不忘初心　牢记使命
以党的十九大精神领航新时代保密事业新发展

□本刊评论员

在全面建成小康社会决胜阶段、中国特色社会主义进入新时代的关键时期，中国共产党召开第十九次全国代表大会，庄严宣告中国特色社会主义进入新时代，系统阐明新时代中国特色社会主义思想和基本方略，开启了全面建设社会主义现代化国家的新征程。学习宣传贯彻党的十九大精神是全党全国当前和今后一个时期的首要政治任务。保密战线全体同志要认真学习、深刻领会、全面贯彻党的十九大精神，不忘初心、牢记使命，切实用党的十九大精神作为行动指南，指导实践，引领推动新时代保密事业新发展。

以党的十九大精神领航新时代保密事业新发展，就要深入学习领会，坚持用习近平新时代中国特色社会主义思想武装头脑。党的十九大围绕坚持和发展中国特色社会主义、进而实现社会主义现代化和中华民族伟大复兴，鲜明提出习近平新时代中国特色社会主义思想，这是党的重大理论创新成果，是指导党和国家事业发展的强大思想武器，具有重大的政治意义、历史意义、理论意义、实践意义。全国保密系统要全面学习贯彻党的十九大精神，深入学习、深刻领会习近平新时代中国特色社会主义思想的时代背景、历史地位、精神实质和实践要求，深入领会贯穿其中的坚定信仰、人民立场和历史担当，切实提高政治素养和思想理论水平，强化理论武装。要通过专题辅导、集中宣讲、交流研讨等形式全面开展学习活动，把思想和行动统一到党的十九大精神上来，把智慧和力量凝聚到落实党的十九大提出的各项任务上来。要准确把握党的十九大对党和国家事业的总体设计和战略部署，把学习贯彻党的十九大精神同贯彻落实中央关于保密工作的决策部署结合起来，创造性地开展本地区本部门保密工作。要坚持原原本本学、深入系统学、突出重点学，采取理论和实践、历史和现实、当前和未来相结合的方法，进一步提高学习的针对性和实效性，把党的十九大精神变为坚定信念、奋发进取的强大动力，变为武装头脑、推动工作的行动指南。

以党的十九大精神领航新时代保密事业新发展，就要认清使命担当，牢牢把握新时代安全保密工作面临的新形势新特点。党的十八大以来，党和国家各项事业发展取得历史性成就，保密事业也取得了一系列重要进步，特别是在打造新时期党和国家秘密安全坚固防线、实现党中央提出的转型升级目标上迈出了新步伐。五年来党和国家的历史性成就和历史性变革推动中国特色社会主义进入新时代，这是党的十九大审时度势作出的重大战略判断。进入新时代，国际安全形势依然严峻，国内安全环境复杂多变，保密事业面临许多新课题新挑战，保密战线必须承担起新的时代使命。全国保密系统要坚持总体国家安全观这一基本方略，牢牢把握新时代窃密与反窃密斗争的新形势新特点，在安全形势的动态变化中抓住规律，在对传统安全威胁和非传统安全威胁的分析中找到共性，在开放多元与安全保密之间构建支点，有效应对信息化网络化发展带来的挑战，以高度的行动自觉和强烈的使命担当，坚决维护我国家安全和发展利益，切实筑牢党和国家秘密安全防线。

以党的十九大精神领航新时代保密事业新发展，就要锻造过硬本领，为夺取新时代中国特色社会主义伟大胜利不懈奋斗。新时代提出新要求，新征程赋予新使命。保密工作始终是一项基础性、全局性、长期性工作，与维护国家安全和利益息息相关。随着形势和任务的变化，保密管理越来越渗入拓展到各行业领域的各项工作中，影响范围不断扩大、关联程度不断加深、保障需求不断凸显。实现十九大提出的决胜全面建成小康社会、开启全面建设社会主义现代化国家

砥砺奋进的5年

看齐跟上 服务大局 打造新时代党和国家秘密安全坚固防线

——党的十八大以来保密工作创新实践

□本刊记者 李 杰

保密战线历来是必争、必守、必保之重地。

保密工作是一项基础性、长期性、全局性工作，须臾不可放松。

党的十八大以来，以习近平同志为核心的党中央站在党和国家事业发展全局的高度，系统规划和全面推动保密工作科学发展，为做好新时代的保密工作指明了方向。

思深方益远，谋定而后动。全国保密系统认真学习贯彻习近平总书记系列重要讲话，特别是对保密工作的重要批示指示精神，全面深入贯彻落实中央关于加强保密工作的决策部署，牢固树立“四个意识”，看齐跟上、积极作为，围绕中心、服务大局，努力打造新时代党和国家秘密安全坚固防线，不断推进保密事业创新发展。

党管保密 顶层设计

沧海横流，首在掌舵。党对保密工作的领导是我国保密管理工作的本质特征，也是做好保密工作的最大政治优势。党的十八大以来，习近平总书记高度重视保密工作，多次就加强和改进保密工作作出重要指示批示，提出明确要求。

2016年，以习近平同志为核心的党中央根据新时代保密工作面临的复杂严峻形势和发展需要，作出了关于加强保密工作的决策部署。习近平总书记再次发表重要讲话，提出确保国家秘密安全的治理方略，为做好新时代的保密工作提供了根本遵循。2016年10月，党的十八届六中全会通过了《关于新形势下党内政治生活的若干准则》，新征程的目标任务，保密工作必须充分发挥好服务保障作用。全国保密系统要强化政治担当，练就过硬本领，确保更好履行保密管理各项职能。**要增强政治领导本领。**党政军民学，东西南北中，党是领导一切的。要始终不渝地坚持党对保密工作的统一领导，充分发挥党管保密的政治优势和组织优势，发挥各级党委（党组）及其保密委员会总揽全局、统筹谋划、协调各方的作用。**要增强科技创新本领。**坚持创新驱动发展原则，不断加强保密体制机制和方法手段创新，充分发挥科技在保密工作中的基础支撑和引领作用，提高保密管理创新发展能力。**要增强依法治密本领。**贯彻全面依法治国基本方略，不断健全覆盖保密管理全过程的保密法规制度体系，提高运用法治思维和法治手段治理国家秘密的能力，推动保密工作在法治轨道上实现专业化、规范化、科学化发展。**要增强风险防范本领。**完善安全保密风险防控机制，坚持技术防护和保密管理并重，建立人防物防技防“三位一体”的综合防范体系，不断提高发现和消除泄密风险隐患的综合防范能力。

走进新时代，踏上新征程。要把保密工作的宏伟蓝图化为行动，把转型升级的目标任务变成现实，离不开稳扎稳打、真抓实干。全国保密系统要迅速掀起学习宣传贯彻落实党的十九大精神的热潮，坚持用习近平新时代中国特色社会主义思想统一思想和行动，以时不我待、只争朝夕的精神，在奋力走好新时代的长征路上，为夺取新时代中国特色社会主义伟大胜利不断做出新贡献。

把“不准泄露党和国家秘密”明确为“政治纪律”的重要内容。

中央保密委员会在以习近平同志为核心的党中央坚强领导下，在栗战书同志的直接指挥下，带头贯彻落实习近平总书记重要批示指示要求和中央决策部署，把新时代的保密工作作为保障国家安全，特别是政治安全的大事来抓，紧紧围绕统筹推进“五位一体”总体布局和协调推进“四个全面”战略布局，从党管保密、依法治密、创新驱动、综合防范等方面科学谋划，系统设计国家保密体系建设。

5年来，一个个直击问题关键、着眼国家保密体系建设的具体部署相继出台，其中既有阶段性的工作部署，如“十三五”全国保密事业发展规划以及每年的工作要点；又有针对突出问题的制度规定，如党政领导干部保密工作责任制规定、党政机关和涉密单位网络保密管理规定等；还有一些重要领域的统筹安排，如“十三五”保密科技工作实施意见等。这些部署充分发挥了党管保密的政治优势，有力推动了国家保密体系建设，为加快保密工作转型升级奠定了重要的制度基础。

一分部署，九分落实。5年来，全国保密系统一方面认真组织学习习近平总书记系列重要讲话精神，特别是仔细领会关于保密工作的重要指示批示精神，并转化为一系列具体举措；另一方面，按照“三个看齐”的要求，在中央保密委员会的带领下，积极协调，强力督导，着力推动全党全国各有关方面，把习近平总书记的指示精神和中央决策部署转变为实际行动，落地生根。

——学深悟透抓落实。抓好贯彻落实，学深悟透、准确把握中央精神是前提。2016年1月，中央作出关于加强保密工作的决策部署。2月，中央保密委员会召开全体会议，栗战书同志带领大家深入系统地传达学习，并对各地区各部门学习贯彻工作作出全面部署。国家保密局组织召开全国保密工作会议进行认真传达学习。6月，全国保密工作高级研修班在北京举办，对学习贯彻工作进行再培训、再动员、再部署、再督促。下半年，国家保密局负责同志分别带队，赴部分地区和部门开展中央决策部署宣讲和解读。各地区、各部门一级抓一级，层层开展学习贯彻，为抓好贯彻落实工作奠定了坚实的思想基础。

5年来，全国保密系统一方面认真组织学习习近平总书记关于保密工作的重要指示批示精神，并转化为一系列具体举措；另一方面，按照“三个看齐”的要求，在中央保密委员会的带领下，积极协调，强力督导，着力推动全党全国各有关方面，把习近平总书记的指示精神和中央决策部署转变为实际行动，落地生根。

——协调攻坚抓落实。抓好贯彻落实，各有关方面的大力支持与积极配合至关重要。为确保中央决策部署的全面落地，中央保密办与有关部门反复沟通协调，多次征求意见，制定印发重要政策措施分工方案，明确了牵头单位、参加单位和工作要求，强化责任主体，充分调动各方面的积极性。为确保中央决策部署关于加强机构队伍建设要求的精准落实，中央保密办加大统筹工作力度，在起草过程中，多次与中央组织部、中央编办、人力资源社会保障部等部门沟通协调，达成一致认识；在落实过程中，联合中央编办召开专题座谈会，就有关机构队伍建设问题进行政策解读，收到很好效果。为确保中央决策部署有关重大项目的精准落实，中央保密办积极与有关部门沟通联系，采取总体设计、任务分解、“各人各框”的办法，整合成果，形成系统性解决方案。

——督导检查抓落实。督导检查是检验落实效果的重要方法，也是推动工作的重要抓手。在贯彻落实过程中，中央保密办从督任务、督进度、督成效入手，逐条对照习近平总书记的指示和中央决策部署要求，逐项检查责任落地、措施到位情况。针对贯彻落实中出现的新情况新问题，中央保密办及时成立督导工作领导小组，建立分片督导工作机制，督促各地区各部门制定出台贯彻落实具体方案措施。2016年，由中央保密办领导带队，分赴部分地区和部门开展现场督导，并以书面形式反馈督导意见。2017年，根据中央保密委员会工作安排，中央保密办协同中办、国办督查室，会同有关部门组成联合督查组，对部分地区和部门进行实地督查，着眼发现问题，注重解决问题，以实际行动维护核心和党中央权威。

看齐跟上　成效显著

好风凭借力，扬帆正当时。5年来，在以习近平同志为核心的党中央的高度重视和坚强领导下，全国保密战线的同志们把千钧重担化作砥砺前行的动力，各项工作取得了显著成效。

夯实政策法规基础，保密依法

管理水平逐步提升。依法治密是实现现代保密工作科学发展、提高保密管理规范化水平的基本途径。5年来，保密战线着力加强依法治密，保密法治建设取得重大进展。保密立法和制度建设更加健全，先后制定出台保密法实施条例、定密管理暂行规定以及保密事项范围制定、修订和使用办法等一批重要法规规章；清理修订涉密信息系统集成资质管理办法等几十个规范性文件；制定修订保密标准，形成比较系统完整的保密技术标准体系；地方和部门保密建章立制力度加大，保密工作总体上实现了有法可依、有规可循。保密行政管理更加规范，印发全面推进保密工作依法行政的意见，明确推进保密工作依法行政的重要意义、总体要求、主要任务和保障措施；建立健全保密行政管理权责清单制度，推进管理职能转变和管理方式创新，开展省级保密部门权责清单编制工作。保密行政执法更加严格，开展保密行政执法人员持证上岗和资格管理制度调研，完善执法程序，规范执法行为；广泛开展保密行政执法培训，加强对保密执法人员的规范管理；一些地区将涉密资质审查审批和保密检查纳入保密依法行政范围，梳理保密行政执法主体、执法依据、执法职权等行政执法事项。

加大指导管理力度，保密管理能力和水平不断提高。推进保密工作科学发展，需要正视问题的勇气，更需要闯关夺隘的魄力。从2014年起，中央保密委员会持续将制约保密工作科学发展的定密管理、涉密人员管理、网络保密管理的突出问题作为重点，迎难而上，持续攻坚，保密管理水平得到全面提升。在定密管理方面，完成部分保密事项范围的制定修订，为规范行业、领域定密工作提供规范依据，规范定密责任人、定密授权、密级标志等定密事项管理。在涉密人员管理方面，会同中央组织部等7部门共同印发加强涉密人员管理意见，会同人力资源社会保障部等开展涉密人员权益保障办法调研，构建涉密人员管理基本制度，在全国组织开展涉密人员分类确定和保密审查工作。在网络保密管理方面，不断加强涉密网络测评，确保全国在用的涉密网络全部达到分级保护标准要求。针对涉密资质审批制度不健全、不规范问题，经国务院审改办批准，明确涉密信息系统集成、国家秘密载体印制、军工保密资格等3项行政许可事项，完成军工保密资格认定体制调整。同时，不断完善保密督导协作机制，对机关单位开展分类指导，对军工企业保密工作加强指导。

5年来，全国保密战线的同志们把千钧重担化作砥砺前行的动力，各项工作取得了显著成效：夯实政策法规基础，保密依法管理水平逐步提升；加大指导管理力度，保密管理能力和水平不断提高；丰富教育培训方式，保密意识和保密常识显著增强；强化创新驱动，保密科技支撑能力显著提升；强化检查查处能力，打击窃密泄密和追责警示作用突出。

丰富教育培训方式，保密意识和保密常识显著增强。保密工作最大的隐患是没有保密意识和保密常识。5年来，全国保密系统把保密教育作为保密工作的重要内容，采取各种方式常抓不懈，保密思想防线日益牢固。积极开展领导干部和涉密人员全员保密轮训，建设中央和国家机关保密教育实训平台，加大在京领导干部、涉密人员、关键岗位工作人员等保密轮训力度；指导各省（区、市）因地制宜建设保密教育实训平台，对当地的领导干部和涉密人员进行保密轮训。积极推进干部保密教育培训经常化、制度化、规范化，会同中央组织部等部门联合印发通知，将保密教育纳入党校、行政学院、干部学院教育规划内容，充分发挥各级党校、行政学院、干部学院的主渠道、主阵地作用；组织开展保密委主任讲党课活动，2014年全国510万余名党员领导干部和涉密人员接受保密专题教育。丰富保密宣传教育素材，编写保密理想信念教育读本《红色往事：镌刻在党旗上的保密故事》，制作大型保密文献纪录片《胜利之盾》和系列保密警示教育片，充分发挥案例警示教育作用。

强化创新驱动，保密科技支撑能力显著提升。5年来，保密战线坚持在创新驱动发展战略指引下，大力推进保密科技创新，加强保密科技研发和创新基础能力建设，着力推进保密科技体制机制改革，不断提升网络信息系统安全保密技术防护能力，交出了一份不平凡的成绩单：调整加强中央和国家机关保密技术服务中心、国家保密科技测评中心的职能与队伍结构，在涉密网络保密管理和重大会议活动服务保障方面发挥重要作用；设立保密科研项目，项目成果转化率达79%；积极推动建设国家信息安全保密技术创新产业联盟，设立保密科技奖，成功举办全国保密技术交流暨产品博览会；积极推进党政机关、涉密单位计算机保密技术防护专用

系统配备，完成机关单位网站保密检查平台、违规外联集中监控平台等平台建设，保密技术监管数据获取能力和失泄密线索发现能力显著增强。

强化检查查处能力，打击窃密泄密和追责警示作用突出。检查查处是推动保密工作责任制落实的有力抓手，也是打击窃密泄密行为的重要手段。5年来，保密战线不断创新监督检查方式，重拳频出，严格追责，成效显著。为推动保密检查长效机制建设，保密部门探索建立机关单位自查自评工作机制，制定印发自查自评工作规则，编写自查自评指导手册，在全国部署开展自查自评工作；2016年组织开展自查自评全覆盖督查，推动自查自评工作常态化、规范化，并指导各地区开展督查。在此基础上，探索“进驻式”保密检查、网络保密监督检查等多种方式，提高窃密泄密线索发现能力。同时，加大窃密泄密案件查处力度，查处了一批大案要案，不但查清了案情，严肃处理了涉案人和责任人，而且从多方面消除相关风险隐患，用作典型案例教育了更多的领导干部和涉密人员。

政治引领　集聚力量

人才蔚，事业兴。做好保密工作，必须把人才队伍建设放在重要位置，只有建设一支思想政治素质和业务能力水平都过硬、又红又专的人才队伍，保密工作才能得到持续健康发展。

5年来，保密战线始终坚持党的领导，把党管保密作为保密工作的根本，把维护习近平总书记的核心地位作为最大的政治，把抓好党建作为最大的政绩，始终不渝抓好思想政治建设和专业能力建设，为各项工作顺利推进奠定了坚实基础和可靠保障。

——坚持党管保密，充分发挥各级党委（党组）及其保密委员会的重要作用。各级党委（党组）不断加强党对保密工作的领导，自觉将保密工作纳入重要议事日程，定期听取保密工作汇报，支持保密部门依法履行职责。各级保密委员会不断提升科学谋划和统筹协调能力，靠前指挥，集聚力量，形成合力。同时，各地区各部门不断健全保密工作的领导体制机制，充分发挥党在保密工作中统揽全局、协调各方的领导核心作用，确保保密事业在党的坚强领导下，始终沿着正确的政治方向稳步前进。

5年来，保密战线始终坚持党的领导，把党管保密作为保密工作的根本，把维护习近平总书记的核心地位作为最大的政治，把抓好党建作为最大的政绩，始终不渝抓好思想政治建设和专业能力建设，为各项工作顺利推进奠定了坚实基础和可靠保障。

——加强作风养成，深化思想政治建设。坚持用习近平总书记系列重要讲话精神和中国特色社会主义理论体系武装各级保密干部，坚定理想信念，使各级保密干部自觉履行党章和保密法律法规赋予的各项职责，严守政治纪律和政治规矩，严格开展保密依法行政。深入践行习近平总书记提出的“五个坚持”和“三严三实”要求，持续深入改进思想作风、工作作风和生活作风，坚守正道、弘扬正气，争做维护国家安全和利益的“无名英雄”和“忠诚卫士”。

——实施人才战略，多措并举引进培养专业人才。国家保密局不断加强保密专业人才引进，各地区各部门也采取各种方式加强专业人才引进。国家保密学院持续加大保密专业毕业生培养力度，加强定向就业指导，为全国保密系统输送新鲜血液和专业人才。

——强化职业培训，全力提升保密干部专业素质。集中开展全国保密系统保密干部专门培训，全国共举办保密干部培训班千余期，培训专兼职保密干部几十万人次。持续开展全国保密干部轮训工作，采取“以练代训”方式，对省一级保密部门案件查办、技术监管、科技测评等专业人才进行轮训。

——推进学科建设，加强保密人才储备和智力支持。成立保密系统工程系列职称评审委员会，开展全国保密系统专业技术职务任职资格评审，为保密干部打造职业发展平台。全国建设国家保密学院十余所，印发加强保密专业人才教育培养工作意见，召开保密学科建设工作座谈会，组织编写十余本保密专业理论教材，努力提高教学质量，培养合格专业人才。

五年辛勤耕耘，五年开拓创新。全国保密战线的同志们始终铭记习近平总书记的重托，用行动书写着对党的忠诚、对人民的忠诚。

站在新的历史起点上，保密战线将继续紧密团结在以习近平同志为核心的党中央周围，以习近平新时代中国特色社会主义思想为指导，按照中央决策部署壁画的新蓝图，看齐跟上，服务大局，努力实现保密工作转型升级，坚决打赢信息化条件下的保密之战，为我们党领导进行伟大斗争、建设伟大工程、推进伟大事业、实现伟大梦想做出新的更大贡献。

★深入学习宣传贯彻党的十九大精神

编者按：刚刚闭幕的党的十九大，是在全面建成小康社会决胜阶段、中国特色社会主义进入新时代的关键时期召开的一次十分重要的大会，在我们党和国家历史上具有重大里程碑意义。当前，全国保密系统正在兴起学习宣传贯彻党的十九大精神的热潮。本刊从本期起开辟专栏，对全国保密系统学习贯彻情况进行宣传报道，努力营造良好学习氛围，推动党的十九大精神深入人心、落地生根。

牢记使命 砥砺前行 努力开创新时代保密工作新局面

□田 静

刚刚闭幕的党的十九大，是在全面建成小康社会决胜阶段、中国特色社会主义进入新时代的关键时期召开的一次十分重要的大会，在我们党和国家历史上具有重大里程碑意义。学习宣传贯彻党的十九大精神，是当前和今后一个时期全党全国的首要政治任务，全国保密系统一定要按照中央统一部署和要求，认真学习、深刻领会、全面贯彻，把思想统一到党的十九大精神上来，把力量凝聚到实现党的十九大确定的各项任务上来，努力开创新时代保密工作新局面。

用习近平新时代中国特色社会主义思想武装头脑，指导保密事业发展

党的十九大提出的习近平新时代中国特色社会主义思想，是党的重大理论创新成果，是指导党和国家事业发展的强大思想武器，具有重大的政治意义、历史意义、理论意义、实践意义。全国保密系统要在学通弄懂做实上下功夫，深刻认识其时代背景、历史地位、科学体系、精神实质和实践要求，准确把握贯穿其中的坚定信仰信念、鲜明人民立场、强烈历史担当、求真务实作风、勇于创新精神和科学方法论。推进新时代保密工作，我们要更加自觉地把习近平新时代中国特色社会主义思想作为保密工作的思想旗帜、理论指引、根本遵循，贯彻落实到保密工作各方面，领航保密事业不断开辟新境界。

进入新时代，我国日益走近世界舞台中央，也面临更加错综复杂的安全保密形势，我们党要巩固执政地位，团结带领人民坚持和发展中国特色社会主义，实现“两个一百年”的奋斗目标，保证国家安全是头等大事。在新的历史方位，我们要更加清醒地认识保密工作面临的形势。

深刻认识当前保密工作形势，标定保密工作新的历史方位

党的十九大作出了中国特色社会主义进入了新时代的重大政治论断。进入新时代，我国日益走近世界舞台中央，也面临更加错综复杂的安全保密形势，我们党要巩固执政地位，团结带领人民坚持和发展中国特色社会主义，实现“两个一百年”的奋斗目标，保证国家安全是头等大事。在新的历

史方位，我们要更加清醒地认识保密工作面临的形势。当前，国家间综合国力的竞争日趋激烈，政治、经济、军事、外交、科技等全方位的综合较量不断加深，围绕信息情报特别是国家秘密的监控、刺探、获取等活动，力度不断加大、领域更加广泛、高技术特征集中凸显，我国家秘密安全将面临更加严峻的风险挑战，窃密与反窃密斗争将更加尖锐复杂。与此同时，保密工作仍处在转型发展的过程中，由于观念、机制、技术、队伍、物质条件等多方面因素的影响，泄密风险隐患还大量存在，严重泄密事件时有发生，保密风险防控还面临不少问题，筑牢保密防线的任务还非常艰巨。我们必须充分认识新时代保密工作面临的新形势，把握新时代保密工作的新特点，切实担负起新时代维护国家安全利益的职责使命。

始终坚持党管保密，牢牢把握保密工作的根本

党的领导是中国特色社会主义最本质的特征。党的十九大把坚持党对一切工作的领导，作为新时代坚持和发展中国特色社会主义基本方略的第一条，强调党政军民学，东西南北中，党是领导一切的。党的领导是保密事业发展的根本保证，党管保密是保密工作的根本原则，也是做好保密工作的最大政治优势。建党九十多年来，革命、建设、改革的实践充分证明，保密工作的一切发展进步和作用发挥，无一不是在党的保密工作方针政策指引下、决策部署落实中实现的。在新时代开创保密工作新局面，必须始终不渝地坚持党对保密工作的领导，充分发挥各级党委（党组）及其保密委员会总揽全局、统筹谋划、协调各方的作用；必须不断健全保密工作的领导机制，提升统筹保密工作的能力和水平；必须严格落实党政领导干部保密工作责任制，努力构建纵向到底、横向到边的保密工作责任体系，形成有关各方齐抓共管保密工作的良好局面。

全面推进依法治密，提高新时代保密工作的法治化水平

全面推进依法治密是贯彻落实全面推进依法治国战略部署、提高保密工作法治化水平的基本途径。目前，我们已经初步形成了以宪法为根据，以保密法及其实施条例为主干的保密法律法规体系，保密行政执法体系也取得很大发展。落实好全面依法治国战略要进一步推进依法治密工作。我们必须加快完善保密法规体系，重点加强涉外、数字国家秘密、大数据、移动互联等新领域的保密管理法规制度建设，适应实践发展，填补立法空白；加强和规范保密行政执法，建立健全保密行政管理权力清单、责任清单制度，依法开展保密审查审批、资格认定、检查查办等行政管理活动，健全监督检查机制，加大保密行政执法监督力度，保证保密法律法规落实到位；提升全社会保密法治意识，积极开展保密法治宣传教育，培育保密习惯和尊法守法意识，不断提升运用法治思维和法治方式管理国家秘密的能力和水平。

党的领导是保密事业发展的根本保证，党管保密是保密工作的根本原则，也是做好保密工作的最大政治优势。在新时代开创保密工作新局面，必须始终不渝地坚持党对保密工作的领导，充分发挥各级党委（党组）及其保密委员会总揽全局、统筹谋划、协调各方的作用；必须不断健全保密工作的领导机制，提升统筹保密工作的能力和水平；必须严格落实党政领导干部保密工作责任制，努力构建纵向到底、横向到边的保密工作责任体系，形成有关各方齐抓共管保密工作的良好局面。

加快保密科技创新，引领保密工作转型升级

创新是引领发展的第一动力。党的十九大作出加快建设创新型国家的战略部署，要求强化基础研究、加强应用基础研究、加强国家创新体系建设、深化科技体制改革、倡导创新文化，体现了把握发展自主权、提高核心竞争力的战略考量。在网络化、信息化时代，保密工作面临着远远超越传统时代的新课题新挑战，坚定不移地推进创新驱动发展，是维护国家秘密安全、确保国家安全优势的核心战略，是保密工作实现转型发展的必由之路，也是打赢信息化条件下保密之战的必然选择。我们要坚持创新引领，制定实施保密科技发展规划，不断加强保密科技体制机制创新，充分发挥科技在保密工作中的基础支撑和引领作用，实现管理与技术的有效融合，带动整个保密工作升级换代；加强保密科研机构、企业主体、主管部门的联合协作，着力构建以企业为主体、市场为导向、产学研相结合的保密技术创新体系，引导各类主体

