作人员的需要，同时又具有强大的态势感知和维修水下作战平台任务的能力。（李 超、谭文伟）