乱局接“盘”，空降老兵力稳军心

——记乌克兰新任代理国防部长米哈伊尔·科瓦利上将

时值乌克兰处于“风暴中心”之际，3月25日，乌克兰代理国防部长伊格尔·捷纽赫向议会递交辞呈，把职位交给58岁的米哈伊尔·科瓦利上将。捷纽赫称这一调整对于保持“最低限度国防力量”至关重要。

对于科瓦利上台，乌克兰议员布雷基涅茨说得更为直白，此前因乌克兰拥有克里米亚半岛，由海军出身的捷纽赫任防长有利于掌控黑海方向的“话语权”。现在随着克里米亚加入俄联邦，缺少海岸线的乌克兰已不太需要海军，由陆军名将科瓦利任防长更合适。

空降部队初露峥嵘

翻开科瓦利的履历，“冒险”和“担当”是主要的关键词，他敢于从事充满危险的军事训练科目，也习惯在矛盾的风口浪尖承担责任。

1979年，科瓦利毕业于前苏联卡缅涅茨-波多利斯基高等军事指挥学院，之后长期留校任教。不过，喜欢冒险的他多次请求前往充满挑战性的王牌部队，甚至表示愿意去阿富汗前线的第40集团军，这在当时受到享乐主义腐蚀的苏联军队中难得一见。上世纪80年代中期，科瓦利如愿进入有“蓝贝雷”之称的空降兵部队，在驻扎于基辅军区的第98空降师担任中级指挥员。

众所周知，冷战期间规模居世界第一的苏联空降兵是克里姆林宫手中仅次于核武器的战略王牌，其中又以第76、98、103和106等4个师的战斗力最强，可以在下达命令后的48小时内抵达千里之外作战。

据一位曾与科瓦利共事的老空降兵回忆，科瓦利善于组织和谋划多兵种合成的空降突击演习，特别对人员与装备车辆同区域投送演习尤其在行。有一次，科瓦利参加第98空降师所属加强营的紧急演练，搭乘伊尔-76运输机前往陌生地域。可是飞机升空后，大家才得知真正的降落地是顿河深处某机场，而那里也只是中转基地，最终目标是夺取一处“蓝军”武器仓库。当时目标地域气象条件恶劣，地面风速达到12米/秒（执行空降任务时通常要求地面风速不超过10米/秒），但科瓦利与诸多战友坚持在恶劣气象条件下跳伞，并在之后的战斗中快速进攻，打得假想敌无力招架。

也许是得益于在空降兵部队的优异表现，科瓦利被保送到莫斯科伏龙芝军事学院深造。1990年，科瓦利从伏龙芝毕业后转入普斯科夫的空降兵训练中心。然而，正当他想要大展拳脚之际，苏联解体，苏军官兵都不得不选择新的效忠对象。科瓦利决定加入乌克兰国防军。

曾经“智取”俄军设施

1997年他在乌克兰国防部的军事进修班完成培训，全盘接受美国和北约的军事理论考核，这也是当年乌克兰外交上“全盘西化”的体现，目的是体现乌克兰在军事上全面与西方国家合作的“政治诚意”。

1997年至1999年，科瓦利担任乌克兰北方军区司令。1999年至2001年，他转任拥有最强部队的西方军区司令。2001年至2002年，科瓦利出任内务部队第一副司令。

之后直到2013年，他担任边防部队第一副司令。在此期间，科瓦利最著名的“军事行动”莫过于2008年“奇袭”驻克里米亚的俄黑海舰队岸上设施。当时，围绕黑海舰队驻军地位问题，乌克兰总统尤先科与俄罗斯总统梅德韦杰夫之间的矛盾激化。科瓦利受命对克里米亚的俄军设施采取“断然行动”。鉴于俄黑海舰队在克里米亚拥有雄厚实力，并得到当地居民的支持，科瓦利决定用“智取”代替“强攻”。2008年3月17日，一批化装成游客的乌克兰强力部门成员夺取了俄黑海舰队位于格尼切斯克市的“火星-75”号导航站和水文站大楼，随即将其转归乌克兰交通运输部所有。这也是乌克兰政府首次成功没收俄国防部管辖的军事设施。