协同创新；充分发挥市场在优化保密科技资源配置中的作用，探索建立以市场为导向的创新服务平台，促进保密科技成果转化，最大程度服务保密工作实践。

加强综合防范，推动新时代国家保密体系建设

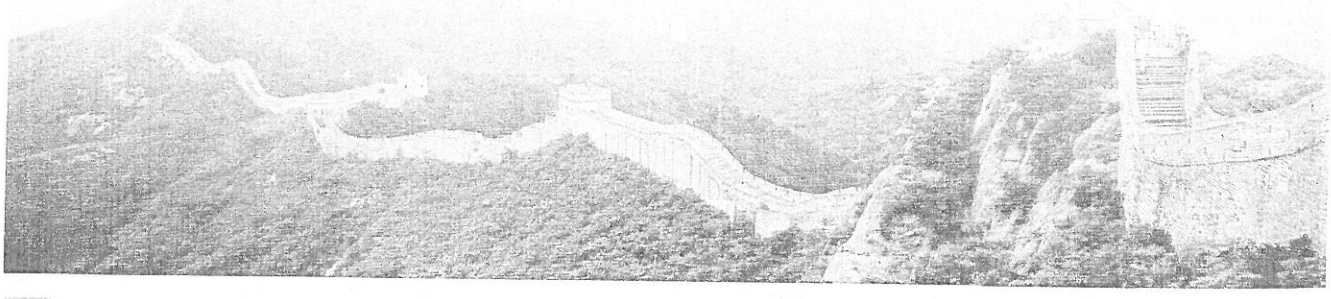
党的十九大报告提出，要完善国家安全战略和国家安全政策，坚决维护国家政治安全，统筹推进各项安全工作；健全国家安全体系，加强国家安全法治保障，提高防范和抵御安全风险能力。这一战略部署，对做好保密工作具有直接重要的指导意义。不断深化保密工作治理体系和治理能力建设、服务强国目标，是新时代做好保密工作的一条主线。我们要在实现强国目标的总体进程中统筹考虑、谋势布局，加快构建一体化、综合化的国家保密体系，有效提升国家保密能力，为实现强国目标提供有力的保密保障；坚持以总体国家安全观为指导，按照中央决策部署，注重国家层面的政策优化、资源整合，科学制定路线图、施工表，并随实践推进不断迭代优化，保证落实到位；坚持技术防护和保密管理并重，推进人防物防技防“三位一体”的综合防范体系建设，不断提高综合防范能力。

锻造过硬保密队伍，践行维护国家安全和利益的重大使命

党的十九大提出一系列新要求，最核心、最根本的是提出了新时代党的建设的新要求，指出“全面从严治党永远在路上”。全国保密系统要把全面从严治党各项要求严格落实到各项工作中，建设一支忠诚可靠过硬的保密队伍，保障保密事业发展。把党的政治建设摆在首位，旗帜鲜明讲政治，切实用习近平新时代中国特色社会主义思想武装广大保密干部头脑，进一步增强“四个意识”，拥戴核心、服从核心、紧跟核心，坚定维护以习近平同志为核心的党中央权威和集中统一领导。牢固树立国家安全和利益高于一切的观念，切实增强责任感、使命感、荣誉感，永葆忠于党、忠于国家、忠于人民的政治本色。坚持保密队伍专业化发展，培养高素质专业化人才，坚持专业知识、专业能力、专业作风和专业精神相统一，不断提升保密工作专业能力。严守政治纪律和政治规矩，严格依法行政，严格遵守廉洁从政各项规定，切实做到心中有责不懈怠、心中有戒不妄为、心中有畏不越规，始终保持保密队伍清正廉洁、风清气正。

不断深化保密工作治理体系和治理能力建设服务强国目标是新时代做好保密工作的一条主线。我们要在实现强国目标的总体进程中统筹考虑、谋势布局，加快构建一体化、综合化的国家保密体系，有效提升国家保密能力，为实现强国目标提供有力的保密保障。

进入新时代，站在新的历史方位，全国保密系统肩负着更加光荣的历史使命。面对国家安全环境的深刻变化，面对服务保障实现社会主义现代化强国的目标要求，我们要更加紧密团结在以习近平同志为核心的党中央周围，坚持不懈用习近平新时代中国特色社会主义思想凝心聚魂，牢记使命、砥砺前行，以永不懈怠的精神状态和一往无前的奋斗姿态，朝着新时代保密工作目标任务奋勇前进，为实现“两个一百年”奋斗目标、实现中华民族伟大复兴的中国梦做出新的更大贡献。



举案说法

堵住转发、引用、汇编涉密文件不按规定定密的漏洞

□刘景松

依照保密法律法规规定，机关单位执行上级确定的国家秘密事项，需要定密的，根据所执行的国家秘密事项的密级确定；摘录、引用、汇编属于国家秘密的内容，应当按照规定报批，不得擅自改变原件的密级、保密期限和知悉范围。然而在实际工作中，转发、引用、汇编涉密文件不按规定定密，甚至擅自抹掉密级标志的违规案例不胜枚举，给国家安全和利益造成损害的同时，也使自己的前途蒙上了阴影。

案例1：转发涉密文件不按规定定密。2011年8月，某市卫生局收到上级1份秘密级文件，时任卫生监督科科长王某，在非涉密计算机上起草了转发该文件的通知，而且未按规定定密，并将另外2份秘密级文件一起扫描，上传至市政府网站，造成泄密。事件发生后，王某受到行政警告处分，其他责任人分别受到相应处理。

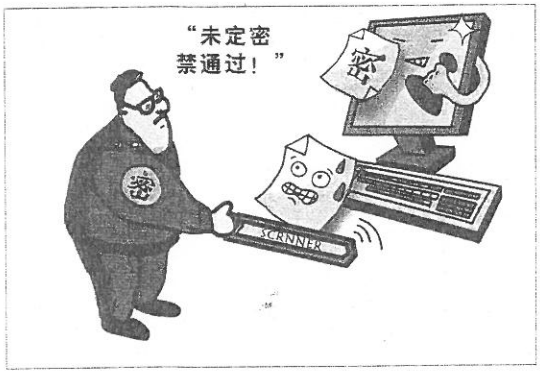
案例2：引用涉密文件不按规定定密。2012年4月，某县人防办综合股股长孙某，在起草本系统队伍组建方案时，引用上级有关涉密文件内容，未按规定定密。文稿拟定后，该办副主任郭某未严格审核把关，导致文稿被发布至县政府网站，造成泄密。事件发生后，孙某受到行政记过处分，郭某受到行政警告处分。

案例3：汇编涉密文件资料不按规定定密。2003年7月，某省直单位决定将国家及省、市出台的相关工作文件资料编印成资料选编，供本部门、本系统工作中使用。办公室工作人员金某具体负责此项工作，收集、整理了包括数十份涉密文件在内的文件资料，并录入形成电子稿，但未按照涉密文件的最高密级定密。后书稿交某出版社，出版社亦未作严格审查，并在未告知该省直单位的情况下，将该书交由某电子图书发行公司制作成电子版图书，造成泄密。事件发生后，有关部门给予相关责任人党纪政纪处理。

案例4：擅自隐去涉密文件密级标识。2014年1月，某县委防范办工作人员丁某在转发上级下发的2份机密级文件过程中，未按规定定密，并擅自将文件密级遮住，发至各乡镇。某乡镇工作人员将该文件主要内容整理后，上传至互联网，造成泄密。事件发生后，丁某受到行政警告处分，其他责任人分别受到相应处理。

上述案件的发生，充分暴露出一些机关单位和涉密人员保密意识淡薄、保密责任懈怠、保密管理松弛的问题，教训极为深刻。分析其原因，主要有以下几个方面。

一是保密纪律执行不严。保密纪律是政治纪律的重要内容。但是，有的机关单位执行保密纪律不严，其工作人员对使用非涉密计算机处理涉密信息、通过互联网传输涉密文件等现象见怪不怪。特别是



一些综合、秘书部门工作人员，经常在互联网上搜索资料，使用非涉密计算机撰写含有涉密或敏感信息的领导讲话、方案计划等；通过互联网邮箱，QQ、微信等社交媒体传输涉密文件信息；随意扫描、复印（复制）国家秘密，且扫描、复印（复制）件没有按规定纳入涉密文件管理范围等，致使保密“铁律”成了“自由律”。

二是保密工作责任制形同虚设。保密工作责任制主要包括领导干部保密工作责任制、定密责任制、涉密信息系统管理和维护人员责任制等。实行保密工作责任制，就是为了加强保密工作组织领导，明确相关人员保密工作职责，确保保密工作落到实处。在查处上述案件中，这些机关单位要么没有制定相关保密制度，工作人员对什么是国家秘密、如何保守秘密、需要履行什么手续、遵循哪些程序，不知不懂；要么虽有制度也只是挂在墙上、写在纸上，联系本机关本单位实际不紧密，缺乏操作性和针对性，工作人员没有入心入脑，在一些具体环节上，把定密要求忘得一干二净，以致发生违规现象。

三是保密审查城门洞开。发生上述案件，一方面是源头没有把好关，不知道应该定密、不知道如何定密、不能按规定定密，使文件流转的下一环节无法正确履行保密程序；另一方面是信息公开保密审查不严格，不遵循“谁公开，谁审查”、事前审查和依法审查原则。一些机关单位政府信息发布保密审查城门洞开，流于形式，没有落实“三审三查制”，即系统信息提供部门自审、信息公开工作机构专门审查、主管领导审核批准的工作要求，导致不能及时发现并有效防止涉密信息上网，最终自酿苦果。

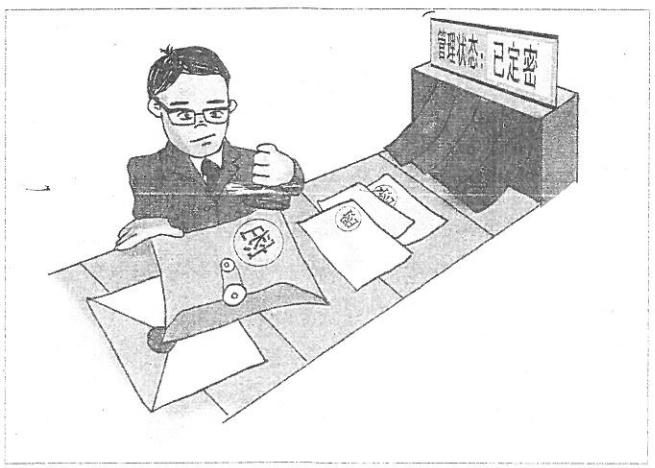
前车之辙，后车之鉴。从源头上遏制不按规定定密的错误现象，要从以下几个方面做起。

一是“两识”教育要如影相随。加强对涉密人员的教育培训，让广大领导干部和涉密人员学习保密知识、掌握定密程序、养成保密习惯。大力抓好日常宣教，引导广大党员干部和群众，学保密、知保密、懂保密，切实将保密意识、保密常识贯穿于各个环节、各个细节，不断提高领导干部和涉密人员的保密意识和信息化条件下的保密常识，筑牢思想防线，增强防范能力。

二是制度执行要铁板钉钉。要依据保密法律法规，结合本机关、本单位的具体情况，制定行之有效的具体管理措施，包括定密解密工作的管理制度、上网信息保密审查制度等，使保密管理工作有章可循。要定期排查保密制度执行过程中存在的突出问题和风险隐患，找准薄弱环节，补足短板，狠抓落实。属于制度不完善的，要督促有关部门抓紧完善；属于执行制度不严格的，要对有关责任人进行批评，对造成国家秘密泄露的，要给予直接责任人和负有领导责任的人员党纪政纪处分，严肃保密纪律。

三是责任担当要高度重视。机关单位是定密主体，应当对本机关本单位行使定密权、履行定密管理职责情况负责。机关单位负责人作为法定定密责任人，对机关单位定密工作负总责。负责保密工作的办公室负责同志和具体工作人员，要严格履行法定职责，确保工作落实。各级领导干部带头遵守好各项保密制度规定，以身作则、率先垂范、身体力行，就能有力带动全机关单位同志从善如流，各尽其责，共同承担起确保党的保密工作方针政策落到实处的重大责任。

四是自查自纠要有的放矢。要对本机关本单位及下级机关单位开展定密工作的情况进行定期检查，发现本机关本单位国家秘密的确定、变更和解除不当的，应当及时纠正。机关单位保密委员会和保密工作机构要承担起定密监督职责，对本机关本单位定密制度落实情况、定密责任人依法履责情况等进行监督检查，发现存在定密不当等问题，应及时予以纠正。要加强对信息公开保密审查制度落实情况的自我监督检查，及时发现并堵塞泄密漏洞，杜绝泄密事件的发生。■



研讨

数字档案保密管理探析

□燕 杨

数字档案以其利用的便捷性、传输的快捷性、存储的高密度性等无可比拟的优势，备受档案界的推崇，应用日益广泛。而与此同时，数字档案易于复制、易于传播，存在较大的安全隐患，也越来越引起人们的担忧。由于数字档案是以二进制代码的形式存在于计算机系统中并在网络中高速传输，具有非人工识读性，不但形式虚拟，难以把控，而且在数字档案的生成、流转、存储和利用过程中泄密渠道较多，安全隐患很大，给人一种无所适从的感觉。那么如何开展数字档案的安全保密防范工作，保证数字档案不丢失、不泄密呢？笔者根据自身工作实践，认为应该抓住问题的关键点，按照数字档案的运动轨迹，从其生成、流转、存储、利用4个环节入手，通过完善的技术手段和严格的管理措施，筑牢数字档案安全保密的4道防线。

加强数字档案生成环节的安全保密防范

数字档案一般通过两种途径生成：一种是原生性的，在线接收各业务系统等电子办公环境及网络环境中的电子文件；另一种是再生性的，通过技术手段将实体档案加工转换成数字档案，其中以纸质档案数字化扫描居多。鉴于目前档案部门所使用的数字档案绝大多数都是通过后一种途径生成的，因此，档案数字化加工过程是其生成环节安全保密防范的重点。

档案数字化加工一般都是档案部门通过外包形式聘请专业公司来完成的，因此，必须严格按照国家档案局印发的《档案数字化外包安全管理规范》的要求进行操作。数字化加工前，要到档案主管部门进行备案，通过备案不仅可以使本单位档案数字化加工项目“记录在案”，更重要的是可以在档案主管部门的指导下全面考察外包公司的资质、业绩、人员、设备等情况，深入了解其是否存在违约行为、安全事故等不良记录，从而选择有资质、业绩优、口碑好的外包公司。外包公司确定后，档案部门要与之签订保密协议，明确档案数字化外包加工的安全保密责任和技术要求，共同制定实体档案交接、数字化过程管理、数字化成果验收、存储介质管理、实体档案保护等操作规程。数字化加工过程中，要建立安全保密管理台账，全程记录项目实施过程；要加强数字化加工操作人员的安全保密教育，明确安全保密责任和安全保密操作规程；考虑到外包队伍工作人员具有较强的流动性，应留存每位参与数字化加工人员的身份证复印件，保证人员的可追踪性。要加强档案数字化加工现场管理，工作场所要与档案库房相连，且为封闭空间，严禁将实体档案带出工作场所，杜绝外来人员随意进入工作场所；数字化加工场所应安装监控录像设施，确保档案存放及作业区域不留死角；录像至少留存6个，且定时回放；要加强对数字化处理设备的管理，档案部门应提供计算机、存储等硬件设备，保证数据的集中管理，以免数据泄露；数字化加工区域内严禁安装任何无线设备，数字化加工操作人员所携带的手机、U盘等移动设备在工作过程中要进行封存管理，严禁带入工作场所。此外，档案部门还要指派专人，加强对数字化加工现场的安全巡查，防止数字化加工过程中的各种泄密行为。这样，通过全过程、全方位的严密监控与管理，确保数字档案生成环节的安全保密。

加强数字档案流转环节的安全保密防范

在档案数字化加工流转过程中，要把实体档案和数字档案安全保密防范工作放在同等重要的地位，不可失之偏颇。

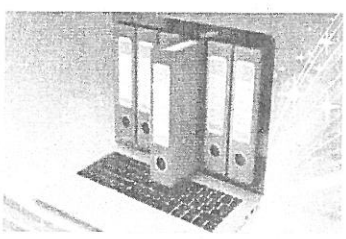
对实体档案，重点要加强流程管理。库藏存量档案的数字化加工流程一般包括档案整理、档案出库、档案拆封、数字化加工、档案复原、档案清点、档案入库等环节。为保证安全，应制订工作计划，分批调档，一个目录一个目录地进行数字化加工：实体档案的出库、入库要有严格的交接手续；完成数字化加工后的实体档案要及时清点、及时入库，不得留存在工作场所；档案的拆封、数字化加工、档案的复原要逐卷进行，做到实体档案与数字档案一一对应，且不能出现混页现象。新产生的增量档案归档后，要及时整理、及时登记、及时交付数字化加工，完成数字化加工后的实体档案同样也要及时装订、及时装盒、及时入库、及时上架，以免散落丢失。

对数字档案，重点要加强跟踪管理。档案部门应指定专人负责档案数据的安全保密管理维护：每天要将数字化加工完成后所形成的合格电子数据及时进行收集，复制到专用移动硬盘后上传至服务器或存储阵列中，进行数据挂接；在数据的复制、上传过程中，要注意做好台账，保证每步工作都“有据可查”。此外，还要进行病毒和恶意代码的检测与查杀，在线运行的数字档案应进行加密处理，使其难以非法读取。

加强数字档案存储环节的安全保密防范

档案数据要存储在专用服务器或存储阵列中，与档案信息系统共同运行在内部网络上，内、外网络要完全物理隔离，严禁移动存储设备随意接入，以防止非法窃取；要加强档案信息系统硬件设备的管理，数字档案设备应专机专用，并采用技术手段或专业物理设备封闭所有不必要的输出端口，如USB接口、蓝牙、SCSI接口、光驱接口等，且定期进行检查；为防止数据丢失，应按照国家标准《电子文件归档与管理规范》的要求做好数据备份，档案数据一般备份三套，一套本地备份，一套异地容灾备份，一套离线备份，离线备份的数据应复制到专用移动硬盘中，并存放在保险防磁柜内；要严格机房管理，外来人员不得随意进入机房，所有机房设备的维修、保养必须由专人负责，设备报废要送至保密局指定地点进行销毁。

在做好数字档案数据存储的安全保密防范工作的同时，决不能忽视实体档案库房的安全保密防范工作。在对实体档案数字化后，由于日常查阅、统计等工作都不再动用实体档案，实体档案处于封存管理状态，这样虽然有利于实体档案的保护，但也带来了新的问题：库房极易疏于管理。为此，实体档案库房及周边要安装各种监控设施，如门禁系统、红外线监控、视频探头，加强对库房的远程监控，防止外来人员非法入侵。



加强数字档案使用环节的安全保密防范

在数字档案查阅使用过程中，首先，要加强档案查询网络的管理，所有接入档案信息系统中的计算机都应进行IP地址绑定，严禁外来计算机非法接入。其次，要根据使用级别的不同，规定档案使用者的查阅权限，严格限制数字档案的在线复制和打印，除非档案部门管理维护需要，数字档案一般不得复制，打印也必须在档案部门内部进行，且必须加盖档案部门专用章，以表明数字档案打印件的合法性。同时，要建立完善的后台管理机制，数字档案的使用“痕迹”要以日志的方式记录在案，保证查阅使用的可追踪性。最后，要严格区分涉密档案和非涉密档案，对于涉密档案，其数字化信息严禁通过网络查阅，必须使用专用涉密计算机进行查阅。此外，档案部门要制定应急预案，遇到突发事件，沉着应对，妥善处置；在平时的工作中，要定期组织数字档案载体及其软硬件的检测，及时发现安全隐患，及时堵住安全漏洞。要突出人防的重要性，通过开展经常性的保密法治宣传、技能培训，使每个工作人员都牢固树立强烈的数字档案安全保密意识，建立健全安全保密责任机制，将数字档案安全保密责任细化落实到每个具体责任人，共同筑牢数字档案的安全保密防线。

国家网络安全宣传周：创新科技充当“阿喀琉斯之盾”

□拾 得

2017年9月，第四届国家网络安全宣传周主体活动在上海隆重举行，这是6月1日网络安全法正式施行以来的首个国家网络安全宣传周，集中展示了习近平总书记网络强国战略思想和十八大以来网络安全领域取得的重大成就，可谓一场感官盛宴。

随着国家网络安全宣传周活动的持续发酵，网络安全为人民、网络安全靠人民的理念逐渐深入人心。但与此同时，愈演愈烈的网络渗透、网络窃密乃至网络犯罪已然成为网络安全的“悬顶之剑”，时刻威胁着网络空间的和平与稳定。有矛就有盾、有攻就有防，历届国家网络安全宣传周上亮相的创新科技成果，正充当着“阿喀琉斯之盾”。今天，笔者就和大家一起揭开这些黑科技的神秘面纱，深入感受网络空间的真实较量。

“白帽子”们的漏洞挖掘

回顾历届国家网络安全宣传周，吸睛最多的莫过于精彩的攻防技术演示，不少互动科技体验直观还原了工作生活场景中的安全陷阱。

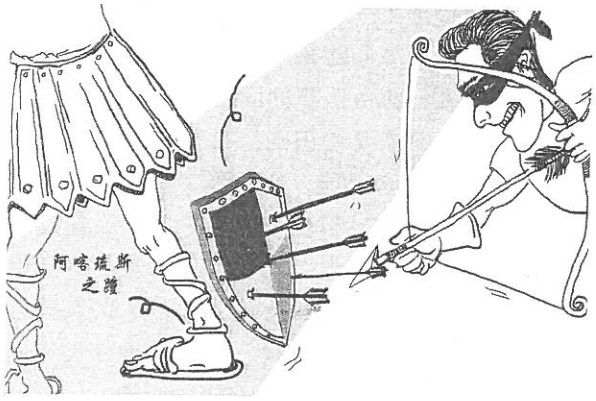
而这一切都离不开“白帽子”们对漏洞的挖掘。漏洞，是指在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而使黑客能够在未授权的情况下访问或破坏系统。与黑客不同，“白帽子”们在漏洞的挖掘上具有公开性和正义性，并不恶意利用，而是以此对抗黑灰产业。

今年，“攻破智能保险箱”项目就演示了手机App与云端服务的通讯数据被截获后，如何利用协议漏洞解密，并再次加密后发送给云端服务，从而控制智能保险箱。利用平衡车漏洞，在不经验证的情况下，就可通过电脑操控平衡车移动、锁车甚至修改密码。而“攻破人脸识别门禁”则利用系统薄弱环节，凭借两部手机、一张随机正面照、一个换脸App及一张3D脸模，骗过了人脸识别系统的活体检测，现场演示了一把刷自己的脸开别人家门的感受，造成感官冲击的同时，也引发大家对智能物联时代如何保证自身网络安全的思考。

“云中漫步”的大数据分析

大数据作为近些年来不断爆红的IT词汇，代表着信息爆炸时代产生的海量数据，以及与之相关的技术发展与创新。目前，全球信息总量每两年就翻一番，单一数据集容量超过几十TB甚至数PB已不罕见，导致常规软件工具无法在容许的时间内对内容进行抓取、管理和处理。因此，基于云计算的大数据分析应运而生。

面对安全问题，云计算可将大量计算资源、存储资源与软件资源聚合，形成规模巨大的共享虚拟信息技术资源池，深度挖掘并关联分析出数据背后的信息，为社会安全



再添一块盔甲。

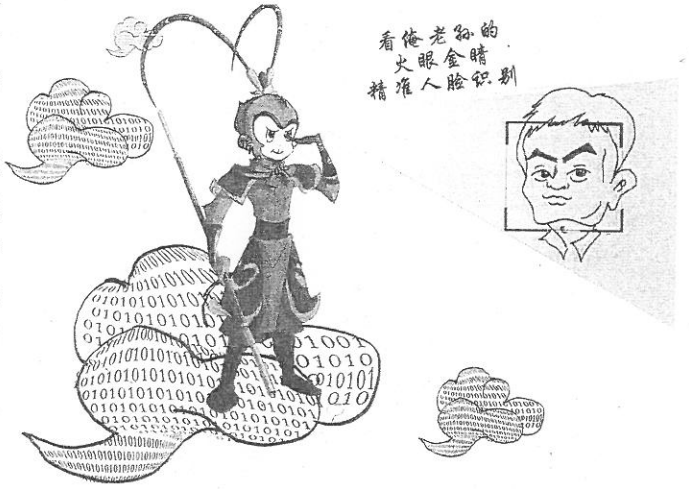
本届国家网络安全宣传周上，公安部儿童失踪信息紧急发布平台——团圆系统的亮相就是典型例证。这一系统接入了包括高德地图、支付宝、新浪微博、手机淘宝、滴滴出行等21个App的数据资源，自动向失踪地周边移动的终端推送信息，多方汇集并挖掘线索，第一时间对犯罪嫌疑人进行信息围堵，助力实现万家团圆。

“鹰眼”智能反电话诈骗盒子基于通话单的大数据分析，在智能引擎的快速模型识别匹配下，可实时检测出正在受骗的用户，通过与警方或运营商合作，对其进行劝阻，第一时间保护用户的财产甚至人身安全。“麒麟”伪基站定位系统则利用大数据分析和位置服务对伪基站定位，从空间、时间维度直观呈现其传播区域和实时运动轨迹，协助警方提高打击伪基站的效率。

“主动免疫”的可信计算

当前，计算机体系结构在设计时往往考虑的是计算速度而非安全因素，这直接导致网络环境下的计算服务存在大量安全隐患，如源配置被篡改、恶意程序植入运行、非法接管系统管理员权限等。

可信计算提出了一种新的主动免疫模式，采用运算和防御并行的双体系架构，在计算机运算的同时进行安全防护，具有身份识别、状态度量、保密存储3大功能，从而确保运算全程可测可控，不被干扰。其核心思想就是在硬件上引入可信芯片，达到与人体免疫一样及时识别“自己”和“非己”的机制。通过构建完整的信任链，未获认证的程序将不能执行，从而实现计算机体系结构的主动免疫。



可信计算在云计算、物联网、工业系统移动互联网等环境中均可提供基础保障。尤其是电力、通信等专控领域，其行业特点非常适合可信计算发挥安全作用。以电网系统为例，随着“震网”“火焰”等新型网络攻击武器不断涌现，建立基于可信计算的电网调度控制系统主动防御体系，将改变被动的“封堵查杀”防护模式，提升对未知恶意代码的免疫力。

在我国，可信芯片、可信计算机、安全操作系统及相关标准等起步较早，目前已形成以密码为基础、芯片为信任根、主板为平台、软件为核心、网络为纽带、应用成体系的可信计算框架，理论和技术水平都居世界前列。未来，可信计算还将在数字版权管理、身份盗用保护、抵御病毒和间谍软件、保护生物识别身份验证数据、核查远程网格计算结果等方面得到广泛应用。

“脑洞大开”的人工智能

人工智能是研究、开发用于模拟、延伸和扩展人的智能的技术科学，通过运用语言学、生理学、心理学等学科技术，使机器逐渐模拟人的某些思维过程和智能行为，从而帮助人们处理工作和生活中的问题。

就计算机网络安全应用而言，智能防火墙在识别和处理相关数据上比传统防火墙具有更高的安检效率，能更有效地防御高级应用入侵和病毒传播。智能入侵检测可通过采集、筛选、分类、信息处理，将计算机及网络安全状态及时反馈给用户。智能反垃圾邮件则可在不影响用户自身信息安全的条件下扫描检测邮件，敦促用户及早发现并处理垃圾邮件，保证计算机系统的整体安全。

国家网络安全宣传周上，基于人工智能的反诈骗实验室“智慧大脑”首次公开亮相。“神侦”资金流查控系统通过机器学习，能快速分析出用于诈骗的恶意银行卡，帮助警方在案发前追踪犯罪团伙活动区域及资金转移路径，冻结被骗资金，阻断诈骗链条中的资金流。“天猫精灵”也是人工智能和诈骗拦截技术相结合的产物，它将国务院钱盾反诈平台独有的诈骗拦截技术注入其中，不仅可以识别诈骗电话，还能向用户作出实时提醒。

涉密资质单位面临的八大难题

——涉密资质单位保密工作难题解析及对策（上）

● 吴同斌　李克光　/　国家保密科技测评中心

扎实有效地开展保密工作，对于涉密资质单位而言，既是维护国家秘密安全的政治任务，也是从事涉密业务、保障单位生存发展的必然要求。在与涉密资质单位的接触与交流中，深切感受到，绝大多数单位对做好保密工作有愿望、有担当，在实践中探索积累了许多成功的做法和经验。但是，随着信息科技的迅猛发展和我国社会经济体制的深刻变革，保密工作的复杂性明显增强、难度明显加大，涉密资质单位会经常遇到一些难题和困惑。特别是新获批涉密资质的非公有制企业越来越多地涉足涉密领域，对保密工作知之不多、理解不深，接手涉密业务缺乏经验、底气不足的问题也越来越显露出来。当前，各类涉密资质单位数量众多，情况各异，梳理大家共同关心的保密工作难题，拿出破解的思路和方法，对于主动应对保密安全威胁和有效管控泄密风险大有必要。为此，笔者重点围绕难题进行梳理、提出对策，旨在为涉密资质单位和有关方面提供参考。

