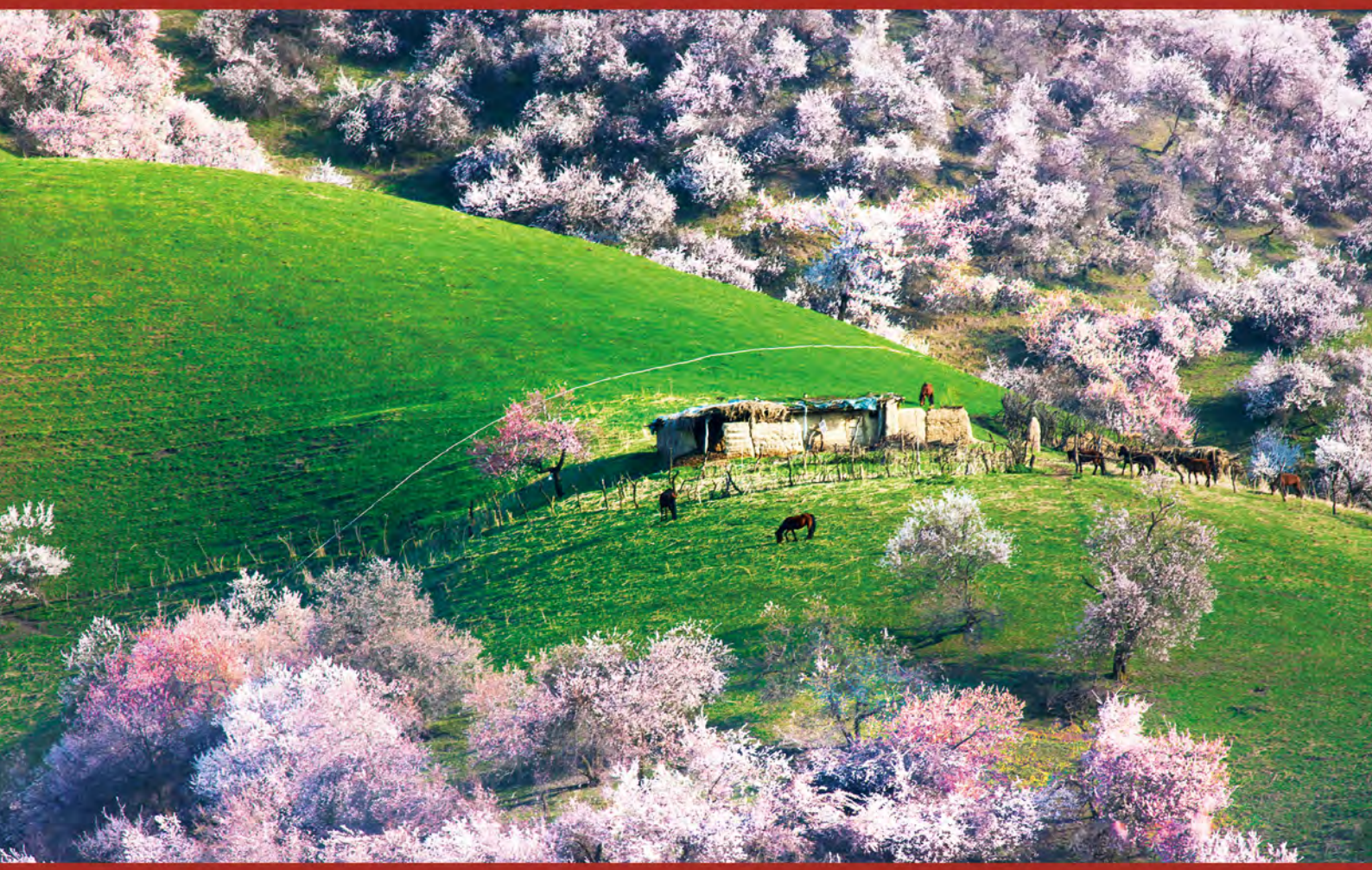
保密工作

2018. 4

国家保密局 主管

www.baomi.org.cn E-mail: bmgz@263.net



- 国务院密集发文，切实加强信息保护
- 本期关注：人工智能与信息安全保密
- 驻守在“第二国境线”上的忠诚卫士

CN11-2785/D

ISSN 1006-5806

本期导读

■ **国务院密集发文，切实加强信息保护** 近日，国务院就科学数据安全、涉及国家安全的知识产权对外转让安全审查、快递业个人信息保护，连续出台《科学数据管理办法》《知识产权对外转让有关工作办法（试行）》《快递暂行条例》3个文件，切实加强信息保护力度。

■ **本期关注：人工智能与信息安全保密** 人类在安然享用人工智能产品的同时，也对其神乎其技表现出无力感，这把双刃剑既带来便利和效率，也带来风险和挑战：它在安全保密领域有哪些应用？它与信息安全有何关系？如何使用它进行情报分析？本期，我们一起关注这些话题。

■ **驻守在“第二国境线”上的忠诚卫士** 北京的东三环，是首都最繁华的商业区之一，使馆区就坐落其间。在这块特别的土地上，驻扎着一支伴随共和国诞生而成长壮大的部队，他们肩负国家使命，代表国家形象，日夜坚守在“第二国境线”上。请看本刊记者来自现场的报道。

■ **大数据格局下的保密、泄密与防范** 去年底，中共中央政治局就实施国家大数据战略进行第二次集体学习。习近平总书记强调，大数据发展日新月异，我们应该审时度势、精心谋划、超前布局、力争主动。大数据时代，对保密工作有何挑战？如何应对？本期，我们一起探讨。

■ **大视野：中国窃取美国知识产权？纯属污蔑！** 连日来，中美贸易纠纷持续发酵，其中，保护知识产权成为美方挑起争端的借口之一。美国依据所谓“301调查”，污蔑中国“窃取”美国知识产权，指责中国“强制”美国企业转让技术。多位专家表示，这些指责纯属诬蔑、毫无事实根据！

声音

从互联网的基本属性和基础性作用出发，判断一个国家是不是网络强国，主要应考虑4条标准：从互联网的技术属性看，是不是网络强国主要取决于对网络信息核心技术的掌握情况；从互联网的工具属性看，是不是网络强国主要取决于对网络信息资源的占有情况；从互联网的经济属性看，是不是网络强国主要取决于数字经济发展情况；从互联网的思想文化属性看，是不是网络强国主要取决于对人类文明进步的贡献情况。

——3月23日《人民日报》，“迈向网络强国建设新时代”，作者谢新洲

开放的时代没有封闭的军营，既然选择拥抱互联网带来的众多便捷，那就要做好准备迎接部队安全管理和保密工作面临的新挑战新问题。其实，只要管理好组织好，互联网这柄双刃剑就能为我所用，成为战斗力的倍增器。要相信信息时代官兵的素质和能力，要相信军队思想政治工作的效率和效力，更要针对可能出现的安全隐患有的放矢开展专题教育，提高官兵自我保护和保守军事秘密的认识，避免对军队和个人造成不必要的损失。

——3月14日《中国青年报》，“‘互联网+军营’的做法值得提倡”，作者房永智

CONTENTS 目录

刊名题字：彭 真

主　　管　国家保密局
主　　办　金城出版社

主　　编　丁　鹏
副 主 编　刘文力
编辑记者　李　杰　满　宁　徐　琛
孙战国　王　娜　武　薇
王　婉　齐　琪
美术编辑　钟　伟　方颖媛　徐穆榕
编辑热线　010-64210050/64210003
010-84254484（传真）
电子邮箱　bmgz@263.net
出版发行　金城出版社
地　　址　北京市朝阳区利泽东二路3号
邮政信箱　北京市1439信箱
邮政编码　100102
定　　价　9.00元

本刊已被如下数据库收录：
CNKI中国知识资源总库
中国学术期刊网络出版总库
中国学术期刊（光盘版）

要 闻

新时代　新征程

本期关注：人工智能与信息安全保密

保密在线

★直　击

★各　地

论　坛

举案说法

强军风采

信息安全

大视野

文 苑

请关注我们

微信保密观 www.baomi.org.cn

发 行
主 管 刘建喜 马名风
电 话 010-64210004/ 64481337
传 真 010-64481202
电子邮箱 bm1439@163.com(发行部)
保密图书 010-84252396(发行部)
传 真 010-64222735

广 告
主 管 王 育
电 话 010-84252396
广告许可证 京朝工商广字第0189号

财 务
电 话 010-64285225
银行户名 金城出版社
开户银行 中国工商银行北京北三环支行
银行账号 0200203319020102604
联名行号 102100020331

印 刷 涿州星河印刷有限公司

国内统一刊号 CN11-2785/D

封面图片：大美中国——新疆伊犁杏花沟
（供稿/视觉中国）

国务院密集发文，切实加强信息保护

［本刊讯］近日，国务院密集发文，就科学数据安全、涉及国家安全的知识产权对外转让安全审查、快递业个人信息保护等，连续出台3个文件，切实加强信息保护力度。

一、《科学数据管理办法》：既要开放又要安全

4月2日，国务院发布《科学数据管理办法》（以下简称《办法》），这是我国第一次在国家层面出台科学数据管理办法，旨在进一步加强和规范科学数据管理，保障科学数据安全，提高开放共享水平，更好地为国家科技创新、经济社会发展和国家安全提供支撑。

《办法》的一大亮点就是突出了科学数据共享利用。按照“开放为常态、不开放为例外”共享理念，明确为公益事业无偿服务的政策导向，充分发挥科学数据的重要作用。《办法》要求科技计划项目产生的科学数据进行强制性汇交，并通过科学数据中心进行规范管理和长期保存。针对科学数据利用率不高的问题，《办法》提出了3项措施：一是实行清单管理制度，由主管部门组织编制科学数据资源目录。二是鼓励科研人员整理形成产权清晰、完整准确、共享价值高的科学数据。三是在数据共享过程中，原则上对公益性事业及公益性科学研究无偿提供，确需收费的应按照规定程序和非营利原则制定合理的收费标准；对商业活动利用数据的通过协商约定。《办法》还提出加强国家科学数据中心培育和建设，明确提出要加强统筹布局，在条件好、资源优势明显的科学数据中心基础上，优化整合形成国家科学数据中心。

对于关注度较高的科学数据的安全保密问题，《办法》始终把确保数据安全放在首要位置，对涉及国家安全和秘密的科学数据如何把握好开放与保密的关系，作了原则性、政策性的规定：科学数据管理必须要以安全可控为前提，按照国家有关法律法规，依法确定科学数据安全等级及开放条件，严格做好科学数据保密工作，建立数据共享和对外交流的安全审查机制。《办法》专门设置“保密与安全”一章明确规定，对涉及国家秘密、国家安全、社会公共利益、商业秘密和个人隐私的科学数据，不得对外开放共享；确需对外开放的，要对利用目的、用户资质、保密条件等进行审查，并严格控制知悉范围。同时，《办法》对主管部门和法人单位的职责作了明确规定，强化了法人单位的主体责任，明确主管部门和法人单位依法确定科学数据的密级及开放条件。针对部分科学数据流出国外的问题，《办法》规定主管部门、法人单位要建立相应的管理制度，确保在国外发表学术论文的作者将支撑论文观点的科学数据汇交到所在单位统一管理。

二、《知识产权对外转让有关工作办法（试行）》：涉及国家安全的知识产权对外转让必须严格审查

3月29日，国务院发布《知识产权对外转让有关工作办法（试行）》（以下简称《办法》），明确了涉及国家安全的知识产权对外转让相关规定。

《办法》规定，对技术出口、外国投资者并购境内企业等活动中涉及国家安全的知识产权对外转让行为进行审查。审查类型包括专利权、集成电路布图设计专有权、计算机软件著作权、植物新品种权等知识产权及其申请权。审查内容包括知识产权对外转让对我国国家安全和重要领域核心关键技术创新发展能力的影响。

《办法》明确了两种审查工作机制。一是对于技术出口中涉及国家安全的知识产权对外转让审查，按照知识产权的不同类型进行归口管理，由相应的国家主管部门按照职责进行审查。二是对于外国投资者并购境内企业安全审查中涉及的知识产权对外转让审查，由相关安全审查机构根据拟转让的知识产权类型，征求国家相关主管部门意见，并按照有关规定作出审查决定。

国家知识产权局保护协调司司长张志成表示，建立完善知识产权对外转让审查机制，是坚持总体国家安全观的重要举措。近年来，我国经济科技快速发展，掌握了一批核心关键技术，拥有了一批质量较高的知识产权，随着知识产权数量的增多，知识产权转让活动日益活跃，其中向国外转让知识产权的情况也逐年增多，2017年，我国知识产权使用费出口额超过40亿美元。

张志成强调，在知识产权对外转让过程中，如果未对涉及国家安全的核心知识产权转让行为进行严格的审查，就有可能影响我国重要领域核心关键技术的自主发展可控性，造成重大经济损失，对培育我国自主创新能力和国际竞争优势将带来重大负面影响。坚持总体国家安全观，统筹发展和安全，完善国家安全制度体系，加强国家安全能力建设，必须对涉及国家安全的知识产权对外转让行为进行严格管理。

三、《快递暂行条例》：加强快递业个人信息保护力度

3月27日，国务院发布《快递暂行条例》（以下简称《条例》），自2018年5月1日起施行，这是我国第一部专门针对快递业的行政法规。

《条例》以促进快递业持续健康发展为重点，规定了一系列保障行业发展的制度措施，制定了一系列安全制度，包括寄件人交寄快件和企业收寄快件应当遵守禁止寄递和限制寄递物品的规定；要贯彻落实法律规定的实名收寄制度，执行收寄验视制度；经营快递业务的企业可以自行或者委托第三方企业对快件进行安全检查等。《条例》完善了快递服务规则，明确各方权利义务，保护消费者合法权益等。

《条例》专门规定用户个人信息保护制度，其中，第三十四条规定，经营快递业务的企业应当建立快递运单及电子数据管理制度，妥善保管用户信息等电子数据，定期销毁快递运单，采取有效技术手段保证用户信息安全。经营快递业务的企业及其从业人员不得出售、泄露或者非法提供快递服务过程中知悉的用户信息。发生或者可能发生用户信息泄露的，经营快递业务的企业应当立即采取补救措施，并向所在地邮政管理部门报告。

《条例》第四十四条还对4种不利于个人信息保护的行为，规定了最高10万元以下的罚款，并可以责令停业整顿直至吊销其快递业务经营许可证的处罚规定：1.未按照规定建立快递运单及电子数据管理制度；2.未定期销毁快递运单；3.出售、泄露或者非法提供快递服务过程中知悉的用户信息；4.发生或者可能发生用户信息泄露的情况，未立即采取补救措施，或者未向所在地邮政管理部门报告。■

各地区各部门认真学习贯彻中央保密委员会全体会议和全国保密工作会议精神(二)

上海 3月8日，上海市召开市委保密委员会全体会议，传达中央保密委员会全体会议精神、市委书记李强近期对保密工作的重要批示。会议要求，全市各级保密组织、保密机构和保密工作者，要将深入学习贯彻习近平新时代中国特色社会主义思想和党的十九大精神，贯彻落实中央和市委关于保密工作的决策部署作为当前全市保密工作的一项重要政治任务，坚持总体国家安全观，在破解保密管理源头性、根本性问题上下功夫，在提高依法治密能力和科技支撑引领水平上下功夫，在推进保密机构队伍建设和体系建设上下功夫。会议强调，一要深入学习贯彻党的十九大精神，把党的十九大精神落实到推进保密工作转型升级各项重点任务之中；二要全面贯彻落实中央和市委关于保密工作的决策部署，为上海保密事业发展提供可靠保证；三要全面推进依法治密，提高全市保密工作法治化水平；四要加快科技创新，引领本市保密工作转型升级；五要夯实保密管理基础，着力提升保密综合防范能力。

江 苏

江苏 3月15日，江苏省委保密委员会召开全体会议，传达学习中央保密委员会全体会议和全国保密工作会议精神，研究部署2018年保密工作。会议指出，党的十八大以来，江苏保密战线深入贯彻落实习近平总书记关于保密工作的重要讲话精神和中央、省委有关决策部署；省委常委会专门对保密工作进行研究，出台有关文件，明确保密工作发展目标、思路和重点；全省保密系统着力健全完善保密工作领导体制机制，不断提升保密科技支撑能力、技术监管能力和服务保障水平。会议强调，2018年是全面贯彻十九大精神的开局之年，全省保密系统要深入学习贯彻习近平新时代中国特色社会主义思想，充分认识保密工作在经济社会发展全局中的重要地位，深刻理解中央和省委关于保密工作的决策部署，积极适应不断发展变化的新形势新任务，着力解决保密管理的源头性、根本性问题，推进保密工作转型升级，努力打造新时代维护党和国家秘密安全的牢固防线。

浙江 3月20日，浙江省召开保密委员会全体会议，传达学习中央保密委员会全体会议和全国保密工作会议精神。会议充分肯定2017年全省保密工作成绩，对做好今年工作提出3点确要求：一是坚持以习近平新时代中国特色社会主义思想为指导，牢牢把握新时代保密工作的新使命新要求，着力破解制约全省保密事业发展的基础性、长期性、关键性问题，推动各项任务落实落地。二是发扬“钉钉子”精神，推进习近平总书记关于加强保

密工作的重要讲话和中央决策部署的贯彻落实，下大力气加强保密机构队伍建设，明确各级保密行政管理部门行政执法主体地位和权限，合理确定机构规格，健全内部组织体系，配齐配强保密干部。三是进一步夯实保密管理基础，抓好精准定密和涉密人员管理，积极稳妥推进解密工作；严格落实依法治密责任，强化对保密工作责任制执行情况的监督考核和追责问责；发挥好保密检查的作用，严肃查处保密违法行为；提高保密科技支撑能力，强化网络保密技术监管，提高保密技术服务和测评能力。

安徽　3月12日，安徽省委保密委员会召开2018年第一次全体会议，深入学习贯彻习近平新时代中国特色社会主义思想和党的十九大精神，传达学习中央保密委员会全体会议和全国保密工作会议精神，总结2017年工作，研究部署2018年任务。会议指出，今年是贯彻落实党的十九大精神的开局之年，是改革开放40周年、全面建设“五大发展”美好安徽的重要一年，全省保密战线要以习近平新时代中国特色社会主义思想为指导，全面学习贯彻党的十九大精神和中央决策部署，以新思想新理念新举措引领保密工作新发展，全面构建新时代维护党和国家秘密安全的牢固防线。会议强调，今年保密工作要着重从3个方面下功夫：一要充分认清严峻复杂形势，切实增强做好新时代保密工作的紧迫感责任感；二要突出重点任务和关键环节，奋力开创新时代保密事业发展新局面；三要加强保密系统党的建设，为做好新时代保密工作提供坚强保证。