然而，科瓦尔再有本事，在如今克里米亚公投加入俄联邦、亲俄自卫队完全控制当地形势的背景下，要想重演昔日“奇袭”的成功，实在是“不可能完成的任务”。

陆军名将强硬亲美

俄政治分析师谢尔盖·马尔科夫向俄《观点报》表示，“科瓦利是前总理季莫申科的人，是乌克兰主要的亲美人物之一。更重要的是，科瓦利长年在乌克兰边防部队工作，这股力量长期受美国情报部门的影响，而科瓦利对此持宽容甚至支持的态度”。基辅议会任命科瓦利担任代理防长，势必进一步加强乌克兰的亲美集团力量。

马尔科夫甚至担心，由于具有强硬的反俄背景，科瓦利有可能挑起与俄罗斯的冲突。他表示“科瓦利有丰富的边防勤务经验，擅长地面作战，他是能让半岛形势陷入危险的人，因为他可以利用美国提供的资金，在美国和波兰情报机关的帮助下培训破坏分子，在克里米亚从事破坏活动”。美国众议院情报委员会主席罗杰斯公开扬言，针对俄罗斯的“扩张威胁”，美国应该考虑为乌克兰提供“医疗、无线电设备或其他防卫性武器系统”，以便“让乌克兰自己保卫自己”。马尔科夫强调，虽然乌亲美力量无法战胜俄罗斯，但可能引发更多流血事件。

俄战略局势中心主任科诺瓦洛夫指出，科瓦利和基辅领导人已流露出邀请美国和北约在其境内部署反导系统的打算，以期逼迫俄罗斯让步，不过这一设想并不现实，首先乌克兰形势尚不稳定，美国和北约都清楚基辅政府的能力脆弱；其次，很多欧洲人反对接纳乌克兰加入欧盟，把它看作是需要投入大量金钱的萧条地区，是“不必要的添头”。

对于科瓦利乃至基辅决策层期待西方军援的问题，科诺瓦洛夫认为，北约不会为了乌克兰而与俄罗斯严重对抗，许多北约国家也不希望看到乌克兰加入北约，因为此举只对美国有利，却会让欧洲充满火药味。乌克兰只是可利用的“棋子”，一些国家可能会投入少量资源，然后期待获取一些利益。 雷炎

军事人物

环球军情

乌将停止与俄军事合作 两国都将承受严重损失

乌克兰第一副总理亚列马4月4日在基辅表示，乌克兰已决定停止与俄罗斯的军事合作。此前，乌克兰国有大型军工联合企业——乌克兰国防工业公司已于3月29日停止向俄罗斯出口武器和军事装备。亚列马称：“为俄罗斯生产今后用来对付我们的产品是彻底丧失理智的行为。”他同时表示，两国在军工领域有着长期合作，骤然停止这种合作会给乌克兰经济造成严重损失。据乌克兰专家估计，停止对俄军事合作后，乌克兰国防工业一年的损失约为6亿美元，俄方的损失约为20亿美元。

美国陆军精简装甲部队 大量坦克进入贮备仓库

据战略之页网站报道，虽然美国陆军仍拥有7000辆M1主战坦克，但真正服役的只有不到20%，具体来说是1288辆M1坦克分为92个连，每个连有14辆。与此同时，美国陆军仍在继续削减规模，从16个装甲旅（64个坦克连）减少到10个（40个坦克连），国民警卫队则仍设有7个装甲旅（28个坦克连），使得最终服役的主战坦克数量降到952辆。按每辆坦克需要4人计算，美军的坦克兵人总数为3808人。据悉，过去10年里，许多美军坦克兵被作为步兵使用，或操作防地雷反伏击车。

韩军成功试射新型导弹 计划明年投入实战部署

韩国国防部4月4日表示，该国已成功测试射程为500千米的新型弹道导弹，并将尝试研制射程800千米的弹道导弹。据介绍，这种射程500千米的弹道导弹可搭载1吨重的弹头，计划在明年投入实战部署。根据2012年10月修改的韩美导弹协议，韩国可拥有的弹道导弹的射程从300千米延长至800千米，因此，韩国军方正在研发射程为800千米、弹头重500千克的弹道导弹。韩国国防部发言人表示，一旦新型弹道导弹研制成功，就可从韩国的任何地方打击朝鲜境内的所有军事设施。