难题一：保密课难讲

保密教育提纲难写、保密课难讲，是涉密资质单位反映比较普遍的难题，也是开展保密工作的“短板”。涉密人员由听课不解渴、不认同到不热心、不认真，势必影响教育效果。分析原因：一是缺少知识储备。授课人员对保密工作缺乏系统的学习了解，理论上讲不清，实践上道不明，往往就事论事、照本宣科，读规章、念条文，既谈不上深入浅出、融会贯通，更谈不上释疑解惑、入心入脑。二是缺少讲课资料。体制内的单位尚有获取讲课资料的条件，而一些民营企业由于渠道不畅、信息不灵，可供参考和利用的宣讲材料和案例片、宣传挂图等缺乏，自己编写制作又十分困难，故难免出现讲课生硬、干瘪、枯燥的问题。三是缺乏授课经验。懂讲课、会讲课、讲好课的人难找，涉密资质单位中的中小企业这类问题更为突出。授课人员一般为保密总监、保密办主任或指定的人员，经过几天培训就走上讲台，往往现学现卖，“半瓶晃荡”。有的刚刚到任，就安排其开讲，连本人也有“赶鸭子上架”的难言之隐。

难题二：涉密等级难定

定密工作一直是保密工作的难题，落实到涉密资质单位更难。原因是，一些单位由于对定密原则、程序和相关要求不了解、不掌握，对国家秘密事项的具体范围及密级确定理解模糊，把握不准，手头又缺乏依据，很难使定密做到最小化、精准化。如，有的没有遵循因岗、因事定密原则，将公司领导班子和中层人员无论涉密与否，全部定为涉密人员，职务越高，定的密级越高，而对重要涉密岗位上的人员却定得较低；又如，有的对保密要害部门部位的定义理解不透

彻，将公司销售部、商务部、广告部在内的所有部门都确定为保密要害部门，理由是涉密单位没有不是要害的。还如，涉密资质单位多数并无定密权限，但有的自认为某个项目比较敏感或重要，在甲方没有定密、自己也没有得到授权的情况下，擅自将相关资料定成了涉密文件。如此种种定密乱象，势必给保密管理增加难度。

难题三：保密标准难记

保密标准难记的问题在一些单位反映也比较普遍。由于记不住标准，致使保密工作中出现许多不落实或落实走偏的现象，直至产生泄密风险。分析原因，一是规章制度本质特性所致。保密标准是名词定义、适用范围、规定条件、实施原则、方法程序和要求融为一体的规范，多数是概念性、规范性的名词术语和条款，学起来枯燥乏味，本身就比较难记，这是客观原因。二是学习方法不当所致。无论是涉密集成类、印制类标准，还是军工保密标准，细化一下，都有上百条之多。如果学习方法不当，又无专业人员对照标准逐条解读、对案例进行剖析，不能做到先理解后掌握，仅靠死记硬背，必然前学后忘。三是急于求成所致。学习掌握标准不能“一口吃个胖子”，尤其是一些申请了多个涉密资质的单位，虽然各类资质的标准出现交叉重叠，有相似之处，但由于业务类型不同，某些具体条款必然有差别，多个标准的条条杠杠叠加起来，数量较大，需经历一个学习积累和适应的过程。

难题四：制度融合难做

现场审查多次发现，一些单位的保密制度是原封不动抄袭别人的。也经常听到这样的议论，即制度融合不知从哪里下手，订出来的制度自己也不满意，属于少不了的“扣分项”“整改项”。然而，制度融合又十分必要，它是一种创新性举措，必须做到位。分析融合难的原因，一是特点把握不够。制度融合首先是特点的融合，各自特点是融合的关注点、结合点。每个涉密资质单位都有区别于其他单位的独特之处，如果不能认真梳理自身日常管理制度的特点，又不能认清保密标准的刚性要求和程序性特点，就没有抓住融合的主要矛盾，订出来的制度便是缺少自己特色的“大路货”。二是主动延伸不够。保密工作是“保障线”，业务工作开展到哪里，保密制度就应跟进到哪里。如果“敲锣卖糖各管一行”，保密是保密，业务是业务，订出来的制度就是“两张皮”，不仅业务工作得不到保障，保密制度也苍白无力。三是细节研究不够。制度融合应体现“你中有我、我中有你”的要求，如果对日常管理和项目实施过程各环节、细节缺少研究，不清楚哪里有泄密风险，哪里需要保密制度规范，制度融合同样没有深进去、融到位。

难题五：不良习惯难改

涉密资质单位反映较多的不良习惯有：利用电子邮件、微信、微博、QQ等发送敏感信息，用移动通信工具谈论不宜公开的事项，涉密文件、资料不及时存入保险柜，复印涉密件不严格履行申请审批程序和未按原件管理等。毫无疑问，这些不良习惯都是泄密的风险和隐患。形成的原因，一方面，个人认识不够、自律不严。有的对新技术运用中的新规定、新要求学习了解不够，对可能造成的泄密风险认识不到、估计不足。有的则为了图方便、快捷、简单，明知是不良习惯而为之。也有的觉得单位多年没有发生泄密案件，没有必要改掉那些习惯。另一方面，单位重视不够、管理不力。表现为教育不到位，提醒不够、警示不够；监管不到位，该订的制度没订，该立的规矩没立；检查不到位，心中不装标准，手中不握“尺子”，见怪不怪、看不到问题；处罚不到位，不敢批评、敲打、问责，甚至对不听话、不守规矩的人不敢采取调离或辞退措施。在某种意义上，单位的管理力度对能否改掉不良习惯更为重要。

难题六：项目过程难控

项目实施过程是防范、管控泄密风险的关键时段。一些涉密资质单位反映，涉密业务在单位内部比较好做，一旦外出施工，难度陡然上升。尤其在距离遥远、人员分散、时间较长或项目过程中突生变化的情况下，就明显感到鞭长莫及、力不从心。新获准的涉密资质单位在初次接手涉密项目时，这种感觉会更加明显。分析项目过程难控的主要原因，一是风险评估工作不到位。没有按照涉密项目流程全面、准确地识别风险点，或者没有针对不同风险等级制定切实管用的措施，导致单位领导和相关责任人员头脑不清、心中没底。二是人员选派不得力。对项目人员的可信、可用、可靠程度不掌握，没有把“好钢用在刀刃上”。特别是项目负责人如果选派不得力，泄密风险就更加不可控。三是教育培训不扎实，没有认真组织项目人员进行培训，对应遵守的规矩没讲清、标准要求没强调、泄密风险没点透、防控措施没说明。四是保密责任不明确。没有明确项目人员各自承担的保密责任，以及发生泄密事件如何追究，致使项目人员自控力降低。

难题七：人才队伍难稳

经济社会快速发展，人才流动不可避免。如果涉密资质单位人才流失严重，尤其是优秀的科研、技术类人才（一般被定为涉密人员和保密队伍骨干），因为流失而导致原单位的商业机密甚至国家秘密泄露，其损失和危害难以估量。某涉密资质单位负责人反映，近几年每年都有25%—30%的涉密人员跳槽，已经成为困扰保密管理的一大难题。毋庸置疑，人才流动能够推动我国人才资源的合理配置，为市场经济发展带来活力。作为涉密资质单位，出现少量流动属于正常，超出正常比例，就会导致涉密人员频繁更换，泄密风险加大。就企业而言，应该深刻反思一下自身的工作，看看有哪些亟须改进的地方：一是在人才招录环节上，有无哄骗现象，是否存在未兑现承诺的问题；二是在确定涉密人员时，有无严格审查，是否存在草率从事或违背本人意愿的问题；三是在管理环节上，是否存在简单粗暴、不够民主、严而不当的问题；四是在生活待遇上，是否存在与同类企业落差明显的问题；五是在文化氛围上，是否存在人文关怀不够、现代企业气息不浓的问题，等等。

难题八：脱密期难管

脱密期管理是对涉密人员实施全程化保密管理的最后环节。《保密法》规定：“涉密人员在脱密期内，应当按照规定履行保密义务，不得违反规定就业，不得以任何方式泄露国家秘密。”然而，由于有的单位对脱密期管理不重视，情况不跟踪，措施不落实，导致涉密人员在脱密期间得不到应有的提醒和监督，不守承诺而泄密。涉密人员离岗仍在本单位工作的脱密管理比较容易些，难的是离职脱密管理，涉密人员到别的单位或外企就业,或出国（境）；更有的联系方式和家庭住址发生变化，电话号码注销，无法跟踪回访，不可控因素增大。随着市场人才流动频率加快，涉密人员离职的数量有逐年增多的趋势，脱密期管理的难度也会随之增加。深入分析原因，一是事前约定不够，在确定涉密人员时，未能依据相关法律法规，制定详尽的脱密管理条款，致使涉密人员自我约束意识淡化。二是离职管理程序缺失，未制定实行离职前报告制度，或未采取先离岗脱密、后离职脱密步骤，有的甚至未严格办理移交登记或签订保密承诺，降低了脱密管理的科学性、有效性。三是跟踪力度不够，对脱密管理缺少研究，不舍得花精力做这项工作，有意回避了脱密期管理的矛盾和困难。END

（下期将为您解读解决这些难题的相关对策，请继续关注！）

（栏目编辑：郝君婷）

破解涉密资质单位面临难题的四种对策

——涉密资质单位保密工作难题解析及对策（下）

● 吴同斌 史雁群 / 国家保密科技测评中心

【编者按】当前，保密工作已经进入转型升级的新时期，挑战和机遇并存。面对上期文章《涉密资质单位面临的八大难题——涉密资质单位保密工作难题解析及对策（上）》中列举的保密工作八大难题，涉密资质单位急需从维护国家安全和利益的高度出发，自觉增强主体责任意识，创新观念，创新思路，开辟新的破解保密工作难题的路径。本期文章将从四个方面细说破解难题的思路与对策。

加强领导 增强自信

切实重视，在实施强有力的领导中增强破解难题的自信。“世上无难事，只要肯登攀。”自信，是破解保密工作难题的前提；缺乏自信，就会丧失决心和行动力。涉密资质单位保密工作的自信，首先来自单位领导的态度、决心和意志，来自对保密工作强有力的领导。如果一个单位像重视抓生产一样重视抓保密工作，难题势必迎刃而解、不攻自破。当前，在领导思想和工作把握上，应重点防止和克服一些单位申请涉密资质“拼命干”、审查过后“减一半”、证书到手“放一边”的功利思想，防止和杜绝“喊起来重要、做起来次要、忙起来不要”的表面文章，防止和克服保密工作的问题越积越多、难题越积越难的现象。具体工作中，**一是突出对思想意志的领导。**采取组织学习、专题会议、宣传教育、外出参观等形式，把上级的精神吃透，把当前的形势论清，把自己的差距找准，把目标任务和举措讲明。通过思想发动，荡涤各种模糊认识和错误观念，真正把大家做保密工作的认识提升起来，把意志和行动统一起来，形成上下一心、充满自信、破解难题、持续发力的态势。**二是注重对组织机构的领导。**按照国家保密标准，切实把保密领导小组、保密办建立健全，把各级保密管理人员配强配齐，把应履行的职能明确到位，把应赋予的权力落实到位，并跟进保障，为其发挥职能作用提供人力、财力、物力等支持。**三是坚持对制度体系的领导。**紧扣国家保密标准，紧贴本单位实际，建立健全针对性、可操作性强的保密制度体系，实现横向到边、纵向到底、重点突出、全面覆盖的保密管理格局，使涉密资质单位保密工作的领导充分体现在保密制度体系科学建立和日常运行上。**四是实行对考绩问效的领导。**量化任务，细化分值，明确责任，客观公正地考核实际工作优劣。单位保密工作分管领导应亲自参与，深入现场，对考评结果亲自监督把关；主要负责人对考绩问效工作应给予大力支持，保证保密工作奖惩激励落到实处。**五是加强对风险管控的领导。**保密领导小组应定期分析本单位保密工作开展现状，查找问题和隐患，全面识别风险，区分轻重缓急，提出行之有效的管控措施。

同时，要领导和监督相关部门落实排查制度和责任，实行网格化管理，进而做到心中有数，增强管控泄密风险的自信。

打牢基础　提高能力

打牢基础，在提高人员素质中增强破解难题的能力。保密工作中的难题往往由人所为、因人而异、靠人破解。涉密资质单位人员特别是保密管理人员和涉密人员的素质高低、能力强弱，是关系保密工作成败得失的决定性因素。面对保密工作的新情况、新问题、新挑战，突破保密工作遇到的各种障碍，应重视抓根本、打基础、谋长远，在提高人员队伍能力素质上下功夫。**一是提高保密领导小组成员谋划全局、科学决策的能力。**保密领导小组是单位保密工作的领导、决策机构，是顺利开展保密工作的重要组织保证。领导小组的每个成员应认真学习掌握保密工作的基础理论，了解保密工作形势，吃透上级精神，熟悉自身状况，尤其对存在的隐患和工作中的“短板”头脑清醒，对本人所负责的业务与单位保密工作的关系胸中有数。只有这样，才懂得如何立足自身、着眼全局谋划工作，做出正确的决策，才会知道人往哪里派、钱往哪里花、劲往哪里使，才能真正取得破解难题的主动权和决胜权。**二是提高保密办人员检查督导、推进落实的能力。**保密办是涉密资质单位保密工作领导小组的日常工作机构，头绪纷繁、任务艰巨，应认真履行保密领导小组赋予的职责，充分发挥参谋助手作用、检查督导作用、协调推进作用，出好主意，狠抓落实。特别是真正熟悉保密标准，善于检查保密工作中的薄弱部位和环节，针对问题和隐患，协调各方，共同研究，拿出行之有效的解决办法和措施，推进工作落实。**三是提高各业务部门负责人照章办事、抓好执行的能力。**业务部门负责人是十分重要的管理层、执行层，也是本部门保密工作的第一责任人。应针对自身接触涉密业务多，距离涉密人员近，对违规行为发现及时，对泄密风险及其发展程度能够先于管控的特点，认真履行检查监督职能，促使各项保密要求在本部门落实到位，不给泄密留下任何缝隙。当科研生产与保密工作发生冲突时，积极寻找结合点，既保护国家秘密，又不耽误业务工作。不能两全时，确保以国家安全和利益为重。**四是提高涉密人员自我控制、严防违规的能力。**涉密人员既是保密管理的对象，又是保密工作的主体。保密工作的成效离不开涉密人员的创造，泄密隐患的存在和泄密事件的发生又与涉密人员的行为直接关联。涉密资质单位一定要在提高涉密人员尽职责、明标准、懂技术、守规矩、严操作的素质上下功夫、多投入，使他们真正做到政治上坚定，思想上纯洁，业务上精通，作风上严谨，工作上细致。同时，也要注意提高非涉密人员的保密能力和素质，为他们后续递补到涉密人员队伍做好必要的准备，以保证关键时刻用得上、过得硬。各个层次人员的能力素质增强了，保密工作的基础水平提高了，许多难题就不再成为难题。

重点突破　积累经验

重点突破，在“解剖麻雀”中积累破解难题的经验。深入调查研究，善于“解剖麻雀”，是我党一贯倡导的工作作风和方法，是把工作做深、做细、做到极致的有效路径。破解保密工作难题也需走重点突破的思路。**一是选准重点。**由于各涉密资质单位的业务种类不同、从事涉密业务的时间和经历不同，文化积淀和人员素质不同，保密工作中碰到的困难也不尽相同。如，对风险识别、制度融合、人员管理、项目管理等如何与保密标准对接，在各单位所表现的难度不等，但不管是何种情形，都需从自身实际出发，本着先急后缓的原则，通过确立重点，“解剖麻雀”，各个击破，积累经验。**二是理清思路。**思路需要深入研究和思考。以不良习惯难改为例，解决的思路可考虑四步走：第一步，从制度立起。进一步规范职责、标准、流程、动作等，实

现制度标准化、全覆盖，不给任何不良习惯留下空白地带。第二步，从技术管起。尽可能地通过上技术手段，随时管控不规范行为，使一些不良习惯的发生成为不可能。第三步，从领导抓起。单位领导以身作则，先做出样子，违规犯错先于甚至重于别人处罚，通过罚出警示、改出成效，形成以上带下、以上促下的态势。第四步，从追责严起。任何人违规都必须严肃问责，受到处理，做到“零容忍”，无“下不为例”，营造告别不良习惯的正气。又如，保密课难讲的解决思路：在选题上，应明确是宣讲形势，还是基础理论、管理方法、技能培训等；在选人上，是内部指定授课者，还是借助外力、外聘专家；在方式上，是授课式，还是问答式、座谈式等；在手段运用上，是多媒体教学，还是播放案例片、参观学习、实训平台教学等。再如，对项目过程难控的问题，可采取先模拟演练的方法，探索出实施过程各环节易发生泄密的管控措施，为日后承接涉密项目奠定基础。**三是搞好积累**。不断总结积累“解剖麻雀”的成功经验，从中探索带规律性的东西。进而，在一个一个难题的攻克中，提高能力，锻炼队伍，积累经验，增强自信，形成适合自身实际的工作套路。

多措并举　生发后劲

多措并举，在营造履职尽责的氛围中生发破解难题的后劲。涉密资质单位要始终保持保密工作的生机和活力，切实发挥“生命线”“保障线”作用，其中很重要的一条，就是千方百计地营造爱岗敬业、履职尽责、愿做会做保密工作的氛围，为破解难题、推进发展提供持续不断的后劲。要做到这一点，需处理好3个关系。**一是处理好选人与用人的关系**。选人是为了用人，用人的需求决定选人的标准。涉密资质单位确定涉密人员的人选，必须着眼于从事涉密业务的重要性、特殊性，坚持进人、选人的标准更高、审查更严、考察更细。既要看现实表现，又要看本人经历；既要看本人状况，又要考察家庭背景；既要注重专业水平，又要注重政治信仰、道德品质、作风纪律、个人秉性等综合素质的考察，做到知人善任、准确录用、可信可靠。值得注意的是，有的单位为急需补充涉密人员，降低标准、省略程序，仓促用了个别从外单位转来或从学校、劳务市场招录不久的人员，由于考察不细、把握不准，发生了前进后出、急进急出的现象，给保密工作开展带来了被动，这种做法不可取。**二是处理好用人与留人的关系**。古人言：“良禽择木而栖。”要做到量才录用、人尽其才，使大家在涉密岗位上稳其心、尽其力，必须营造拴心留人的好环境。许多单位在这方面有好的做法和传统。概括起来，就是用事业留人，持续不断地进行宣传教育，营造健康向上的文化，引导大家认识涉密岗位的光荣和重要，在心中充满希望和期待中稳定思想，把根留住；用感情留人，给以更多的关心、关怀和关爱，把企业打造成“遮雨的伞”“避风的港”“温暖的家”，使大家在无限感恩中生发爱岗敬业、干事创业的热情；用待遇留人，适应社会经济发展和人民日益增长的美好生活需要的总趋势，参考同行企业的待遇水准，力所能及地提高广大员工的工资水平和生活待遇，特别是提高涉密人员保密津贴和相关待遇，不让大家因差别明显产生失落感、疏远感。**三是处理好留人与育人的关系**。坚持以人为本，着眼人的全面发展，把关怀人、教育人、培养人、锻炼人、提升人有机统一起来，把提高涉密人员队伍的综合素质，作为开展保密工作的首要任务，作为单位持续发展的百年大计，舍得下本钱、花时间、用气力、下功夫，坚持不懈地抓到底。改进保密人才管理、使用制度，建立有利于他们成长的激励机制，让有能力、有水平、有贡献的涉密人员人尽其才、脱颖而出。在正确处理留人与育人的关系上，要防止只“放电”不“充电”、只看眼前不看长远的短期行为；防止对专业人才教育管理失之于软，发生问题不敢处罚的现象。通过正确的育人工作，使大家把单位对自己真正负责的深切感受，化为植根企业、成就事业的不懈动力。END

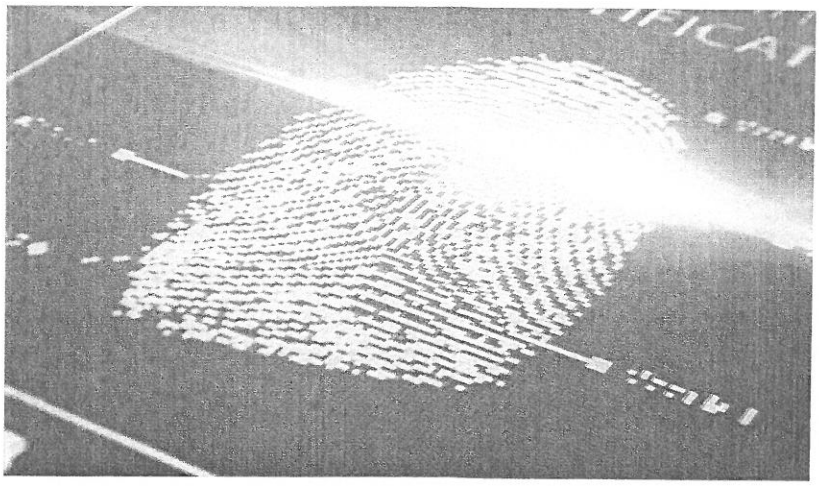
信息安全小百科

《碟中谍》背后暗藏的身份识别技术

在汤姆·克鲁斯主演的系列片《碟中谍》中有一个不可或缺的元素，就是炫酷的暗黑科技产品。这些高科技产品总会瞬间逆转，成功拯救人类。随着互联网以及智能城市、智慧家居的发展，曾经在科幻电影里看到的画面已不只处于想象之中了。影片中暗黑高科技里暗藏哪些玄机？本文要给大家揭秘其中的身份识别技术。

身份识别技术

身份识别（Identification，ID）是指能够识别本人身份的凭证，如我们每天使用邮箱的密码口令、安检出示的身份证、出入境的护照及指纹锁等。这些ID形式主要有以下特征：根据你所知道的信息来识别你的身份（What You Know，你知道什么），比如邮箱私有秘密口令；根据你所拥有的东西来识别你的身份（What You Have，你有什么），比如身份证、护照；直接根据独一无二的身体特征来识别你的身份（Who You Are，你是谁），比如指纹、面貌、DNA等。



ID除了上面所列举的技术外，还利用静态密码、短信密码、动态口令、生物识别等技术。生物识别技术是指通过可测量的身体或行为等生物特征进行身份识别。生物特征是指唯一的可以测量或可自动识别和验证的生理特征或行为方式。

身份识别与信息安全

随着信息技术的不断发展，一些传统的ID技术已不能满足人们对个人身份识别在安全性、灵活性和准确性方面的更高要求。在生物识别技术日趋成熟的时代，ID技术呈现出了多样性发展趋势。

尽管生物特征很难伪造，仍有黑客通过信息技术手段破解部分ID技术。例如，黑客恶意收录用户声音样本，通过合成后的声音重复使用可达到破解声纹识别的效果；指纹识别技术早已被破解，黑客通过用户接触过的物体，甚至根据照片，都可提取出可用于ID的指纹，然后通过3D打印技术打印出手套或指纹用于伪造用户信息。此外，目前流行的虹膜识别也存在风险。

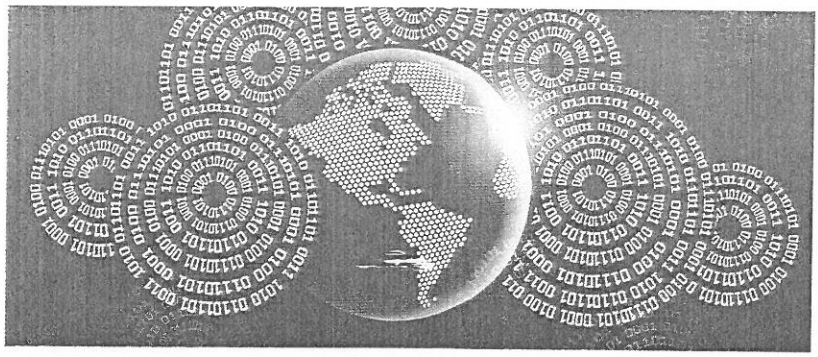
为进一步加强ID的安全性，单一依靠某一种ID技术已难以胜任“不可能完成的任务”了。在未来，两种及以上的ID技术相结合使用将成为趋势，也就是《碟中谍》中所展现的多模态生物识别技术，即根据应用场景、用户条件、安全等级等选择两种以上的识别技术进行匹配。将不同识别精度、采集距离、设备成本、防盗防伪、简单易用等特征融为一体，这比任何单一ID技术更安全可靠，可全面提升应用系统的安全性，确保用户信息的安全。END

（康双勇/国家保密科技测评中心）

（栏目编辑：郝君婷）

信息安全小百科

全同态加密将是云计算安全的“救命稻草”



在当前信息化时代，云计算、大数据、物联网、移动互联网均处于快速发展中，每个人“裸露”在外的隐私数据越来越多，为了不让别人看到自己的隐私数据，可通过加密手段把这些信息变成密文。于是，好比把这些数据放在了一个“安全盒子”里，如果需要利用或者查看这些数据，需要使用解密密钥把“安全盒子”打开。那么，我们能不能不打开盒子，就使用这些数据呢？这就要说一说全同态加密了。

全同态加密

全同态加密（Fully Homomorphic Encryption，FHE）是一种加密技术，是能够在不解密的条件下对加密数据进行任何可以在明文上进行的计算，即对于任意复杂的明文操作，都能够构造出相应的加密操作。因此，对FHE方案产生密文的任意计算，计算结果解密后与对明文进行相应计算的结果相同。这听起来就像是不知道问题也能给出问题的答案一样，使得加密数据信息被刻意打乱后仍能够被深入和无限地分析，而不会影响其保密性。

全同态加密守护云计算安全

当前，云计算发展突飞猛进，已被公认为未来ICT发展趋势。但是，在云计算热闹繁华的背后，困扰云计算数据的安全性、用户隐私的保密性问题迟迟不能得到很好的解决。近期，云计算平台发生多次安全事故，引起用户对云计算这种模式的安全性、保密性的强烈担忧。

从现有信息安全措施来看，加密技术无疑是解决云计算安全最根本的办法。FHE因其具有的良好特性，有专家学者宣称FHE将是云计算安全的“救命稻草”，把FHE应用到云计算中，可从根本上解决当前大部分云计算的安全问题，其原因如下。

其一，FHE可从根本上解决将数据存储和数据操作委托给第三方进行操作时的保密问题。用户可受托在任意互联网环境中将自己的隐私数据信息存在远程服务器里，既避免从当地的主机端发生泄密，又保证了信息的使用和搜索。用户也得以使用搜索引擎进行查询并获取结果，而不用担心搜索引擎会留下自己的查询记录。如，远程计算服务提供商收到客户发来的加密医疗记录数据库，借助FHE技术，远程计算服务提供商可像以往一样处理数据却不必破解密码；处理结果以加密的方式发回给客户，客户在自己的系统上进行解密读取，使用搜索引擎进行查询并获取结果。

其二，FHE在保证云计算数据安全的同时为云数据利用提供全新思路。当用户要对云端数据进行操作时，不再需要对密文数据进行解密，可直接对云端的密文数据进行操作。相对于传统的加密手段，FHE可让用户数据以密文形式放在一个“安全盒子”里，一旦需要利用或者查看，只需使用解密密钥把“安全盒子”打开即可，这极大减少了通信和计算资源的开销，同时也保证了数据在处理过程中的安全。

其三，目前FHE不断有突破性的进展，更加高效、可用的FHE方案增强和扩展了云计算的应用模式。利用FHE技术加密后的云端数据由于始终处于密文状态，云服务提供商可在避免窥探用户隐私的情况下进行海量的数据挖掘，为分析利用海量数据找到新途径，为云服务提供商合法有效利用海量云数据提供可能。END

（康双勇/国家保密科技测评中心）

（栏目编辑：郝君婷）

举案说法

调岗交接忌踩“保密红线”

□姚昙度

涉密人员调岗，必须依法交接，不得违反保密法纪。倘若对保密法纪规定的禁令不为、不碰、不抗，则可以顺利完成交接，而为之、碰之、抗之，则必将受到保密法纪的惩罚。

踩“保密红线”常见情形

（一）岗调了，交接未作

1.当甩手掌柜，不交接就离岗。用当下时髦的网络语言形容，有的涉密人员“心很大”，遇到岗位调整，不按规定交接，就拍屁股走人。如，在“涂某遗失涉密文件案”中，当事人涂某系A省某人民团体机要秘书，负责文件收发。2016年4月，涂某调到B市人民法院工作，但其在离岗前，未按规定与原单位交接。7月清退文件时发现，原由涂某保管的1份机密级、1份秘密级文件下落不明。经多方查找，仍未找到。事件发生后，有关部门给予涂某党内警告处分，并通报批评。

