积极防范网络安全问题

●莫果夫　林　欣

目前，不少部队都在营区接入互联网，在极大丰富基层思想政治教育的同时，也给网络信息安全带来隐患。由于官兵对互联网缺乏深入的了解和应有的警惕，容易造成网络失泄密问题，应注重抓好防范。

一、强化主动防范意识。保密教育是做好网络信息安全工作的基础和前提。要坚持把网络安全教育纳入经常性思想教育之中，重点解决好网络安全“与己无关”、基层单位“无密可保”、落实安全管理规定“心存侥幸”等错误认识问题，扎实抓好保密法规教育、保密常识教育和形势政策教育，努力营造“人人学、人人讲、人人抓、人人防”的群防群治氛围。在教育内容上，要结合网络安全保密工作的新形势、新情况、新问题和新要求，注重引用和剖析近年来发生在军内外网络失泄密的典型案例，运用多媒体手段，充实改进内容，贴近教育对象，增强教育说服力；在教育方法上，围绕落实保密规定、典型案例分析，开展讨论交流，进行警示教育，也可组织官兵到地方安全部门、网络公司等地参观见学，聘请网络信息方面的专家做专题讲座或现场模拟演示和指导；在教育形式上，可组织知识竞赛、观看录像、举办演讲或讲座等，还可充分利用局域网、板报、小广播等媒介进行宣传教育，增强教育的趣味性和实效性。通过教育，不断增强广大官兵信息安全保密的责任感、紧迫感和强烈的保密意识，使官兵被动的防范意识变为积极的防范行为，从而确保各项法规制度的落实，有效防范失泄密问题发生。

二、健全安全运行机制。充分发挥网络保密领导小组和专业骨干作用，建立健全网络安全运行机制。要建立日常运行管理机制，对官兵登陆互联网的时间、登陆的方式、浏览的网页、使用的网名等作出明确，登陆前有登记，下线后有审查，尤其要严禁官兵在网上发表涉军言论、聊及涉密信息，防止发生问题。要建立应急处理机制，针对网络攻击、病毒入侵、网上窃密等可能出现的突发情况，制订应急处理预案，明确处置力量、原则、方法、责任和分工，使情况报告、检测评估、危害控制与恢复等各环节运转顺畅，特别是要采取技术措施防范涉密计算机接入互联网，做到及时发现、及时跟踪、有效阻止。要建立齐抓共管机制，按照责任分工，不仅要建立支部和主官为主导、专业技术骨干与思想骨干相结合的保密工作网络，而且要形成上下衔接、左右协调、关系顺畅、齐抓共管的运行机制，确保工作有条不紊地展开。

三、建强专业骨干队伍。信息安全保密是一门综合性学科，涉及学科领域众多，需要一支懂技术、会管理、政治思想好、作风纪律强的高素质专业人才队伍。当前，基层专业人才紧缺是制约信息安全保密工作发展的“瓶颈”，因此，要加大培训力度，培养一支数量充足、架构稳定的专业骨干队伍。要选准苗子搞好培养，按照能谋划、会管理、懂技术的标准，调整充实网络管理人才队伍，逐步形成以老带新、新老接替的局面，防止出现“青黄不接”的现象。要拓宽人才培养渠道，注重发挥上级组织网管员培训的主渠道作用，以驻地院校、科研单位为依托，优选送学培训，还要采取专题集训、以会代训等形式，有针对性地组织网络管理人员进行业务和技能培训。要优化成才、用人环境，高度重视网络管理人才的使用、保留与储备，特别要针对编制调整的实际，制定网络信息管理人才成长计划和培养办法，对优秀网络管理员在送学和选改、晋升时要给予优先考虑，创造有利于人才生长和稳定的良好环境，为基层网络安全保密工作提供强大的发展后劲。

四、充分运用前沿技术。信息化条件下信息安全保密工作的技术含量明显增加，因此，技术的支撑与相应的设备、设施的支持是做好信息安全保密工作的关键所在。要建立健全网络安全技术管理平台，主要加强网络信息资源管理、入网资格鉴别管理、访问控制管理、运行监管，努力做到“没有密码进不去、规定以外登不上、发生涉密走不脱、外部人员窃不了”。要引入使用信息安全保密产品，尤其是驻城区部队营区周围环境复杂，要配备计算机屏蔽桌、加装信号干扰仪等，防止营区内声、光信息被窃取。要警惕技术设备引进中的信息安全风险，在配置带摄像头的显示器、扫描仪和碎纸机等自动化设备时，要把好采购关，优先使用国内自行研制或经过国家有关部门批准的产品，防止敌对势力将窃密系统嵌入、带入军营引发问题。

【作者系武警广东总队二支队后勤处处长、广东科技学院讲师】