周边军情

日本建“网络防卫队”发展进攻能力

3月26日，日本自卫队的网络战专门部队——“网络防卫队”正式成立。该部队初期编制90人，隶属内阁防卫省，是防卫大臣的直属部队，由统合幕僚长负责指挥。其主要任务是每天24小时监视防卫省和自卫队的网络，应对网络攻击，同时负责收集、分析、调研网络攻击和威胁相关情报。据分析，与过去组建的日本自卫队网络战力量相比，新成立的网战部队不仅加强了“进攻”能力，也扩大了“防御”范围。

新网军突出进攻能力

据日本媒体报道，此前，自卫队负责应对网络攻击的部队是自卫队陆海空联合部队“指挥通信系统队”（约150人）。其中负责防御自卫队指挥通信系统的“网络运用队”仅有数十人。此次新成立的网络防卫队则是由来自陆上、海上和航空自卫队的人员组成的联合部队，集网络信息安全情报收集共享、网络防护、网络安全训练、调查研究与技术支持于一体。为提升该部队能力，日本已派出自卫队员赴美学习网络战课程，加强与美情报交换。未来，还将与美国网络战部队举行联合训练，并共同研究网络攻击手段。

有军事专家指出，日本近年来通过筹组网络防卫力量、研发网络攻击系统等手段，加快推进自卫队的网络攻防实战部署。过去，日本自卫队网络战部队主要用于保障自卫队内部网络安全，防御外来网络攻击。但此次成立的新部队不仅可应对网络攻击，本身也将具备进行网络攻击的能力，其武器不仅包括“过去曾攻击日本的电脑病毒”，还将包括今后研发的专用木马程序和电脑病毒。由此可见，新成立网络战部队的最大特点就是具备进攻能力。

谋立法为“网战”铺路

日本自卫队网络战的指导思想是通过掌握“制网权”达到瘫痪敌人作战系统的目的。为配合网络防卫队成立，日本政府还计划加快相关立法，为“未来网战”铺平道路。由于日本现行宪法等法律对于自卫队的对外攻击仍存在一定限制，所以日本防卫省准备“立新法破旧法”，具体方法就是通过立法将来自其他国家的网络攻击视为“武力攻击”，然后启动所谓的“自卫权”。

有分析人士指出，根据日本现行应对“武力攻击”的法律规定，日本防卫省可能将满足以下3个条件的网络攻击视为“武力攻击”：第一、外界攻击手段是计算机病毒和非法网络入侵；第二、重要基础设施和生活设施遭到大规模损害；第三、攻击威胁到国民的生命和财产安全。一旦这样的立法得以通过，未来日本自卫队以遭到某方网络攻击为由启动“自卫权”的门槛并不高。

打造政、军、商联动网络

事实上，日本政府除了在自卫队中大力推进网络战部队的建设，还在政府机构和民用基础设施领域加强网络安全建设，试图打造一个政府、军事部门、民营商业机构联动的网络安全体系。

从2010年到2013年的4年间，日本政府各部门实施了数百条与信息安全相关的政策。从2006年起，日本总务省连续多年组织电信运营商和政府部门共同举行“应对电信领域网络攻击的演习”，并请美国的网络安全权威专家前来指导。演习假定网络受到多种网络攻击，政府部门和电信经营者联合拿出应对措施，并展开协同合作。演习中出现的各种经验和教训也被总结成文，发放到相关部门。

去年5月21日，日本“网络安全战略”最终草案终于出炉。草案提出多项强化措施，其中包括在自卫队中设置“网络安全卫队”，以及在2015年组建“政府网络安全中心”。草案还提出，2015年前对政府机构和重要基础设施（如核电站、煤气公司、铁道公司等）的网络安全信息进行整合，实现网络攻击信息共享；2020年底前，将目前规模不到7000亿日元的国内网络安全市场扩大一倍。此外，日本还将加强与其他国家开展网络安全合作，在现有80多个国家的基础上增加3成。

今后，日本在网络战领域可能的发展趋势是：在加强进攻的同时，将政府机构、军工企业、先进技术企业等政治、经济主体纳入网络战的防护体系之中。 李大光