2.打个人算盘，避交接私拷贝。有的涉密人员公私不分，为了一己之便，擅自拷贝原单位涉密文件资料，带到新单位使用。如，在“乔某非法获取国家秘密案”中，当事人乔某系C研究所一项目组长，2012年7月，准备跳槽到D研究所，遂利用工作便利，采取把涉密文件资料混在非涉密文件资料中刻录光盘的手段，将C研究所大量涉密文件资料拷贝至家中私人笔记本计算机和D研究所工作计算机上。经鉴定，其中有15项机密级、58项秘密级国家秘密和59项不宜公开的文件资料。事件发生后，乔某被以非法获取国家秘密罪判处拘役3个月。

3.说葫芦忘瓢，漏交接忘载体。有的涉密人员粗心大意，记不清手中所持涉密载体，乃至未交接。如，在“唐某所持涉密书籍被违规销售案”中，当事人唐某系E银行分行原办公室主任，其2015年1月领取了1本秘密级书籍，存放在办公室中。7至10月间，唐某因岗位调整，要去新部门上任，但他忘记办公室中还有上述涉密书籍，未作交接，致使该书被当作旧图书卖给废品收购人，在淘宝网上出售。事件发生后，有关部门给予唐某党内严重警告处分，对其他人员作出相应处理。

（二）交接了，方式不对

1.图工作便利，为交接错违规。有的涉密人员作调岗交接时，方式错误，违反了保密法第四十八条规定。如，在“金某违规使用非涉密计算机存储涉密文件资料案”中，当事人金某系F中央国家机关综合处原处长，2015年12月，因要调往G中央国家机关，为做好交接工作，便对所用计算机内文件资料进行整理汇总，拷贝到处内工作人员使用的连接互联网计算机，刻录成两张光盘，并存储备份。经鉴定，其中有6份机密级、6份秘密级国家秘密。事件发生后，有关部门给予金某行政记过处分。

2.犯粗心大意，虽交接误销

毁。保密法第二十五条明确规定，任何组织和个人都不得私自销毁涉密载体，但有的涉密人员在调岗交接时，仍免不了犯过失销毁的低级错误。如，在“王某违规销毁涉密文件案”中，当事人王某系H省直单位文件管理员，2011年底，因岗位调整，整理办公室文件资料，与继任者交接。在此过程中，王某清理出大量过期文件资料，未认真翻看具体内容，直接交付销毁。经该局办公室工作人员确认，其中有1份秘密级文件被当作过期文件资料销毁。事件发生后，有关部门给予王某行政警告处分，并予以通报批评。

3.走形式主义，已交接不核对。有的涉密人员到新岗位后，接手别人交接的涉密载体或设备，未按要求核对，结果存在夹杂或遗漏密件的情况。如，在“陈某违规使用非涉密计算机存储涉密文件资料案”中，当事人陈某系I国有企业战略发展部秘书，其2013年10月调入后，与原部门秘书周某（2013年11月离职）交接，接手对方所用的非涉密计算机，并继续使用，未发现机内存有2份秘密级国家秘密，导致持续违规。事件发生后，有关部门对陈某进行严肃批评，并处3000元经济罚款。

主观思想与客观要求的偏差

（一）涉案人员的主观思想

1.“图省事”。面对调岗，很多人都希望尽快到新岗位，这是人之常情。但部分涉密人员任由这种想法脱缰而行，为图一时省事，将自身保密义务抛之脑后，未严格按规定交接。如，在“涂某遗失涉密文件案”中，涂某作为机要秘书，本应对涉密文件倍加上心，但他为及早到岗，竟连交接程序都未履行，就直接去新单位上班；在“金某违规使用非涉密计算机存储涉密文件资料案”中，金某本应采取符合保密规定的方式交接涉密电子文件资料，但他为了操作方便，用其他同事的联网计算机刻录光盘，并在该计算机上备份。

2.“松了气”。部分涉密人员以为，调岗了，就能松口气，哪知道胸中这口气一泄，国家秘密也随之被泄。如，在“唐某所持涉密书籍被违规销售案”中，唐某压根不记得先前领取的秘密级书籍，当作旧图书处理；在“王某违规销毁涉密文件案”中，王某不够细心，将涉密文件当成了过期文件资料，违规予以销毁；在“陈某违规使用非涉密计算机存储涉密文件资料案”中，陈某只是机械地交接，既没自行核对周某计算机内的文件资料，也没请内部保密工作机构处理，致使该计算机在存密的情况下长期连接互联网。

3.“私心重”。部分涉密人员公私不分，以为自己在涉密岗位上工作，没有功劳也有苦劳，不能吃亏，于是将岗位上形成的文件资料，不论是否涉密，都视为囊中物，调整到新岗位时也必须一并带上。如，在“乔某非法获取国家秘密案”中，乔某在案件调查过程中陈述，其一方面为了以后工作方便，另一方面也想留下纪念，便偷偷把承担的一些涉密项目资料、技术资料拷贝带走，乃至触犯“保密红线”，受到刑事处罚。

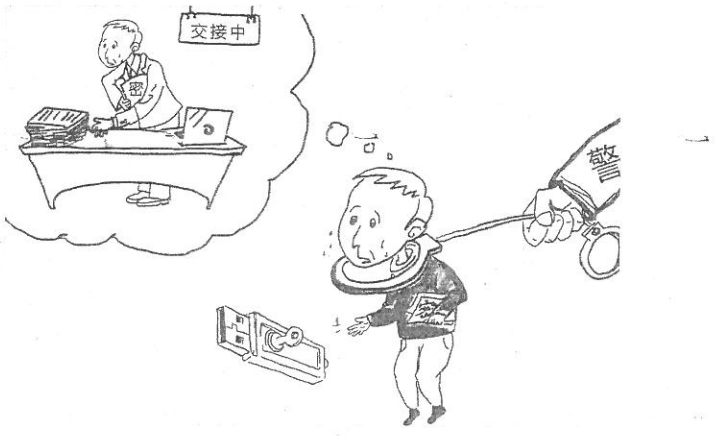
（二）调岗交接的客观要求

涉密人员在涉密岗位上工作，一旦调岗，则必须按照保密法律法规规定进行交接。

1.交接涉密载体。涉密人员调岗，应当交接个人所持有和使用的国家秘密载体和涉密信息设备。如文件资料、软盘、U盘、光盘、涉密信息设备等涉密载体，不得继续保管或存储。交接时，必须认真清理清点，登记在册，办理移交手续，并作为办理调岗手续的条件。

2.签订保密承诺书。涉密人员调岗，应当与原单位或者工作部门签订保密承诺书，明确调岗后应履行的保密义务及违反承诺应承担的法律责任，给调岗交接程序再加一道“心锁”。

3.脱密期管理。到非涉密岗位



上工作的涉密人员，应当在交接完成后进行脱密期管理。调岗到本单位其他部门的涉密人员，脱密期管理由本单位负责；调岗到其他涉密单位的涉密人员，脱密期管理由调入单位负责。

纠正思想偏差的要诀

1.用“引”字决，树好国家“大局观”。一方面，要引导涉密人员从讲政治的角度看待保守国家秘密问题。保守国家秘密安全就是讲政治，必须从国家安全大局高度，正确认识个人付出和国家秘密的关系，学会保持心理平衡。另一方面，要引导涉密人员从讲规矩的角度看待个人执行保密制度问题。保密工作无小事，保密制度必须落到实处。无论在日常工作中，还是在调岗交接环节，都必须始终不折不扣地执行保密制度。个人工作岗位上形成的，哪怕是一针一线，只要是国家秘密，就绝对不能占为己有。

2.用“教”字决，念好保密“紧箍咒”。一方面，要强化对涉密人员的保密教育。重点讲好涉密载体、涉密人员管理规定，做到制度宣传与释义讲解相结合，使涉密人员真学、真懂、真会，并常记心头。另一方面，要强化对涉密人员的警示教育。要把有关调岗交接环节发生的案例作为生动教材，对机关单位内部涉密人员进行经常性保密警示教育，使大家从中吸取教训，得到启示，真正做到时时刻刻如履薄冰、如临深渊，时时刻刻居安思危、警钟长鸣。

3.用“管”字决，打好监管“组合拳”。一方面，要严把涉密人员出口关。机关单位必须加强对调岗涉密人员的保密管理，严格开展交接，严格保密审查，对不符合条件的人员，要进行调岗限制。另一方面，要严把涉密载体管理关。机关单位要坚持按制度管载体，按规定做交接，严格控制涉密载体的知悉范围，明确掌握各个涉密人员掌握的涉密载体数量，在涉密载体制作、传递、使用、销毁等各个环节采取有力措施，履行相关手续，使涉密载体始终处于有效控制状态。

4.用“严”字决，拧好问责“压力阀”。一方面，要发挥保密检查的巡逻作用。机关单位要经常开展检查，以涉密人员管理和涉密载体管理为对象，重点检查相关交接工作做没做、审没审、严不严，做到仔细查、严格查、反复查，坚持常查不懈，以保密检查筑牢防护网。另一方面，要发挥案件查办的威慑作用。机关单位对调岗交接环节中发生的案件，要严肃查处、紧抓不放，切实使那些心存侥幸的涉密人员及有关领导干部，认识到保密法纪是一条不可触碰的“红线”。

保密知识小测试

判断题

1.机关单位在涉密岗位确定、保密要害部门部位确定、涉密信息系统分级、涉密工程确定、涉密会议活动确定、信息公开与对外提供资料保密审查、密级鉴定、泄密案件查处等工作中，要依据相关保密事项范围的规定进行。（ ）

2.如果机关单位发现同一事项在不同保密事项范围中均有规定，但密级、保密期限和知悉范围互不相同的，应当先按照规定密级较低的保密事项范围拟定密级、保密期限和知悉范围，采取相应的保密措施，并立即向保密事项范围制定机关反映。（ ）

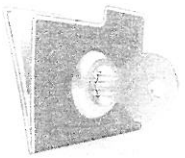
3.机关单位可以根据实际工作需要，按照有关保密事项范围，系统梳理本机关、本单位可能产生的全部国家秘密事项的名称、密级、保密期限和知悉范围，编制国家秘密事项一览表，供实际定密工作使用，并根据保密事项范围的调整变化及实际工作情况，对一览表的内容及时作出增补、删除或者调整。（ ）

4.国家秘密和工作秘密、商业秘密、个人隐私之间存在重叠、交叉，有的信息可能既是国家秘密，又是工作秘密或者商业秘密。（ ）

（答案见本期）

研讨

泄密案件调查的强制性



□姚 斌

根据保密法第四十二条、保密法实施条例第三十五条规定，泄密案件调查是保密行政管理部门的常规性行政行为。按照行为的强制性程度不同，行政行为分为强制性行为和非强制性行为。那么，泄密案件调查的强制性如何？实践中，由于上述两个条文既未规定调查的具体方式，也未明确能否在调查中采取强制措施，导致对此分歧较大，亟须厘清。

从调查目的看调查的强制性

一、泄密案件调查的目的

判断一种行政行为是否具有强制性，首先要从其行为目的上分析。泄密案件调查作为一种行政行为，具有以下两个特有目的。

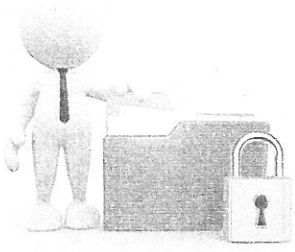
其一，保守国家秘密。这是泄密案件调查的根本目的。保密行政管理部门通过对涉嫌泄密的案件线索进行调查，核实是否发生保密违法行为、有没有造成泄密后果、存不存在泄密隐患，进而对调查发现的问题和隐患进行整改，以防止窃密泄密后果的发生或者及时止损、挽救泄密损失，维护国家秘密安全。

其二，打击保密违法行为。这是泄密案件调查的直接目的。泄密案件调查具有一定的威慑性，客观上会起到惩前毖后、以儆效尤的规范作用。尤其在案件调查结束后，保密行政管理部门对责任人员进行处理，更能督促机关单位及其工作人员遵守保密法律法规规定，不敢触碰保密“红线”。即使被调查对象没有实施保密违法行为，保密行政管理部门也可以通过讲解保密知识和保密常识，为他们打好“预防针”。

二、调查目的折射出的强制性要求

一方面，“保守国家秘密”之目的必须以泄密案件调查的强制性为后盾。首先，为了保守国家秘密，保密行政管理部门可以依法采取具有强制性的调查手段。根据行政强制法第三条规定，发生或者即将发生突发事件的，行政机关依法采取具有强制性的应急措施或者临时措施。从案件发生的特点看，所有的泄密案件都具有紧急性、临时性、突发性，皆属于保密突发事件。在此意义下，泄密案件调查满足“突发事件”的前提条件，理应可以“采取具有强制性的应急措施或者临时措施”。其次，为了保守国家秘密，所有被调查对象都负有自觉接受泄密案件调查的义务。根据宪法第五十三条规定，所有中华人民共和国公民都有保守国家秘密的义务。这意味着“保守国家秘密”既是泄密案件的调查目的，也是每个公民必须遵循的义务。从逻辑上界分，义务有积极与消极之分。就积极履行“保守国家秘密”义务而言，无论是否实施保密违法行为，所有公民都应当自觉配合保密行政管理部门的调查，主动交代事实、说明情况。

另一方面，“打击保密违法行为”之调查目的决定了泄密案件调查的强制性要求。第一，基于“打击”本身之“强制”内涵，任何组织和人员都不得违反泄密案件调查。在“党管保密”的基本原则下，以“打击保密违法行为”为目的的泄密案件调查，是一种既代表党又代表国家的行政执法行为，必须维护其严肃性和权威性。调查工



作一旦启动，就必须全面、彻底地开展，所有组织和人员都必须无条件配合，直到案件查清、人员处理到位为止。第二，配合“打击保密违法行为”，是机关单位保密管理义务的另一种表达。从保密工作实践看，泄密案件调查能起到“以查促教、以查促管、以查促改”的效果，这与机关单位的保密管理目标是一致的，二者在方向上具有同一性。换个角度说，机关单位接受、配合泄密案件调查，其实也就是在履行所担负的保密管理义务。

从调查方式分析调查的强制性

一、泄密案件的调查方式

判断一种行政行为是否具有强制性，最直观的方法是从其行为方式上进行分析。根据保密法律法规规定，泄密案件调查的主要方式有以下几种。

1.查阅有关材料。根据保密法实施条例第三十三条规定，保密行政管理部门可以依法“查阅有关材料”。泄密案件调查中的“查阅有关材料”，即保密行政管理部门为及时查清案情，发现、堵塞泄密隐患，查阅被调查对象的文件资料、监控录像、录音等，必要时，还可以依法复制、提取这些材料。

2.记录情况。根据保密法实施条例第三十三条规定，保密行政管理部门可以依法“记录情况”。泄密案件调查中的“记录情况”，即保密行政管理部门书面记录泄密案件调查情况，以固定调查的过程和结果。当然，为了确保调查记录的客观性、真实性，被调查对象应当在调查记录上签字确认。拒绝签字确认的，保密行政管理部门可以邀请无利害关系的第三人签字证明。

3.保密技术检测。根据保密法实施条例第三十三条、《保密检查工作规定》第二十一条规定，保密行政管理部门可以对有关设施、设备等进行保密技术检测。泄密案件调查中的“保密技术检测”，即保密技术核查，是指保密行政管理部门利用技术手段对案件相关网络、计算机、存储介质等设备的情况进行技术检验核查，提取有关违规使用或者涉嫌泄密的原始证据，形成技术核查取证报告。

4.询问人员。根据保密法实施条例第三十三条规定，保密行政管理部门可以在泄密案件调查中“询问人员”。询问人员，即保密行政管理部门就公民举报、机关单位报告、保密检查发现、有关部门移送的涉嫌泄密以及其他保密违法行为的案件线索，向当事人及其他相关知情人员进行询问，了解、知悉相关情况，并制作询问笔录。

5.保密检查与现场稽查、查看。根据保密法第四十二条、第四十四条以及保密法实施条例第三十二条规定，保密行政管理部门可以在泄密案件调查中进行保密检查。当然，保密检查并非泄密案件调查的必备环节。保密行政管理部门对机关单位进行调查，大部分时候只对有关涉案场所进行现场稽查、查看，判断被调查的机关单位在场所管理上是否符合保密法律法规规定的要件。

6.责令作出说明。宪法第五十三条规定了公民的“保守国家秘密”义务，因此，保密行政管理部门可以在泄密案件调查中督促机关单位或者人员依法履行该义务，责令其依法作出说明。拒绝说明的，应当承担相应不利后果。如，根据刑法第二百八十二条规定，保密行政管理部门在案件调查中发现当事人非法持有属于国家绝密、机密的文件、资料或者其他物品，但拒不说明来源、用途等情况的，应当移送司法机关追究刑事责任。

7.封存、暂扣国家秘密载体及工具。根据保密法实施条例第三十三条规定，保密行政管理部门可以对有关设施、设备、文件资料等依法先行登记保存。在泄密案件调查语境中，“先行登记保存”作为调查方式的一种，其实就是对有关涉案的国家秘密载体及工具进行封存、暂扣。

二、蕴含在调查方式中的强制性属性

首先，泄密案件调查本身就具有强制性属性。这包含以下几层意思：第一，泄密案件调查作为保密行政管理部门的职权行为，具有命令行性、强制性和执行性。其根据是规定调查职权的保密法律法规、规定调查对象应当遵守的法律规范或应当执行的行政决定和命令。第二，部分泄密案件调查方式在实施过程中体现出间接强制性。如，保密行政管理部门可以在调查中采取复制、拍摄、录音等具有间接强制特点的调查方式，获取案件相关信息，为人员处理提供事实依据。第三，泄密案件调查不以被调查对象的意志为转移。无论被调查对象主观上是否愿意，客观上是否作出不配合、逃避、妨碍甚至抗拒行为，保密行政管理部门的泄密案件调查工作都会依法依纪开展。

其次，泄密案件调查以行政强制作为担保手段。根据保密法律

法规规定，被调查机关单位或者人员拒绝、逃避调查取证或者采取暴力、威胁等方式阻碍调查取证的，保密行政管理部门可以就遏阻情况采取相应的行政强制措施。如，根据保密法第四十五条、保密法实施条例第三十六条规定，保密行政管理部门可以依法收缴泄密案件调查中发现的国家秘密载体；根据保密法实施条例第三十三条规定，保密行政管理部门可以依法对有关设施、设备、文件资料等进行先行登记保存；根据保密法实施条例第四十三条规定，保密行政管理部门可以依法责令停止违法行为；根据保密法第二十八条，保密行政管理部门可以责令停止传输涉密信息；根据保密法第四十四条，保密行政管理部门可以责令机关单位对存在泄密隐患的设施、设备、场所停止使用。

最后，泄密案件调查以处分作为担保手段。在泄密案件调查中，被调查对象必须无条件配合、接受，不得拒绝、对抗，否则将承受不利的法律后果。根据保密法实施条例第四十条规定，如果有关机关单位或者人员在泄密案件调查中，存在拒不配合、弄虚作假、隐匿销毁证据或者以其他方式逃避、妨碍泄密案件调查的，可以对直接负责的主管人员和其他直接责任人员依法给予处分。由此可见，以处分手段为罚则，实质上就是强行要求有关机关单位或者人员接受保密行政管理部门的调查。

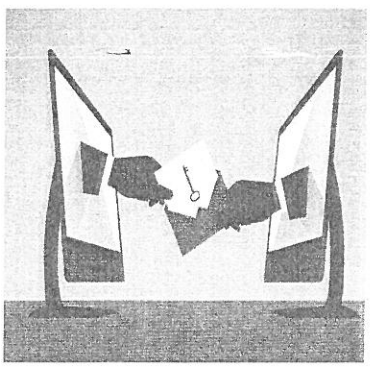
调查的限制与被调查对象的义务

一、泄密案件调查的限制

保密行政管理部门行使泄密案件调查权时，必须恪守依法行政要求，遵守法律保留原则和正当程序原则的制约。

第一，泄密案件调查必须遵守法律保留原则。法律保留原则，是指行政行为只能在法律规定的情况下做出，法律没规定的就不能做出。根据这一原则，保密行政管理部门的泄密案件调查不能随心所欲，只能依据保密法律法规的规定，依法实施相应的调查方式。例如，目前的保密法律法规未对人身自由方面的调查方式进行规定，保密行政管理部门就不得对行政相对人拘留、监视居住等，即使案件调查确有此需要，也不能直接实施，而必须通过其他部门来操作。

第二，泄密案件调查必须遵守正当程序原则。正当程序原则，是指行政机关做出影响行政相对人权益的行政行为，必须遵循正当法律程序，包括事先告知相对人，向相对人说明行为的根源、理由，听取相对人的陈述、申辩，事后为相对人提供相应的救济途径等。对此，我们一方面要正视当前泄密案件调查相关程序性规定缺位的现实，积极推动泄密案件查处办法的制定工作，另一方面要在遵循现行保密法律法规规定已明确要求的基础上，恪守最低限度的程序正义规则。



二、被调查对象的义务

鉴于泄密案件调查行为的强制性，被调查对象需担负起相应的容忍与协助义务。

1.被调查对象的容忍义务。所谓的容忍义务，是指对泄密案件调查中所产生的不利影响，被调查的机关单位或者人员负有不得抗拒、不得阻止的义务。客观地说，调查工作多少会对被调查的机关单位或者人员的生产、生活或者其他社会活动产生一些不利影响，如影响工作效率等。对于正常的、合法的泄密案件调查行为，基于维护国家安全和利益的需要，被调查的机关单位或者人员依法负有容忍义务。

2.被调查对象的协助义务。一般情况下，泄密案件调查需要进入被调查的机关单位，被调查的机关单位及其上级主管部门负有协助开展调查的义务。但在实践中，由于调查中发现的事实可能会引发后续的人员问责，故被调查的机关单位或者人员可能基于自身利益考虑，会不予协助甚至拒绝调查。一旦在泄密案件调查中发现拒绝接受、配合调查情况的，那么充分发挥泄密案件调查行为的强制性是十分必要的。

综上所述，泄密案件调查具有强制性，保密行政管理部门可以表现得更强硬一点。当然，这并不意味着所有的泄密案件调查都要秀“肌肉”。要知道，强制是万不得已的手段，即使采用了这种手段，有时也未必能够实现调查目的。有时在调查过程中采用柔性规劝、利益引导等方式，或许更能促进被调查机关单位或者人员接受、配合调查。

经向社会公开征求意见并修改完善后，《网络产品和服务安全审查办法（试行）》正式对外公布，并成为首个正式生效的网络安全法配套办法，标志着我国网络安全基本制度建设又朝前迈进了一大步，维护国家安全特别是网络空间安全有了重要的新抓手。围绕审查办法的出台及试行效果，本刊邀请网络安全专家进行解读。

《网络产品和服务安全审查办法（试行）》为网络安全构筑“铜墙铁壁”

□张 莉

数月前，国家互联网信息办公室发布《网络产品和服务安全审查办法（试行）》（以下简称《审查办法》），这是贯彻落实网络安全法第三十五条的重要措施，也是我国网络安全保障工作思路与制度的一项创新。

《审查办法》的出台，预示着我国网络管理方式由表层化向深层化发展，网络安全保障范围由党政军重要信息系统扩大至关系国家安全的所有网络及信息系统。同时，也标志着我国决心改变信息技术产品和服务受制于人的局面，并迈出了实质性步伐。

《审查办法》的内涵

围绕一个中心。《审查办法》明确提出，对网络产品和服务进行安全审查，目的就是提高安全可控水平，防范网络安全风险，维护国家安全，所有审查环节及行为都围绕这一核心思想展开。

*审查两大方面。*审查并非针对所有的网络产品和服务，而是关系国家安全的网络和信息系统采购所涉及的重要网络产品和服务。同时，审查也不是泛泛而言，而是聚焦于产品和服务的安全性、可控性。

*遵循三大原则。*具体操作中，审查须遵循3个相结合的原则，分别是坚持企业承诺与社会监督相结合，第三方评价与政府持续监管相结合，实验室检测、现场检查、在线监测、背景调查相结合。

*建立四个机构。*为保证审查顺利开展，《审查办法》提出设立4个机构，一是网络安全审查委员会，由国家互联网信息办公室会同有关部门成立，负责审议相关政策及协调重要问题；二是网络安全审查办公室，主要负责安全审查的具体组织实施；三是网络安全审查专家委员会，主要对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估；四是第三方机构，由国家依法认定，具体承担网络安全审查中的第三方评价工作。

*防控五大风险。*对网络产品和服务进行安全审查，目的是防控5大类风险：一是产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；二是产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；三是产品和服务提供者利用便利条件非法收集、存储、处理、使用用户相关信息的风险；四是产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险；五是其他可能危害国家安全的风险。

《审查办法》的三大亮点

动态与静态相结合。《审查办法》把落脚点放在关系国家安全的网络和信息系统采购的重要网络产品和服务上，是相对静止的概念。3个相结合的原则中提出了供应链的概念，进一步明确细化了有关要求，把审查拓展至网络产品和服务整个生命周期，形成了动态追溯的过程，这对于网络安全保障中的风险评估和态势感知具有重要现实意义。

总体统筹与分类操作相结合。根据《审查办法》，网络安全审查委员会在审查过程中发挥统筹协调和总体组织的作用，重点行业和关键信息基础设施以外的网络安全审查由审查委员会和办公室组织实施。

对涉及国计民生的重点行业，以及关键信息基础设施的重要领域，例如公共通信和信息服务、能源、交通、水利、金融、电子政务等，由各自主管部门组织开展本行业、本领域网络产品和服务的安全审查工作。其他关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，也应通过网络安全审查。

平等性与开放性相结合。根据《审查办法》，只要是关系国家安全的网络和信息系统采购的重要网络产品和服务，无论从外国企业还是国内企业采购所得，都需要接受网络安全审查，对国内外企业一视同仁。网络安全审查的出发点不是贸易保护主义，国内市场永远向合格、友善的网络安全产品和服务商开放。同时，《审查办法》也详细阐明了开展审查时重点关注的要素，体现出审查过程的开放性。

具体操作中的建议

明确一些基本概念。《审查办法》的出台，为网络安全审查提供了法理性依据，但在目前的《审查办法》试行稿中，有些概念仍然比较模糊，例如，什么是“关系国家安全的网络和信息系统”，什么是“重要网络产品和服务”，其内涵和范围应得到进一步明确，这对于《审查办法》的具体实施至关重要。

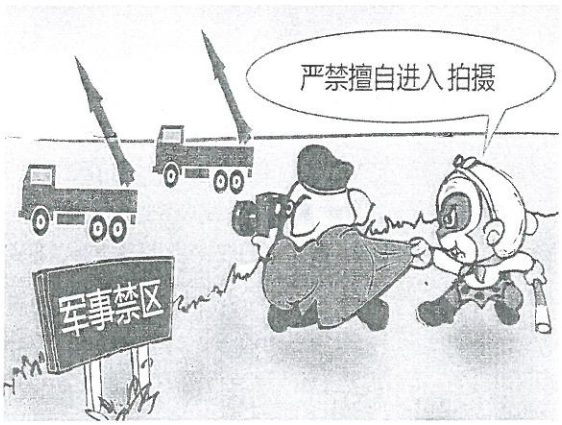
列出关键信息基础设施清单。关键信息基础设施是审查的重要对象，虽然网络安全法第三十一条已明确规定，关键信息基础设施的具体范围和安全保护办法由国务院制定，但网络安全审查办公室也可根据审查过程中的现实情况，提出关键信息基础设施清单，一方面有助于在国务院文件出台前理顺审查工作，另一方面也可为国务院文件制定提供基础和借鉴。

设立审查结果的互认规则。从目前的审查机制看，具体行业或关键信息基础设施的安全审查由各自主管部门负责，网络安全审查办公室负责审查“金融、电信、能源等重点行业和领域主管部门”以及“关键信息基础设施保护工作部门”之外的网络产品和服务。为了提升审查的效力与效率，还需制定各方主体审查结果互认规则，以避免不必要的重复审查。

建立第三方机构资格认定标准。《审查办法》提出，网络安全审查第三方机构由国家依法认定，但认定标准在具体操作过程中略显模糊。网络安全审查委员会可制定第三方机构的资格认定标准，由网络安全审查办公室、重点行业和关键信息基础设施主管部门依照标准认定合适的第三方机构，提高审查的公正性与客观性。■