湖 南

福建　3月12日，福建省委保密委员会召开2018年全体会议，学习贯彻中央保密委员会全体会议精神，研究审议2018年工作要点。会议指出，2017年全省保密工作紧紧围绕党的十九大精神，认真贯彻落实中央和省委的决策部署，抓主线取得新进展、抓大事展示新作为、抓基础实现新突破、抓队伍迈出新步伐，为服务全省改革发展稳定大局做出了积极贡献。会议要求，要深入学习贯彻习近平新时代中国特色社会主义思想和党的十九大精神，深刻领会新时代保密工作的新要求；坚持底线思维，积极应对新时代保密工作面临的新形势新挑战；突出工作重点，全面提升新时代保密工作的整体水平；加强保密系统党的建设，为做好新时代保密工作提供坚强保证。会议强调，要切实做好今年在福建举办的首届数字中国建设峰会、第五届世界佛教论坛、第十届海峡论坛等重大会议活动的保密工作，确保万无一失。

湖北　3月8日，湖北省委保密委员会召开全体会议，听取2017年全省保密工作情况汇报，审议通过2018年工作要点。会议强调，全省保密系统要把学习贯彻习近平新时代中国特色社会主义思想和党的十九大精神作为首要政治任务，深刻领会精神实质、科学要义和实践要求，牢牢把握政治性这一保密工作根本属性，把“党管保密”作为最高政治原则，同以习近平同志为核心的党中央保持高度一致，进一步强化“四个意识”，坚定“四个自信”，学出使命担当，提高能力水平。会议要求，各级保密委员会要把保密工作放在党和国家工作大局中去谋划、去推进，认真履职尽责，确保党中央决策部署和省委工作要求及时落地见效；保密委员会成员单位要切实抓好本单位、本系统保密管理，切实履行政治责任、组织责任、领导责任和抓落实责任，发挥成员单位职能作用，在基础设施建设、保密队伍建设、重要工程立项、经费保障、干部培养使用等方面给予更大支持，为全省保密工作发展营造良好环境。

湖南　3月5日，湖南召开省委保密委员会全体会议，传达学习党的十八大以来习近平总书记关于保密工作的重要讲话和指示批示精神、中央保密委员会全体会议和

全国保密工作会议精神，审议通过有关文件，研究部署2018年保密工作。省委常委、秘书长、保密委员会主任谢建辉，副省长、省委保密委员会副主任许显辉出席会议并讲话。3月7日，湖南省保密工作会议召开。会议强调，要牢牢牵住保密管理的“牛鼻子”，把国家秘密定准，把涉密人员管住，着力解决保密管理源头性、根本性问题；要大力推进依法治密，完善保密法规制度体系，规范保密行政审批行为；要严格落实《泄密案件查处办法》要求，切实发挥保密检查“利剑”作用；要加强网络安全管理，在总体国家安全战略格局中思考谋划保密工作，推进保密管理体系和能力现代化；要加强保密系统自身建设，打造忠诚、干净、担当的保密工作队伍。

广 东

广东 3月19日，广东省委保密委员会召开全体会议。省委副书记、保密委员会主任、广州市委书记任学锋主持会议并讲话。会议要求，做好新时代保密工作，要立足服务大局，提高政治站位，坚持问题导向，突出工作重点，强化定密和涉密人员管理，严格落实保密工作责任制，加强督查问责。继续开展中央和省委关于保密工作决策部署督查回头看，结合深化党政机构改革，规范保密机构设置，明确行政执法主体地位，健全内部组织体系，充实保密工作力量，推动党中央和省委关于保密工作决策部署不折不扣得到贯彻落实。会议强调，要认真贯彻落实新时代党的建设总要求，以政治建设统领党的建设，加强保密干部专业能力培养力度，持续开展保密系统全员大轮训，持之以恒正风肃纪，努力打造一支忠诚可靠、业务精湛、勇于创新、作风优良的保密干部队伍。

重庆 3月22日，重庆市委保密委员会召开全体会议，传达学习中央保密委员会全体会议和全国保密工作会议精神，审议通过市委保密委员会2018年工作要点及《重庆市重要军事设施周边环境安全保密协商联席会议工作规则》。会议指出，2017年，全市各级保密委员会和保密战线在党委（党组）的坚强领导下，以贯彻落实习近平总书记关于加强保密工作的重要讲话精神和中央关于保密工作的决策部署为主线，按照中央和市委决策部署，抓重点、强弱项、补短板，在法治建设、宣传教育、监督管理、技术服务、队伍建设等方面做了大量卓有成效的工作，为服务保障全市改革发展稳定做出了新贡献，成绩值得肯定。会议就做好2018年工作提出3点要求：一是坚持用习近平新时代中国特色社会主义思想和党的十九大精神武装头脑，切实增强做好新时代保密工作的使命担当；二是深入贯彻落实中央和市委关于保密工作的决策部署，持续推动全市保密工作转型升级；三是认真贯彻新时代党的建设总要求，全面加强保密系统自身建设。

甘肃 3月15日，甘肃省保密工作会议在兰州召开，省委常委、秘书长、保密委员会主任王嘉毅出席会议并讲话。会议指出，做好全省保密工作必须做到“五个结合”：在保密工作大局中要将习近平系列讲话精神与落实中央、省委决策部署结合起来；在保密宣传工作中要将“专业化”与“全覆盖”结合起来；在保密管理工作中要将制度建设与督促检查结合起来；在推进保密工作转型升级中要将科技支撑与基础设施建设结合起来；在推动保密事业发展中要将队伍建设与协同配合结合起来。会议强调，要提高政治站位，深入学习贯彻习近平新时代中国特色社会主义思想和党的十九大精神；要增强忧患意识，深刻认识当前保密工作面临的严峻形势；要强化政治建设，始终坚持党对保密工作的绝对领导；要聚焦重点问题，大力推进落实中央和省委决策部署；要提升自身实力，打造对党绝对忠诚的专业化工作队伍。■

责任编辑/徐 琛

◆人工智能与信息安全保密

人类在人工智能包围中已浑然不觉：在安然享用人工智能产品的同时，也对其神乎其技表现出无力感。人工智能是把双刃剑，既带来便利和效率，又给信息安全保密工作带来极大风险。我们应怎样面对？请看本期专题——

人工智能及其在安全保密领域的应用

□中国科学院信息工程研究所　朱大立

从阿尔法狗说起

2016年或许可以被称作普通大众了解人工智能（Artificial Intelligence, AI）的元年。

2016年3月，谷歌公司DeepMind团队携人工智能围棋程序阿尔法狗横空出世，以4:1击败韩国棋手李世石，进而化身围棋大师在互联网上设下擂台，横扫中日韩众多围棋顶尖选手，无一败绩。2017年5月，阿尔法狗在中国乌镇以3:0战胜中国围棋世界冠军柯洁，赢得了人机大战终极对决。就在全世界围观群众震惊，并好奇这条据说靠人工智能学习了人类所有高手棋谱之后，修炼进阶成绝顶高手的阿尔法狗会不会感到空虚、寂寞、冷的时候，谷歌DeepMind团队再次祭出阿尔法狗的升级版阿尔法元，这个角色更狠，通过左右手互搏对弈，自学自悟勘破围棋无上法门，最终以100:0的绝对优势战胜阿尔法狗。

围棋人机大战事件始于2016年3月。借用围棋术语，这次事件3月布局，年底中盘，转年5月以击败人类最后一个挑战者完美收官。最后在10月份，迎来了整个事件的真正高潮：阿尔法元以一种颠覆性的方式，推翻了人类围棋的经验大厦，人类在围棋领域输得心服口服，最后演变成对人工智能新技术的无比震惊。

借助互联网时代的信息传播，围棋人机大战成为吸引眼球的科技事件之一。从此，人工智能成为搜索中最热的词汇，AI像一股旋风横扫学术界、科技界、新闻界、娱乐业直至普通大众。

人工智能的前世今生

其实，2016年并不是人工智能的开始，计算机也不是第一次在棋类这种智力游戏中战胜人类。

人工智能，依据维基百科的解释是指由人制造出来的机器所表现出来的智能。通常人工智能指通过普通电脑实现的智能，同时也指研究这样的智能系统是否能够实现、以及如何实现的科学领域。AI的核心问题包括推理、知识、规划、学习、交流、感知、移动和操作物体的能力等。

AI的概念来自1956年达特茅斯会议。与会者是最早从事人工智能研究的一批科学家。他们的观点是“学习或者智能的任何其他特性的每一个方面都应能被精确地加以描述，使得机器可以对其进行模拟”。因此，人类可以通过研究实现Artificial Intelligence。从此AI成为本研究领域的统一名称，这次会议也被认为是AI诞生的标志事件。同一时期，计算机科学家图灵提出了人工智能经典测试（亦称图灵测试）：如果一台机器能够与人类展开对话而不能被辨别出其机器身

份，那么称这台机器具有智能。

人工智能概念的提出以及任务的确立催生了该领域几次研究的热潮，从20世纪50年代到90年代，出现了以数理逻辑、搜索式推理、自然语言理解、专家系统、仿生机械运动、神经网络等技术为核心的几次研究高潮，这些技术的进步带动了该领域的发展。但是，以往的人工智能主要在学术和科学领域范围内进行讨论，离普通人很远。由于缺乏落地的应用，加之计算和存储能力有限对算法的制约，都没有形成广泛的社会影响力。

目前的人工智能热潮以深度学习技术为推动，大数据和高速计算两项技术给深度学习插上了翅膀，涌现出大量应用。加之互联网时代信息的快速传播，这次人工智能兴起的影响力远远超过以前。众多大胆的预言家都在讨论，人工智能将带来继工业革命、信息革命之后的第三次人类社会的深刻变革。

人工智能离人类智能还相距很远

在人工智能概念迅速传播的时候，人们充分发挥自己的想象，各种脑洞大开的言论层出不穷。比如，“人工智能将来会统治人类，奇点就要到来，人类面临永生或者灭绝的命运审判”等等。其实目前的人工智能还远远不是人类的智能。

以阿尔法狗为例，其胜利其实是DeepMind团队，以算法驱动计算能力的胜利。在这里算法是关键，计算能力是手段，本质属于人类智力的延伸。人类从计算能力来讲，一败于算盘，二败于计算器，三败于计算机，人类早就一败再败。就像速度跑不过汽车火车，力气比不过发动机，人的计算能力被机器超越并无本质不同，应该说这是人类智慧的伟大胜利。就是下棋这种智力游戏，早在1997年，IBM超级计算机“深蓝”就战胜了国际象棋世界冠军卡斯帕罗夫。这次阿尔法狗的胜利，恐怕谈不上划时代，只是人类不断追求进步的里程碑。谷歌董事长施密特就说无论人机大战的最终结果是什么，赢家都是人类。因为与其说李世石输给阿尔法狗，不如说他输给了谷歌的科学家团队。

DeepMind把围棋的胜负问题，转化为数学模型的最优解求解过程。围棋的19×19的棋盘成为样本存在空间，不同的布局走子作为可能存在的向量样本，利用人工神经网络，深度学习算法，监督学习和增强学习，从人类棋谱开始训练，直到最后脱离人的经验，完全在空间内探索所有样本可能并评估求解，最终成就了围棋上帝阿尔法元的诞生。阿尔法狗还是以人类经验为指导学习的，而阿尔法元已经脱离人类经验，完全凭借强大的运算能力探索围棋世界里人类从未涉及的未知情形和走法，进而完成了对人类在某一特定领域几千年智慧和经验的超越。这是算法设计的重大进步，一方面，说明人类能够探索和感知范围的局限性；另一方面，也指明人类可以借助算法和计算把人类的探索感知空间大大拓展，从而带来人类认识客观世界的再一次飞跃。

尽管如此，阿拉法狗系列也有其自身的局限性，本质还是人类设计好的完成特定任务的工具。没有思维能力，也不会思考。从这个意义上讲，这样优秀的人工智能产品其实和真正的人类智能还有很遥远的距离。这一程序只是个围棋工具，或者说数学工具，只会在围棋空间里计算，它甚至不会意识到自己在下围棋，唯一做的就是计算求解。这和在计算器中输入1+1然后输出等于2从思维角度来看没有本质不同。如果没有科学家团队的介入，这个程序永远不会获得举一反

三、触类旁通的能力。这是一个数学工具，这是算法和计算技术的胜利。

而真正的人类智能除了感知、计算、处理这些技术层面的问题外，还包括自我意识、情感、欲望、情绪之类的生物特征，更别说道德、责任感之类的社会属性。人类对于人类智能核心大脑的研究，还处于起步阶段。所以尽管人工智能已经被舆论炒作成热词，但是现阶段真实的人工智能都是面向特定领域的专用人工智能技术，这些突破性的进展，都属于单点突破或在局部智能水平的单项测试中超越人类智能。但是距离人类智能、机器模拟人类进行思考还相差很远。因此，中国科学院谭铁牛院士说，当前的人工智能系统“有智能没智慧、有智商没情商、会计算不会‘算计’”。

尽管人工智能已经被舆论炒作成热词，但是现阶段真实的人工智能都是面向特定领域的专用人工智能技术，都属于单点突破或在局部智能水平的单项测试中超越人类智能。但是距离人类智能、机器模拟人类进行思考还相差很远。因此，中国科学院谭铁牛院士说当前的人工智能系统“有智能没智慧、有智商没情商、会计算不会‘算计’”。

人工智能时代即将来临

人工智能虽然不像有些人脑洞大开想象得那么夸张，但是人工智能确实是人类面临的一次重大技术变革甚至革命。人工智能时代的到来将开创更高程度的人类社会和科技文明。

人工智能可以解决人类生产、生活、工作、学习各个环节确定性高、重复性强、规则明晰但复杂烦琐、精准度和实时性要求高的各种各样的任务。目前，人类社会面临一些共性的巨大挑战，比如能源、交通、医疗、环境、气象等都有可能通过人工智能来加以解决。以阿尔法狗为例，DeepMind发表声明，他们正在利用类似的技术发现创造性的新方法管理散热，从而降低大规模工业系统能源消耗，这将有可能解决全球环境保护和资源高效利用问题。同时谷歌人工智能团队也在积极参与医院的研究合作，探索在医疗领域应用人工智能技术取得重大突破，进而造福人类。

在我们普通人的身边，具备一定智能的软件硬件也会像雨后春笋一样大量涌现。其实，现在很多App背后都有人工智能技术的影子。以Google Photos为例，现在最新的功能是根据用户相册的内容，自动制作DV，这样的视频短片对个人而言不但贴心而且具有相当水准。很快，家庭机器人、个人智能助理这些有形或无形的人工智能产品，会逐渐走进人们的生活。未来，人和机器会在各种场景中和谐相处，人工智能会带来人类社会又一次文明和科技的飞跃。

安全保密领域人工智能的应用

安全保密领域，以深度学习为基础的人工智能也大有可为，值得期待。

*一是以人脸识别为代表的基于生物特征的身份认证技术。*目前人脸识别技术已经进入实用阶段，智能系统对人脸的识别准确率已经超越人眼。机器通过对大量样本的反复学习和深度训练，可以掌握人类面部的细微特征，识别精度远远高于人类。有些人眼很难判断的情形，比如双胞胎的识别，判别对象不同灯光拍摄效果以及服饰发型的改变，这些都逃不过人工智能明察秋毫的特征鉴别能力。这项技术对于智能安防、海量监测视频事件回溯、涉密人员户籍化管理、保密要害部门部位准入、访客管理等具有重要意义和价值。

*二是基于大数据的窃密监测与保密防护。*面对互联网的海量数据，大数据技术提供了存储和处理机制，加之人工智能技术的应用，完全可以在网络空间形成以人工智能为核心的保密代理程序。这个虚拟的智能保密工作者通过模式训练和学习，熟悉保密工作的基本要素，掌握窃密行为的关键特征，可以7×24小时有效鉴别海量网络用户、数据和行为的异常，做到对涉密信息、涉密用户在网络空间的有效监管与防护。

*三是专家系统智能辅助定密和密级鉴定。*定密和密级鉴定一向是保密领域的热点和难点问题。某一领域的专业信息是否关系国家安全和利益、涉及国家秘

人工智能时代即将来临，这是大势所趋。一切简单重复或烦琐但规则明晰的工作都将被机器所代替。与其担心在机器的竞争面前失去工作被替代，不如顺应时代，寻找新的机遇。面对人工智能，被打败的不是人类，而是人群中因循守旧故步自封的人。这已经被历次技术变革的经验一再证明。

密的判断，既需要对保密管理和相关政策的深刻理解和熟练把握，又需要对该技术领域从整体到细节有行业专家级别的认知。因此，能够准确进行定密和密级鉴定的人员是行业专家和保密管理干部的双重角色，这样的人才少之又少。但是，这项极具挑战性的工作恰恰是机器学习技术的擅长领域。在某一专业范围内，只要把已有的涉密资料文档作为标注数据集对系统的人工神经网络进行训练，并不断反馈校正，最终，系统可以成为该领域的定密专家，对给出的文字、图像、视频材料进行辅助定密判决，当然最终的审核还要人工介入。需要指出的是，计算机在处理定密问题的时候，其实并不真实理解语义内容，现阶段人工智能这样的缺点却带来了保密领域实实在在的好处——不用担心定密人工智能专家系统泄密。

人工智能时代即将来临，这是大势所趋。一切简单重复或烦琐但规则明晰的工作都将被机器所代替。与其担心在机器的竞争面前失去工作被替代，不如顺应时代，寻找新的机遇。面对人工智能，被打败的不是人类，而是人群中因循守旧故步自封的人。这已经被历次技术变革的经验一再证明。