（作者系中国电子信息产业发展研究院副研究员）

西游新记 保密知识篇



（作者：徐子建）

“两识”教育

国家秘密与工作秘密、商业秘密、个人隐私有何区别

国家秘密不同于其他类型的秘密或者隐私，它们之间存在着明显的界限，不能将同一信息既界定为国家秘密，又界定为商业秘密或工作秘密。

国家秘密与工作秘密。一般认为，工作秘密是指机关单位在公务活动和内部管理中产生的，一旦泄露会直接干扰机关单位正常工作秩序，影响正常行使管理职能，在一定时间内不宜对外公开的事项和信息。

工作秘密与国家秘密存在明显区别：一是关系的利益主体不同。工作秘密直接关系的利益主体是有关机关单位，国家秘密直接关系国家安全和利益。二是确定方式不同。工作秘密主要由各级机关单位自行确定，国家秘密的确定必须严格遵守保密法律法规，依照法定程序进行。三是秘密标志不同。工作秘密没有法定的专属标志，一般以“内部文件”“内部事项”等方式作出提示，国家秘密则有专属标志。四是管理方式不同。工作秘密的管理方式、方法和措施，没有统一的制度规范，国家秘密管理由保密法律法规作出明确规定。五是适用法律不同。工作秘密保护所适用的法律规范主要是公务员法，国家秘密的保护，则要严格依据保密法律法规的规定。六是法律责任不同。泄露工作秘密的法律责任是行政责任，泄露国家秘密，不仅要承担相应行政责任，符合条件的，还要承担刑事责任。

国家秘密与商业秘密。商业秘密，是指不为公众所知悉，能为权利人带来经济利益、具有实用性，并经权利人采取保密措施的技术信息和经营信息。

商业秘密与国家秘密存在显著区别：一是涉及利益不同。国家秘密关系国家安全和利益，商业秘密直接涉及权利人的经济利益和竞争优势。二是所有权性质不同。国家秘密的所有权属于国家，商业秘密的所有权属于自然人或法人。三是定密主体不同。国家秘密的确定主体是依法拥有定密权的国家机关和依法获得定密授权的机关单位，商业秘密的确定主体是从事科研生产和经营活动的企业事业单位。四是确定程序不同。国家秘密必须依照法定程序确定，以保密事项范围为依据；商业秘密的确定没有严格的程序，由权利人自行确定（央企确定商业秘密，执行国资委的有关规定）。五是处置权限不同。国家秘密未经合法审批，不得擅自对外提供或转让；商业秘密只要权利人同意即可参与市场交易并进行转让，也可自行处置。六是适用法律不同。国家秘密依据国家保密法律制度管理，其保密措施由法律明确规定；而商业秘密受反不正当竞争法等法律保护，主要由权利人自行管理。

国家秘密与个人隐私。个人隐私，是指公民个人生活中不愿为他人知悉或公开的信息。比如个人的日记、相册、通信、财产等。个人隐私与国家秘密的区别是非常明显的。一是法律属性不同。个人隐私属于私权利的范畴，国家秘密属于公权力的范畴。二是所有权主体不同。个人隐私属于自然人，国家秘密属于国家。三是所有权内容不同。个人隐私限于个人事务，国家秘密涉及公共事务。但在一些特殊情形下，特定自然人的个人隐私可能基于国家安全和利益的考量，纳入国家秘密范围。例如，在国家面临政治动荡、国家间出现战争冲突等情况下，一国领导人的身体疾患等情况可能作为国家秘密保护，以防止个人信息公布后对国家安全和利益造成风险和危害。

保密干部须知

已经依法公开或者无法控制知悉范围的事项为何不能确定为国家秘密

已经依法公开的事项。机关单位依照法律法规规定，经严格履行信息公开审查程序后公开的信息不得再确定为国家秘密。这是保持国家秘密严肃性、权威性以及可保性的必然要求。在此，要重点把握“依法”二字。

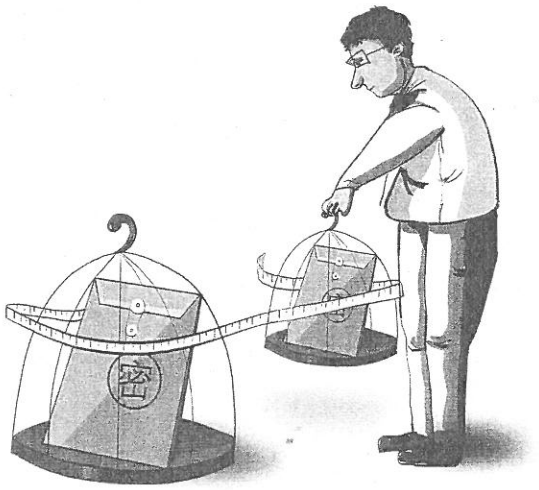
首先，公开的主体要合法。公开信息的机关单位必须是产生该信息的机关单位，或者是为该信息定密的机关单位。例如，中央文件的公开只能由中央决定，机关单位未经授权，擅自在公开的文件资料、出版物、会议和新闻媒体、互联网上使用的，不属于“已经依法公开的”情形。

其次，公开的依据要合法。机关单位公开信息应当属于法律法规明确要求公开或者依申请可以公开的信息。

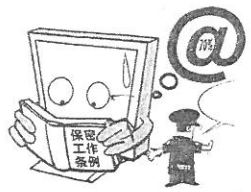
最后，公开的程序要合法。机关单位应当按照法律法规规定的程序进行信息公开，特别是要在公开信息前进行保密审查。对于没有严格履行信息公开程序，没有经过保密审查就擅自公开的信息，不属于“已经依法公开的”情形。

法律、法规或者国家有关规定要求公开的事项，应当是有利于国家安全和利益，有利于社会进步的。例如，《政府信息公开条例》等规定的应当公开的事项，是对公民权益具有保障和促进作用的，对于这些信息，不能将其确定为国家秘密。但是，《政府信息公开条例》第十四条明确规定，行政机关在公开政府信息前，应当依照保密法以及其他法律、法规和国家有关规定对拟公开的政府信息进行审查；属于国家秘密、商业秘密、个人隐私的政府信息一般不得公开；对政府信息不能确定是否可以公开时，应当依照法律、法规和国家有关规定报有关主管部门或者同级保密行政管理部门确定。此外，对于已经确定为国家秘密，但是新制定的法律、法规或者有关规定要求公开的，机关单位应当及时解密并予以公开。

无法控制知悉范围的事项。国家秘密必须在可控制范围内，即在一定时间内只限一定范围的人员知悉。这是构成国家秘密的三大要素之一。客观上不能控制知悉范围的信息，或者已经为公众广泛知晓、不可能再严格控制知悉范围的信息，已经不具备成为国家秘密的时空要素，不得确定为国家秘密。■



举案说法



加强机关单位互联网网站管理 片刻不能松懈

□宋筱婷

随着信息化的快速推进，机关单位互联网网站日益成为人民群众获取各种信息，特别是获取党政机关公务信息的最主要途径，也是信息公开的最主要方式。近年来，一些机关单位互联网网站违规发布或者转载涉密文件资料，严重危害党和国家秘密安全，其直接原因就是机关单位对拟在互联网上登载的信息缺乏保密审查或者保密审查不严所致。国家有关部门为此出台了一系列法规制度，对互联网网站信息发布管理作出明确要求，但一些机关单位仍然有令不行、有禁不止，造成此类案件仍然频发多发。同时，我们也从这些互联网网站泄密案件中发现，机关单位在文件转发、扫描、汇编、转载等方面保密管理存在较为突出的问题，成为网站泄密的间接原因，客观上为网站泄密提供了“条件”，值得深入思考。

典型案例

案件一：转发文件不定密。2017年2月，有关部门在工作中发现，某县人民政府网站违规发布了1份秘密级文件。经查，这份文件系对省直某部门秘密级文件的转发落实。省直某部门起草的秘密级文件印发后，市有关部门迅速贯彻落实，起草了转发通知，将省直某部门下发文件作为附件进行了转发。该县某县直单位收到市有关部门的转发通知后，办公室文件收发员孙某片刻不敢耽误，也立即起草转发通知，将市有关部门的转发通知作为附件，要求所属各乡（镇）人民政府、下属服务中心及有关县直单位认真抓好工作落实。由于工作时间要求较紧，孙某保密意识淡薄，没有对省直某部门下发文件的密级进行认真审核，未按规定对其起草的转发通知进行定密，也未履行保密审查程序，便擅自将其上传至县政府网站，造成泄密。案件发生后，有关部门给予孙某解聘开除处理，责令该县直单位副局长郑某在局班子上作深刻检查，对该县直单位和有关责任人员在全县范围内通报批评。

案件二：违规扫描、上传涉密文件。2017年3月，有关部门在工作中发现，某市属单位网站违规刊登1份秘密级文件扫描件。经查，该文件为该市属单位上级部门印发的秘密级文件，内容与该市属单位管理、服务的对象有密切利害

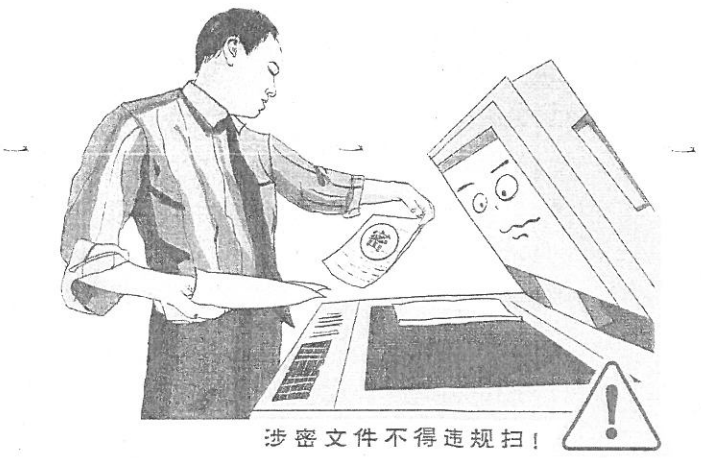
关系，大家对文件的具体内容都非常关注。为此，该单位副主任辛某准备立即着手组织集体学习，以尽快传达贯彻文件精神。但在电话通知有关人员参加集体学习时，却遇到了意料之外的麻烦。原来，该市属单位管理、服务的对象中年龄大、行动不便的为数众多，常年在外地居住的也占有相当比例，短时间内集中到一起学习该文件非常困难。电话沟通中，大家纷纷表示，想尽快、全面地了解文件内容。为了尽快传达，辛某自以为也是为了工作，就放松了保密这根弦，无视该文件为秘密级文件，直接将文件全文进行了扫描，未履行保密审查程序便上传至单位网站，供大家阅读。案件发生后，有关部门给予辛某党内警告处分。

案件三：违规汇编不标密。2016年11月，有关部门在工作中发现，某市政府网站违规刊登1份秘密级文件。经查，2016年11月下旬，该市某市直单位为全面提升业务工作水平，安排某科副科长王某将相关业务文件汇编成册，供大家学习参考使用。任务下达后，王某立即着手文件的搜集整理工作，向本单位办公室借阅了标注秘密级的涉案文件，将其密级抹去后编入文件汇编，且未在汇编封面标密，仅标注“内部资料 妥善保存”字样。随后，该汇编被印制300本分发给市委、市政府、各县市区和市直相关部门。11月27日，王某未履行保密审查程序，将汇编电子版提供给该市政府网站工作人员，由其编辑整理后上传至网站，造成泄密。案件发生后，有关部门给予王某行政警告处分，责令其作出深刻检查；对该市直单位分管保密工作的副局长鲍某和分管相关业务工作的副局长夏某进行约谈，对办公室主任徐某进行诫勉谈话，对市政府网站相关工作人员处以罚款。

案件四：转载文件不核实。2017年6月，有关部门在工作中发现，某区人民政府网站刊登1份秘密级文件。经查，2016年9月，该区政府网站完成改版升级投入使用后，区政府电子政务办公室为及时更新和丰富网站信息内容，要求区政府所属单位每月至少提供两篇信息稿件。10月10日，负责某区直单位信息报送工作的工作人员白某，在互联网上浏览信息时发现了涉案文件。其阅读后发现该文件与其业务工作关系较为密切，具有较大参考价值，且没有密级标识。同时，白某还发现许多互联网网站上都刊登了这份文件，也都没有密级标识，便想当然地认为这份文件不属于国家秘密，未经保密审查，将其上传至区政府网站服务器。10月11日，区政府电子政务办公室工作人员贾某在未见到白某所在单位主管领导审查意见，也没有了解事情原委的情况下，就直接将存储在服务器上的涉案文件发布到网站上，造成泄密。事件发生后，有关部门给予白某、贾某党内警告处分，并责令其深刻检查；对该区直单位副局长白虎某、区电子政务办公室主任白永某进行保密警示训诫，并责令其深刻检查。

原因分析

1.保密意识薄弱。一是疏忽大意。主要表现为工作不认真负责，草草应付。案例1中的孙某，主观上疏忽大意，没有对省直某部门下发文件的密级进行认真审核，为泄密留下了隐患。案例4中，白某草率鲁莽，看到涉案文件被多家互联网网站刊登且未标密，未经求证，就认定该文件不属于国家秘密；贾某盲目轻信，在没有看到相关领导的审查意见、没有了解事情原委的情况下就将文件发布到网站上。二是明知故犯。案例2中的辛某、案例3中的王某，都是在明知文件是国家秘密的情况下，依然违规对其扫描、汇编，最终导致国家秘密被上传上网。



涉密文件不得违规扫！

2.保密审查不严。上述案件中，保密审查形同虚设是导致案件发生的直接原因。《政府信息公开条例》第十四条规定："行政机关在公开政府信息前，应当依照《中华人民共和国保守国家秘密法》以及其他法律、法规和国家有关规定对拟公开的政府信息进行审查。"由此可见，保密审查是防范机关单位互联网网站泄密的"安全阀"和"保险闸"。案例1中的孙某、案例2中的辛某、案例3中的王某、案例4中的白某，不论是明知文件是密，还是因疏忽大意未发现文件是密，或是没有确切证据，便想当然地认为不涉密，均没有履行保密审查程序，便擅自将涉密文件上传至网站。"安全阀"和"保险闸"出了问题，从而导致泄密案件的发生。

3.保密管理缺位。上述案例中，文件转发、扫描、汇编、转载等方面保密管理缺位是造成案件发生的间接原因。案例1中孙某转发文件时未按规定进行定密，案例2中辛某扫描文件时未按规定进行请示登记，案例3中王某汇编文件时私自抹去密级且未按规定对汇编进行定密，案例4中白某将互联网浏览下载的文件直接作为政府网站信息来源，这些违规操作的存在都为后来泄密案件的发生提供了条件。实际上，如果这些行为被及时发现并妥善纠正，就能在很大程度上避免泄密案件的发生。

深度思考

"一叶落而天下知秋"，事物普遍联系的基本属性决定了我们看问题要有全局观念，不能头痛医头、脚痛医脚。加强机关单位互联网网站管理，严防泄密案件发生，不仅要加强保密"两识"教育和相关保密法律法规的培训，还要在制度上做文章。"法贵必行"，不仅要继续加强信息公开审查制度本身的贯彻落实，还要在公开"前"和公开"后"上下功夫。

1.加强保密"两识"教育。对工作人员加强保密"两识"教育，紧密结合机关单位互联网网站管理具体业务工作，对网站泄密风险点进行逐个梳理、排查，使大家时刻绷紧保密这根弦，真正使保密要求入脑入心。同时，创新培训方式，日常培训与专项培训相结合，个体学习与集中座谈相结合，使大家真正认识到保密无小事，切不可草率应付、疏忽大意，更不可明知故犯、突破"红线"。

2.严格文件日常管理。一是严格定密管理。转发文件，要严格按照所执行文件的密级进行定密；汇编文件，要严格按照汇编中文件的最高密级和最长保密期限对汇编进行定密；信息整理，要按照相关活动本身的保密要求进行定密，严禁"私抹"密级。二是严格复制管理。复制绝密级文件，应当经密级确定机关单位或其上级机关批准；复制制发机关单位允许复制的机密、秘密级文件，应当报本机关本单位主管领导批准。复制涉密文件应当严格履行登记手续，复制件视同原件管理。三是严格来源管理。机关单位互联网网站转载其他机关单位的文件，应当从文件的制发机关单位官方门户网站或该机关单位授权的媒体转载，严禁从未经授权的网站转载。同时，转载页面要注明转载来源、转载时间、转载链接等。

3.强化信息公开审查。一是健全审查机制，明确岗位职责。坚持"先审查、后公开""一事一审"的基本原则；同时，将保密审查与公文运转制度相结合，明确分管、提供、审查、上传等各岗位具体职责。二是严格审查标准，明确审查重点。明确将转发文件、扫描文件、文件汇编、转载文件等作为重点审查对象，确保对拟上网文件进行逐页审查、逐份审查。

4.落实网站检查查处。一是加强检查力度，定期组织对机关单位互联网网站进行拉网式检查，发现一起，整改一起，不留死角。二是严格责任人员处理。对发生泄密案件的，发现一起，查处一起，依法依纪严肃追究直接责任人员和负有领导责任人员的责任。三是加强通报力度。及时对重大、典型泄密案件进行通报，及时发现工作中的薄弱环节和突出问题，有针对性地改进提升。

当前，我国已经进入经济社会发展转型的关键时期，信息技术的发展日新月异，保密工作面临前所未有的挑战，要确保本单位互联网网站既确保国家秘密安全、又便利政府信息的公开使用，这就要求每个机关单位必须采取切实措施，加强保密"两识"教育，严格文件日常管理、信息公开审查和网站检查查处，常抓不懈、警钟长鸣，最大程度地防范泄密案件的发生。■

★“全面推进保密工作依法行政”系列谈

关注

一个必须抓住的保密依法行政“关键少数”

——谈落实领导干部保密工作责任制

□景凤启

各级保密行政管理部门主要负责同志是第一责任人，对本部门全面推进保密工作依法行政负总责；分管业务工作的负责同志在职责范围内对保密工作依法行政负直接领导责任。这是全面推进保密依法行政意见着眼加强领导干部对保密依法行政工作的领导，作出的决策部署和制度安排。领导干部这个“关键少数”作为保密依法行政的重要组织者、推动者和执行者，只有自觉在法律范围内活动，积极履行主体责任、带头落实责任制，才能形成示范效应，影响和带动全系统厉行法治。

“关键少数”肩负着主体责任

把领导干部定位为全面推进保密工作依法行政的“关键少数”，是由他们承担的职责使命决定的。作为行使保密行政权力的特殊群体和领导干部保密工作责任制的实施主体，虽然人数不多，但作用关键、责任重大。因此，必须始终把落实保密工作责任制的主体责任记在心上、扛在肩上、抓在手上。

把落实领导干部保密工作责任制的主体责任记在心上。领导干部保密工作责任制作为保密法律法规体系的重要组成部分，直接体现了保密依法行政的内在要求，必须深刻认识、时刻牢记。始终以高度的政治自觉把主体责任记在心里，牢固树立抓好保密工作责任制落实是本职、不抓是失职、抓不好是渎职的理念，把落实领导干部保密工作责任制作为保密依法行政的重要内容，列入领导工作议事日程，纳入领导班子、领导干部目标管理，推动依法治密不断取得新成效；始终以高度的思想自觉把主体责任放在心上，充分认识领导干部在机关单位所处的地位和应起的作用，切实增强责任感、使命感和紧迫感，以抓铁有痕的决心、一以贯之的恒心，守好土、尽好责，推动本机关本单位保密工作落实；始终以高度的行动自觉把主体责任印在心头，坚持与人防、物防、技防制度落实紧密结合，时刻不忘同部署、同推进、同检查、同考核。各级领导干部特别是对保密工作负总责的主要领导干部，只有把主体责任记在心里、放在心上、印在心头，才能做到心中有责、心存敬畏，做出样子、带好班子，确保领导干部保密工作责任制的主体责任不折不扣落到实处。

把落实领导干部保密工作责任制的主体责任扛在肩上。保密工作责任制是为解决领导干部责任意识不够强、责任内容和责任考核不规范等问题而设立的。因此，把落实领导干部保密工作责任制的主体责任扛在肩上，就要认清肩负的职责，强化主体意识。时刻想到自己肩上扛着谋划保密工作的责任，切实把落实领导干部保密工作责任制与推进保密依法行政工作和各项业务建设一起研究、共同实施、同步督导，贯穿于各项保密业务工作的各环节、全过程；时刻想到自己肩上扛着实施保密工作的计划，切实把落实领导干部保密工作责任制与强化保密管理、搞好服务保障一起组织实施，与规范定密、依法解密一起组织实施，与发展技术、管好网络一起组织实施，与严格、规范、公正、文明执法一起组织实施；时刻感到自己肩上扛着推进保密工作的压力，把落实主要领导干部、分管保密依法行政领导干部和分管业务工作领导干部应履行的保

密工作责任制情况，作为述职不可或缺的部分，作为考核评价的重要内容，真正把履行领导干部保密工作责任制职责、落实监督和被监督责任做到位。

把落实领导干部保密工作责任制的主体责任抓在手上。实行责任制是宪法和法律赋予的重要职责。推进领导干部保密工作责任制落实是坚持依法行政、推进依法治密的重要体现，必须紧紧抓在手上，确立良性的责任导向，做到不放手、手不松，抓领导、领导抓，抓具体、具体抓，决不能有任何敷衍塞责和被动应付。无论是负总责的主要领导，还是负直接责任的分管领导，对保密依法行政工作都必须握紧拳头、夯实抓手，对“三大管理”等重点工作亲自抓部署、信息公开和行政审批等重大问题亲自抓落实、监督检查和“双随机”抽查中的重要环节亲自抓协调、领导批示和群众举报的重特大案件亲自抓督办。尤其要抓好重点领域区域、重要部位岗位、关键环节细节的保密行政行为的监督检查，使压力层层传递、责任层层落实、工作层层到位，在推进领导干部保密工作责任制主体责任落实的同时，切实把保密依法行政的主体责任落到实处，抓出成效。

推进领导干部保密工作责任制落实是坚持依法行政、推进依法治密的重要体现，必须紧紧抓在手上，确立良性的责任导向，做到不放手、手不松，抓领导、领导抓，抓具体、具体抓，决不能有任何敷衍塞责和被动应付。

“关键少数”应履行的主体责任

在保密工作责任制中，领导干部保密工作责任制居于首要位置，这个“关键少数”作为重要或者核心涉密人员，既要严格履行保密义务，又要认真履行对保密依法行政工作的领导和管理职责，真正做到守土有责、负责、尽责，切实推动主体责任深化、细化、实化。为此，应从5个方面履行主体责任。

应履行对保密工作的领导之责。推动保密依法行政各项工作落细落实、落地生根，领导干部必须切实担负起全面组织领导保密工作的责任、具体组织领导保密工作的责任和分管工作范围内的保密工作责任，完整落实领导干部保密工作责任制。既要履行好贯彻落实保密工作方针政策、上级指示、决定及有关保密工作重大部署的责任，又要履行好组织实施国家保密法律法规和规章的责任，更要履行好定期听取情况汇报、提出工作要求、作出决策部署的责任。同时，应当充分发挥保密委员会及其办事机构、职能部门的作用，并主动要求对自己履行领导干部保密工作责任制情况进行监督检查。

应履行带头遵守保密纪律之责。领导干部由于所处工作岗位特殊，知悉和接触的国家秘密事项多、密级高，一旦泄密危害严重。因此，保守党和国家秘密就成为领导干部必须遵守的政治纪律。特别是在当前我国面临的安全环境日趋复杂、安全威胁和挑战更加严峻，各类窃密泄密事件呈高发多发态势，领导干部必须坚决维护、严格执行党的保密纪律和保密规矩，切实增强敌情观念，不断强化保密意识，增强保密自觉，时刻保持高度警惕，自觉抵制各种诱惑，绷紧反奸防谍之弦，以自身的示范作用带动保密法律法规和各项保密规章制度的落实。

应履行学习保密知识技能之责。新形势下，保密工作的专业性、规范性和技术性越来越强，领导干部要履行好担负的保密责任，必须加强对相关知识和技能的学习。建立健全领导干部学法用法制度，把宪法、保密法和相关法律法规及党内保密法规制度等列入领导班子学习内容，利用中心组学习、专题讲座、实训平台等形式学习，了解掌握党和国家保密工作的方针政策，认识把握依法治密工作实践。同时，要学习掌握一定的保密技术，熟悉并认真执行计算机信息系统、通信、办公自动化等方面的知识、规定，通过提高自身保密技能来应对信息化网络化带来的挑战。

应履行自觉接受保密监督检查和考核之责。自觉接受保密监督检查和考核，是对领导干部的保密要求，也是对领导干部的保护和爱护，特别是通过监督检查可以及时发现问题和隐患，及时采取措施堵塞漏洞，防患于未然。对此，领导干部应自觉将保密工作责任制主体责任落实情况纳入领导班子成员综合考核评价内容，既要自觉接受来自上级保密行政管理部门的保密监督检查和考核，又要自觉接受本机关本单位的保密监督检查和考核；既要自觉接受日常的保密监督检查和考核，又要自觉接受专项的保密监督检查和考核；既要自觉开展保密自查自评，又要自觉接受“进驻

式”和“双随机”进行的保密监督检查和考核，以此促使领导干部自觉尽职尽责，不断提高履行保密工作责任制主体责任的能力和水平。

应履行严管亲属子女和身边工作人员之责。这是衡量保密工作责任制主体责任是否落实到位、自身是否过硬的“试金石”。因此，领导干部要在坚持不懈抓班子、带队伍的同时，言传身教，加强对亲属子女和身边工作人员的保密管理，要求他们必须不折不扣地保守国家秘密，一丝不苟地遵守保密法律法规，严肃认真地恪守入党诺言。尤其要针对不同层次、不同对象、不同职级人员的特点，让机关单位按照保密规定进行保密教育和监督管理，切实做到严管严教、严控严防，严遵严做、严束严行，营造安全保密环境，固牢保守秘密底线。

把“严、实、准”作为“关键少数”落实主体责任的重要举措

有责必履、失责必问，这是我们党的基本政治规矩。落实领导干部保密工作责任制的主体责任尤其要在抓严、抓实、抓准上持之以恒、精准发力，严格制度执行，健全工作机制，通过完善相关“责任链”、监督考核“出重拳”、用好追责“撒手锏”，推动主体责任落地生效。

坚持抓严，完善明责履责问责“责任链”。形成横向到边、纵向到底的责任链条，是实现领导干部保密工作责任制落地的内在要求。落实这一要求，就要以严肃的态度、严格的标准、严厉的举措、严明的纪律保障主体责任落到实处。一是在明责上体现严的要求。严格落实属地管理、分级负责和谁主管谁负责原则，对领导干部保密工作责任制的主体责任列明清单，细化操作，形成自上而下一级抓一级、一级对一级负责的责任体系。二是在履责上体现严的分量。对领导干部履行保密工作责任制的主体责任实行动态管理，将责任目标从目标任务、工作措施等方面进行分解量化，通过区分保密责任事项、落实责任单位和责任人，确保主体责任落实到位。三是在问责上体现严的精细。以哪个领导需要在哪些问题上承担什么责任为主题，对落实领导干部保密工作责任制如何问责、谁来问责、问什么责、问责程度等列清具体标准，防止问责无的放矢，“空挡空转”。

落实领导干部保密工作责任制的主体责任尤其要在抓严、抓实、抓准上持之以恒、精准发力，严格制度执行，健全工作机制，通过完善相关“责任链”、监督考核“出重拳”、用好追责“撒手锏”，推动主体责任落地生效。

努力抓实，坚持在督促考核上“出重拳”。加强督促考核，是推动领导干部保密工作责任制主体责任落实的有效抓手。为此，应在“督实”“考准”上下功夫。“督实”，就是要按照《党政领导干部保密工作责任制规定》要求，对领导干部未履行保密工作职责或履行职责不力，致使职责范围内存在泄密隐患、发生严重保密违规行为或泄密案件的，应进行约谈、责令作出书面检查、进行通报批评或组织处理等。“考准”，就是要将领导干部履行保密工作责任制情况纳入年度考评和考核事项，建立健全考评体系和考核机制，明确考核内容、方法、程序、步骤，推动考核工作规范化、常态化。对认真履行保密工作责任制主体责任，在保守、保护国家秘密方面成绩显著的领导干部，依照有关规定予以表彰或者奖励；对因违反保密工作职责受到党纪政纪处分的领导干部，在影响期内不得提拔使用，切实强化结果运用。

切实抓准，努力用好责任追究“撒手锏”。严格责任追究，是倒逼领导干部保密工作责任制主体责任落实的关键一招。不讲责任，不追究责任，再好的制度也会成为“稻草人”。因此，必须坚持有错必纠、有责必追，特别是对那些不认真落实领导干部保密工作责任制主体责任，疏于保密管理或在保密工作方面失职的，更要强化刚性追责，既追失职渎职，也查怠政懒政；既追为官不为，也查为官慢为。像抓其他责任制落实一样，领导干部保密工作责任制也要实行“一责双追”“一案双查”，除了严肃追责、查处当事人外，还要对保密工作负总责的“一把手”和直接分管的负责人进行责任倒追倒查，硬起手腕追究追查，真正把落实领导干部保密工作责任制主体责任的规矩立起来、树起来、挺起来，确保铁规发力、制度发威。■

（本系列谈七篇文章连载结束，谢谢关注。）

网络安全问题已经成为需要全人类共同面对的严峻挑战，其中，网络空间军事化是最大的隐患。军备竞赛、武器失控、网络攻击扩散等，将会给网络空间以及人类生活造成严重危害。网络安全管控是维护网络空间和平的有效途径，这需要世界各国携手共进，“兴天下之利，除天下之害”，共同经营好网络空间这一人类共同营建的“家园”。

网络安全管控应携手共进，铸剑为犁

□杨 建

放眼全世界的网络空间，既有欣欣向荣，也有暗流涌动，安全问题始终是人类挥之不去的梦魇，不知道是否会愈演愈烈，也不知道下一次网络攻击将以何种方式、在何时何地发生。个别国家不遗余力地推进网络空间军事化，研制并运用各种网络空间武器装备，暗地里进行网络入侵、窃密、监听，这些都背离了“更好地发展和运用网络空间”的方向，也不符合当前人类和平与发展的时代主题。

网络安全管控是保持网络空间安宁祥和的最佳途径，也是避免由于网络空间军备竞赛引发战争冲突、祸及民众百姓的重要基础。在这个问题上，世界各国都不能置身事外、独善其身，应当携手共进、铸剑为犁，共同耕耘这片希望的“土地”。

毋以穷兵黩武为快

网络空间是一个人造的虚拟空间，美国是其发源地，从诞生至今已有几十年时间。正是有了世界各国人民的广泛参与，网络技术才得以迅速发展、不断丰富。随着我们对网络空间的依赖性越来越强，有的国家逐渐发现了网络手段对军队提升作战能力的巨大作用，也发现了如果利用先进的科技手段获取对手国家网络数据信息、扼住网络资源命脉、影响网络舆论，将收获巨大的政治、军事、经济效益。因此，以美国为首的西方国家大力推进网络空间军事化，组建网络空间作战力量，装备网络空间作战武器系统，谋求网络空间的军事优势和霸权能力。

有关国家加强网络空间对

抗之后，人类的网络空间变得安全了吗？答案是否定的。近年来，网络攻击、窃密、欺诈、煽动等违法犯罪行为有增无减，呈持续上升的趋势，跨网攻击、跨国攻击等接连不断，运用的手段和技术越来越高超，给包括我国在内的相关国家造成的损失也越来越大。应该说，最具破坏力的还是国家主导下的网络空间作战力量。网络空间武器种类广泛、数量繁多，攻击目标既包括有关国家政府、军队重要系统，也包括大量关键基础设施网络。关键基础设施网络通常是社会正常运行所必须依赖的大型网络，如能源、交通、金融、通信等网络系统。因此，美国专门研发了“震网”“火焰”“毒区”等病毒，在渗透对方网络、攻击窃密的同时，对关键基础设施网络目标实施精确攻击，收效很好。恰恰是这些针对关键基础设施网络的病毒武器，很可能会给人类造成骇人听闻的袭击或灾难。

兵者，不祥之器

网络武器与其他尖端武器装备一样，都具有非常高的制造难度，一般人很难完成针对一个庞大复杂网络系统的攻击武器。但是，具有国家背景的军队部门，往往可以集中网络领域高端人才，耗费大量物力财力来完成。在这些武器成功运用的同时，我们还应当看到其不可控性可能造成的危害。

在美国掀起网络空间军备竞赛，相关国家积极推进网络空间军事化的同时，我们不能不感到阵阵隐忧。一方面，网络空间作战作为一种新型作战样式，可能在未来国家之间冲突对抗中走上战场，除了对军政网络系统进行攻击之外，还会攻击敌对方国家关键基础设施网络，破坏其战争支撑体系，从而达到作战目的。这种网络攻击必然危及广大人民群众，破坏社会正常生活，甚至产生人道主义灾难。另一方面，有关国家争相研制和使用网络武器，将导致这种破坏力巨大的武器进一步扩散，增加网络恐怖组织得到此类武器的可能性。

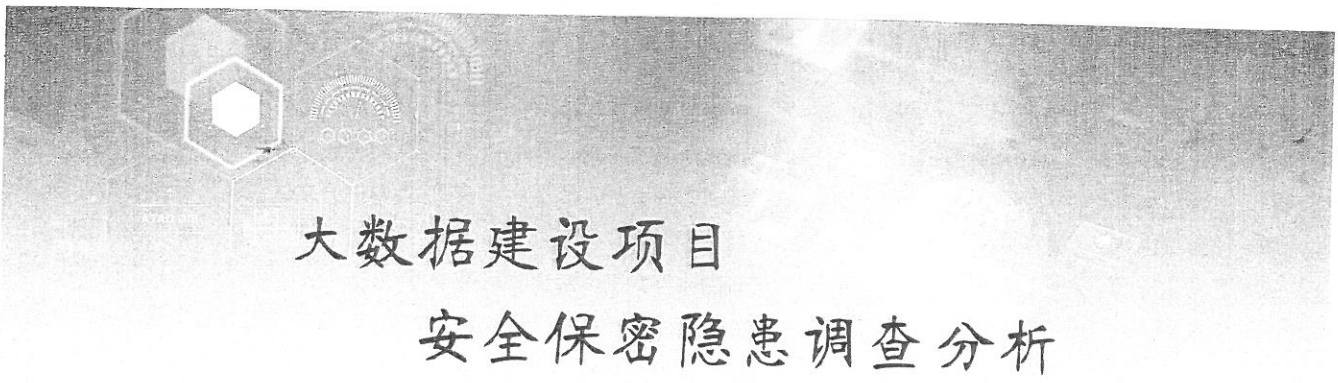
正是看中了网络病毒武器能发动攻击、引起恐慌、制造轰动效应的特点，网络恐怖组织才会对其兴趣十足。一是网络病毒武器的传播性，很多武器需要通过网络突破、潜伏、渗透等过程，才能达到预定的“作战”位置，在这一过程中有可能被“截获、俘获”，这就给网络恐怖组织获得网络病毒武器提供了途径。二是网络病毒武器的便携性，不像常规武器或核生化武器受到物理空间的严格管控，网络病毒武器只是一种特殊的计算机程序，且体积往往都不大，网络恐怖主义通过“暗网”、虚拟专用网、加密措施等即可交易传递，逃避网络监管。三是网络病毒武器的可修改性，尽管网络恐怖组织掌握不了高深的病毒技术，也无法自主研制病毒武器，但是他们得到某些病毒武器模块后，通过修改部分功能参数，重新设置攻击目标、攻击强度等，就可以形成符合其意图的网络病毒武器。一旦网络恐怖主义获得此类病毒，他们很有可能将目标锁定在能产生“大动静”的重要网络上，这些目标往往是关乎大规模人群的国家基础资源，以及可能造成环境危害、生命财产损失的关键基础设施网络。如果成功实施破坏活动，那么，对国家、社会所造成的冲击可能远远超过恐怖分子以暴力攻击、自杀式袭击等方式产生的效果。

铸剑为犁应有日

通过以上种种事例和迹象，我们可以看出，网络空间军事化所造成的危害或潜在危害巨大，就如同打开了“潘多拉的盒子”，因为一时的贪欲，给世间带来不尽的灾难。

中国人自古以来就爱好和平，力求避免各种类型的战争冲突。早在春秋战国时期，诸子百家就对战争提出了自己的看法，儒家主张以德服人，墨家以其鲜明的态度、系统的论述及坚决的反战实践而成为中国古代和平主义的典型代表，这些都为我们更好地解决网络空间安全问题提供了思想指引。我国接入国际互联网的时间比较晚，在网络空间理论和技术装备等方面与美国等国家相比还存在差距。目前，我国在网络安全方面面临着严峻的挑战，国内网络系统遭受攻击的频次居高不下，但是，我们依然尽最大努力维护网络空间的和平与安全。

2015年12月，习近平主席提出世界各国“共同构建网络空间命运共同体”的5点主张，指出网络空间不应成为各国角力的战场，也不能成为违法犯罪的温床，为推进全球互联网治理贡献了中国智慧。2017年3月，我国发布《网络空间国际合作战略》，进一步为国际社会解决网络空间治理难题提出鲜明的中国方案，引起国内外的广泛关注。正如习主席所强调的，“网络安全为人民，网络安全靠人民”。这里的人民不仅仅是我国的公民，更应该是世界各国的人民。只有世界各国共同携起手来，通过开展有效的网络安全管控，让网络核心技术不再成为威胁他人的利器，而成为开启光明、普惠大众的“法宝”，才能真正维护好网络空间的和平与安宁。



大数据建设项目安全保密隐患调查分析

□任凌云 朱宏杰

近年来，大数据、云计算、物联网等现代信息技术风起云涌，受到了各行各业的重视与青睐。不久前，习近平总书记提出实施国家大数据战略，加快建设数字中国。中共中央政治局集体学习时，习总书记深刻分析了我国大数据发展的现状和趋势，并提出要推动大数据技术产业创新发展，构建以数据为关键要素的数字经济，运用大数据提升国家治理现代化水平，促进保障和改善民生，切实保障国家数据安全5方面的要求。

随着大数据热度的攀升，其应用价值和开发潜力也越来越为各领域所重视。目前，全国各地都在积极试水，探索建设社保、医保、公民征信、公安维稳、电子政务云等大数据信息系统和平台，为经济建设、城市管理等各方面提供强大的数据支持。但大数据也是一把“双刃剑”，它不仅意味着海量、多元、迅捷的信息处理，是一种颠覆性的思维方式，一项智能的基础设施，一场创新的技术变革，还是一重全新的安全挑战。

一方面，网络化的体系架构，使大数据更易成为攻击目标，攻击者也许使用相对低的成本就可获得“滚雪球”效益。另一方面，大数据的处理和存储离不开“云”，其运营环境的特殊性突破了传统的网络边界，安全防护手段能否有效跟进，也是一大难题。在国务院印发的《关于促进大数据发展行动纲要》中，安全成为与共享、开放同等重要的关键词之一，可以说没有数据安全，就没有大数据产业发展。笔者所在的保密行政管理部门通过考察调研大数据建设项目，梳理分析出其中的安全保密隐患，以期引起大家的思考与重视。

安全保密隐患分析

调查研究发现，目前大数据项目建设中的安全保密风险表现在以下5个方面。

1.定密及安全保密防护缺乏标准。当前各大数据建设项目中，除个别有明文规定的除外，大多数缺乏定密依据，以及有针对性的安全保密标准，部分建设单位对大数据项目是否涉密，以及该执行何种安全保密标准感到无所适从，甚至有单位认为建设项目不涉密，对高度集中的敏感数据少设防或不设防，导致安全保密隐患横生。而大量有关联性的工作信息汇集后，就很可能引起质变，形成涉密信息，但目前尚缺乏有效的判断依据与标准。据悉，国家有关部门正在研究制定相关规定和措施。但在新的规定和措施出台前，怎样堵上漏洞，在过渡期又如何确保大数据项目系统的安全保密，对管理者和建设者而言都是一项重大考验。

2.不少系统存在使用进口设备的情况。当前在用、在建的大数据或云计算系统中，有的虽然在服务器、交换机等核心硬件及防火墙、入侵检测系统等安全设备上选用了国产产品，但在数据库、虚拟化软件等方面仍然存在使用进口设备的情况，难以排除留有“后门”，或埋藏着“木马”病毒，甚至有可能直接将攻击指令固化在硬件芯片中等情况。如果现有技术手段不能及时检测或预防，未来就很有可能引发针对性的攻击，导致系统瘫痪、数据被窃等严重后果。

3.部分建设项目有外资企业参与。有的外资企业在医疗保险费用核查与控制等方面有较为先进的技术和经验，想以合作为名，在我国寻找落地点，从而参与医疗、保险等领域的大数据建设项目。有的外资企业采取分包、转包、在国内成立分公司等迂回方式，推动与政府机关、企事业单位的合作，这些都应该引起我们的警觉。随着全民社保、医保的深入推进，政府机关、军工企业等重要单位、重要岗位的人员信息逐步纳入其中，外资企业参与相关数据库建设，很有可能接触到其中的敏感信息，相当程度上留有保密安全隐患。

4.人员保密意识不强。这一症结主要表现在大数据项目主导单位保密意识不强，认为项目没有定密就无须考虑保密问题，在建设过程中未咨询当地保密行政管理部门，在并不具有涉密信息系统集成资质的公司中选择承建单位，而后者又缺乏此类高度敏感的信息系统的开发建设经验，在系统安全设计、设备选型、资料保管等方面未充分考虑保密需求，导致问题丛生。

5.安全保密防控把关不严。走访考察中，大部分大数据或云计算系统建设、使用单位能够认识到其中业务数据的敏感性，通过严格的权限分配、资料审查和制度管控，防止无关人员接触敏感数据，但仍有部分单位重视不足、保密审查不严，将系统资料不加区分地提供给承建公司。也有的单位技术防护措施滞后，未能严格采取身份鉴别、访问控制、安全审计、边界安全防护、信息流转控制等安全保密防护手段，致使系统存在漏洞。

对策与建议

1.加快制定相关保密规定与标准。一方面，要加强顶层设计，从国家层面抓紧制定大数据建设项目保密规定与标准，明确相关部门职责分工并建立起协调联动机制。另一方面，针对当前各大数据建设项目中出现的安全保密问题，管理者和建设者要站在国家安全战略的高度，主动作为，在建设过程中及时制定专门方案，采取措施，切实加强安全保密管理。

2.大力推进国产化替代。实施国产化替代是信息安全领域的重要举措，一方面，新建、扩建以及升级换代的大数据建设项目，在设备选型时应尽可能选用国产产品，特别是在操作系统、数据库、虚拟化软件等领域加大国产化替代力度。另一方面，现有的大数据项目还应对所用国外产品进行安全保密风险评估，及时采取防护措施，并在后续升级和维护过程中逐步实现国产化替代。

3.严格承建方背景审查。各大数据项目主导单位在招标阶段就应考虑到这一问题，确保参与竞标的公司没有外资背景，若本单位没有条件开展背景审查，可向当地工商、保密和国家安全部门请求支持协助。对部分特别敏感的大数据系统，应当从具有涉密信息系统集成资质的公司中选择承建方。对已经在建的大数据项目，若发现有外资公司参与，应及时调整更换，无法立即更换的，应对人员、资料、设备等采取严格的保密管理与管控手段，防止敏感资料扩散。在系统后续建设、维护工作中及时更换国内公司进行合作。

4.加强人员保密宣传教育。各大数据项目主导单位应与承建公司签订保密责任书，与项目参与人员签订保密承诺书，明确保密要求与操作规范，并开展针对性的保密教育，使其掌握保密知识，增强保密观念。同时，各级保密行政管理部门应主动掌握当地大数据项目的建设情况，将项目主导单位和承建公司相关人员纳入保密教育范围，通过开展专项培训，提高人员的保密意识和防范技能。

5.强化保密检查指导。各级保密行政管理部门应加强对本地大数据建设项目全流程的保密管理与指导，实行登记备案制，建立各项应急预案，尤其要对技术防范措施、保密制度执行和人员管理情况等进行检查，及时发现风险隐患并提出有效应对措施，确保安全可控。各大数据项目主导单位要加强保密审查，把握“最小”和“必要”原则，向承建公司提供相关资料，避免造成敏感信息和工作秘密的泄露与扩散，同时主动加强与当地保密行政管理部门的联系，及时登记报备项目相关信息，沟通保密管理事项，形成共同参与、合力推进的良好局面。

责任编辑/武 薇

履行保密工作责任制 拒绝“打白条”

□黄长胜

日前，党报刊文批评责任书“打白条”现象：一些地方签了责任书，有的缺考核，有的没问责，引发形式主义和弄虚作假，严重影响整体部署的推进。中办、国办印发的《党政领导干部保密工作责任制规定》（以下简称《规定》），为抓好“关键少数”提供了“尚方宝剑”。然而，不少地方除了开开会、念念文件、发发提醒函外，似乎再无实质性动作。一些保密工作者感慨，雷声大雨点小的老毛病不改，再好的责任制也只能是水中月、镜中花。依笔者之见，构建“抓领导、领导抓”的保密责任机制，应着重念好“敲、推、扪”三字经。

经常“敲”才会上心

保密意识是遵守保密法纪的内心觉醒和内在自觉，是引领领导干部履行保密职责的“总开关”。保密教育提醒要树立问题导向，有的放矢，使守土尽责成为每个领导干部的基本信条。

要力戒“不上心”。有的领导干部没有从落实全面从严治党的政治高度认识保密工作，潜意识里将严守保密规矩、履行保密责任游离于自觉接受党内监督之外；有的抱怨时下各类责任考核应接不暇，自己所分管的工作与保密扯不上关系，讲保密工作责任制有点节外生枝；有的认为相比发展经济第一要务，保密工作不过是小事。对于这些错误认识，应当大喊一声、猛击一掌，用“领导干部始终是境外敌对势力渗透、策反、窃密的重点目标”这一严峻事实，消除其高枕无忧的麻痹思想；用“领导干部保密领地失守如同100-1=0”这一深刻定律，纠正其懈怠心理，切实提高政治定力，增强政治责任，把保密制度、规矩、要求印在脑海中、刻在心坎上。

要力戒“不明白”。少数领导干部平时很少静下心来学习党中央保密工作方针政策、决策部署和保密法律法规，对领导干部应履行哪些保密责任、做不好怎么办、由谁来问责这些强制性规定不甚了解，对信息化条件下泄密风险和保密防范管理基本知识不知不懂，对分管范围内的保密工作现状如何、要求有哪些心中无数，如此“以其昏昏”非但难以“使人昭昭”，甚至还会步入盲人瞎马、临深池而不察的险境。因此，务必要开展针对性、实效性强的保密教育培训，提高领导干部保密素养，使其识大势、知风险，明责任、敢担当，履行好维护国家安全和利益的政治责任。

要力戒“低标准”。有些领导干部认为只要自己不触线、不泄密就算履行了保密责任，至于分管业务中的保密工作问题则懒得过问，

这种只求独善其身，把自己混同于一般群众的做法，是对领导干部保密工作责任制的错误理解，是不担当、不作为的突出表现。应运用典型案例对其进行警示，领导干部无论身居何职，如果对家人、身边人的保密行为管束不力，对眼皮底下的失泄密隐患熟视无睹，真到出了问题的时候恐怕就难辞其咎了。因此，领导干部应把保密工作与业务工作同部署、同落实、同检查，使自己的保密“责任田”隐患穷尽、问题归零。

用力“推”才能担当

考核评价是推动保密工作的“指挥棒”“风向标”，发挥好惩戒机制的强大外力作用，领导干部保密工作责任制这个“牛鼻子”才会显灵。

要真纳入，避免“挂空挡”。据笔者所知，目前述职不述密和考核不纳入的情况比较普遍，领导干部个人述职和民主生活会报告中难觅保密工作方面的表述，领导班子和领导干部年度考核、换届和任前考察过程未见履行保密责任的情况，更遑论听取保密委员会意见，失去考核的责任制无异于一纸空文。各级组织人事部门要按中央要求，严格督促落实述密制度，切实把履行保密责任情况作为领导干部综合评价的重要依据，把“保密工作是硬任务、履行保密责任是硬道理”体现在选人用人机制上。

要真考评，不搞“假把式”。要把《规定》中的原则性要求具体化，结合保密工作重大决策部署、年度保密工作计划，根据主要领导、分管保密工作领导、分管业务工作领导的岗位特点，细化责任清单，明确目标要求，制定考核标准。一些领导干部往往讲起保密工作的重要性慷慨激昂，表起决心信誓旦旦，但落实工作却落入“一文、二会、三总结”的形式主义窠臼，看到烫手山芋就放手，导致“年年喊落实、年年难落实”，这种口惠实不至、表态不表率的做法是保密工作之大忌。应严格考核标准，改进考核办法，不能简单看材料、听汇报而一锤定音，要注重平常考核和动态考核，防止政绩注水、掩盖问题等弄虚作假行为。此外，考评要奔着“一把手”去。为什么贯彻落实中央关于保密工作决策部署在一些地方行动迟缓，保密机构、编制、人员等“老大难”问题喊了多年未能破冰，领导干部保密工作责任制推进力度层层递减，主要症结在于一些地方主要负责同志没有扑下身子亲力亲为。因此，要把考核镜头对准“一把手”，看看有没有把督促落实保密责任作为抓班子、带队伍的重要内容，看看有没有在总揽全局中为保密工作定好盘子、开好方子，看看有没有为保密部门依法履职撑腰打气、雪中送炭。

要真挂钩，防止“两张皮”。用人导向是最大的导向。考核结果运用要体现在有功必奖、有过必罚上。要把领导干部履行保密责任情况与绩效管理、评优评先、选拔任用、岗位调整挂钩，从根本上改变保密工作是软任务、干好干坏一个样的不良风气，形成主要领导真抓、分管领导真挂帅、其他领导真管的责任机制。

动真“打”才有敬畏

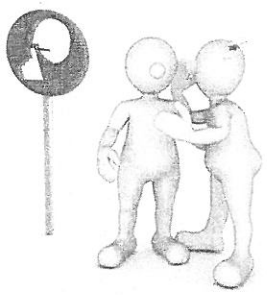
动员千遍，不如问责一次。责任追究发声不发力，等于天天喊“狼来了”，最终导致藐视践踏保密制度的“破窗效应”。

要“点穴式”督查。近年来，保密检查密集度高，投入大量人力和时间，对推动工作落实、强化保密管理的确产生了很大作用，但检查中对领导干部保密工作责任制落实情况却似乎很少涉及，这不能不说是一大不足，个中原因值得反思。要通过多种形式对领导干部保密工作责任制落实情况严督实查，聚焦短板，对症施策，削除盲区和死角。对工作薄弱的地方和单位实行“点穴式”督导，排除阻力，打通关节，用挂账销号的办法倒逼整改。

要“甩石子”警示。选择若干单位开展领导干部履行保密工作责任制情况点评，不留情面指出问题，直截了当提出要求，让那些落实不力者坐不住、冒虚汗。对一些典型问题在一定范围内曝光，对广大领导干部产生心灵冲击和思想触动，达到警示效应。

要“亮利器”震慑。问责到底、敢于碰硬，《规定》中的强制性要求才有“钢牙利齿”之威。对那些有规不依、有令不行、有禁不止的，对那些推动、落实不力导致职责范围内保密工作亮红牌的，该约谈的约谈，该通报批评的通报批评。实行一案双查，既追究泄密或严重违规当事人的直接责任，又追究主管领导的保密主体责任。特别对造成严重后果的，组织人事部门要及时将其调离领导岗位，依照党纪政纪进行严肃处理，真正使失责必问、问责必严成为常态，让那些无视保密规矩者害怕，不抓不管保密工作者后悔。

责任编辑/徐 琛



依照保密法规定，在私人交往和通信中涉及国家秘密，应当依法给予处分；构成犯罪的，要依法追究刑事责任。但在具体实践中，此类情况仍时有发生，部分机关单位工作人员利用职务便利或职务提供的环境，忽视保密法纪，在私人交往和通信中故意传递国家秘密，严重危害国家秘密安全。

私人交往忌传国家秘密

□锦泽庭

典型案例

一、为向妻子表忠心泄密

案例1：2015年12月，A市某机关工作人员王某被借调至位于B市的上级主管机关工作。但两市相距较远，王某只能与妻子李某两地生活。借调期间，王某业务工作繁重，加之离家较远，对李某照顾难免不够，导致两人矛盾不断。12月23日，李某给王某打电话，称其特意请好了假，想趁圣诞节和元旦期间来B市和王某团聚。很是不巧，恰逢王某这几天有重要任务，需要连续值班，根本无法陪伴李某，就让李某不要过来。李某一听就急了，认为王某可能有了外遇，说什么都要去B市看个究竟。王某反复劝说无效，正好手里有1份刚刚接到的机密级文件，便用手机偷拍了文件全文后用微信发给李某，以证明自己确有工作安排，并未出轨。李某看到照片后，知道了文件内容，觉得“奇货可居”，为向朋友炫耀，将其转发给张某，张某又将其上传到自己的网络博客，导致大范围泄密。事件发生后，有关部门给予王某党内严重警告、行政撤职处分。

本案中，涉密文件不仅成了王某向妻子表忠心、确认没出轨的“证明信”，还成了李某、张某向他人炫耀、满足自己虚荣心的工具。

二、为向亲姐传消息泄密

案例2：2015年11月，C市某司法机关工作人员茅某到机要秘书蔚某的办公室送还公章印模时，看到办公桌上有1份已拆封准备传阅的机密级文件。该文件与某重点案件的处理意见有关。茅某的亲姐茅某某，正是该案件的受害人之一，为此精神极度抑郁，茅某这段时间可没少安慰她。茅某觉得，茅某某作为该案的受害人，并非无关人员，知道一些内部信息，应该不能算泄密；况且，茅某某知道之后，也能早吃“定心丸”，免得胡思乱想。于是，茅某趁蔚某不备时，私自用手机偷拍了该机密级文件的首页后通过微信发给了茅某某。茅某某看到图片后大喜，觉得这是好事，应该让所有的受害人都知道，便将图片发布到该案件受害人的微信群中，导致大范围泄密。事件发生后，有关单位给予茅某党内警告和行政记过处分，给予茅某某党内严重警告和行政记大过处分。

本案中，涉密文件成了茅某向其姐茅某某传递消息的“鸡毛信”，抱着“受害人不是无关人员”的想法踩了红线。茅某某则认为好消息应该分享，忽略了涉密文件的核心属性。

三、为供妻子学习参考泄密

案例3：2017年10月，D市某机关业务科科长陆某，向单位保密员

张某借阅了1份机密级文件供自己学习研究使用。在学习过程中，陆某发现文件中有些思路、观点对妻子的业务工作也会有一定启发，认为“学习参考并非直接使用，问题不大”，便用手机偷拍了文件部分内容后通过微信发给妻子张某。张某收到后也没有向第三人转发。事件发生后，有关部门给予陆某党内警告、行政记过处分，调离原工作岗位；给予陆某主管领导韩某党内警告处分。

本案中，涉密文件成了陆某提供给妻子的“参考书”。诚然，陆某学习的积极性很高，不仅自己积极学习，还想带动妻子一起学习。但是，借阅的涉密文件并非私人财产，岂能随意处置？

四、为向好友讲义气泄密

案例4：2015年12月，E市某事业单位负责人杨某收到上级机关印发的1份机密级工作方案后，当日下午转交某科科长徐某，要求写出方案上报。徐某即安排工作人员周某撰写方案。12月4日，该单位合同制聘用人员王某来到周某办公室，在周某处理该文件时偷看到文件内容，认为该工作方案的内容与其好友余某的利益切身相关。为表现自己讲义气、够朋友，王某趁周某不备时，用手机偷拍了文件内容。12月5日，王某将该文件照片通过手机微信发送给余某。12月6日，余某又通过蓝牙方式传给好友李某，李某又将照片提供给好友苏某翻拍，造成严重泄密。事件发生后，公安机关对王某、余某、李某采取了刑事拘留强制措施，苏某被公安机关采取取保候审强制措施。有关部门对杨某进行约谈；责令徐某作出深刻书面检查，取消年度评优资格，扣罚当月职务津贴；责令周某作出深刻书面检查，取消年度评优资格，并作内部通报批评处理。案件正在后续办理中。