接纳人工智能，人与机器和谐相处，人类社会和人类文明都将进入一个崭新的时代。■

责任编辑/满 宁

◆人工智能与信息安全保密

关于人工智能与信息安全的思考

□中国科学院信息工程研究所 诸焰军 荣文晶 张珠君

关于人工智能

随着社会信息化的飞速发展，一项划时代的技术正在掀起新的技术革命浪潮，那就是人工智能。

自1956年“人工智能”一词第一次出现在达特茅斯会议上，已经过去60多年。在经历了第一阶段的符号主义、第二阶段的数学建模之后，人工智能来到了移动互联网、大数据、超级计算、万物互联为技术基石的信息时代。在算法和计算能力的驱动下，这项曾经只在科幻小说里被人们津津乐道的技术，终于化茧成蝶，第一次真真切切地站在普通大众面前，以阿拉法狗在围棋领域颠覆性的胜利为标志，宣告了信息时代又一次新技术革命的到来。

根据中国电子技术标准化研究院在2018年1月最新发布的《人工智能标准化白皮书》，人工智能被定义为利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。人工智

能通常被划分为弱人工智能和强人工智能两类。弱人工智能是能制造出真正地推理和解决问题的智能机器，但这些机器不具备自主意识；而强人工智能则是让这些智能机器拥有思维能力和自主意识。现阶段的人工智能研究主要集中于弱人工智能，并且已经在计算机视觉、语音识别、自然语言处理、大数据应用和决策系统等方面取得重大突破。但是，关于强人工智能的研究仍处于探索阶段。

人工智能是信息社会的核心技术

当今社会已经进入信息时代。信息社会的主要资源就是信息。这些信息资源及其以大数据、人工智能、云计算和网络通信为主的信息处理技术共同形成信息产业，逐步在经济和社会发展中发挥主导作用。当信息的共享突破时空限制的时候，所有人类高端的生产、生活、学习形态都以信息的获取、存储、处理以及再产生为基本模式。这其中又以信息处理环节为核心。而人工智能技术正是借助算法和计算能力，仿照人脑同时在很多方面超越人脑的信息处理技术，因此人工智能技术将是构成信息社会的核心技术。

鉴于人工智能技术对信息社会的重大推动作用，我国“国家互联网+行动计划”和“十三五”国家科技创新规划均将人工智能作为战略型新兴产业，同时部署了智能制造等国家重点研发计划和专项，对人工智能产业予以大力扶持。在2017年7月国务院发布的《新一代人工智能发展规划》中对人工智能的发展制定了三步走的目标：第一步，到2020年人工智能总体技术和应用与世界先进水平同步，人工智能产业成为新的重要经济增长点；第二步，到2025年人工智能基础理论实现重大突破，人工智能成为带动经济转型的主要动力；第三步，到2030年人工智能理论、技术与应用总体达到世界领先水平，成为世界主要人工智能创新中心。这是国家层面的战略规划，必将得到强有力的推进和实施，

我们正站在又一次技术大变革时代的门口。

工业革命中出现了动力和机器，曾经大量繁重的体力工作被机器所替代，从而大大提高了社会的生产效率。人工智能的出现也将把人们从繁重的脑力劳动中解放出来。人工智能技术是知识和数据双驱动下的产物，随着信息社会中数据的膨胀，人工智能的数据样本趋于丰富，人类的一些规则明确、烦琐单一的脑力劳动直至分析、决策、规划等高端脑力劳动都可以逐步被人工智能所替代。人工智能技术给人类带来的影响，可能远远超过计算机和互联网在过去几十年间给人类世界带来的改变。

人工智能的安全问题

人工智能是信息社会的革命性技术，是智能化的信息社会的核心技术，目前正处于爆炸式发展的初期阶段。但是，正如任何一个事物的出现都有其两面性一样，人工智能的加速发展也已经带来一些实际问题，最为突出的就是信息安全问题。

首先，是人工智能应用带来的安全问题

人工智能具有广泛的应用前景，目前已经涉及制造、农业、物流、金融、商务、家居等行业和领域。伴随着人工智能应用的推广，其安全问题越来越凸显出来。

以目前非常热的智能交通领域为例，很多汽车厂家和互联网公司都推出了无人驾驶汽车以及智能交通系统。在智能交通方面，目前在我国深圳，首批无人驾驶的公交车已成功运行，预示着人工智能技术在决策系统应用上有了重大突破。在人工智能控制交通的时代，指挥交通运行的效率可以达到最优，交通事故率理论上可以趋近于零。但是在已有风险消除的同时，新的风险被引入：曾经驾驶员人为的交通事故可能被智能交通系统的信息安全事故所替代。黑客可以从无线渠道侵入智能汽车终端、从有线渠道侵入后台信息控制系统，从而接管无人驾驶汽车甚至智能交通系统的控制权；也可以破坏自动驾驶系统的信息采集和传输途径，进而诱导终端和后台的智能算法作出错误判断。实际上，无人驾驶汽车或者智能交通系统由复杂的自动化机器和信息系统组成，其信息采集、传输、处理各个要素环节都面临安全风险，目前已有黑客通过盗取移动App账号密码进而控制自动驾驶汽车的案例。

人工智能技术应用于其他领域也同样如此。安全问题最突出的包括工业智能制造、智慧城市管理、智慧医疗、智慧家居等和人们社会生产生活密切相关的领域。由于人工智能处于信息社会的核心层面，控制着大量生产、生活设备、数字化资产乃至社会运转规则，一旦黑

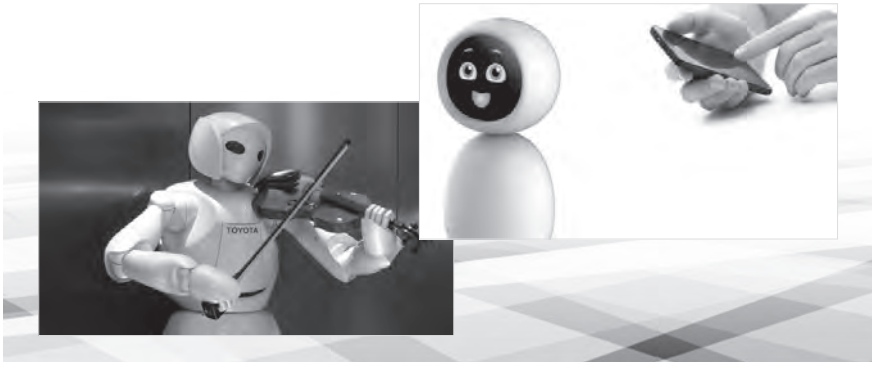
客入侵后台控制系统，技术系统遭到破坏，将带来与其技术重要性相同的破坏力，严重威胁信息系统安全乃至人身安全和社会安全。

其次，人工智能作为一项信息领域的关键技术，其自身也存在一些安全问题

在信息领域，任何代码、算法、开发框架乃至工程实现的软件系统，毫无例外都会存在一定程度的信息安全问题。代码量越大，系统越复杂，往往暴露出的安全问题越多。人工智能领域的专家往往不具备信息安全专业知识，因此，在这项技术的发展过程中，他们专注于实现机器模拟、延伸和扩展人的智能这些核心目标，安全问题往往被当作次要因素加以忽略。目前，安全届已经暴露出人工智能技术自身存在的一些安全漏洞，包括开发框架稳定性、算法设计缺陷、代码自身漏洞等方面。以代码漏洞为例，根据公开报道，国内外安全技术团队曾发现数十个深度学习的软件漏洞，其类型包括内存访问越界、空指针引用、整数溢出、除零异常等常见类型。人工智能技术自身的安全性和健壮性问题会导致人工智能系统出现错误甚至崩溃，或被攻击者利用进行破坏、侵入乃至劫持系统。随着人工智能应用的推广，其自身的安全问题也越来越引起人们关注。

再次，人工智能暴露出人们的隐私保护问题

人工智能技术的普及大大提升了人们生活的便利，但是，也带来了非常严重的隐私保护问题。人工智能技术本身算法的准确率高度依赖于海量用户数据的训练分析，尤其需要获取大量用户个人信息，以便提供个性化、定制化服务，这些都会导致用户个人信息泄露。谷歌DeepMind公司曾与英国NHS医疗服务机构联合开发了一个名为Streams的基于人工智能的手机应用程序，希望能给患者提供更加个性化的智能服务。但是作为医疗服务机构，NHS并没有向患者明确说明他们的医疗信息将被如何使用，也没有询问患者是否同意DeepMind处理自己的医疗数据。它们之间的数据交易被英国信息专员办公室认定为“没有遵守数据保护法案”。从这个案例可以看出，人工智能技术的普及在为人们生活带来便利的同时，存在非常严重的隐私保护问题。实际上，获得生活便利和保护个人隐私，目前已经成为一个两难选择。交出个人隐私和数据，获得个性化、人性化的全方位技术服务，这是人工智能时代的基本模式。不管是无人驾驶、智能管家、数字助理还是机器人保姆，这些人工智能技术和产品能更好为你服务的前提都是全面收集处理你的各种行为数据。小到兴趣、爱好、行为习惯，大到道德、宗教、政治倾向、人生观价值观，人工智能比你自己还要了解你自己。这样一种生活状态不管是拒绝还是欢迎，都会在未来20年左右的时间来到我们身边。技术上为了保护用户的隐私，在采集数据的时候可以对数据集进行模糊处理，使得收集到的海量数据无法和个体用户相对应。这种信息模糊技术从上个世纪就存在，但是其发展速度远远落后于人工智能技术的发展。目前，我们的隐私和个人数据，在大数据和人工智能这些收集、处理和分析技术面前基本上处于裸奔的状态。



人工智能在信息安全领域的应用

人工智能技术在信息安全方面带来的不只是威胁和风险，也对信息安全技术的提升有很大帮助。人工智能在信息安全领域的应用十分广泛，包括生物特征识别、漏洞检测、恶意代码分析等诸多方面。

基于生物特征的身份认证和访问控制是目前人工智能技术应用最成功的信息安全领域。从前制约生物特征识别技术在信息安全领域应用的关键问题是漏报率与误报率达不到实用要求。而利用以深度学习为核心的人工智能技术，科研人员已经将人脸、语音、指纹等等生物特征的识别率大大提升。以人脸识别为例，目前的准确率已经达到99%以上，技术的进步为生物特征识别的应用打下了良好基础。目前，已经有人脸支付等相关产品面世。支付领域的应用涉及社会和金

融安全，在人脸识别的漏报、误报和检测准确率这些指标没有大幅提升的前提下是不可想象的。

在信息安全中尤为重要的漏洞检测技术领域，目前还缺乏高效、准确的漏洞分析自动化技术，很多安全威胁和风险需要专业工作人员的经验作深度的分析和最后的判断。人工智能在处理海量数据方面极具优势，通过对样本的训练可以模拟大量的攻击模式，可以基于人类已有经验也可以抛开人类经验进行全新的样本空间学习和探索，这样的技术解决思路将大大提高漏洞检测的全面性、准确性和时效性。

在恶意代码检测领域也是一样。传统的网络安全技术应急响应速度慢，不能适应恶意代码的迭代进化速度。而人工智能拥有强大的自主学习和数据分析能力，能够加速响应的流程，提升自动化和响应效率，缩短从发现到响应的间隔。这就为提前预知危险，及时预警并处理，将危险扼杀在摇篮中提供了可能，进而大大提高网络安全防御的敏捷性。

人工智能将成为推动我国信息社会变革的创新科技。国务院颁发的《新一代人工智能发展规划》提出，“人工智能在教育、医疗、养老、环境保护、城市运行、司法服务等领域广泛应用，将极大提高公共服务精准化水平，全面提升人民生活品质”。但是，这项技术的发展也会产生冲击法律与社会伦理、侵犯个人隐私、引入新的安全风险等问题。

为最大程度降低人工智能带来的安全风险，应从管理和技术两方面采取一系列应对措施。在管理上展开立法研究、标准制定、监管体系建设，加强对人工智能技术和产品的监管。在技术上，推动大数据时代用户隐私和数据保护技术的研究、提高人工智能技术和产品的内生安全性设计水平、对智能产品和技术应用可能带来的威胁风险进行从监测到应急处置等全安全要素的监控，提高风险控制与处置能力。

我们相信唯有正视问题的存在，在发展技术的同时，重视可能存在的安全风险，在政府层面约束规范，进行良性引导，在技术层面最大程度地规避风险，才能确保人工智能技术在我国安全、可靠、可控地发展。■

责任编辑/满 宁

速读

中国的人工智能当前世界第二，在第一梯队，是世界顶尖水平。为把中国的人工智能世界排位说得更清晰明了，我们可以拿日本做一个比较。

从最具权威的美国人工智能学会的国际会议看，最近3年来，美国和中国发表的成果出现激增。2015年美国的大学和企业发表的成果达到326项（48.4%），中国为138项（20.5%），两国占整体约7成。日本排在第8位，仅为20项（3%）。

很多人把人工智能理解成机器人，认为日本在人工智能上领先。日本机器人技术领先，是硬件的运动能力和精度部分，如果做机械动作是比中国强；但让它识别语音和图片，让它说话、翻译、判考卷，让它做复杂语言认知，和中国的差距就出来了。

以前在国际口语机器翻译评测比赛（IWSLT）中，汉译英项目是日本全球第一，英译汉项目是美国全球第一。2014年11月，中国终结了这个历史：科大讯飞的英译汉和汉译英翻译都是全球第一。

在人工智能上，中国不仅在高端论文数量和国际顶尖比赛中领先日本，而且随着百度、科大讯飞、腾讯、阿里巴巴、华为等企业的AI产品实现落地，已经渗透到国人生活的方方面面。

比如下载e代驾App，即可对司机人脸识别与后台数据库进行比对；公安部已经在酒店试点人脸识别入住；打开支付宝App，和你对话的都是阿里机器人；打开苹果手机Siri，用的是国产语音识别技术；下载讯飞输入法，可以享受世界最高精度的语音转换成文字的服务；打开百度，可以进行语音搜索和图片搜索……

互联网、云计算、大数据和人工智能都是超级新兴产业，中国弯道超车冲到最前列，而日本还在原地发呆。■

◆人工智能与信息安全保密

人工智能与情报收集分析

□席彩云 邓胜利 郑 晗

人工智能是引领未来的战略性技术，世界上一些主要发达国家把发展人工智能作为提升国家竞争力、维护国家安全的重大战略。随着互联网的普及和飞速发展，人工智能渐渐成为国际竞争的新焦点，将深刻影响情报收集分析能力。

人工智能对情报收集分析的影响

人工智能是计算机科学、信息论、神经生理学、心理学等多种学科互相渗透而发展起来的一门综合性学科。人工智能解放了人脑，让人从繁重的重复性工作中解放出来，专注于发现性、创造性的工作。

大数据时代，我们身边充斥着各种各样的数据与信息，这些数据与信息成为重要的情报源。美国国防情报局总部的墙上就有一行字，告诫要注意普通民众的意见、评论和玩笑。由此可见我们身边的数据与信息具有非常大的价值，准确高效地收集并分析这些信息为我所用，人工智能将会发挥极大作用。

2017年7月12日，美国权威智库发布的《人工智能与国家安全》报告提到，情报工作者如果能从监控、社交媒体等渠道获取越来越多的数据，通过对这些数据进行筛选、分类和组织，有助于及早发现威胁国家安全的各种情报。

当前，数据海量增长，只靠人力要想收集全部数据，很难完成，也不太现实。因此，推进机器学习或者应用人工智能来收集分析情报，将大大缓解分析人员的负担。人工智能对于情报收集分析的主要影响集中在以下两点。

一、信息来源更加广泛。相比于人工智能收集数据的能力，之前计算机技术只能算是小儿科。以往我们获知的情报信息大多是邮件、手写文档、电话录音和照片等，这些情报是陈旧的、小范围的，信息的不确定性高。

如今步入大数据时代，摄像头和无人机正在源源不断地向情报机构输送着大量的图片和视频，社交网络上每分每秒都在生成海量的信息，这使得信息来源更加广泛，如果能及时对这些信息进行处理，将把很多社会安全事件遏制在萌芽阶段。

二、分析方法更加科学。以前，情报学在研究中普遍采用的是确定性研究方法。但是，该方法必须适应于人类社会组织，而人类社会组织属于复杂系统，本身带有不确定性，因此确定性研究与情报活动本身并不匹配。分析技术又被认为是情报学的核心技术，人工智能分析技术是基于大数据建立研究范式的，在特定条件下，人工智能对于不确定性研究对象的分析能力已经超过人力分析，而且对于大量、多维性的数据分析占有绝对优势。因此，人工智能采用的分析方法更加科学，分析结构更加准确，有效避免了某些人为因素导致的偏差，这将会大大节省人力。

基于以上两点，我们可以看出人工智能有着强大的信息优势，将极大提升数据收集与分析能力，并提升产生新数据的能

力，这对于情报收集分析将产生重大影响。

情报收集分析中的人工智能应用

当前，人工智能广泛应用于公开信息的深度挖掘，主要用于发现数据与数据管理、信息与事实之间的关联。作为信息技术革命的发源地和领跑者，美国在迎接人工智能新未来的过程中一马当先，也不断将人工智能运用到情报收集分析工作当中。

一、人工智能用于军事情报的收集分析。随着移动互联网基础设施的普及，以及无人机、摄像头等传感器的发展，情报工作要处理的数据量激增。以美国为例，美国国防部大量采购和部署了配有高清摄像头的无人机，并将其广泛应用于阿富汗和伊拉克两个战场，以期从源源不断传回的海量视频资料中获得敌人异常行动的蛛丝马迹，然而这些海量的视频信息让数量庞大的美国情报分析员忙得焦头烂额，效率十分低下。为解决这一问题，美国国防部于2017年4月成立“算法战跨职能小组”，推动国防部加速运用人工智能、大数据及机器学习等关键技术，以期从海量情报中快速获取有用的战场情报。这将有助于减轻全动态视频分析方面的人力负担，将情报分析员从海量的信息辨识、分拣和提炼工作中解放出来，产生更多具有实际价值的情报，提高军事决策水平。

二、人工智能用于社交媒体信息的收集分析。除了用于军事领域的情报收集分析外，美国中央情报局也将之用于日常生活信息的收集分析。以人工智能为基础的算法不仅可以挑选出关键词和名字，还可以分析出数据里隐藏的规律以及与其他事件之间的关联，并且在一次次的规律寻找中不断自我完善。人工智能的运用可以扩展情报处理的手段和范围，找到有价值的碎片信息，可以为防务、情报以及国土安全分析人员就潜在的危机提供早期预警。因此，美国中央情报局充分利用人工智能技术，提升数据收集分析能力，尤其注重获取社交媒体数据。他们通过搜索社交媒体，梳理海量的公共记录信息，形成社交媒体大数据，并对这些数据进行筛查。这种方式，改变了美国情报机构过度依赖人类经验的现状，借助人工智能，提高了情报分析的精准度。

三、人工智能用于网络舆情的分析。互联网每天产生海量数据，大大增加了舆情信息的挖掘难度。运用人工智能，可以实现对互联网所有舆情信息的实时跟踪，并通过文本挖掘、自然语言处理、可视化分析技术，提供舆情监测、专题分析、智能报告、趋势预测、舆情画像、危机预警等服务。可以说，人工智能实现网络舆情分析的自动化、智能化、精准化。当前，人工智能已经广泛应用于政府公共管理和公共服务舆情方面，未来，随着知识图谱、图片音视频信息处理（感知智能）、自然语音处理技术（认知智能）的不断应用，网络舆情的自动化和智能化水平将显著提升，比如把简单的正负面倾向性分析上升到多维度的情感判断，比如用机器人取代大部分舆情分析师的工作，让舆情分析师将精力放在建模和效果评估上，而不是花大量时间进行日常枯燥报告的撰写。

人工智能在情报收集分析中应注意的问题

人工智能需要数据的支撑，没有数据的驱动，就无法进行各种分析与预测，也不能提供精准信息服务。海量数据的收集与分析，可能带来用户隐私信息的泄露。因此，人工智能应用于情报的收集，要充分考虑智能化应用与隐私安全的平衡。具体而言，

要注意以下问题：

一、信息收集需要充分授权。2018年1月3日，支付宝的晒“个人账单”事件，遭到国家互联网信息办公室和工信部的先后约谈，其中不妥之处就是提前替用户勾选同意芝麻信用收集用户信息，并向第三方提供。这种做法侵害了用户的知情权和自由选择权。尽管用户为了享受智能化服务，让渡部分个人信息，但对用户个人信息的收集与分析，必须首先获得用户授权。

二、大数据分析应有边界。在人工智能条件下，一个国家的个人信息数据——包括年龄、血型、学历、病历、收入水平、消费记录、思想倾向等都被收集、存储和智能化计算，就可能关系国家安全。比如，通过各种智能穿戴设备、网络平台或者其他公共服务的智能系统可以生成和采集很多个人信息，这些信息经过网络传递和设备之间的数据同步，被更强大的大数据中心所收集和处理，就可以实现对某一国人口信息、经济社会信息的相关性分析。因此，对于敏感的密码、指纹、签名字迹、人脸特征等身份认证信息，更应该有明晰的界限，除特定情况并征得用户授权外，用户本人应绝对掌控，信息采集方也无权违规使用。

三、信息收集与利用要防止用户隐私数据泄露。人工智能的各种应用会越来越多地抓取个人信息，如何防止用户隐私数据泄露将是很大的挑战。一方面，信息收集方要承担起保障数据安全的义务，防止用户隐私数据信息泄露，切实贯彻网络安全法中“谁收集，谁负责”的原则。另一方面，用户也要提高自身安全意识，对社交媒体上的各种行为要采取安全防范措施，注意保护自己。■

（作者单位：武汉大学国家保密学院）

责任编辑/李 杰

保密知识小测试

判断题

1.某机密级中央文件发放至省军级机关。因工作需要，某省军级机关拟将该件转发扩大至其下级单位，此时，某省军级机关应当向该机密级中央文件发文单位（一般为定密单位）提出扩大知悉范围的申请，经发文单位批准同意后，才能转发。（ ）

2.国家秘密的解除，简称解密，是指已定为国家秘密的事项，因为情况的变化，失去其国家秘密属性，不具有保密价值，按照规定程序，将其从国家秘密事项中分离出来，不再按照保守、保护国家秘密的措施进行管理，知悉范围内的机关单位和人员不再对该事项履行保密义务和承担保密责任。（ ）

3.审查解密的工作由定密责任人负责。情况紧急时，也可以由其上级机关、业务主管部门或者制定保密事项范围的中央有关机关直接解密。（ ）

4.不属于本机关本单位产生的国家秘密，也可以直接对其解密，亦可以向原定密机关单位或者其上级机关、保密行政管理部门提出解密建议。（ ）

（答案见本期）

厉害了！草原上这支销毁队伍

——内蒙古自治区涉密载体销毁中心工作掠影

□本刊记者 满 宁 特约记者 张 禄

内蒙古自治区是我国成立最早的少数民族地区，外接俄蒙，内连8省，有着绵延4200多公里的边境线，既是祖国北大门，又是首都“护城河”，苍茫草原上有沙场演兵纵横驰骋的豪情，有神舟飞船穿梭寰宇的激昂。特殊的区情和军工军事重地，决定了自治区历来处于窃密与反窃密斗争的前沿，对做好保密工作提出了更高要求。近年来，内蒙古自治区涉密载体销毁中心（以下简称中心）在加大保密服务保障力度上狠下功夫，不断强化人员队伍建设，规范销毁监督管理，拓展保密服务范围，保密服务保障水平不断提升。

忠诚的种子根扎沃土

干事业，需要忠诚，干好保密工作尤其需要忠诚。忠诚之树要想根深叶茂，需要用心、精心培护。

保密工作有着很强的政治属性，要始终把政治建设摆在首位。中心承担着把守保密管理最后一道关口的重任，旗帜鲜明讲政治，既是传统、更是纪律，容不得丝毫含糊。在政治上，中心把加强干部职工理想信念教育和忠诚教育作为一项长期工作，积极开展党员干部讲党课、每周四例会学习、“比学赶帮超”学习竞赛等活动，引导干部职工时刻把保密纪律和保密规定印在脑中、刻在心上，始终牢记自己是党的保密干部，严守党的政治纪律和政治规矩，全力锻造一支可靠、可信、可用的队伍。

政治“养分”充足，管理也绝不能懈怠。在自治区保密局的关怀支持下，从2010年成立至今，8年时间里，中心由原来的5个人发展到23人。在人员使用和管理上，中心树立“风险就在自己身上”“危险就在自己身边”意识，严格把关，确保进入中心大门的人员干净、纯正、忠诚。

中心负责人任政胜告诉记者，这儿的职工从进门到正式上岗前，有个“三个必须”的规矩。

其一，对拟用人员必须按照规定和程序严格政审，审查通不过坚决不用；其二，政审合格后，必须签保密协议，严明工作纪律、岗位职责、保密责任和奖惩措施，并为每个人建立一份详备的职工档案；其三，人员上岗前，必须经过保密培训，考试通过方能上岗。

上岗后规矩就更多了。2015至2016年，中心制定完善了《内蒙古自治区涉密载体销毁中心制度（试行）汇编》，涵盖涉密载体管理、销毁、回收、押运、运输、检查及人员分工等35项管理内容。销毁人员直接接触密件，该汇编即规定了“5个不”：不能看、不能拿、不能说、不能问、不能记。

用制度管人管事，看似条条框框多，其实职工心里最清楚：保密非同小可，严，才是爱护。

平日里，职工还能感受另一种爱：中心像大家庭一般温暖，有非常人性化的一面。中心有个“五必

谈”“五必访”之说。“五必谈”即中心领导在干部职工岗位变动、工作失误、家庭困难、廉政、工作作风等方面听到反映，必须开展谈心谈话活动；“五必访”即中心领导在干部职工生病住院、遭遇天灾人祸、直系亲属去世、生活遇到困难、思想情绪出现波动时，必须走访看望。中心职工原来工资待遇、保障偏低，自治区保密局和中心领导为此没少向上级部门争取，去年终于有了好消息：从2018年起，中心经费单独列入自治区财政预算，职工工资福利一下子提高了近千元。

政治把关、管理从严，以及组织关爱，严似冰、热如火，却又紧紧组合在一起，给职工以一种特别的吸引力与归属感，滋养着这一方沃土，忠诚之树在其上生根发芽，长出干、枝、叶，有生命、有温度、有定力。新招录的小刘说：“保密事业很光荣，我愿意扎根在这里。”这也是大家的心声。

草原上来了不速之客

“风吹绿草遍地花……骏马好似彩云朵，牛羊好似珍珠撒。”德德玛浑厚的女中音，把人们带到多彩多姿的内蒙古大草原。可是锡林郭勒阿巴嘎旗这几天却来了几个奇怪的客人，不看美景看破烂儿。原来是自治区销毁中心的几名干部职工到各盟市巡查旧货市场来了。

工作人员不顾车马劳顿、蚊虫叮咬，一头扎进废纸堆。旧货市场没遮没挡，火辣的阳光下，工作人员一份份地翻找，汗水湿衣浑然不觉。草原的天，说变就变，刚才还是骄阳似火，转眼间就切换成瓢泼大雨。市场里的纸品有油布苫盖，埋头干活的工作人员却被浇个“透心凉”。骤雨一停，几人忙又跟废纸较劲。“我找到一份内部文件。”“再找，仔细找，一定不能让涉密文件流入旧货市场。”

酷热淋雨，组员杨常青得了急性肠胃感冒，腹泻脱水，而阿巴嘎距离盟市中心有100多公里，一路上他只能蜷缩在检查车后座上，待送到盟医院时，已经脸色惨白。同事担心他的病情，劝他第二天休息。他却说：“能扛住，不耽误去下一站。咱组程主任刚做完心脏搭桥都没当个事儿，我这算啥！”凭着这股子憨劲，几个人一共查到了3份内部文件，虽不涉密，但对盟市销毁管理工作的震动和警醒却不小。

内蒙古地广线长，旧货市场是监管难点。近年来，中心成立专门检查队伍，分赴全区12个盟市的旧货市场进行暗访式检查，不打招呼，突然现身，查出真情况、真问题。为保证成效，他们提出“三对”工作方法：一是对旧货市场从业人员，要加强保密教育，解释违法收售涉密载体应承担的法律责任，阐明其中的严重危害，鼓励其主动上缴收购的涉密载体，并签订保密协议书，建立电话联系。二是对各盟市销毁管理人员，检查反馈时要进行保密警示教育，使他们爱销毁、懂销毁、管销毁，增强积极性和主动性。三是对发现问题的相关责任人，进行约谈，指出问题、明确要求，限期整改，把保密检查的利剑作用发挥出来，把保密检查的权威形象树立起来，坚决把泄密隐患和危害降低到最小。

哪里需要，我们就出现在哪里

“做人要像石灰，清清白白才立得住；做事要像砖头，哪里需要就哪里搬。”这是军人出身的任政

上门服务

销毁线上工作

外出查旧货

胜常挂在嘴边的话。

2017年大事多、喜事多，党的十九大胜利召开，自治区举办成立70周年庆祝活动，相关保密服务保障时间紧、任务重，涉及方方面面。任政胜要求中心全体干部职工24小时待命，随叫随到、全程保障，哪里需要就去哪里。中心人员不仅要做好清退待销载体登记收运这个主业，还派出人员参与会场保密警示提示牌、手机屏蔽柜摆放等工作。

中心工作人员坚决服从指挥，立得住、搬得动，打得响、过得硬。为了不让销毁件积压，中心工作人员布日古德顾不上照顾生病的幼子，连夜跟车押运6个小时，将销毁件送到外地造纸厂进行化浆。会议活动期间，中心全体人员加班加点，坚持对每个环节严格把关，对每个细节仔细研究，对每处场所反复巡查，及时消除了潜在的保密安全隐患。2017年，中心参与会议服务保障43次，高素质、高效率、高质量完成各项任务，受到各方的充分肯定和好评。

中心负责人和干部职工合影

会议服务保障做得好，日常服务保障也同样不落后手。任政胜始终有非常清晰的“窗口服务”意识和“保障有力”使命感，积极主动地与各机关单位进行经常性的沟通协调，不断强化保障水平。

自治区党委办公厅、政府办公厅产生的涉密文件数量多、密级高，中心每周上门服务一次，大大方便了“两办”工作；公安部门、银行系统文件多，多时达几十吨，甚至上百吨，中心为他们开辟绿色通道，进行集中销毁。对其他无法自行送销的机关单位，中心克服人少车少困难，开展上门销毁服务。同时，中心还十分注重与各盟市销毁中心的沟通和协调，与12个盟市和90多个旗县区建立了18个经常联系点，强化对边境旗县（区、市）涉密载体销毁工作的监督指导，积极帮助他们解决实际困难。

这支草原上的销毁队伍，用忠诚和汗水把住国家秘密最后一道关口，守护着祖国北疆这道亮丽的风景线。■

微言大义

保密前提定准密，
编制条目要精细，
对照范围来知悉，
遵规守纪是前提；
借用密件有限期，
超期续借莫忘记，
流转记录常梳理，
保证账物无问题；
涉密会议要审批，
保密方案早确立，
会场禁止带手机，
无线话筒要清理；
电脑维护须定期，
内网外网要隔离，
程序安装必审批，
信息系统要审计；
各种移动存储器，
区别使用心要细，
外部标识看清晰，
定期检查严管理；
科研成果出成绩，
保密先行是根基，
人人有责人人记，
保密工作常警惕。

——中国科学院大连化学物理研究所

直击

甘肃庆阳：十年两获全国先进集体的背后

□本刊记者 李 杰 特约记者 李佳珉

2006年，庆阳保密人从北京捧回了“全国保密工作先进集体”的荣誉奖牌。2016年，庆阳保密人再次从北京领回这份至高的荣誉。

庆阳，这颗镶嵌在陇东的璀璨明珠——甘肃省唯一的革命老区，十年两获全国先进绝非偶然，荣誉的背后，是庆阳保密人不忘初心、砥砺前行的不懈探索。

使巧劲补短板

一直以来，机构不全、人员不齐是制约基层保密工作发展的最大短板。但庆阳使巧劲补短板，一步一个脚印，迎来了一个个可喜的变化。

早在1992年，庆阳就成立了全省首个公文销毁机构——庆阳公文销毁站。2006年，随着保密技术工作的开展和办公自动化设备的日益普及，保密技术检查应运而生，庆阳开始谋划在全省率先成立专门的保密技术检查机构。

成立一个新机构，叫什么名称，怎样定位其职能，这些看似简单的问题，在当时做起来却不容易，特别是市保密局已经有一个公文销毁站，再单独设立一个机构，困难肯定不小。

他们决定“迂回”一下，在申请成立新保密技术检查中心的同时，申请将公文销毁站更名为公文销毁中心，与新成立的庆阳保密技术检查中心合署办公，两块牌子一套人马。事实证明，这种做法是对的。

2011年，针对互联网泄密问题，庆阳保密技术监管工作开始起步，保密局内部机构建设也提上了日程。他们再一次“迂回”，撤销原有的两个中心，将人员编制全部划归保密局机关，成立保密技术、保密宣传、综合管理3个科室。

2016年，中央作出关于保密工作的决策部署，给保密工作发展带来了新机遇。庆阳市保密局抢抓机遇，明确提出成立保密技术服务中心，并与机构编制部门达成了共识，又一个拥有3名编制的科级机构即将诞生。

多年以来，随着机构建设的不断规范，庆阳市保密局的人员力量逐渐壮大。进入新时代，他们又把发展壮大队伍目标放在了挑选调动、争取组织部门选调生和军转干部上，同时积极争取大学生就业援助岗位，先后从市直部门选调1名，争取优秀选调生两名，军转干部两名，争取两个就业援助岗位，工作人员增加到11人，成为全省人员配备最精壮的市州。

“庆阳是革命老区，早在1947年就成立了专门的保密工作领导机构，高度重视保密工作是历届党委政府的优良传统，庆阳机构队伍的逐步壮大离不开历届党委政府的大力支持。”市保密局局长刘选明说。

省政协副主席、庆阳市委书记员建民，市委常委、宣传部长、保密委员会主任闫晓峰非常重视保密工作，多次到市保密局调研，现场协调解决重大问题。

使实劲打基础

在采访时，市保密局工作人员使用的笔记本引起了记者的注意，一问才知，他们从20世纪90年代就开始印制含有保密常识的笔记本，向县处级以上领导干部免费发放，20多年从未中断，已连续设计印制6个版本，印刷量达到3万多册。系列保密笔记本见证了庆阳保密工作历史的变迁。

多年来，庆阳始终把宣传教育作为做好保密工作的基础，通过多形式、多内容、多载体的宣传教育培训活动，不断提高干部群众的保密意识。特别是近年来，庆阳逐步建立健全党校保密教育培训机制，多次邀请专家学者走进来讲授保密知识或走出去进行保密业务培训，

举办保密知识竞赛和元宵节灯谜答题活动，挖掘革命战争时期南梁红色保密经验，整理汇编了4册革命历史时期红色南梁保密工作资料……

省保密局局长张云戟对此评价道：“庆阳的宣教工作扎扎实实、有声有色、入脑入心，这是他们之所以成为全国先进的经验之一。”而对于庆阳来说，宣传教育只是手段之一，他们同样看重的还有监督检查。

庆阳的监督检查绝不搞“花架子”。他们突出重点行业领域，瞄准保密要害部门部位，不断创新形式，通过单位自查、远程搜查、网页巡查、专项督查和跟踪复查，不打招呼、不走过场、不留死角，推动保密管理措施全面落实。

对检查中发现的问题，他们敢于动真碰硬，对于工作迟缓，拒不整改或整改不彻底的单位进行严肃通报，约谈单位领导。近年来，共通报违法、违规事件32起，查处泄密案件2起，处理违法、违规人员50余人。

实实在在的监督检查提升了保密部门的权威，也得到了各单位的理解和支持。市直某单位工作人员说：“一开始，对保密局三天两头不打招呼就来检查还比较抵触，但慢慢发现，他们来不是为难我们，而是在帮助和警示我们，消除泄密隐患……”

使韧劲促转型

对庆阳来说，抓实宣传教育和监督检查是做好基层保密工作的重要手段，不断强化技术防范是推动基层保密工作转型升级的重要支撑。“当前信息技术的迅速发展和网络泄密事件频发的严峻形势使我们深深认识到，做好信息化条件下的保密工作除了抓实宣传教育和监督检查外，还必须狠抓技术防范，着力提高保密技术监管能力。”刘选明说。