本案中，王某见到涉密文件与好友利益密切相关，不惜铤而走险，用手机偷拍。余某、李某、苏某，一连串的“讲义气、够朋友”，导致知悉范围不断扩大。

深度分析

从上述案例中，我们不难看到，在私人交往和通信中涉及国家秘密，主要呈现出以下特点：

一、责任人员存在认识误区

1. 误区一：涉密文件难以造假，作证明很合适

主要表现为涉案人员为了证明自己所说的情况属实而泄密。涉密文件仅限在一定时间内一定范围的人员知悉，不可能无缘无故的持有，难以造假，在证明力方面的优势是其他材料所无法比拟的，用来作证明很合适。例如，案例1中王某泄密的目的就是为了向妻子证明确实在工作并未出轨。将涉密文件作为证明材料使用，实践中还出现了某机关单位工作人员去上级部门领取涉密文件时，用手机将该文件拍照后传给同事，以证明自己确实不在本单位的情况。

2. 误区二：受害人不是无关人员，不算泄密

主要表现为无视涉密文件知悉范围和保密期限的规定，擅自将合法占有或非法获取的涉密文件内容传播给亲属、好友等利害关系人。这里的利害关系人主要为受害人等将因文件内容而获益的一方，并非因文件内容而利益受损的一方。涉案人员往往会因其与涉密文件内容密切相关而误认为其并非无关人员，自己的行为是为善而非作恶，更不是随意传播、故意泄密。例如，案例2中的茅某为了防止其亲姐茅某某胡思乱想、缓解其抑郁心理而告知文件内容；茅某某觉得好消息应该分享而将涉密文件转发至微信群，均属于这类情况。

3. 误区三：学习参考并非直接使用，问题不大

主要表现为传播对象对涉密文件并没有具体的用途，而只是可能提供某种思路、见解上的参考作用。例如，案例3中的陆某即属于此类情况。相对于案例1、案例2而言，用途更为抽象，作为资料搜集、积累使用更为常见。此外，这

不准在私人交往和通信中泄露国家秘密

类情况往往自己个人使用，即一对一发送、不再转发居多，很少出现广泛传播、大范围泄密的情况，容易给人造成“问题不大”的错觉。

二、责任人员存在主观故意

这种故意可以体现为案例1中王某的“求证明”、李某和张某的“图炫耀”，也可以体现为案例2中茅某为了亲姐不焦虑、茅某某为了其他受害人早分享，还可以体现为案例3中陆某为妻子做参考，以及案例4中王某、余某、李某、苏某的“为朋友、讲义气”，都是突破了涉密文件知悉范围和保密期限的规定，通过自己的行为直接引起泄密后果的发生。究其根本，都是将个人利益凌驾于国家利益之上，为了实现个人目的、证明个人情况而不顾保密纪律，不顾国家秘密安全，把涉密文件当成自己的私有材料，想怎么用就怎么用，想给谁用就给谁用。

三、责任人员存在违规行为

上述案件中，虽然泄露范围有所差异，有的仅限于接收人知晓，有的被上传至微信群分享或个人博客被公开浏览，但无一例外的是，都是由责任人员的违规行为直接或间接导致的。首先，以“点对点”公开传播作为违规行为的发端。案件初始时，责任人往往通过微信等手段“一对一”发送给亲属、朋友，且自以为较为隐蔽、安全，并没有大肆宣扬的故意。再者，从传播渠道来看，微信、蓝牙、QQ、博客等手段成为主流，传播速度快、范围广，补救整改难度大。国家秘密一旦泄露，危害难以估量。第三，从行为方式来看，单一违规行为和复合违规行为并存。有的是合法占有后直接使用微信、蓝牙等单一违规行为泄密，有的是先非法获取偷拍、再使用微信传播等复合违规行为泄密，行为发生均较为隐蔽，难以在源头上及时发现。

对策建议

鉴于上述情况，笔者建议，要杜绝此类问题的发生，必须从以下两个方面想办法、下功夫。

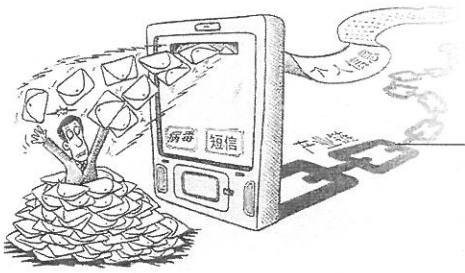
一方面，扭转认识误区。意识决定行为，认识出现了偏差，行为上必然会出问题。加强“两识”教育，必须多管齐下，采取“组合拳”。一是全覆盖。从培训范围看，不仅要加强机关单位正式人员的培训，还要加强对借调、聘用、试用期内人员的培训，后者更要作为培训重点。从培训内容看，要将私人交往不得涉及国家秘密作为培训的重要内容，将“不该问的不问、不该说的不说、不该传的不传、不该留的不留”等各项具体要求从工作中延伸到生活中，切实落到实处。二是深渗透。结合具体文件内容，不仅要明确知悉范围、保密期限等传达要求，还要明确不得私下打听文件内容、不得私自泄露给利害关系人、不得上传至互联网等各类禁止行为，并通过会议传达、保密提醒、问卷调查等多种方式反复强调，确保每一名同志都入脑入心。三是明典型。及时对在私人交往中传递国家秘密的典型案例进行通报，编撰案例警示材料，对将涉密文件当作“证明信”“鸡毛信”“参考书”等错误认识和误发、误传涉密信息等过失行为进行深入剖析，深挖思想根源、排查风险环节、撰写心得体会，确保警钟长鸣，防患于未然。

另一方面，切实加强监管。私人交往中传递国家秘密的存在，必然是涉密文件管理这个源头出了问题，因此要从源头入手，重拳出击。一是加强涉密文件流转管理。加强对涉密文件收发、持有、借阅、保管、回收等各个环节的动态监管，严防文件收发无登记或登记混乱、文件持有肆意上网、文件借阅长期滞留借阅人手中、文件保管不善被偷拍偷录、文件回收不及时等问题的发生，切实堵住漏洞，使私人交往无密可传。明确文件管理责任人，确保各环节记录详细准确，出了问题，随时责任倒查。二是加强办公场所安全管理，特别是保密要害部门部位管理。例如，来访人员区域与涉密文件放置区域隔离，严防偷拍、偷记、偷阅；涉密文件阅读区域不配备连接互联网的计算机，防止随机上传网络；在办公场所适当位置配备视频监控、物品存放柜，阻断泄密渠道等。

责任编辑/孙战国

如今，智能手机已经成为人们工作生活中不可或缺的组成部分。人们在享受全新的舒适便捷体验的同时，也面临着日益突出的信息安全威胁。在当前复杂的安全保密形势下，军人作为智能手机特殊的用户群体，如何加强其使用管理，已经成为军队安全保密工作不容忽视的一个重要问题。

加强顶层设计 破解智能手机管控难题



□吴建军

近年来，随着以移动互联网、物联网、大数据为核心的“互联网+”技术迅猛发展，拍摄录制、信息定位、视频直播、“云端”备份等手机功能逐渐融入官兵日常工作和生活中，为大家获取信息、积累知识、沟通交流带来了诸多便利。我们在充分享受智能手机带来便利的同时，也面临着诸多失泄密隐患。如何有效对智能手机进行管控、严防失泄密事件发生，成为当前各国军队普遍关注的问题。

智能手机是如何泄密的

（一）翻拍涉密文件泄密。这是最常见的泄密方式之一。某些掌握关键信息的人员，用手机翻拍涉密信息，通过微信等即时通信工具传递，极易被别有用心之人利用恶意程序窥视和窃取。即使文件上传后被立即删除，也不能保证万无一失，因为只需利用数据恢复技术便可使其“重现金身”。此外，不少官兵聊天谈论涉军信息时，喜欢用拼音、谐音代替敏感字段，这样做乍一看不知所云，但只要稍微有一点军事常识的人读几遍就能知道其大概意思，也容易引发失泄密事件。

（二）语音传递信息泄密。在我重大演训活动中，曾出现个别人员保密意识淡化，直接通过手机传递涉密信息，被我安全部门截获。目前，美国等军事强国已经建立起覆盖全球的电子监听网络，广泛收集对手的电子情报。最著名的如美国国家安全局建立的“梯队系统”，整个系统动用120颗卫星，在加拿大、新西兰和澳大利亚设置了数十个大型地面接收站，在美国和英国设有两个数据中心。它利用美国的卫星网络，截取移动电话通信的微波信号，在同一时间，可记录数百万个电话的通信信息，然后利用搜寻设备，筛选可能对安全构成威胁的信息。可以说，我们每一次使用手机，都要经过他们的“过滤”。

（三）定位服务泄密。近几年，随着大数据的广泛应用，地标分享日益普及，地理信息安全问题也越来越引人关注。导航、社交、外卖、跑步、旅游、网购……这些我们平日经常使用的各类移动应用，都需要开启或记录位置信息，有的甚至被默认为“开启”状态。官兵在使用外卖软件、户外运动、社交分享等应用时，同样会不经意地暴露自己的位置信息，一旦获得这些数据，经过简单的分析就不难得出诸如营区位置、军事设施地点等重要信息。

（四）视频直播泄密。不法分子通过特殊手段，可以在视频通话中远程获取视频或截图，倘若在装备场、办公室等场所视频聊天，极易造成失泄密。同时，手机在关闭状

态下也可能通过特殊手段被远程唤醒，通过摄像头和麦克风，收集周围环境信息。个别纪律观念不强的官兵着军装进行视频直播和视频通话，不仅存在失泄密隐患，还可能出现军容不整、言语不当等有损军人形象的情况，容易引发涉军舆情。

（五）“云端”备份泄密。用智能手机自带的云备份功能，个人可将相关信息存储到“云端”，既节省存储空间，又便于多平台信息共享和恢复，非常实用快捷，但这种做法也存在很大安全风险。存储在远程服务器上的数据极易被非法浏览、拷贝或篡改，从而造成信息泄露。现实中，有的官兵为了防止通讯录丢失，经常将联系人信息发送到“云端”，有的竟带有联系人职务和军内办公电话号码，失泄密风险极大。同时，微信朋友圈、QQ空间等官兵常用的社交工具也具备一定的存储功能，官兵随意发布涉军图片和视频等，容易被陌生人浏览和下载。

现行的防范措施有哪些

目前，全军各级各单位高度重视智能手机的保密管理，采取多种手段进行防护，主要有以下几种方式。

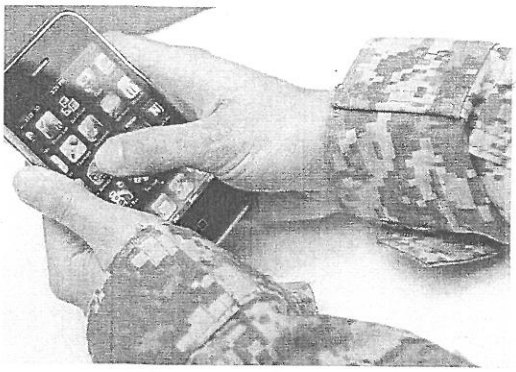
（一）严禁带入手机。常见于指挥机构、战备工程、重大会议会场等重要涉密场所防护。一般通过设置警卫和使用技术手段检测的方式，禁止携带手机入场。该方式杜绝了因使用智能手机造成的失泄密问题，防护效果明显，不足之处是需要投入大量人力物力，只能用于临时任务或重大活动场所，可持续性和操作性不强，无法在全军推广使用。

（二）只能使用指定电话。统一配置只能接打电话和发送短信的手机，智能手机不允许带入办公场所，这是目前使用较广的防护方式，也是解放军保密委员会推荐的方式。该方式可以避免因手机拍照、录音、信息定位、上网等方式造成的泄密，防护效果较好。不足之处是，如果没有配套的严格管控措施，少数人仍会违规将智能手机带入办公区，存在一定的失泄密隐患。

（三）通过技术手段管控。与地方公司合作研发智能手机管控平台，通过技术手段对手机进行管控；或购置手机信号探测器和干扰器，对带入涉密场所的手机进行识别和监测，通报监测结果。该方式能够对违规带入和使用智能手机起到一定威慑作用，防护效果较好。不足之处是需要投入大量的人力物力，且受制于研发力量和技术管理水平，持续性不强，一些单位实行一段时间后都会有不同程度的放松，导致管控效果弱化。

（四）通过规章制度管控。根据军队《保密条例》制定相应的规章制度，对智能手机使用行为进行约束，再结合保密检查对使用智能手机管理情况进行通报。该方式从制度层面对智能手机使用进行规范，如果能够严格执行，防护效果较好。不足之处是缺乏强制手段，对个人要求比较高，如果检查力度不够，则相应的规章制度容易流于形式，起不到应有的防护效果。

上述防护手段对智能手机的使用和管理起到了一定的约束和规范作用，但都存在一些缺点和不足。如管控散，全军各单位各自为战，缺乏统一的顶层设计和战略筹划；层次低，大部分单位研发的管控平台受制于各种主客观因素，导致建立的管控系统防护薄弱，实用性不强。



加强顶层设计和战略统筹

深入破解智能手机管控难题，应认真查找矛盾，分析问题，充分运用军民融合战略思维，立足全军搞好顶层设计和战略筹划。

要从全新角度认识智能手机作用。应从作战角度考虑，充分认识到智能手机是先进科技的产物，要把智能手机等同于武器装备，而不仅仅是一种通信手段。根据美军《联合作战顶层概念：联合部队2020》中描述的全球一体化作战构想，美军计划研发便携的云指挥系统，通过先进的移动网络技术将指挥部与战场“实时连接”，增强指挥官和参谋们了解战局、制订作战计划的能力。该指挥系统就是依托智能手机，不仅能发短信和语音通话，还可以显示周围地形、友军和目标的位置，有地图标注功能。每个士兵携带智能手机产生的数据可以通过部署在附近的战车，实时传输到后方指挥部，让指挥官全面、实时了解战场情况。

要改变管控思路。目前，军用

手机只配发到军以上机关参谋人员和团以上领导干部，占部队主体的基层军官和士兵并未配发，导致军用手机与非保密手机通话时无法对内容进行加密，安全保密防护作用弱化。同时，由于军用手机功能较为单一，在现实中普遍存在同时携带军用手机(或定制手机)和地方手机情况，加大了智能手机管控难度。应改变管控思路，将军用手机作为作战装备配发到每名官兵，作为官兵遂行作战任务的重要组成部分，直接服务于作战，同时避免因携带智能手机导致的管控难题。

要完善现有军用手机功能。军队主管部门应与地方军工企业积极合作，扩展现有军用手机功能，将相关语音、信息、图像和地理位置结合起来，形成战场态势感知系统，用于部队训练、作战、非战争军事行动等场合。在保障安全的情况下与互联网互联，实现地方智能手机的全部功能，个人只需携带军用手机就能满足日常工作生活需要，杜绝私自携带智能手机到办公场所的问题。

要实施军民融合战略集中统管。军用手机应由全军主管部门统一配发，统一号段，统一防护。应充分借鉴国家互联网管理经验，建立全军安全防护中心，在军队通信主管部门和地方电信公司建立两道“防火墙”，统一对军用手机信息进行管控，杜绝各单位单打独斗、分散管理现象。军队要与地方信息安全公司合作，充分借鉴大数据功能，统一为军用手机安装防病毒软件，制定相应防护规则和“黑白名单”，设置关键字，对相关信息进行拦截，做到信息、图像、语音等涉及部队涉密信息无法与地方非涉密部门交换，防止失泄密问题发生。

»延伸阅读

各国政府及军队如何管理智能手机

智能手机问世以来，许多国家和军队将其管理问题上升到国家安全的高度，通过建立健全技术标准、法规制度，加强政府监管，因势利导拓展应用等方式管理智能手机，取得了一定成效。

（一）重视技术标准自主化。外国十分注重智能手机无线接入标准的制定和国际化推广，从源头控制信息失泄密渠道。美国利用其技术优势，抢先注册了手机无线接入标准，并通过大企业联盟垄断技术和产业，进而控制无线接入的话语权。日本、韩国、芬兰等国家的大企业采取加入联盟的方式参与标准制定，进而达到分享标准、技术和话语权的目的。

（二）强化政府依法监管。外国非常注重网络环境下的个人隐私保护，出台了一系列规定。如美国《有效保护隐私权的自律规范》，欧洲《保护自动化处理个人资料公约》，日本《个人信息保护法》。这些法律法规对不法分子起到了相当的威慑作用，有效遏制了手机泄露个人隐私的事件，净化了网络空间。

（三）采用手机实名登记制度。2001年，韩国采取机号一体的手机号码入网登记制，居民购买手机时，电信运营商必须将顾客的身份证号码、住址等信息输入数据库。2008年，英国政府规定，凡购买手机者必须出示护照或其他身份证明，这些信息将存入国家数据库，政府有关部门将通过数据库对英国所有手机用户的通话记录实施监控。

（四）限制特殊人群的手机使用。2007年，驻阿富汗英军下令禁止军人使用手机，所有电话都必须通过安全的军方电话线路。2011年，德国政府明令禁止国家部长级人士和高级公务员使用苹果和黑莓手机，防止恶意软件通过手机感染政府网站。印度、沙特及阿联酋等中东国家也以安全原因为由对黑莓手机下了禁令。

（五）发挥手机军事应用价值。2010年以来，美军意识到智能手机的军事价值，在加强使用管理的同时，注重功能开发，制订了军用智能手机发展计划，并积极开发配套的作战应用系统，将商用智能手机应用推广到战场，使改装后的军用智能手机能够感知战场信息、传递情报、跟踪目标，从而成为战场上士兵的标准配置。美陆军甚至举办“智能手机应用程序大赛”，鼓励军人自行开发手机智能软件，使其充分应用于官兵的日常生活和训练中。■（刘东华）

责任编辑/徐 琛

手机权限管理切莫太随意

——从“支付宝被约谈事件”说开来

□李佳君

今年1月，支付宝（中国）网络技术有限公司、芝麻信用管理有限公司因“支付宝年度账单事件”被国家网信办约谈。此消息一出，立即引起网友和支付宝用户的围观。支付宝方面通过设置极不明显的勾选框及默认勾选设定，不光彩地拿到了收集用户信息的权限，其行为涉嫌侵犯用户隐私且不符合《个人信息安全规范》国家标准的精神，违背了其前不久签署的《个人信息保护倡议》。支付宝方面表示，将认真落实监管部门要求，汲取教训，全面整改。

在互联网时代，放眼众多的手机App，涉嫌侵犯用户隐私的不在少数，因此类问题被约谈的远不止支付宝一家。如百度、今日头条等，也曾因涉嫌或疑似盗取用户通话数据、定位，读取手机联系人，修改系统设置，利用麦克风窃听用户隐私等问题，被有关部门约谈。

移动互联网越来越融入我们生活的方方面面，用户信息就好比一座数据金矿，谁掌握的用户信息越多、越全面、越精细，谁就可能挖掘出更多有价值的信息，创造出更多的利润与财富。假如一个搜索网站把用户经常搜索的关键词收集起来，那么，就可以大致了解这个用户的喜好、需求或关注重点，再通过一定的算法分析，就可得出更精准的信息，从而在广告推广、软件运营、服务质量提升等过程中有的放矢，获得收益。如此，也就解释了为什么我们在日常生活中会遇到一些“奇葩”事件。比如，我们在A网站搜索了一款“水杯”，结果在打开B购物App时，竟弹出了刚才搜索水杯的推送信息。这些便是用户信息对于企业、商家和某些有特殊需求的人的价值所在。相应的，对于用户本人而言，对外提供或暴露的个人信息越多，其所带来的风险隐患也就越多。

在保护个人信息的过程中，我们是否了解手机各项权限的设置和作用，以及各类App的权限请求是否合理？很多智能手机用户在使用手机时，基本没有关注过手机权限管理这一功能，绝大多数用户在安装App时，根本不会去看该App要求用户授权哪些权限，而这些权限又是否真的是该App功能使用过程中的“必需品”。例如，当我们在安装一款运动软件时，它要求提供“读取位置信息”“读取运动数据”“读取已安装应用列表”这些权限时，相信大多数人还可以理解，毕竟这些权限都和用户运动及软件运行有关。然而，如果这个运动软件还要求我们提供读取短（彩）信、发送信息、获取上网记录，甚至启用录音、调用摄像头等权限，那我们就应当警惕了，因为这些权限不是运动软件主要功能运行的必要权限。一旦我们允许其使用这些权限，那么，将意味着这款程序可以任意打开我们的摄像头和麦克风，监视和监听我们的一举一动，甚至知道我们上网都干了些什么，细思极恐。

因此，笔者建议，用户在安装、更新和使用各种App的过程中，要谨慎留心，根据个人的实际需求及软件主要功能来配置权限，尤其是对于“读取手机通讯录”“调用摄像头”“启用录音”“访问上网记录”等涉及个人隐私的“高危”权限时，更要慎之又慎，防止个别软件滥用权限，窃取我们的个人信息和隐私数据。一旦授权了不合理的权限，也要及时更改，无论是哪种手机操作系统，都可在“设置”中找到“应用管理”或“权限管理”选项并进行相应修改。

大数据时代，个人信息的保护不仅关乎自身利益，也可能造成更大范围的影响。我们个人能做的，就是把已知风险防范好，尽可能地保护个人信息安全。

责任编辑/徐 琛

权威解读

开栏的话：党的十八大以来，国家保密行政管理部门站在总体国家安全观的高度，为适应新形势下保密工作转型升级的发展需要，及时出台针对性保密政策措施，积极开展保密法律法规的立改废释，为进一步推动依法治密打下了坚实基础。为准确掌握保密相关政策、法律法规的核心要旨，及时解决保密实践中遇到的难点问题，从2018年起，本刊推出全新栏目——权威解读，邀请相关部门、专业人士就保密工作政策、法律法规进行阐释和解说，突出针对性、指导性、统一性。

对定密管理若干具体问题的认识和理解

□国家保密局政策法规司

2014年《国家秘密定密管理暂行规定》颁布以来，各地区各部门认真执行落实，定密管理规范化水平不断提高，定密工作不断取得新的成效，为打好定密攻坚战奠定了坚实基础。同时，在实践中，也遇到一些具体问题。为更好地执行《国家秘密定密管理暂行规定》，持续推进规范定密，国家保密局政策法规司对具有一定普遍性问题进行了梳理、归纳、总结，并给予明确解答。

一、关于定密授权期限的设定

依法具有定密权的机关单位对承担其涉密科研、生产或者其他涉密任务的机关单位主动授权的，授权期限应当与该涉密科研、生产或者涉密任务的保密期限一致。

对因申请，向经常产生国家秘密事项的机关单位授权的，授权期限根据实际工作需要确定。考虑到保密事项范围定期审核修订、工作形势发展变化等因素，建议此种授权期限一般不超过5年。授权期限即将届满，被授权机关单位仍需获得定密授权的，可以再次向授权机关提出授权申请。

二、关于指定定密责任人的数量

保密法及其实施条例、《国家秘密定密管理暂行规定》对指定定密责任人的职级、数量、权限没有作出限制。根据定密工作最小化、精准化原则，指定定密责任人的数量应当参照本机关、本单位实际产生国家秘密的数量、涉密岗位和涉密人员数量，以实际工作需要为据确定。

原则上，指定定密责任人不必按照机关单位内部管理层级层层设置，数量不宜过多。一般包括机关单位分管涉密业务的负责同志和办公厅（室）负责同志。必要时，业务部门负责同志和其他同志也可以被指定为定密责任人。这样既有利于机关单位建立内部定密工作机制，又有利于推动相关领导同志了解定密工作，切实履行定密责任人职责。承担专业性较强的涉密科研、生产或者涉密任务的单位，可以指定项目组负责同志为定密责任人，确有需要的，也可以指定项目组工作人员为定密责任人。

三、关于定密责任人之间定密权限的区分

法定定密责任人的定密权与所在机关单位的定密权一致。指定定密责任人的定密权由法定定密责任人确定。按照定密工作权责明确的要求，不同定密责任人的定密权限

可以作出区分。一是区分不同密级的定密权。指定定密责任人的定密权可以与法定定密责任人一致，也可以小于法定定密责任人。不同指定定密责任人之间也可以明确不同密级的定密权。二是区分行使定密权的范围。法定定密责任人有权对所在机关单位产生的所有国家秘密事项行使定密权。对指定定密责任人可以限定其行使定密权的范围，要求其在分管工作或者特定工作领域定密。

四、关于多个定密责任人签署同一份涉密文件时的定密责任人认定

机关单位定密应当就定密责任人、承办人等作出书面记录。因此，多个定密责任人签署同一份涉密文件时，在书面记录“定密责任人”一栏签字的人员为相关文件的定密责任人。没有定密书面记录或者书面记录没有特别注明“定密责任人”的，第一个签字的定密责任人视为该文件的定密责任人。后签字的定密责任人对之前签字定密责任人的定密决定作出更改且生效的，作出该更改决定的定密责任人为该文件定密责任人。

五、关于定密程序

按照保密法实施条例和《国家秘密定密管理暂行规定》，定密由承办人提出具体意见，报定密责任人审核批准。这是定密的一般程序。机关单位可以根据实际工作或者公文运转流程需要，增加其他人员（如定密审核人、定密专家等）或者其他程序（如提请定密小组研究），对定密提出意见建议，作为本机关单位内部定密工作程序的一部分。经过其他人员和程序提出的定密意见，供定密责任人作出定密决定时参考，相关事项的定密仍由定密责任人负责。

六、关于保密事项范围内容的类推使用

禁止比照类推是保密事项范围使用的一个基本原则。2017年实施的《保密事项范围制定、修订和使用办法》（国家保密局令2017年第1号）明确规定，机关单位应当严格依据保密事项范围，规范准确定密，不得比照类推、擅自扩大或者缩小国家秘密事项范围。

不得比照类推，主要是指在保密事项范围目录没有明确规定的情况下，不能仅根据事项的相似程度，按照产生层级提高或者降低密级定密。例如，保密事项范围仅就中央一级有关事项作出规定时，产生于省（区、市）或者市（地、州）一级的类似事项不能降低密级定密；保密事项范围仅就全国的某类数据作出规定时，各地方的该类数据不得降低密级定密。

机关单位认为产生的事项保密事项范围没有规定但确需定密的，应当按照《保密事项范围制定、修订和使用办法》第二十七条或者保密法实施条例第十九条规定处理。

七、关于国家秘密事项一览表（细目）

国家秘密事项一览表（细目）是机关单位依据相关保密事项范围，对本机关、本单位可能产生的国家秘密具体事项内容、密级、保密期限（解密条件或者解密时间）、产生部门或者岗位、知悉人员以及载体形式等进行的详细列举。它是对法定定密依据——保密事项范围的具体化，有利于承办人和定密责任人查找定密依据，提高定密“对号入座”的准确率。

机关单位制定国家秘密事项一览表（细目），应当严格遵守保密事项范围使用的要求，不能超越保密事项范围的规定，创设新的国家秘密事项。国家秘密事项一览表（细目）应当经本机关、本单位审定后实施，并报同级保密行政管理部门备案。

八、关于以上级机关单位名义印发涉密文件的定密

公文定密与发文审核的责任一致，由发文机关负责。下级机关单位起草的，以上级机关单位名义印发的涉密文件，由上级机关单位负责定密。但是，起草机关单位应当依法履行“承办人”义务，对起草的涉密文件提出具体定密意见，依法拟定密级、保密期限和知悉范围并规范作出国家秘密标志，报请上级机关单位审核批准。必要时，应当对定密的依据或者理由进行说明，供上级机关单位参考。

同理，对这类文件的变更和解密，也由印发该文件的上级机关单位负责。承担起草工作的机关单位认为所起草的涉密文件符合变更或者解密条件的，应当向上级机关单位提出工作建议，由上级机关单位作出决定。

九、关于涉密文件资料过

程稿定密

过程稿涉及国家秘密的应当定密。根据保密法实施条例，机关单位应当在国家秘密产生的同时，由承办人依据有关保密事项范围拟定密级、保密期限和知悉范围，报定密责任人审核批准，并采取相应的保密措施。从时间上看，国家秘密可能产生于涉密文件资料起草的各个环节。有的文件资料从起草开始就涉及国家秘密，有的在修改之后才涉及国家秘密，有的文件资料过程稿涉密但正式件不涉密。承办人应当根据实际情况，对涉及国家秘密的过程稿依法拟定密级、保密期限和知悉范围，作出国家秘密标志，并采取相应保密管理措施。按照公文处理的一般要求，承办人应当先在过程稿上标注国家秘密标志，待公文送审稿形成后报定密责任人审核批准。定密责任人的定密决定与承办人的拟定密意见不一致的，承办人应当及时对过程稿的国家秘密标志作出相应更改。