竞赛现场

然而，对基层保密部门，特别是西部欠发达地区的基层保密部门，在地方财政紧张的情况下，做好技术防范工作特别不容易，需要不畏难、创造条件也要上的精神，更需要久久为功的韧劲。而这种精神和韧劲在庆阳历代保密人身上体现得最为充分。

1994年，在庆阳公文销毁站成立之初，市保密局没有经费购置销毁设备，但为了保证大量涉密文件及时安全销毁，他们想方设法向企业求助，在农机厂的帮助下，将一台坏掉的铡草机和面粉机结合起来，改装为全省第一台文件销毁设备。国家保密局有关领导在甘肃调研时，专程来到市保密局，对此给予高度评价。

2013年，为了升级改造违规外联和移动介质存储监管平台，市保密局向市财政申请经费240万元。经过多次沟通，财政部门初审同意，但还需要向市长汇报。整整一个月，在排队汇报的过程中，时任保密局局长韩湘波恰巧每次都能碰到财政局局长，终于，在第6次偶遇时，财政局局长被深深打动了，他主动对韩湘波说：“就为了你们这种工作精神，我来帮你们汇报”。很快，项目经费得到落实。

就凭着这股子韧劲，近年来庆阳累计投入技术经费800多万元，建立起从“内”到“外”，从单机到网络，从市直到县（区）的立体化、多层面、全方位的保密技术监管体系。正是凭着这股子韧劲儿，庆阳的技术防范工作始终走在全省前列，为全市保密工作转型升级提供了强有力的科技支撑。

一路走来，庆阳的保密事业由小到大、由弱到强，无论是基础工作还是重点工作都在不断突破，取得了骄人成绩。“走进新时代，面对新时代保密工作的新情况新问题新要求，我们将始终坚持以习近平新时代中国特色社会主义思想为指引，牢记使命、勇于担当，以真抓的实劲、善抓的巧劲、常抓的韧劲抓好中央关于保密工作决策部署的贯彻落实，进一步推动全市保密工作的转型升级，坚决打赢信息化条件下的保密战。” 刘选明坚定地说。■

直击

湖北荆门：以科技创新引领保密工作转型升级

□本刊记者　孙战国

近几年，面对新形势新挑战，荆门市保密局围绕“打赢信息化条件下的保密战”这条主线，把科技摆在更加突出的位置，把创新贯穿于保密工作全过程，提出“一手抓保密日常工作，一手抓保密科技，两手抓两手都过硬”的工作思路，趟出了一条科技保密的新路子。

做好顶层设计

“信息化条件下，地市级保密科技工作最紧缺的就是技术力量和科技工作机构，要想推动保密工作转型升级，必须做好保密科技工作的顶层设计。”荆门市保密局局长许敬原告诉记者：“这一直是局班子的共识，我们在保密科技的顶层设计上下了很大功夫。”

一是从体制上破题。为打破体制不顺这一瓶颈，荆门市保密局积极争取领导支持，整合技术资源，成立了市保密科技中心，增加人员编制；争取部门支持，吸纳全市信息化专业技术人才，聘请省级专家，组建市保密科技工作领导小组和专家库；通过请进来、走出去的方式，开展多层次的保密技术培训，培育技术人才，形成了保密部门牵头挂总、部门协调联动、专家咨询会商、技术人才支撑的保密科技工作新格局。

二是从规划上点题。荆门市保密局坚持规划先行的理念，立足“全省领先、全国一流”的目标，制定了《荆门市保密科技工作三年行动计划》和《全市“十三五”时期保密事业发展规划》，从总要求、总目标、重点项目建设等方面，对平台构建、装备配备、技术创新、技术力量培育等进行了总体布局，为构建立体化的综合防范体系提供了行动指南。

三是从实战中入题。自2015年起，荆门市保密局每年突出一个创新主题，先后组织开展了全市“保密科技创新年活动”“保密改革创新年活动”“保密管理创新年活动”，实施了“六个中心”“三大平台”等十多个项目的招标和建设，完成投资1500多万元，基本构建了保密技术防护监管一体化体系和保密技术服务保障体系，为实现保密工作转型升级打下了坚实基础。

打造综合防范体系

构建保密技术防护监管体系是实现保密综合防范的重要载体和途径。围绕“如何建”“建成什么模式”，荆门市保密局立足“瞄准前沿科技，体现荆门特色”，提出建设“荆门市保密预警监控中心”的设想，并进行了大胆探索和创新。

为打造保密综合防范体系，荆门市保密局赴成都市、宜昌市保密局和有关公司进行学习考察，开展联合调研、联合技术攻关，并组织专家、技术人员到荆门研讨交流，形成了《荆门市保密预警监控中心建设方案》（以下简称《方案》），提出了“三个依托”的建设路径，即依托电子政务内网建平台，依托大数据中心建系统，依托综合业务管理系统上应用。《方案》经过反复论证，经湖北省保密局批复，于2015年正式分阶段实施。荆门市保密局副局长李红武告诉记者：“按照因地制宜、彰显特色，上下同步、全域贯通，防监并重、业务协同的原则，探索、形成了保密技术防范监管一体化平台建设‘1+2+3+N’模式，大大提升全市的保密技防能力。”

这个模式体现3个融合：一是上下融合，同步构建。立足全区域、全方位、全时段，实现对涉密

信息的全区域同步、全网络同控、全时段同管。二是平台融合，打破孤岛。立足互联互通，打破各个平台孤岛和数据交换壁垒，构建保密大数据中心，实现平台之间相互联通、信息数据即时交换，利用保密态势感知和数据追踪系统，为领导决策提供服务。三是应用融合，业务协同。立足技术防护、技术监管、教育培训、技术演练、考试考核、业务办公一体化，网上监控检测与实地取证督查结合，实现综合防范、业务协同。目前，市预警监控中心建成挂牌，5个县市区分中心建设稳步推进，各系统已完成开发，实现了上线运行、融合应用。

在功能提升上，该模式实现“三化同步”。一是实现了对互联网、内网违规信息全时段、全过程预警监控常态化。技术监管预警系统主要作用是采集违规信息，对违规信息进行筛选、清洗和处理，为保密态势感知和综合分析系统提供数据。二是实现了保密基础数据采集、业务应用和办公信息化。保密业务信息化管理系统主要作用是将业务管理工作流程化、基础信息数字化，实现保密基础数据采集、责任制管理和考核、违规信息核查、检查督办等日常业务管理功能，形成“二横二纵、纵横贯通”“自查与抽查、办公与管理”为一体的保密业务综合管理新模式。三是实现了安全监管、业务开展、教育培训一体化。通过保密技术防护监管一体化平台，构筑起功能全面的保密综合防范体系。

提升保密技术服务能力

建设区域性的保密技术服务保障体系是提升区域性保密技术服务能力的重要途径。荆门市保密局按照“主体支撑、人才保障、重点推进”的工作思路，探索并初步形成了以市保密科技中心为支撑，保密技术人才队伍能力建设为保障，覆盖党政机关和涉密单位，载体销毁、维修维护、数据恢复、重点领域保密服务“四位一体”的保密技术服务保障体系和工作新格局，有效提升了全市保密技术服务和保障能力。重点是推进四个中心建设。

荆门市保密技术防护监管一体化平台

在涉密载体销毁中心建设上，2017年，新建200平方米的荆门市涉密载体销毁中心，配置有纸介质销毁机1台，打包机1台；磁介质粉碎机2台，消磁机1台；销毁用货车1辆。全年销毁纸介质40吨，光盘等磁介质3000余张，基本上做到了重要涉密单位涉密载体销毁全覆盖、常态化。

在涉密设备维修维护中心建设上，自2014年起，在全省率先开展了涉密设备维修维护，2017年新建了涉密设备维修维护中心，采取委托涉密资质企业维修、保密部门监管的方式，免费上门维修维护年达200余次。

在涉密数据恢复中心建设上，率先在全省建设涉密数据恢复中心，按照年数据恢复量150−200台（块）标准设计，占地70平方米。目前，已经购置了部分设施设备，今年将开展涉密数据恢复工作。

在保密专项服务保障中心建设上，先后购置了屏蔽、检测和移动检测车辆等设施设备，开展了保密检测、内网测评等工作；每年为市委市政府重要会议活动提供保密服务20次以上，为国家、省、市级考试提供保密服务10次以上；积极服务企业保密需求，协助企业申报涉密资质、涉密等级，全市共有涉密资质企业8家。

保密科技工作的创新实践，保密监管和技术服务能力的提升，加快了全市保密工作转型升级的步伐，全市保密工作实现了3个转变，呈现出“三新”格局：保密监管防范由人防、物防为主向人防、物防、技防相结合，以技术防范为主转变，探索构建了“1+2+3+N”保密技术监管新模式和“四位一体”保密技术服务保障新体系；保密宣传教育由传统方式向传统方式与现代信息技术相结合转变，建立了网上网下联动、宣讲实训结合的保密宣传教育常态化新格局；保密业务管理由制度化管理向制度化管理与信息化管理相结合转变，建立了保密业务信息化管理新系统，全市没有发生一例重大失泄密事件，保密工作跃上了新台阶。■

各地

贵州：用“蝴蝶效应”掀起保密工作新篇章

□黄 炜

“当手机扫描来历不明的二维码或连接钓鱼Wi-Fi时，可能会被植入木马病毒，造成信息泄露，甚至带来窃听窃视等风险。各位领导，请看我演示关机后手机如何继续窃听。”

这是贵州省保密教育培训中的一幕。为深入贯彻落实党的十九大精神和中央决策部署，省保密局在近1个月的时间里举办60余场培训，省四大班子、200多家省直机关领导干部和涉密人员共2000多人参加，是近5年来全省规格最高、规模最大的一次保密教育培训。

“虽然我们的保密教育实训平台尚未建成，但宣教培训必须跟上，要创造性地开展工作，把难点变成亮点。”贵州省保密局局长唐仁勇多次在专题会议上强调。结合全国“七五”保密法治宣传教育研讨会要求，省保密局在向省委保密委汇报的基础上，开展全省保密教育培训，并以窃密泄密典型案例展、攻防技术演示和播放警示教育片为主要内容，得到了省委书记孙志刚的肯定。

为保证培训效果，班子成员靠前指挥，青年干部主动承担起讲解任务。展厅内外寒意阵阵，许多同志连续布展1个多月，冻感冒了也不在意，坚守岗位不叫一声苦；有的同志起早贪黑在展厅、办公室两边奔忙。

省领导观看攻防技术演示

经过多次彩排预演，贵州省保密局迎来了“大考”的日子。受省委书记委托，省委副书记、省长谌贻琴率省四大班子及党组成员集体参加保密教育培训，并在现场语重心长地指出，贵州是军工重镇和国家大数据综合实验区，维护数据安全、做好保密工作任务艰巨，全省上下要深入学习贯彻党的十九大精神和习近平总书记重要指示，切实加强保密意识、保密培训，强化保密技术、保密责任，坚决打赢信息化条件下的保密战。

“此次保密教育培训组织有力、成效明显，全省保密系统要以此为契机，认真研究谋划新时代保密工作的新举措，统筹推进保密监督管理、依法行政、宣传教育等工作，加快推动全省保密事业取得新突破。”时任省委常委、秘书长、政法委书记、保密委主任唐承沛说道。

参训领导干部普遍反映，此次培训案例展示触目惊心、攻防演示贴近实际、教育片深刻震撼，是一次十分直观、生动的保密警示教育。省委办公厅等16家省直机关及贵阳市要求增加专场培训。

“开展培训以来，保密宣教书刊的需求大幅增加，自查自评工作开展得更加顺畅，各级党政机关抓保密的自觉性进一步增强，‘蝴蝶效应’已经产生，一场保密教育热潮正在涌动。我们要让‘蝴蝶效应’持续发酵，随着省保密教育实训平台的建设，宣教培训常态化、专业化水平将进一步提升，全省保密战线必将发挥团结奋进、拼搏创新、苦干实干、后发赶超的新时代贵州精神，续写保密事业发展新篇章。”唐仁勇信心满满地说道。■

责任编辑/武 薇

各地

国网湖南省电力有限公司：以“安全+”应对“互联网+”下的电网风险

□宁 政 夏哲辉 钟 红

“乌克兰电网遭受黑客攻击，造成大面积停电，主要诱因是电力系统工作人员网络安全意识淡薄，随意点击恶意邮件，为网络攻击打开了缺口。”

“电网安全防护体系也存在漏洞，网络隔离严重不足，专业人员监管不力。”

国网湖南省电力有限公司（以下简称湖南电网）作为保障全省电力供应的主力军，也是网络安全重点保卫单位。乌克兰发生大面积停电事件后，公司第一时间召开内部研讨会，保密委员会指出，保障电网安全运行务必把防范网络攻击作为当务之急，湖南电网须提高警惕，重新审视自身安全保密工作。

一场以“安全+”应对“互联网+”形势下的网络安全保卫战由此打响。

精准防御 破解木桶效应

眼下，随着智能电网的全面铺开和特高压等交直流工程的推进，网络和信息技术广泛深入地应用于电力系统。这一方面实现了信息自动采集与上传、海量数据集成与共享，使相对孤立的电力控制系统得以互联互通；另一方面，软硬件设备和智能终端运营主体的多样性，供应链、网络应用等各个环节遭遇恶意软件及渗透监听的风险也越来越高，一旦受到网络攻击，后果不堪设想。

面对严峻复杂的网络安全形势，为避免木桶效应带来的软肋，湖南电网根据国家电网公司总体安全防护策略，形成了对安全区域、网络边界等综合防御体系。突出对电力工控系统建设与运行过程中失泄密薄弱环节的研究，有针对性地抵御信息网络瘫痪、应用系统遭破坏及终端染毒事件。

2012年，湖南电网成立信息通信调度运行监控中心，优化了风险预警、分析研判、主动防御、应急处置流程，切实增强防攻击、防篡改、防病毒、防窃密能力。

在具体项目系统中，公司则根据需要量体裁衣，逐个击破短板。以湖南电网输变电设备防灾减灾技术国家重点实验室为例，它承担着电网防冰灾及防山火工作，曾解决电网冰情预测这一世界性难题，荣获国家科技进步一等奖。为此，国家电网公司依托该实验室成立了输电线路覆冰预测预警中心和山火监测预警中心。

准确预警离不开海量数据的收集与处理，为加强对大数据的安全保密管理，湖南电网根据防御系统的个性化需求，结合信息系统业务授权管理，规范了账号权限，进一步防范摆渡攻击和数据泄密，确保数据安全看得见、看得深。

勤于实战 打造安全屏障

网络安全的对抗是一场速度、耐力与智慧的较量。为加强安全防护技术研究，湖南电网从省保密局、湖南大学、电力科学研究院、信息通信公司等聘请专家，组成顾问团队，定期开展专题会讲与技术交流，并以项目责任制形式，重点攻关保密监测、安全防护和应急响应等技术，解决了配电自动化系统无线通信引发的网络安全保密问题。

为加强网络安全日常运维，打造一支精英护卫队，公司组建了网络信息安全红蓝队。其中，蓝队是“盾”，负责在已有漏洞库的

基础上全面开展信息系统的自查与加固，及时整改复核；红队则是“矛”，密切跟踪首发漏洞，关注最新态势，并从外部开展渗透测试，及时发现安全漏洞。矛与盾互为补充，密切配合，齐头并进。

2016年，网络信息安全红蓝队取得了中国信息安全技能竞赛管理运维赛三等奖；在国家电网公司2017年度网络安全攻防总决赛上，这支队伍更是一举夺得冠军。

在G20杭州峰会期间，他们中走出的骨干力量全程参与网络安全保障，开展网络安全实时监测预警，并完成木马查杀、智能编解码和弱口令检测等多个自研工具，圆满完成保电任务，荣获浙江省政府和国家电网公司的表彰。在2017年全球勒索病毒爆发过程中，湖南电网超前防范，开展专项护网行动，实现了用电零影响、计算机零感染的工作目标。

笃于创新　筑牢保密防线

正如“赫勒法则”所言：“没有有效的监督，就没有工作的动力。”安全保密工作亦然。每年，湖南电网都坚持开展关键保密风险排查、主要场所检测督查、重点网络终端保密检查。

近年来，湖南电网将保密和网络安全工作纳入春季、秋季安全检查及重大活动特检项目，以“不发通知、不打招呼、不听汇报、不用陪同，直奔基层、直插现场”的方式开展隐患排查，全年整治200多项问题，力度不可谓不大。

公司内部，建立了企业负责人业绩考核、全员绩效管理、督查督办3大体系，制定实施安全保密“二十四节气表”，对重点工作进行责任分解，实行月总结、月督查、月通报，执行红黄牌预警和保密风险等级评估等机制。针对所属送变电工程公司承接的境外工程，还建立了总公司、分公司、项目部3级审查制度。

湖南电网在国家电网公司2017年度网络安全攻防总决赛中夺冠

日常督查中，湖南电网保密办留意到，有的员工因加班频繁，长期以来形成了离开工位不关计算机的习惯。而办公计算机中存储大量工作信息，极有可能造成数据泄露。对此，公司自主研发了桌面终端安全节能运行管控程序，借助计算机桌面管控探头及标准化管理系统，推送至各终端，无须员工安装软件或配合操作，就能实时监测每台办公计算机的鼠标键盘空闲时间及CPU、网络运行状态，并针对办公室、变电站、监控值班台等不同区域设置计算机定时自动锁屏，部署智能关机策略。

后台数据显示，该程序运行1年以来，办公计算机在非工作时段的运行数量大幅降低。目前，该程序已获得国家版权局颁发的著作权证书。湖南电网还制作了微信版动画“谁是不关机的人”，并在员工中宣传推广，进一步提升大家的安全保密意识。

为了让安全保密理念入脑入心，把“有意义”的事做得“有意思”，湖南电网还在公司内网和微博开辟“保密在线”专栏，用微交流引发思想碰撞；自导自拍保密教育微电影、动漫短片在楼宇间循环展播，用微镜头以案说法；推广“保密观”微信公众号，每月利用单位微信平台发布自行开发的保密课件，用微课堂给人以启迪。通过多种多样的“微感受”，进一步提升了保密教育的灵活度与吸附度。

“安全保密工作要建立清单制，将工作事项具体化、精细化。”“建议把偏远供电所的网络信息安全列为下一步的管控重点。”在公司保密工作交流群，每天都活跃着各种奇思妙想。

朝受命、夕饮冰，昼无为、夜难寐。面对“互联网+”下潜在的电网风险，湖南电网人沉着应对，勠力同心，时刻保持警觉，绷紧安全神经，织就一道又一道安全防护网。在他们身后，是连续8年被评为全省安全生产先进单位的荣誉；在他们面前，是更具挑战的安全保密使命，“安全+”虽任重道远，但志在必得。■

责任编辑/武 薇

宣教培训

合肥市开展军转干部岗前保密培训。为切实加强退役军人保密教育培训工作，近日，合肥市保密局协调市委组织部、公务员局等，将保密教育纳入军转干部岗前培训课程。市保密局安排师资进行专题授课，重点围绕保密历史、形势任务、问题隐患及常识技能等方面进行讲解。全市2017年度接收安置的181名军转干部参加培训。

河北迁安市举办政法系统保密知识培训。针对扫黑除恶行动中涉密文件流转频繁的情况，迁安市保密局组织政法系统60余名干部职工开展保密知识培训，专题讲解涉密载体和文件资料管理办法。此次培训以警示教育为切入点，通过对涉密载体销毁、涉密文件资料传递保存、非涉密计算机存储和处理涉密信息等方面的违法违规案件进行分析，指出工作中常见的失泄密隐患，教授相关保密知识。

河南许昌市组织机关单位文印人员开展保密培训。近日，许昌市保密局组织全市机关单位文印人员150余人，开展保密工作专题培训。培训内容包括保密工作常识、涉密计算机保密管理、涉密文件管理等，特别强调了机关单位内部印制文件过程中的禁止事项，并要求文印室计算机做到专机专用、专人管理，杜绝失泄密事件的发生。

湖南醴陵市多种形式宣传保密法律法规。近期，正值醴陵市保密学习宣传活动月，市保密局持续利用醴陵电视台等社会媒体以及各机关单位电子显示屏、板报、保密工作QQ群等宣传平台，对保密法及其实施条例进行宣传。为扩大覆盖面，市保密局还与有关部门协调，利用交警滚动显示屏等户外媒体，在全市重要路口播放相关内容，取得良好宣传效果。

广西梧州市举办保密技术检查培训班。为进一步提升保密干部业务水平，梧州市保密局近日在藤县举办保密技术检查培训班，系统讲解保密技术检查的流程规范、注意事项等内容。课后，市保密局还组织学员到县直机关单位进行实操训练。全市60余名保密检查支队成员及有关单位保密技术人员参加培训。

南昌市湾里区打造机关保密主题文化墙。近日，湾里区保密局通过定制、悬挂一批保密主题书法、绘画作品，在机关大楼内打造了保密主题文化墙，受到来往干部职工的关注。该行动旨在增强保密文化氛围的同时，让“保守机密慎之又慎”“保密就要滴水不漏”的观念入脑入心，在日常工作中起到常提醒、常督促的作用。

辽宁岫岩县开展窃密泄密演示活动。作为“百场演示进机关，万名干部受教育”主题系列活动的组成部分，岫岩县保密局近日组织了窃密泄密演示。现场工作人员不仅还原了黑客通过计算机及网络窃密、无线Wi-Fi窃密、智能手机扫二维码和抢红包窃密、办公自动化设备窃密等技术手段窃取国家秘密的全过程，还讲解了相关防范方法。县直机关、各乡镇、办事处保密工作分管领导和重点涉密人员230余人参加活动。

新疆博尔塔拉州举办国家安全教育日保密宣教活动。为迎接十九大以后的第一个国家安全教育日，博州保密局联合州文体广新局、文物局等单位，举办安全保密警示教育展。本次展览为期20天，设置展板区、演示区和考试区，依次通过3区域后，参展人员还可领取保密宣传资料。截至目前，州直、市直乡镇场、街道社区1000多家单位上万人参加活动。

贵州兴仁县开展国家安全教育日宣传活动。为做好党的十九大后第一个国家安全教育日工作，兴仁县保密局在城市公园开展集中宣传活动，通过悬挂宣传横幅、发放宣传资料、讲解相关法律法规、提供法律咨询等方式，向来往群众宣传国家安全法、反恐怖主义法、保密法等法律法规。现场发放宣传资料近3000份，接受群众咨询100余人次。

国家电网浙江宁波供电公司开展保密宣传活动。近日，宁波供电公司举办“保密学习月”活动，围绕保密法及其实施条例、公司各项保密规章制度等，定制保密学习微课、失泄密案件展板及保密宣教丛书，在公司网站开设保密知识学习专栏，组织开展全员保密应知应会测试和保密知识竞赛。同时，为进一步强化责任落实，公司将保密教育纳入领导干部轮训学习内容。

保密知识小测试答案：1.✓ 2.✓ 3.✓ 4.×（无权直接解密）

监督检查

南宁市开启全年保密检查工作。近日，南宁市保密局印发《关于开展党政机关保密工作检查的通知》，围绕“保密检查全覆盖、重点单位重点查”的工作目标，开启2018年度全市保密检查工作。检查涵盖自查自评、涉密载体管理、要害部门部位管理、定密管理、制度建设等，力图实现项目全覆盖。严格责任追究，对检查中发现的问题限期整改，对整改不及时、不彻底的进行通报批评或领导问责。

江苏江阴市开展高中学业水平必修科目测试考试保密检查。为确保考试万无一失，江阴市保密局分析考试形势，制定保障方案，会同教育、公安等部门对试卷保密室、各考点环境进行检查，重点查看保密设施及监控系统状况、人员值班及保密规章制度落实情况等。同时，加强对考试相关人员的保密提醒，严格试卷发放、启用、交接等环节的规范操作。

江西抚州市临川区开展保密检查。近期，临川区保密机要局将保密检查与安全移动协同办公系统使用督查结合起来，成立由区保密局、区委督查室、政府督查室、信息中心组成的联合检查组，采取听汇报、查文件、清设备、看数据、观操作等方式，对全区所有机关单位进行检查。针对发现的保密工作与商用密码应用问题，检查组现场协助制定整改方案，下发整改通知书，并对消极整改单位进行通报。

四川泸州市江阳区针对2018年自考开展保密检查。近日，江阳区保密技术检查中心深入区大学中专招生委员会和自学考试委员会办公室，开展保密专项检查。检查组现场查看保密基础硬件设施设备运行情况，并要求各部门对照《国家统一考试保密自查登记表》逐项开展自查,对发现的问题按期整改。

云南禄丰县开展“查隐患、补短板”专项行动。为增强各机关单位做好保密工作的责任感、紧迫感，禄丰县保密局持续开展“查隐患、补短板”专项活动，对全县14个乡镇、66家县级部门保密工作进行现场考评。近日，在县级领导班子办公室主任2018年第一季度联席（扩大）会议上，县委主要领导就专项行动又作出进一步强调和部署，力图推动专项行动取得实效。

指导管理

吉林梅河口市加强智慧城市建设保密服务保障。近日，梅河口市加入建设智慧城市的行列，市保密局严把设计关，深度参与项目立项、汇报会、建设方案审议过程，对所有参与智慧城市项目建设、使用、维护的工作人员进行备案并开展保密教育。同时，部署经常性检查，将所有相关项目纳入重点检查范围，确保项目全程安全保密。

江苏无锡市开展2018年度公务员招录笔试保密保障工作。近日，无锡市保密局参加2018年全市公务员招录笔试工作联席会议，围绕落实保密工作责任制，签订保密承诺书，加强试卷运送、保管、交接等环节的保密管理建言献策。同时，组织人员对试卷保密室进行验收，实地查看视频监控、红外报警器、试卷存放柜、手机存放柜等各项安全防范措施和保密环境状况等。

贵州安顺市加强智慧城市建设保密管理。自2013年全市智慧城市建设启动以来，市保密局主动介入，运用多种手段加强智慧城市建设各个环节的保密管理工作，不仅督促领导小组保密工作责任制落实、对承建单位进行资质筛查、优化秘密事项确定流程，还加强了对数据信息使用等方面的监管，获得各有关单位好评。

河南禹州市开展“保密工作落实服务年”活动。近日，禹州市保密局以提高保密管理能力为主线，开展“保密工作落实服务年”活动，并拟定活动方案。方案对涉密人员管理、涉密领域国产化替代工程、保密宣传教育等重点工作进行详细规划，并提出进一步加大保密督查力度，对全市机关单位进行拉网式督导检查，实现保密检查全覆盖。

河北滦南县强化保密工作。将保密责任履行情况纳入领导干部绩效考核内容，在科级领导班子和科级干部考评细则中增加相关扣分规定，加大奖惩力度；将保密科技经费纳入年度预算，增强多类别保密技术装备配备；将保密知识纳入干部培训内容，以普及知识、强化技能为宗旨，科学设置多种课程；将保密法律法规知识纳入公务员普法考试内容，以考促学，全面提高全县机关单位工作人员保密素养。

安徽当涂县多举措推动保密工作落实。加强保密宣传教育，将保密教育向基层单位、县直单位和社会延伸；强化保密检查，主动寻找保密管理中存在的薄弱环节和突出问题，助力各机关单位逐个击破；落实保密责任，确定全县各乡镇、园区和县直单位主要领导为保密工作主要负责人，谁主管谁负责，谁分管谁负责，不负责就问责，推动落实各项保密工作决策部署。■

责任编辑/齐 琪

“钉钉子”抓落实，保密干部要有精气神

□徐金春

春回大地，万物勃发。中央决策部署印发以来，多数地方和部门贯彻落实形势是好的，有思路、有章法、有实效，一些长期困扰保密事业发展的重大问题已经或正在逐步得到解决，保密工作呈现前所未有的勃勃生机和活力。

然而，必须看到，一些地方和部门的贯彻落实情况并不乐观。有的学习过、传达过了，没有结合实际出台实施意见，把政策利好传导下去；有的制定实施意见没有很好地结合本地本部门实际，照搬照抄，操作性不强；有的文件写得很漂亮，主要领导也有态度，但在推动有关事项特别是机构编制等关键问题解决时，却瞻前顾后，难以突破。这些都反映出在贯彻落实中央决策部署上，一些地方和部门，或多或少存在麻木不仁“不想落实”、应付了事“不真落实”和束手无策“不会落实”等现象。

这些年来，党和国家对保密工作不可谓不重视，要法律有法律，要条例有条例，要规定有规定，要文件有文件，顶层设计可谓下足了功夫，保密事业迎来了历史上最好的发展时期之一。在这一背景下，许多地方和部门抓住各种机遇，积极作为，保密事业得到快速发展。而有的地方和部门则不然，对中央决策部署、国家法律法规以及上级文件规定精神总是反应迟钝，总是“慢半拍”，习惯性地拖、等、观望，硬生生把一个个政策红利拖小了，拖黄了，拖没了。

同一个决策部署，为什么贯彻落实起来会千差万别：有的乘势而上，有的无动于衷？综合来说，原因是多方面的，但笔者认为，说一千、道一万，还是不少干部缺少一股干事创业的精气神。究其原因无外乎4种：**一是“麻木症”**，对中央关于保密工作决策部署，对中央保密委员会工作要求，对新时代保密工作的新情况新问题不敏锐、不关切、不研究，思想僵化，反应迟钝，习惯用老药方看新毛病，以不变应万变；**二是“依赖症”**，工作中碰到难题、遇到阻力，不是想着如何去攻坚克难，而是眼睛向上，寄希望于上级大包大揽，一旦不如意，总是把责任一股脑儿全推给上级，推给领导，从不找自身原因，检讨自己的责任；**三是“畏难症”**，保密战线需要解决的问题大多是长期历史遗留问题，多是些“硬骨头”，一些同志认为，这么多年都解决不了的问题，现在要解决谈何容易，继而成为自己敷衍塞责的理由；**四是“逍遥症”**，有些干部认为自己快要退休了，或者要调到别的岗位了，能放就先放一放，能推则推一推，不愿意再咬紧牙关来啃那些“硬骨头”。

2017年，中办、国办就各地各部门贯彻落实中央决策部署情况进行书面督查，之后又组成联合督查组对若干个省（市、区）和中央国家机关进行实地督查，并作出书面反馈。反馈意见条分缕析清清楚楚，白纸黑字明明白白。不久前召开的全国保密工作会议对2018年工作作出了全面部署，对贯彻落实中央决策部署提出了新的要求。此刻，摆在我们面前的任务明确而艰巨——提升精气神，以“钉钉子”精神抓好各项工作的落实。

提升精气神，要有“气吞万里如虎”的豪气。抓工作、干事业，容不了患得患失的自私者、鼠目寸光的短视者，需要志存高远的瞭望者、逆水行舟的搏击者。2018年，保密工作目标已明确，我们应该提高政治站位，放眼国内外大势，视党和国家保密事业为共同的使命担当，自觉在任务重与时间急、要求高与进度快、压力大与身心累中不断“淬火”，在火热的工作实践中聚集起虎口夺食的胆气、用我必胜

从《抓间谍者》出版风波看英国新闻出版保密

□李 杰

考察西方新闻出版泄密史，美国可谓“首屈一指”，不仅影响大，且数量多，如早前的“五角大楼文件”事件和最近的“斯诺登事件”等，据统计，从1979年到1988年10年中，美国有记录的新闻出版泄密事件大约500起，平均每年50起。与美国相比，英国新闻出版泄密事件较少，其中产生深远影响的是1986年《抓间谍者》出版风波。

《抓间谍者》出版风波及其影响

《抓间谍者》是原英国军情五处高级特工彼得·赖特撰写的回忆录，书中涉及英国情报机关的大量内幕和一些政界要人的丑闻。1985年9月，英国政府获悉该书将要在澳大利亚出版，派人前往澳大利亚，以损害英国国家安全为由，向澳大利亚新南威尔士州法院起诉，要求法院禁止《抓间谍者》在澳大利亚出版。1986年底，英国《卫报》《观察家报》摘要刊登了《抓间谍者》一书的内容。英国总检察长遂向英国衡平法院申请了禁制令，禁止这两家报纸继续刊登。

然而在两家报纸不服开始上诉期间，英国《独立报》《伦敦晚旗报》《伦敦每日新闻》也刊发了该书的摘要，英国总检察长以藐视法庭罪起诉这3家报纸，一审胜诉，但二审败诉。随后，英国总检察长上诉至上诉法院获得胜诉。上诉法院的结论是3家报纸的行为构成藐视法庭罪，其出版行为损害了保密制度，对司法审判程序造成了阻碍。

但在此后，企鹅出版社在美国出版了该书，英国《星期日泰晤士报》在获得授权后开始连载。英国总检察长对《星期日泰晤士报》也

的锐气、所向披靡的朝气。

提升精气神，要有“咬住青山不放松”的硬气。新时代保密工作的深度、广度、难度前所未有，各种不确定的风险与挑战层出不穷，遇到的困难和压力还会加大。正如邓小平同志所说：“没有一点闯的精神，没有一点冒的精神，没有一股气呀、劲呀，就走不出一条好路，走不出一条新路，就干不出新的事业。”这要求我们要有足够的定力、耐力和毅力，既要蹄疾步稳、一鼓作气，又要发扬“钉钉子”的精神，一锤接着一锤敲，持续发力。

提升精气神，要有“打铁还需自身硬”的底气。在复杂形势、繁重担子面前，不少同志感到力不从心。面对诸多矛盾与难题，任何唉声叹气都无济于事，我们更应该反躬自问：自己有没有理想滑坡、思想懈怠、斗志退化，有没有观念落后、知识老化、素质缺失、本领恐慌，有没有瞻前顾后、干劲不足。要对照党中央和中央保密委员会的要求，洞察细照深究，查找短板不足，列出问题清单，敢于刀口向内、刮骨疗伤。只有这样，才能不断补足精神之钙、缩短能力之差、清除作风之弊，才能汇聚起干事创业的磅礴力量。■

责任编辑/徐 琛

提出指控，并要求前述禁制令亦适用于《星期日泰晤士报》。该指控在一审中得到了支持，但是该案最终被上诉至英国上议院后败诉。上议院认为该书中原有的保密信息在出版后已经为公众知晓，发出禁制令已没有意义，故驳回了公诉人的请求。

《抓间谍者》出版风波在英国产生深远影响。《观察家报》一针见血地指出，《抓间谍者》出版风波产生了两项新的法律规范：一是法院可以限制英国媒体对涉密案件的报道，二是媒体的行为开始正式受到保密法律制度的限制。而这两项法律规范直接影响英国《卫报》对“斯诺登事件”的报道策略。

英国《卫报》对“斯诺登事件”的报道策略

2013年6月，“斯诺登事件”最早由《卫报》美国分社正式曝光，成为美国有史以来最大的泄密事件，引起全球舆论哗然。实际上，当《卫报》驻巴西分社专栏作家格伦·格林沃尔德在香港拿到斯诺登文件后，对于如何报道该事件《卫报》非常慎重。经反复考量曝光后面临的法律风险，《卫报》决定由美国分社首次在美国曝光，因为美国宪法第一修正案可以给媒体和编辑记者提供较好的保护。

随后，《卫报》伦敦总部也拿到了斯诺登持有的文件，其中包括大量英国政府通信总部参与互联网监控——Tempora项目的秘密文件。《卫报》总编辑艾伦·拉斯布里杰与媒体律师加文·米勒进行了深入研究。米勒建议，最安全的处理方式是立即销毁所有与英国相关的机密文件，另一种安全的备选方式是将文件交官方进行保密审查。但拉斯布里杰选择与政府沟通后曝光Tempora项目。在沟通过程中英国政府表示强烈反对，但并没有使用严厉的法律手段。6月21日，Tempora项目在《卫报》网站曝光，立刻引起反响。

7月12日，英国政府的态度逐步变得强硬，明确表示《卫报》必须返还政府通信总部的资料。英国内阁秘书长杰里米·海伍德说：“这件事我们可以愉快地解决，或者诉诸法律。”7月13日，英国内阁副国家安全顾问奥利弗·罗宾斯给《卫报》打来电话，称如果不交出文件，政府将关停《卫报》。迫于压力，《卫报》决定主动销毁文件。7月20日，在政府通信总部工作人员的监督下，《卫报》员工将存有涉密资料电脑的各个部件一块块地砸碎，再把砸碎的部件投入消磁器。此后，《卫报》被迫与《纽约时报》合作，继续披露美国国家安全局的相关文件。