十、关于涉密载体收发登记本定密

根据有关保密管理规定，用于记录涉密载体收发、使用、清退、销毁的登记本，应当指定专人妥善保管。鉴于这些登记本一般只是记录涉密文件资料的名称、文号、密级、收发日期等简要信息，不涉及文件资料密点或者核心内容，对这些登记本进行妥善保管，不需定密。如登记本摘录涉密文件资料密点或者相关内容的，应当按照派生定密要求做好定密工作，同时，按照所登记密点或者核心内容的最高密级和最长保密期限标注国家秘密标志，并采取相应保密管理措施。

十一、关于派生定密权限

保密法第十三条第三款规定，机关单位执行上级确定的国家秘密事项，需要定密的，根据所执行的国家秘密的事项密级确定。派生定密是在执行或者办理已定密事项过程中，为继续履行对已定密事项的保密义务而采取的具体保密管理措施，无需定密权。无定密权机关单位可以因执行或者办理已定密事项，派生确定国家秘密。具有较低密级定密权的机关单位可以因执行或者办理较高密级的已定密事项，派生确定超出本机关、本单位定密权限的国家秘密。

十二、关于派生定密程序

派生定密是定密的一种特殊形式，程序上应当遵守定密管理的一般要求。即，机关单位在派生国家秘密产生的同时，应当由承办人依据所执行或者办理的已定密事项拟定密级、保密期限和知悉范围，报定密责任人审核批准。同时，作出书面记录，注明承办人、定密责任人和定密依据，并在相关载体上作出相应的国家秘密标志。

十三、关于派生国家秘密标志

机关单位对执行或者办理已定密事项产生的国家秘密，应当按照该已定密事项确定密级、保密期限和知悉范围，并作出相应国家秘密标志。

已定密事项没有标注保密期限且未作书面通知的，根据《国家秘密定密管理暂行规定》第二十四条第四款规定，该已定密事项的保密期限按照绝密级三十年、机密级二十年、秘密级十年执行，由其派生的国家秘密的保密期限应据此确定，并作出相应标注。机关单位明确知悉该已定密事项保密期限的，或者依据有关保密事项范围可以判断该已定密事项保密期限的，按照所知悉或者规定的保密期限确定并作出标注。

十四、关于落实国家秘密定期审核、年度审核制度

保密法第十九条规定："机关、单位应当定期审核所确定的国家秘密。"《国家秘密定密管理暂行规定》第三十一条规定："机关、单位应当每年对所确定的国家秘密进行审核，有下列情形之一的，及时解密。"

为贯彻落实保密法律法规关于定期审核、年度审核的要求，建议机关单位建立与档案工作、信息公开等工作相结合的解密审核制度。一是可以要求本机关、本单位各部门在对上一年度文件资料进行归档的同时，以及向各级国家档案馆移交涉密档案前，做好涉密文件资料审核工作。对符合解密条件的，及时解密；对已经解密的，作出解密标志；对维持原定密决定的，确保相关国家秘密标志完整、规范；对需要降低密级、延长保密期限或者扩大知悉范围的，做好相应变更工作。二是借助信息化手段，建立机关单位涉密文件资料信息目录和保密期限届满提醒制度，在本机关、本单位定密的涉密文件资料保密期限届满前（建议至少提前三个月），提醒原定密部门进行解密审核。三是根据有关工作部署或者信息公开等实际

需要，及时集中组织开展解密审核工作。特别是对长期积压、保存多年但从未进行审核的涉密文件资料，适时集中组织开展审核工作，实现国家秘密动态化管理。

十五、关于涉密文件资料部分内容解密

涉密文件资料的部分内容符合解密条件，对该部分内容解密确有必要且不影响其他内容继续保密的，可以对该部分内容作解密处理。

对涉密文件资料部分内容解密的，应当履行解密程序，即，由承办人提出部分内容解密，以及不予解密部分的密级和保密期限的意见，报定密责任人审核批准，并作出书面记录。涉密文件资料的部分内容决定公开的，正式公布之日起该部分内容即视为解密。部分内容予以解密但不予公开的，原定密机关单位应当书面通知知悉范围内的机关单位或者人员，告知部分解密和继续保密的内容、日期等。

十六、关于集中印发解密通知

按照保密法律法规规定，机关单位解除国家秘密，应当书面通知知悉范围内的机关单位或者人员。由于各国家秘密事项知悉范围不尽相同，解密应当一事一通知。机关单位根据工作需要集中开展解密工作时，对知悉范围基本相同的文件资料，可以目录形式一并印发解密通知。解密结果可以公开的，机关单位可以通过集中公开发布解密目录的方式，通知知悉范围内的机关单位或者人员。

十七、关于公文的失效、废止与解密

公文失效、废止，是指公文的内容不再具有约束力或者规范作用。公文解密，是指公文内容不再具备关系国家安全和利益的本质属性，不再属于国家秘密。因此，涉密公文宣布失效、废止的，并不等于该涉密公文的内容解密，可能存在公文不再继续有效，但仍需保密的情形。机关单位在开展文件清理工作时，应当将解密工作一并纳入考虑。宣布有关涉密文件失效、废止时，需同时对该文件是否解密作出说明。对需要继续保密的，明确其保密期限，规范作出国家秘密标志，继续作为国家秘密进行保护。

十八、关于解密审核和信息公开保密审查

解密审核是国家秘密提前解密的必经程序，其目的是审查国家秘密是否符合解密条件，能否提前解密。信息公开保密审查是信息公开前的必经程序，其目的是审查拟公开的内容是否涉及国家秘密、商业秘密或者个人隐私等不宜公开的内容。信息公开保密审查范围大于解密审核的范围。

对已解密的事项拟公开的，仍需进行保密审查。《国家秘密定密管理暂行规定》第三十六条明确规定，机关单位对所产生的国家秘密事项，解密之后需要公开的，应当依照信息公开程序进行保密审查。政府信息公开条例等法律法规对信息公开前的保密审查也提出了明确要求。

解密审核程序可与公开前的保密审查程序合并。机关单位拟公开涉密文件资料的，应当同时进行解密审核和保密审查。机关单位对所产生的国家秘密组织开展解密审核时，可以扩大审查范围，一并研究提出有关国家秘密能否解密、解密后能否公开的审查意见。

责任编辑/孙战国

一家之言

从部队转业到地方任职以来，深感保密工作形势的严峻性，保密工作转型升级的必要性、紧迫性。保密工作是党和国家事业的重要组成部分，必须不忘初心，继续前进；承担保密工作必须勇当“冲锋者”，才能一往无前。作为有军人特质的保密工作者，干好保密工作必须做到：脑子里面永远有任务，牢记使命意识；眼睛里面永远有敌情，增强风险意识；肩头之上永远有责任，树立担当意识；胸膛里面永远有激情，坚守热爱与信仰；身体里面永远有劲头，强化执行意识。唯有如此，才能以责任和担当把保密工作抓紧抓实。

——孝感市保密局副局长 乔敬奎

权威解读

严把对外交往与合作提供涉密资料关口

——国家保密局有关负责人就《对外交往与合作提供涉密资料保密管理规定》接受本刊记者专访

□本刊记者 王 婉

对外交往与合作提供涉密资料保密管理是保密工作的一项重要内容。为进一步加强和规范对外提供涉密资料的保密管理，国家保密局于近日印发《对外交往与合作提供涉密资料保密管理规定》（以下简称《规定》）。本刊记者就有关问题，采访了国家保密局有关负责人。

记者：请介绍一下《规定》的制定背景和主要过程。

负责人：随着改革开放的不断深化，特别是“一带一路”战略的实施，我国对外交往与合作的形式、方式和领域不断拓展，各地区、各部门、各行业与境外的经济交往、科技文化交流、学术研讨等日益频繁，加强对外交往与合作保密管理更为重要。《中华人民共和国保守国家秘密法》第三十条规定：机关、单位对外交往与合作中需要提供国家秘密事项的，应当报国务院有关主管部门或者省、自治区、直辖市人民政府有关主管部门批准，并与对方签订保密协议。保密法的规定较为原则，实际工作中需要通过具体法规制度予以落实和细化。之前，对外提供涉密资料保密管理的具体法规依据是1993年印发的《对外经济合作提供资料保密管理暂行规定》（以下简称《暂行规定》），迄今已20多年，一些内容较为陈旧，特别是有些内容与现行保密法规定不一致，已不能适应当前形势和任务需要，亟须修订出台新的规定。

2017年3月，国家保密局启动《暂行规定》修订调研工作，向全国人大常委会办公厅等10个中央国家机关、中国进出口银行等5个中央管理企业和北京市保密局等10个省（区、市）保密行政管理部门进行书面调研。随后，组成调研组赴吉林、上海、江苏、宁夏、新疆等地实地调研，了解对外提供涉密资料保密管理工作情况，就修订工作听取意见建议，在此基础上起草《规定（征求意见稿）》，于7月上旬送各省（区、市）保密局和部分中央国家机关征求意见，并根据各地区和有关部门意见作进一步修改完善。《规定》自2018年1月1日起施行，《暂行规定》同时废止。

记者：《规定》主要包括哪些内容？

负责人：《规定》主要包括以下内容：

一是明确适用范围。机关单位在对外交往与合作中，向境外组织、机构、人员提供涉密资料的保密管理，适用本规定。二是强调工作原则。机关单位对外提供涉密资料应当坚持工作需要、规范审批、严格管理原则，既确保国家秘密安全，又有利于对外交往与合作的顺利进行。三是严格保密审查。明确对外交往与合作项目的主办单位或者其上级机关、业务主管部门负责对外提供资料的保密审查工作，并明确审查依据。四是完善批准制度。根据拟提供资料的密级和涉及范围，明确国务院有关主管部门、中央有关机关及省（区、市）人民政府有关主管部门、省（区、市）有关机关的批准权限。同时，规定机关单位申报和主管部门审批程序。五是严格责任追究。明确擅自对外提供涉密资料，或者擅自扩大对外提供涉密资料范围的，要严格追究有关责任人员的责任。六是设置特殊条款。明确机关单位对外提

供不属于国家秘密但尚未公开的内部资料，可以参照本规定进行审批和管理；国家另有规定或者我国缔结、参加的国际条约另有规定的，依照其规定执行。

记者：《规定》对《暂行规定》有哪些重大调整？

负责人：最大的调整就是进一步依法明确适用范围。一方面，保密法关于对外提供资料仅规定了提供“国家秘密事项”的管理要求，而《暂行规定》把对外提供的范围确定为资料，其法律依据不够充分，因此，《规定》将适用范围明确为对外提供“涉密资料”的保密管理。另一方面，《暂行规定》使用“对外经济交往”的限定性表述已不能适应实际需要，《规定》取消了这一表述，将其修改为“对外交往与合作”，既符合工作实际，又与保密法的表述相一致。

记者：《规定》关于审批权限有哪些要求？

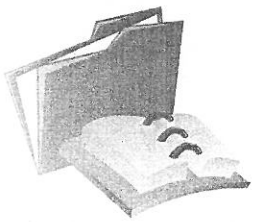
负责人：根据保密法第三十条规定，对外提供涉密资料应当报“国务院有关主管部门或者省、自治区、直辖市人民政府有关主管部门”批准，《规定》据此取消了地、市级主管部门的审批权限。同时，考虑到党委、人大、政协、法院、检察院等系统的工作实际，《规定》明确除政府部门外，中央有关机关和省（区、市）有关机关也具有相应的审批权限。

记者：《规定》对对外提供不属于国家秘密的内部资料有何要求？

负责人：工作中对外提供内部资料的情况较为普遍，考虑到工作秘密、内部敏感信息的管理主体虽然是机关单位，但向境外提供应当审慎对待、严格管理。同时，鉴于目前对内部资料的概念界定和管理要求尚缺乏法律依据，《规定》对此提出原则要求，规定“对外提供不属于国家秘密但尚未公开的内部资料，可以参照本规定进行审批和管理”。

记者：《规定》对审批程序和责任有哪些要求？

负责人：为实现对外提供涉密资料的全过程管理，《规定》进一步细化了机关单位在保密审查、申报审批、签订保密协议等环节的责任要求。同时，明确责任追究的具体情形。对外交往与合作中提供涉密资料既涉及国家秘密，又涉及对外交往，政策性很强，相关机关单位要认真学习领会《规定》的各项要求，加强对外提供涉密资料的保密管理，完善有关保密管理措施，实践中严格履行规定程序，落实责任要求，确保《规定》的各项制度措施落到实处。



保密知识小测试

判断题

1.一般而言，国家秘密“谁确定，谁变更，谁解除”。国家秘密的变更应当由该国家秘密确定的主体负责。同时，保密法规定，国家秘密的密级、保密期限和知悉范围的变更，由原定密机关单位决定，也可以由其上级机关决定。上级机关有权直接变更下级机关单位确定的国家秘密。（ ）

2.不属于本机关、本单位确定的国家秘密事项，认为需要对其密级、保密期限和知悉范围进行变更的，可以向原定密机关单位或者其上级机关提出建议，也可以直接予以变更。（ ）

3.为了切实履行定期审核职责，实现国家秘密事项动态管理，机关单位保密办应当定期组织开展国家秘密审核工作，组织定密责任人对本机关、本单位已确定的国家秘密事项定期进行审查，以便对需要变更的国家秘密事项及时作出变更决定。（ ）

4.机关单位变更国家秘密的密级、保密期限或者知悉范围的，应当书面通知知悉范围内的机关单位或者人员。有关机关单位或者人员接到通知后，应当在国家秘密标志附近标明变更后的密级、保密期限和知悉范围；也可以不作出标志标明变更后的密级、保密期限和知悉范围，而以通知的形式告知机关单位的有关人员。（ ）

（答案见本期）

谨防“微生活”变身“危生活”

□沈霞民

作为当下最有活力的网络力量之一，微信已经潜移默化地融入广大官兵的工作生活，其简单、快捷、高效的通信方式，强大的软件功能，吸引了不少年轻官兵。有了微信，日常生活方便了，娱乐内容丰富了，人与人之间的距离更近了。工作之余，打开微信，聊聊近况、发发动态、转转朋友圈，再点上几个“赞”，这已成为青年官兵的生活常态。

然而，网络泄密风险无处不在，近年来，微信泄密事件时有发生，上传军服照、截图转发、拍摄小视频等行为，都可能造成军事秘密泄露。

◎微信可以“摇一摇”，但理想信念不能“摇”。当下正值军队规模结构和力量编成改革期间，有关军改的言论层出不穷，我们要正确看待问题、理性分析观点，做到政治立场坚定，不随意、盲目评论、转发、跟帖。朋友圈中的动态真假难辨，尤其个别别有用心之人歪曲事实、混淆视听，利用微信造谣。因此，我们应当擦亮双眼，对“微谣言”不听、不信、不传。

◎微信可以“晒一晒”，但军事秘密不能“晒”。“三军之事，莫重于密”，军事信息始终是必争、必守、必保之重地。朋友圈中可谓“处处都有闪光灯、人人都是发言人”，每个人都可以晾晒自己的喜怒哀乐。因此，我们要自觉守住底线，明确什么能“晒”，什么不能“晒”，绝不能将部队生活、涉军信息公之于“网”，成为敌特分子的信息员。

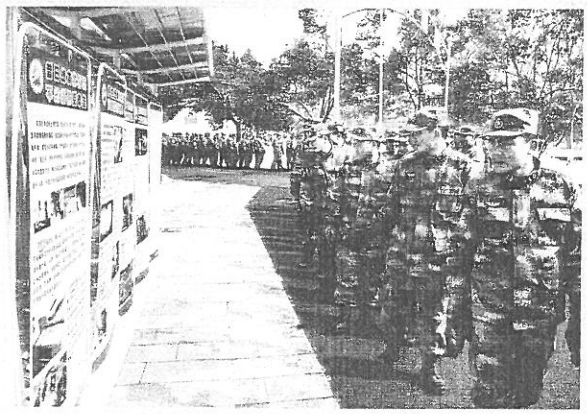
◎微信可以“扫一扫”，但保密意识不能“少”。只有在思想上树立牢固的保密意识，行动上才不会失去底线，才能从根源上减少失泄密事件的发生。要始终居安思危，警钟长鸣，严防网络泄密，严格遵守《手机使用“十个严禁”》《军人使用微信“十不准”》，给自己的网上言行自觉“加密”，真正做到上网不涉密，涉密不上网。

在微信设置中，少一些“允许”，自然多一些“安全”；在微信使用上，要从管好自身向相互监督迈进，真正成为微信的主人。在安全保密的前提下，做到“微”而有度，“微”不失范，“微”我所用。微信改变了人们的沟通交流方式，但不变的是军人的本质。我们要时刻提高自我防范意识，守住心中保密底线。■

责任编辑/徐 琛

73047部队：组织观看保密警示教育图片展

如今，智能手机在部队已广泛普及，成为官兵网上学习的第二课堂。为了防止智能手机失泄密事件发生，近期，73047部队通过图片、漫画以及案例展示和文字剖析，展示了最新的失泄密警示案例，以案施教，以案释法，增强了保密宣传教育的针对性和实效性，收到了较好效果。（图文/徐剑云）



[保密法律责任的基本形式有哪些]

保密法律责任的基本形式包括行政责任和刑事责任。

第一，行政责任。根据保密法第四十八条、第四十九条和第五十一条的规定，保密行政责任包括行政处分和行政处罚两种形式。

一是行政处分。行政处分是指国家行政机关或其他组织依照隶属关系，对违反行政法规的国家公务员或所属人员给予的惩罚措施。行政处分具体包括警告、记过、记大过、降级、撤职、开除等形式，由任免机关或者监察机关具体实施。

二是行政处罚。行政处罚是特定行政主体依法对违反行政管理秩序尚未构成犯罪的行政相对人（即公民、法人或其他组织）给予的行政制裁。根据保密法第五十条的规定，行政处罚的主体不是保密行政管理部门，而是公安机关、国家安全机关和信息产业主管部门，行政处罚的对象是互联网及其他公共信息网络运营商、服务商。

第二，刑事责任。保密法第四十八条规定，违反保密法的行为，情节严重的，应当依法追究刑事责任。

保密法律责任除了上述两种基本形式外，还有一种特殊的情形，即保密法第四十八条第二款所规定的，对尚不构成犯罪，且不适用处分的人员，由保密行政管理部门督促其所在机关单位予以处理。这类人员不属于组织人事和监察机关规定的可以给予行政处分的范围，应依据所在机关单位内部管理规定，或者合同约定条款追究相关责任，具体处理方式包括经济处罚、解聘等。

[追究保密法律责任应注意的几个问题]

对于任何违反国家保密法律法规、危害国家秘密安全的行为，都必须严肃追究法律责任，在具体工作中，应注意把握两个问题。

第一，要严格依法追究责任。

一是防止以批评教育等方式替代行政处分。在追究保密行政法律责任时，对应当给予行政处分的责任人员，必须严格依据公务员法等相关规定追究责任，不允许以其他处理方式代替行政处分。

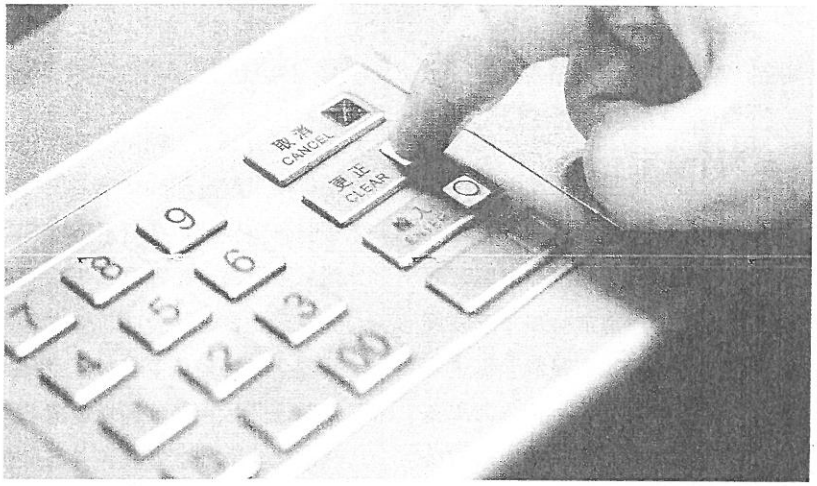
二是防止以行政责任替代刑事责任。在工作中，追究涉嫌构成犯罪的过失泄密的刑事责任往往比较困难，主要原因在于，大多数人认为过失泄密多是在工作中疏忽大意或存在侥幸心理才导致泄密，主观恶意不大，无须采取刑事制裁方式。同时，一些机关单位有法不依，在一定程度上对责任人员包庇纵容。在当前泄密事件呈高发态势下，对构成犯罪的泄密行为，必须依法移送有关司法机关追究刑事责任，决不能以行政责任替代刑事责任。

第二，要切实履行处分监督职责。

为强化对严重违规和泄密责任人员的责任追究，确保法律责任有效落实，保密法第四十七条明确了保密行政管理部门处分监督的职责，规定机关单位对违反保密规定的人员不依法给予处分的，保密行政管理部门应当建议纠正，对拒不纠正的，提请其上一级机关或者监察机关对该机关单位负有责任的领导人员和直接责任人员依法予以处理。

信息安全小百科

ATM机的安全风险与防范



ATM机安全风险案例

近期，国外网络安全专家Brian Krebs发布一份报告，指出黑客利用红外插入式卡槽器针对美国俄克拉荷马城至少4家银行的自动取款机（Automatic Teller Machine，ATM）展开网络攻击活动。

目前，一些单位经常租用商务宾馆举办重要会议活动，很多活动场所设有ATM机，一旦这些ATM机被恶意安装红外插入式卡槽器，所有与会进出人员均可能被拍摄图像并通过无线信号发射出去，有可能造成重要信息被窃取。

ATM机安全风险现状

近年来，ATM机盗窃方式呈现多样化，主要原因是许多ATM机仍在使用过时的操作系统，这类系统无法及时更新安全软件。

网络犯罪分子常使用恶意软件实施攻击。正如上文所述，如今这些网络犯罪分子发现了一个更天衣无缝的感染途径——红外插入式卡槽器，无需插入可移动硬盘，更不会留下指纹和监控录像等证据，ATM机也毫无遭遇物理干预的迹象，但里面的现金却被洗劫一空。安装在偏远地区、隐蔽街道或其他不安全地点的ATM机均面临着这类攻击风险。除此之外，ATM机还存在被不法分子“动手脚”的安全风险，如在插卡口、密码键盘或出钞口安装伪装摄像头、读卡装置等。

ATM机安全风险防范

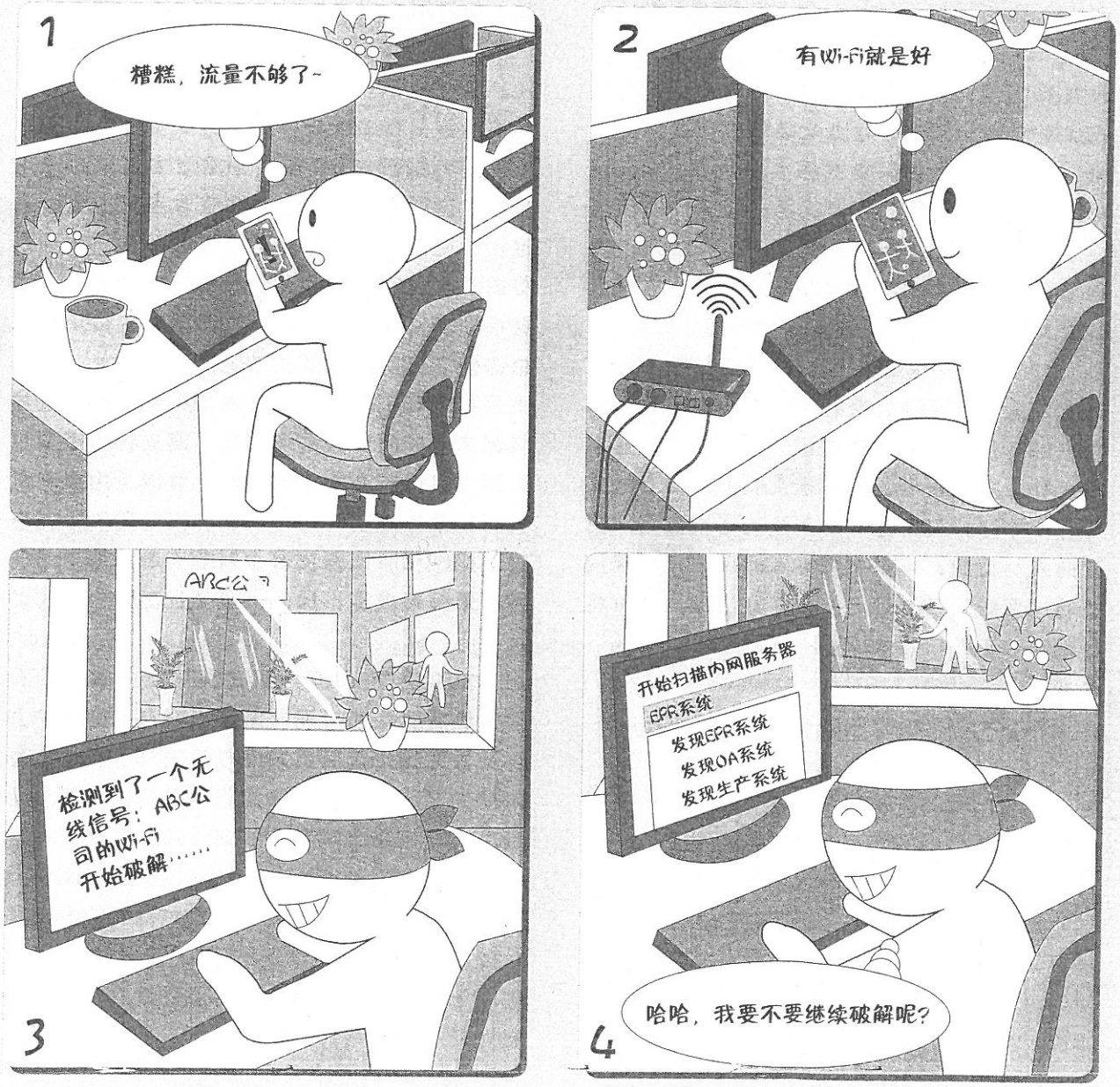
在此，对持卡取款用户给出如下4条防范措施：放置ATM机的房间常常需要刷银行卡才能进入，这时应谨防假冒门禁系统；谨记ATM机在正常吞卡时，会出“吞卡单”，否则可求助银行客服；谨记不要随意丢弃取款回执单，以防泄露银行卡信息；谨记在ATM机上查询、取款时，注意周围有无可疑人员，留心旁边是否有人偷窥，对易被改装的部位，如入卡口、出钞口、隐蔽探头等进行详细检查，特别注意密码键盘是否被改装或被贴上薄膜，在ATM机输入密码时用手或衣物遮挡，以防被偷窥。

简言之，ATM机的安全风险防范主要集中在人防、物防和技防3个方面：人防是提升内部工作人员安全防范意识和持卡用户的自我保护意识；物防是对建筑体本身进行防护，如在ATM机附近安装24小时监控器、门禁监控系统等；技防主要是通过现代化技术手段对ATM机进行安全风险控制管理，如对经常出故障的ATM机进行检测，查看是否有异常无线信号等。END

（康双勇/国家保密科技测评中心）

信息安全意识漫谈——Wi-Fi安全篇

◆ 私搭Wi-Fi热点



◆ 案例解析

无线路由器有较多的安全隐患，比如之前的WEP认证能很轻易被破解。个人架设无线路由器若配置不当，家用时可能导致蹭网或个人资料泄露；在公司使用可能导致内网被入侵，进而导致公司秘密、客户资料泄露，后果不堪设想。

◆ 安全建议

◎ 在办公网络架设无线路由器必须经过公司批准并进行安全检查 ◎ 认证方式使用安全的WPA2算法
◎ 建议隐藏SSID，绑定接入设备的MAC地址 ◎ Wi-Fi密码必须8位以上，包含大小写、数字和标点符号，并定期修改

下期将为您继续介绍信息安全常识，希望您继续关注！ END （绿盟科技供稿）