《官方秘密法》对新闻出版的法律规制

《抓间谍者》出版风波之所以影响深远，《卫报》在报道“斯诺登事件”时之所以如此谨慎，主要是英国制定了世界第一部完整的成文保密法——《官方秘密法》，这部法律把公务员、政府合同商及其他人员（包括新闻出版从业者）的泄密行为定为犯罪。

英国的政治传统认为，公务人员应当对英王保持忠诚，不得泄露国家秘密。但直到19世纪中后期，法律上均未将泄密行为定为犯罪，泄密者只受道德谴责。在几个重大泄密案件中，政府均因此无法惩治泄密者。1887年，一名造船厂的制图员将军舰图纸泄露给某个国家。当时英国发动的殖民战争正进一步扩大，该军舰图纸对国家安全和战争胜负起着至关重要的作用。但指控因为证据不足而失败，泄密者最终只是被船厂解雇。英国海军部还专门就此向国会提交了需加强保密立法的提案。这份提案最终促成了1889年《官方秘密法》的出台。《官方秘密法》第一次规定，公务员、政府合同商及其他人员未经授权泄露政府机密信息应受刑事处罚。从此，保密成为英国公务员、政府合同商及其他人员（包括新闻出版从业者）应遵守的一项法定义务。

随着形势发展，英国分别于1911年和1989年对《官方秘密法》作了较大的修订，特别是1989年的《官方秘密法》将官方信息中秘密的范围进一步限制，压缩到4类信息：安全与情报、国防、国际关系、犯罪与特定调查权。现行《官方秘密法》第五节第一款规定了“未经合法批准而披露信息或披露

《官方秘密法》第一次规定，公务员、政府合同商及其他人员未经授权泄露政府机密信息应受刑事处罚。从此，保密成为英国公务员、政府合同商及其他人员（包括新闻出版从业者）应遵守的一项法定义务。

受委托保密的信息”的适用情形，行为人基于如下原因获得任何受本法前述各条之规定而不应泄露的信息、文件或其他文书：(1)公务员、政府合同商未经合法批准而擅自向他人泄露的保密信息；(2)经公务员、政府合同商授权在要求其保密的前提下或在公务员、政府合同商所从事的工作中理应要求其保密的前提下获得的保密信息；(3)通过上述第二种途径获得保密信息的人员未经合法批准擅自再次向他人泄露的保密信息。根据第三种适用情形，该法并未将新闻出版从业者排除在外。同时《官方秘密法》规定，违反本法规定者，要受到3个月至两年的监禁或罚金，或两罚并处。

英国政府除了依据《官方秘密法》对涉嫌泄密的媒体进行起诉外，同时还可以向法院申请禁制令，禁止媒体对涉嫌泄密事项公开报道。在英国，禁制令是典型的普通法救济手段。禁制令从字面上看似乎是一种禁止某种行为的法院命令，但实际上它既可以用于阻止、禁止、停止某人的某种侵权行为，这可被称为禁止性禁制令；也可以用于命令某人必须做出某种行为，这种命令则被称为强制性禁制令。禁制令可以是临时性的，旨在维持现状，等待法院进一步审理，作出终结性处理结论，以防可能产生的侵权行为发生，特别是防止某种不可弥补的损害发生。禁制令也可以是永久性的，除非法院另有命令，某人则永远不能做某事。在上述《抓间谍者》系列诉讼中，英国总检察长原本申请的是永久性禁制令，但法院最终签发的是临时性禁制令。

作为法院的命令，禁制令具有极大的权威，违反者以藐视法庭罪论处，或坐牢或处罚金。英国藐视法庭罪涉及的范围非常广泛，表现形式多样，早期主要是通过判例发展起来的。1981年，英国议会通过《藐视法庭法》，使普通法上的藐视法庭罪转化为制定法上的罪名。

以沟通机制化解政府与媒体之间的冲突

实际上，英国政府和媒体都尽量回避使用司法手段来解决彼此之间的冲突和争议，因为这将使双方陷入一场漫长的、前景不明朗且代价高昂的法律战。为了有效解决政府和媒体之间的冲突和争议，英国早在第一次世界大战时期就建立了一个常规性沟通机制——国防和安全媒体知会系统（Defence and Security Media Advisory Notice System）。

国防和安全媒体知会系统的核心是国防和安全媒体咨询委员会（Defence and Security Media Advisory Committee，DSMA）。2015年以前，该委员会称之为国防部、出版和广播咨询委员会(Defence，Press and Broadcasting Advisory Committee，DPBAC)。委员会主席通常由国防部副部长级官员担任，委员会副主席由媒体方面推举的首席代表担任，委员会秘书长是全职职位，通常由退役将军担任。政府方面的代表来自国防部、外交部和安全情报等部门，媒体方面的代表来自《卫报》《每日邮报》以及英国广播公司、独立电视台、天空电视台等十几家主流媒体。现任委员会主席为英国国防部彼得·沃特金斯局长，副主席为英国出版业联盟荣誉编辑乔纳·森格伦，委员会秘书长为退役将军杰弗里·多兹。

国防和安全媒体知会系统的运作程序是：当政府代表向国防和安全媒体咨询委员会提出某些信息因涉及国家安全而须媒体谨慎处理时，媒体代表要及时对该建议进行回复。当得到媒体代表的确认后，国防和安全媒体咨询委员会应向省级以上报纸、出版、广播和电视组织的编辑发出通知，要求停止传播某些涉及国家安全的信息。这种通知被称为“DSMA—Notices”。目前，该通知适用于5类情形：1.军事活动、计划和能力；2.核武器、非核武器及装备；3.密码与保密通信；4.敏感设施与内部地址；5.联合王国的特别安全与情报机构。

国防和安全媒体知会系统就其本质来说是一个沟通平台，其所下发的通知不具有法律约束意义，不遵守该通知可能导致的唯一结果是，政府和涉案媒体之间的信任关系将受到破坏并影响未来业务的开展。但总体上讲，国防和安全媒体知会系统在实践中对保障媒体出版权和国家安全起到积极作用。

例如，在“斯诺登事件”中，2013年6月16日，时任国防和安全媒体咨询委员会秘书长——退休空军少将安德鲁·瓦兰斯曾通过该系统，向《卫报》、英国广播公司、天空电视台等其他主流媒体下发通知，因事关国家安全，劝阻媒体不要跟进报道“斯诺登事件”，绝大多数英国媒体表示遵守，几乎没有媒体对该事件进行报道。《卫报》因不听劝阻受到政府的警告和打压，而其竞争对手《每日邮报》随后以爱国的名义攻击《卫报》“帮助英国的敌人”，犯有“致命的不负责任”之错误。■

历史的长河不知湮没了多少人和事。人类史上，被遗忘的东西如此之多，被记下来的东西少之又少。然而，伴随着数字技术和全球网络的发展，数千年来遗忘与记忆的平衡被打破，遗忘成为例外，记忆却成了常态。

当遗忘变成例外，而记忆成了常态

——数字化记忆与“被遗忘权”

□朱晓玲 齐 琪

现代信息技术，特别是大数据技术的蓬勃发展，使海量信息的存储和分析成为可能。一旦在互联网中发布信息，那么这则信息便可能永远存在，成为一个随时可被抓取的“标本”。特别是区块链概念产生后，数字化记忆的永久性更令人咂舌——如果区块链分布得足够广泛，那么删除或改写存储在区块链中的历史数据将变成一项不可能完成的任务。

基于此，“被遗忘权”的概念被提了出来。所谓“被遗忘权”，是指“一个人可以要求网络服务提供商（如搜索引擎或社交媒体）移除网站中与自己相关的内容”。其主旨在于，一个人应当拥有与自己相关信息的“所有权”，而数字化记忆使这种“所有权”不仅指向空间，还指向时间。需要注意的是，“被遗忘权”与许多国家确立的“删除权”有很大不同，差异最大的地方就在于，“被遗忘权”的行使不必基于违法行为，只要公民有删除个人信息的意愿，便可以提出诉求。

目前，“被遗忘权”已经被许多国家、地区和组织（如韩国、澳大利亚、欧盟等）确立为一项正式法案，在我国，这项权利也不乏关注者。2016年的任甲玉与百度公司名誉权纠纷案，就被不少公众视为“被遗忘权第一案”，引起广泛议论。此后，探寻“被遗忘权”本土化路径的呼声越来越高。

历史溯源

“被遗忘权”在西方国家早有雏形。有人认为，“被遗忘权”之所以在西方世界得到广泛认同，与欧美国家普遍重视信息保护的传统有关。早在1984年，英国出台的《数据保护法》便有公民有权删除个人信息的相关规定，该法甚至提出，即使公民未作相关要求，数据控制者也“应与数据主体保持定期联系，或向数据主体提供开放的数据库，以方便数据主体查询并发现不正确的个人数据”。1995年欧盟制定的《欧洲数据保护指令》等也规定了相关内容，可被视为整个欧洲范围内关于“被遗忘权”的确立。

“被遗忘权”成为近代西方司法实践中的正式用语，则起源于2014年5月的“谷歌西班牙案”。此案中，一家报纸刊登了西班牙公民冈萨雷斯（Gonzalez）因无力偿还债务而拍卖房产的公告。16年转眼而过，冈萨雷斯早已还清债务，但当他试着在谷歌搜索引擎中输入自己的名字时，仍会出现两个指向那则公告的链接。冈萨雷斯认为，这些信息已经过时多年，且与自己不再具有相关性，属于具有误导

性的负面信息，谷歌理应删去或隐藏相关链接。西班牙资料保护局批准了该项申请，随后冈萨雷斯与谷歌双方陷入诉讼。最终，欧盟法院对此案进行了宣判，表示谷歌将被要求删除“不适当、不相关或不再相关或超出其处理目的，以及已经过时的”数据，而这一审判的理由是“人们的隐私权重于公众的兴趣”。

第一次付诸司法实践后，“被遗忘权”很快在不少国家、地区被确立为正式法案。然而，美国大部分地区及一些其他国家和地区，却明确提出反对“被遗忘权”立法。围绕这项权利的争议始终纷纷扰扰，接连不断。

可行性之争

有关“被遗忘权”的质疑之声，大体可以分为两种：其一，认为其本身便存在逻辑问题，并且与法律的基本价值存在冲突；其二，对其本土化前景存疑，认为其难以成为一项“放诸四海皆准”的“基本权利”。

“被遗忘权”的主要功能无疑在于避免保存在网络上的、已经过时的信息继续侵扰信息主体当前的生活状态（比如，删除过去发布的求租信息，可以有效避免房产中介的骚扰）。然而，也有人认为，该项权利是对“自由”这一法律基本价值的侵害。比如，美国学者杰佛瑞·罗森就曾直接指出：“‘被遗忘权’是未来10年内互联网言论自由的最大威胁。”

确实，美国大部分州并不认同“被遗忘权”的价值。美国宪法极度突出自由的意义，任何其他法律法规的确立与实施都必须以自由为前提。互联网媒体无疑与传统媒体一样，拥有发布信息的自由。假如传统媒体出现错误报道，公民可以通过名誉权诉讼等制度得到救济。然而，“被遗忘权”的一大内涵在于，公民要求删除的信息可以不以违法行为为基础。也就是说，公民仅因为希望“被遗忘”，就可以提出删除合法存在于网络空间中的信息的诉求。这无疑是对网络媒体新闻自由权利的一种侵犯，“被遗忘权”一旦滥用，将会造成不可估量的恶果。

同时，有人认为，“被遗忘权”在澳大利亚、韩国及欧洲国家得到确立，一个重要的原因就是这些国家和地区都没有信息网络服务产业巨头以及网络产业集群，法案这块“板子”实际上是打在了别人家的“孩子”身上。更有人表示，这块“板子”甚至已经成为这些国家在个人信息保护及信息产业发展领域维护自身国家利益的工具。

中国与美国在互联网产业发展方面有不少相似之处，百度、腾讯、阿里等网络巨头影响着全世界数以亿计的网民。我国学术界的基本观点是，要引入“被遗忘权”，不仅需要对这项权利的基本内涵进行明确和论证，更须斟酌立法后的政治、经济、文化等多领域问题。比如，审理我国“被遗忘权第一案”的陈昶屹法官就提出，在大数据时代还没有发展定型的时候，即在相关法律还比较混沌的时期，不要过多增加干扰，而应该让其自然成长，在现有的规则下保持一种宽容。

除此之外，也有不少人担心“被遗忘权”将导致道德危机。诚然，“被遗忘权”给了人们自我保护的机会，但也因为可以任意提出申请将个人信息隐去或删除，人们犯错的成本大大降低，社会风气有可能受到不良影响。■

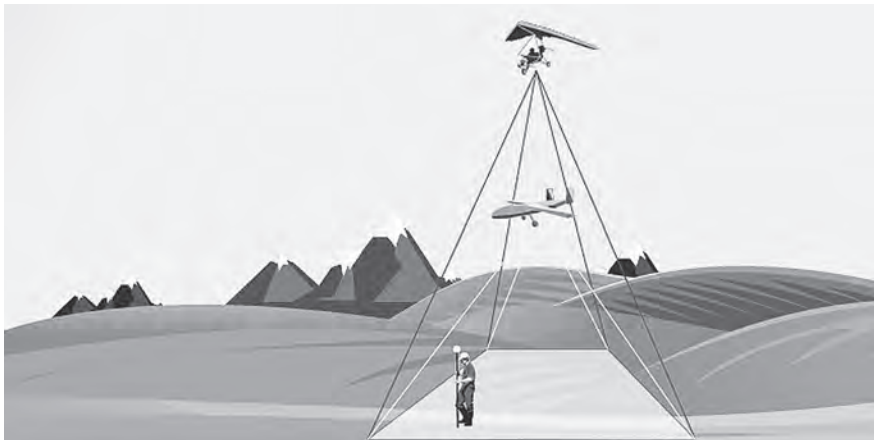
密言密语

工作再忙，“保密”不忘。
谨言慎行，重在日常！

保密就是爱国，
泄密就是害国，
窃密就是卖国。

保密，无处不在；
泄密，无形之中；
窃密，无孔不入。

作者：陕西凌云电器集团有限公司保密办 翟 宁



案析 国家基本比例尺地形图的保密管理

□吴 瑞

国家基本比例尺地形图是基础测绘成果的主要表现形式之一，涵盖了从1：500到1：100万在内的11种比例尺地形图，在各行各业中得到了广泛利用。按照保障国家秘密安全、促进地理信息共享和应用的原则，国务院测绘地理信息主管部门会同国家保密行政管理部门规定了测绘管理工作保密事项范围，明确了部分国家基本比例尺地形图的密级、保密期限和控制范围。一段时间以来，少数涉密测绘成果使用单位和测绘资质单位（以下简称用图单位）对相关保密管理制度执行不力，涉密测绘成果存储处理、使用保管和对外合作等方面存在突出问题，国家基本比例尺地形图被泄露的案件时有发生，给国家安全和利益造成严重威胁。

典型案例举要

案例1：制度缺失。2016年7月，某市保密局和国土局开展测绘地理信息保密专项检查时，发现辖区某县水务局无法提供在省测绘地理信息局申领的全套涉密测绘成果。经查，2008年7月，时任该县水务局设计队队长的刘某从省测绘地理信息局购回1套秘密级的本县地图，未明确专人看管，也没有建立图纸使用、借阅、归还、登记等相关保密管理制度，涉密测绘图纸日常使用、借取随意，管理混乱、交接不清，单位分管领导也未对涉密地图及相关涉密载体加强管理，结果导致地图遗失。事件发生后，有关部门给予直接责任人刘某行政警告处分，对负有领导责任的分管领导冯某诫勉谈话。

案例2：执规不严。2013年12月，某区保密局、测绘局在对辖区某县农牧局保密检查中，发现该局存在涉密测绘成果管理不规范，未建立台账，部分涉密地形图查无实物的问题。经查，2011年10月，该局副局长达某前往区测绘局申购了21幅（63张）涉密地形图，因草场承包经营责任制工作需要，该局局长琼某默认同意，部分涉密地形图借到部分乡镇使用，虽有借用记录，但未标注涉密地形图的密级和借用事由。负有保管职责的达某和专技人员欧某二人对涉密地形图的去向和返还情况均不掌握，琼某也从未过问。后经多方查找，找回失控的部分地图，另有1幅（3张）涉密地形图被确定为遗失。事件发生后，有关部门给予琼某党内警告处分，达某留党察看、行政降级处分，欧某党内严重警告、行政记过处分。

分析：以上两起典型案件反映出来的共同问题：用图单位没有建立或落实涉密测绘成果保密管理制度，最终导致地图失控乃至遗失。申领涉密地形图的单位不但要确保测绘成果存放设施与条件符合有关保密规定和要求，而且应当建立健全相应的保密管理制度，按照积极防范、突出重点、严格标准、明确责任的原则，对落实保密制度的情

况进行检查。案例1中，用图单位根本就未建立起基本的保密管理制度，把涉密地图混同于一般的文件资料，可以说这一套秘密级的县域地图自测绘成果档案库出库起，就处于完全失控的状态，遗失或被窃只是早晚的事。案例2中，用图单位没有真正落实涉密测绘成果保密管理制度，只有项目不全的借用记录，在各乡镇使用地图开展基本草场划定工作的过程中，普遍存在着涉密地形图被无序流转到基层单位和办事人员手中的现象，最终造成地图遗失的后果。

案例3：缺少登记。2013年8月至2014年3月期间，某市水管总站规划办主任李某在开展地区生态保护规划编制工作中，未按照规定对涉密地形图办理相关交接登记手续，保管不善，造成2幅1：5万机密级地形图在野外使用过程中丢失。事件发生后，有关部门给予直接责任人李某行政警告处分。

分析：本案的基本情节是在野外工作中丢失涉密地形图，但根源仍然是涉密测绘成果保密管理制度执行不力。用图单位应当根据相关规定对申领、接受的涉密测绘成果建立台账，按照管用分开的原则区分存放保管与日常使用，对涉密测绘成果使用、管理人员进行专项教育培训。特别是对于野外作业这类客观上将涉密测绘成果置于较高风险的工作环境、工作环节等，用图单位要重点管控并加强对相关人员的教育和提醒。

案例4：违规销毁。2015年8月，某省、市两级保密局会同市规划局对某电力工程咨询公司进行检查时，发现4张秘密级地形图查无下落。据当事人回忆，4张地形图由于在工程现场使用中受到污损，已无使用价值，故于2014年7月用碎纸机进行销毁。在销毁过程中，公司档案管理部门没有向上级主管单位提出书面销毁申请并进行销毁登记，也没有销毁审批和监销记录，销毁事实难以查证。事件发生后，有关部门给予责任人员王某、李某、赵某行政记过处分，并扣罚数月奖金。

分析：在使用目的或项目完成后，用图单位应当按照相关规定及时销毁涉密测绘成果，由专人核对、清点、登记、造册、报批、监销，并报涉密测绘成果提供单位备案，也可以请涉密测绘成果提供单位核对、回收并统一销毁。对于这类用图单位声称涉密测绘成果已经销毁但无法提供审批（备案）手续，同时也不能认定为泄露或遗失的情形，仍然应当按照保密法律法规追究涉案人员的责任。

案例5：扩大范围。2015年8月，某市规划局开展全市地理信息保密检查时发现，辖区某县水务局违反测绘成果提供使用的审批程序，于2012年2月向县规划局提供了全县域1:1万秘密级地形图；2013年9月，县规划局又将部分地形图提供给县旅游局；县旅游局在编制某旅游休闲专项规划的过程中，擅自将地形图提供给某社会公司。事件发生后，该县有关部门对水务局原局长马某、副局长周某、经办人员张某，规划局局长李某、副局长徐某，旅游局局长龙某、副局长谭某进行诫勉谈话；给予规划局直接责任人刘某行政警告处分，旅游局直接责任人高某党内警告处分。

分析：用图单位领取的国家基本比例尺地形图仅限于在被许可使用人本单位的范围内，按照批准的目的使用，不得扩展到所属系统和上级、下级或者同级其他单位。这是一起涉及多重违规提供涉密测绘成果的特殊案件，水务局等3家县直单位都存在未经审批向外单位提供涉密地形图的情节，所不同的是规划局和旅游局本身都没有按照法定程序来获取涉密测绘成果，而后者竟然还将涉密地形图扩散到社会上。

对国家基本比例尺地形图性质认识的偏差

用图单位对涉密测绘成果的管理不够重视，相关保密制度不建立、保密要求不落实是造成此类案件发生的根本原因，但对国家基本比例尺地形图的性质在认识上存在偏差，也是导致相应泄密案件发生的主观原因。

一是对涉密地图国家秘密属性的认识偏差。部分从业人员仅仅将包括国家基本比例尺地形图在内的各种涉密测绘成果视为本单位资产，根据业务工作需要简单处置，却对地形图的国家秘密载体这一本质属性视而不见。

二是对有偿规范使用的认识偏差。除用于国家机关决策和社会公益性事业外，各级人民政府及其有关部门和军队因防灾减灾、国防建设等公共利益需要，测绘成果依法实行有偿使用制度。用图单位在支付一定金额的费用，从测绘成果资料保管单位领取涉密地形图后，普遍存在一种将图“买”回的观点。为实现“效益最大化”，个别用图单位不顾保密法规，违规擅自复制、转借已申领到的国家基本比例尺地形图，更有甚者自定、协议价码，将涉密地形图转卖（包括复制转卖）给其他社会主体，在故意泄露国家秘密的同时也造成了极坏的社会影响。即便是正常使用完毕、相关项目终结的用图单位，也愿意将涉密地形图作为单位资产和档案留存，“舍不得”销毁的现象大量存在。

1：2.5万、1：5万和1：10万的国家基本比例尺地形图属于机密级国家秘密，1：50万、1：25万和1：1万的国家基本比例尺地形图属于秘密级国家秘密，涉及军事禁区的密级可能更高。由于涉密测绘成果具有较强的稳定性，长期关系国家安全和利益，因此测绘管理工作保密事项范围将所有涉密测绘成果的保密期限均设定为长期。可见，国家基本比例尺地形图首先是一种长期保密的国家秘密载体，这是所有用图单位必须清醒认识的关键所在，也是各项具体保密要求落到实处的前提条件。

强化用图单位涉密地形图的流程管理

涉密测绘成果的生产和使用涉及到政府、社会不同主体，同时也牵涉到汇交、保管、公布、利用、销毁等众多环节。从20世纪80年代后期，原国家测绘局系统的各资料部门对其保管供应的各种比例尺地形图均进行了统一编号登记，开具发图单时也注明相应地形图的编号，为便利检核、准确溯源提供了保障。

国家基本比例尺地形图泄密案件作为一种案件类型，主要发生在管理后端，特别是用图单位存在较多泄密隐患，而根源深植于对地形图性质认识的偏差，当前需要突出以下3个流程环节方面的保密管理。

一是入库环节。用图单位申领、接收国家基本比例尺地形图，应当将其保存于安全保密的场所和部位，并配备必要的保密设备，按照“管”“用”分开原则及时建立台账，指定专人专管。

二是使用环节。严格按照批准的目的和范围在本单位内部使用国家基本比例尺地形图，杜绝一切形式的复制、转让、转借行为（包括系统内其他单位），所有使用行为都应当做出书面记录备查。

三是销毁环节。使用目的或项目完成后，应当及时（至多在6个月内）按照规定销毁申领的国家基本比例尺地形图，不宜长期留存在用图单位。■

责任编辑/孙战国

作者：胡井泉（广东省清远市保密局）

记者走军营

北京的东三环，是首都最繁华的商业区之一，坐落其间的使馆区是中西方政治文化的交会地，风格迥异的各国建筑鳞次栉比，不同语言、不同国别、不同肤色的人们穿梭其间，展现了别样的神秘气息。在这块特别的土地上，驻扎着一支伴随共和国诞生而成长壮大的部队。作为我国唯一一支成建制的外事警卫部队，他们肩负国家使命，代表国家形象，日夜坚守在“第二国境线”上。本期，请随记者一起走进这支部队。

驻守在“第二国境线”上的忠诚卫士

——走进武警北京总队执勤第九支队

□本刊记者　徐 琛

3月，南方已是繁花绿水，北京的冬天才刚刚松动。仿佛一夜间，杨树高高的枝头挂满了柔荑花序，这是北京早春最常见的景象。

早上6点半，晨曦初露，第九支队某大队哨兵陈虹嶝已经出操。他今天的第一班岗哨是8点至10点。完成每日晨间的一系列训练、学习等任务后，陈虹嶝穿戴好自己的衣帽、皮鞋和手套，来到整容镜前，对着镜子仔细整理了自己的着装。7点50分，他和同班哨兵们集合列队，来到英雄卫士李登贵烈士的雕像前，郑重敬军礼，并高喊口号：“向英雄学习，保目标安全！”之后，他们整齐列队，走向自己的哨位。

向英雄雕塑敬军礼并宣誓的“仪式”，是该大队每班哨卫上岗前的“规定动作”。这一传统，他们已经坚持了42年。

清晨，一队哨兵行进在去往哨位的路上

有我在，就有使馆安全在

筚路蓝缕，以启山林。1928年，随着井冈山胜利会师，中央警卫师三团一营诞生。在那战火纷飞的年代，这支部队始终跟随党中央、毛主席转战南北。新中国成立后，根据外交任务需要，改编为武警外事部队，历经10余次编制体制调整，成为今天的武警北京总队执勤第九支队。从烽火之年到盛世之治，他们始终战斗在任务一线；从青萍之末到浪潮之巅，他们始终守卫着祖国尊严。

驻华使馆虽然在中国领土，但是根据《维也纳外交关系公约》和《中华人民共和国外交特权与豁免条例》规定，驻华使馆之内区域不得侵犯。因此，使馆门前那条泾渭分明的白线和使馆高高矮矮的围墙，就成为一种国界的象征。新中国成立初期，周总理曾来到外事警卫部队看望慰问哨兵，他称使馆哨兵为“小外交家”，使馆大门被形象地称作“第二国境线”。

使馆无小事，事事连政治。使馆区是国际政治风云的“晴雨表”，国际上刮起一阵风，使馆区就会掀起千层浪，很多国际局势动向会第一时间在使馆区有所表现。第九支队常年担负着外国驻华使

严冬，在使馆区周边执勤的哨兵

馆、联合国驻华使馆和外交部机关等执勤目标的警卫任务，警卫目标特别敏感，担负任务特别繁重，所处环境特别复杂，各级领导也特别关注。支队官兵始终在“聚光灯”下执勤，稍有闪失，就会在国际上造成负面影响，后果不堪设想。对于这一点，支队历任主官都有着清醒的认识。

早在1976年，英勇无畏的警卫战士李登贵就用行动诠释了哨兵的忠诚本色。那年，在苏联驻华使馆门前，领班员李登贵发现一名可疑人员随身携带的书包在冒烟，他迅速向来人迎去，疯狂的歹徒歇斯底里地狂喊：“我有炸药，快闪开！要不炸死你！”千钧一发之际，李登贵将歹徒死死抱住，随即“轰”的一声巨响，顿时，使馆区门前硝烟弥漫，李登贵壮烈牺牲。他用年仅23岁的生命，践行了“有我在，就有使馆安全在”的铮铮誓言。他是使馆警卫的脊梁，外交事业的功臣。如今，李登贵的雕像被摆放在其生前所在连队，供官兵瞻仰。2016年9月10日上午，俄罗斯驻华大使安德烈·杰尼索夫率使馆工作人员向李登贵烈士雕像敬献了花篮。

英雄壮举彪炳史册，英雄精神永励后人。一茬又一茬的外事警卫循着英雄的足迹，把哨位当战场，视执勤如打仗，为使馆区筑起一道坚不可摧的安全屏障。

严审核，确保哨兵“绝对忠诚”

新时代，习近平主席高度重视武警部队建设，给北京总队提出了“建设一支听党指挥、能打胜仗、作风优良的首都维稳精锐之师”的期望重托。如何把习主席的嘱托落到实处，是摆在支队党委首长面前的头等大事。在这个过程中，保密工作不可或缺，是重要一环。

使馆区的安全离不开保密工作的保驾护航，在外事警卫勤务中，保密工作有着特殊的意义。保密工作的特殊性在于讲政治，政治属性是保密工作的根本属性。尤其是近年来，随着国际形势的发展和恐怖活动的蔓延，高危敏感目标越来越多，预警信息不断，冲闯、拦车、投掷以及企图爆炸、袭击、破坏等安全事件时有发生。

面对新形势，支队党委始终按照“党管保密、领导带头、专职主抓、主体主责和群防群治”的原则，将保密工作摆上重要位置，纳入重要日程，在硬件建设上给予经费支持，在人员调配上给予重点倾斜。特别是将保密工作与安全管理结合起来，统筹兼顾，科学用力。

支队政委告诉记者，作为外事警卫的精兵劲旅，他们在官兵的选拔和培养方面要求非常高，除了具备征兵的基本条件外，还要特别关注兵员的政治条件，经过层层筛选和严格的政治考核。

“当时，和我一起入伍的几个朋友，他们的政治审核表只有一两页，而我的则有一厚沓，部队领导家访就做了四五次。那时，我并不知道这支部队的任务是什么，就觉得挺神秘的，领导要求不该说的不说，不该问的不问，纪律很严，我在脑海中形成了最初的保密概念。”2016年9月入伍的陈虹嶝回忆道。他还告诉记者，新兵入营后，他接受的第一项教育就是保密教育，除了学习相关的保密法律法规和制度规定，还观看了失泄密案例警示教育片。“当时，指导员跟我们说，作为九支队的兵，必须绝对纯洁，绝对忠诚，绝对可靠。那天看到、听到的一切，我印象特别深刻，一辈子也忘不了。”

重教育，真正实现“管住脑子”

地处商业繁华地带，身在中外文化交会地区，岗台对着吧台，商场对着操场，九支队官兵每天工作和生活的环境，一定意义上说，就是“四反”斗争的最前沿。他们这样总结：“每天看着外国旗，始终想着五星红旗；每天看着外国人，始终不忘自己是中国军人；每天听着外国话，始终牢记党的话。”

为了筑牢思想防线，真正有效“管住脑子”，支队党委在加强官兵的思想政治建设和保密教育方面没少花心思。每季度，由支队常委带头，为全体官兵进行集中保密授课；每月组织一次保密专题教育；每周一的常态化安全教育中，要有保密工作情况通报。他们还开设了“使馆卫士大讲堂”，邀请军地专家结合当前的国际国内形势、军内军外情况作专题讲座，进一步拓宽官兵视野，让大家了解大势，掌握大局，以便在执勤过程中更好地处理突发事件。“‘第二国境线’影视厅”的开设也是支队党委在忠诚教育、信念教育、保密教育方面的有力举措，通过播放传统红色影片和当前的爱国主题大片，有力促进官兵民族自信心、国家自豪感的养成，很受大家欢迎。

哨兵是使馆安全的第一道屏障，使馆警卫任务的特殊性告诉大家：勿以职务不高而认为人微言轻，勿以知密多少而认为无关紧要。每逢重大任务前，支队必先重申保密规定，制定保密措施，进行保密检查。执行任务中，所有人员坚决做到：个人不携带涉及任务、人员、装备等信息的资料，不使用个人手机进行拍摄，不通过非保密通信设备传递任务指令、谈论任务事项，不擅自接受媒体采访，等等。

过不了网络关，就过不了时代关。当前，手机上网已成常态，失泄密风险倍增。武警北京总队领导高度重视手机安全保密工作，总队保密部门每月对所属支队进行一次不打招呼的手机保密检查，查到问题立即通报。压力层层传导，责任层层压实，支队党委决定，要有针对性地加大对互联网和智能手机的保密检查力度。2017年8月，支队抽调5名机关干部，对近3000部手机进行保密检查，查看是否存有涉军图片和视频资料，是否违规开启定位功能等。去年，还对一名士官违规使用手机问题进行了公开处理，举起了戒尺，警示了部队，真正打出了教惩并举的“组合拳”。

某使馆门前，哨兵正在执勤

塑形象，练就过硬本领

采访中，支队指导员表示：“使馆警卫哨兵既是保卫使馆安全的压舱石，又是异域文化间传播和平与友谊的使者。我们站在使馆门前，代表的是国家，既要完成好警卫任务，也要体现出中国武警的良好形象。”

从新兵入伍那一刻起，除了严格的军事技能训练，支队还围绕“看功”“听功”“站功”“问功”“走功”“辨功”“嗅功”等内容加强特色训练。外国驻华大使馆共有100多个，再加上国际机构，共有数百个车号。作为一项基本功，官兵们要熟记这些车号对应的国家和驻华机构。“看车识人，见号识馆”，是每个使馆哨兵的必备素质。在此基础上，他们还要对警卫目标的所在国国旗、人口、面积、首都、民族、货币、政党、禁忌、领导人，以及宗教文化、风土人情、语言、艺术、建筑风格等情况有所了解。通过学习和训练，每一名哨兵都要逐渐成为问不倒的“美国通”“俄罗斯通”“日本通”……

进入新时代，随着我国综合国力的增强，外交地位的提升，第九支队使命任务不断拓展，实现了由传统模式执勤向多元常态维稳的历史性转变。近年来，他们圆满完成了历年全国“两会”、历届“党代会”、亚运会、奥运会、APEC会议、一带一路峰会等重大活动，圆满处置了涉美、涉日、涉菲等大规模游行示威活动，多次受到党和国家领导人、军委、总部首长的褒奖。

执干戈以卫社稷，舞长缨以守安全。武警北京总队第九支队不仅是一支敢于打硬仗、勇于打大仗的雄狮劲旅，更是一支有礼有节、不卑不亢、作风优良的文明之师。他们是不折不扣的忠诚卫士！■

武警贵州总队：军地融合抓好保密工作

□武警贵州总队副司令员　李 沛

为深入贯彻习主席关于抓好保密工作的重要指示精神，武警贵州总队紧密结合形势任务和单位实际，积极借助地方资源抓保密工作，为圆满完成多样化任务提供有力支撑。

请进来教，着力增强拒腐防变的“免疫力”。一是注重前瞻性。着眼信息技术发展给保密工作带来的严峻挑战，借助贵州发展大数据的资源优势，多次邀请省公安厅、国安厅、保密局等单位的专家领导到总队授课辅导，给大家普及信息技术常识，不断强化官兵的敌情意识和自律意识，提高安全防护技能。二是注重灵活性。着眼新形势新任务保密工作的特点规律，精心制定保密教育“食谱”，在新兵入营、老兵退伍、干部转业、重大活动等时机，对口邀请地方业务部门到部队举办知识讲座，积极开展保密科普进军营活动。同时，将保密规定做成警示卡片，时时处处警示和提醒官兵。三是注重实效性。在突出保密常识、法规制度和文件精神学习的基础上，邀请地方专家现地教学，介绍信息技术前沿动态和发展趋势，了解掌握新型的窃密方式和泄密渠道，积极参加省（市）保密局网络知识和防护技能培训；及时梳理官兵在学习过程中遇到的问题，让专家有针对性地一一讲解，用小话题破解大课题，进一步激发和增强官兵勤于学习、善于思考、勇于创新、敢于实践的自觉性和主动性。

融起来建，着力打造防间保密的“隔离带”。一是搞好统筹规划。总队始终把信息化建设、安全保密建设作为重要内容纳入整体建设，统一规划设计，提前预留经费，同步组织实施。同时，进一步加强与地方信息部门、大数据中心的沟通联系，聘请地方专家进行技术指导，避免盲目建设造成资源浪费，切实建成“非法用户进不来、涉密信息盗不走、网络基础摧不垮”的安防体系。二是搞好常态交流。定期参加地方保密工作会议，加强沟通联系，密切协作配合，形成工作合力；参加地方组织的保密工作协作小组活动，增强交流，互帮互学，共同提高；积极参加地方组织的考核评比和比武竞赛，取得较好成绩，既锻炼了队伍，又展示了形象；多次选派骨干到省保密局、档案局、机要局等地方保密单位进行业务培训和参观见学，进一步拓宽视野、增长见识，提高能力。三是搞好资源共享。邀请有关部门专家对集中采购的涉密办公设备进行保密检测，严把办公设备“入口关”。与地方资质企业分别签订涉密载体印制、信息系统集成、电子设备维修等保密协议，既弥补了自身能力不足的问题，又避免了乱印、乱修、乱恢复的现象发生。将整理归档的涉密载体定期集中送交贵州省涉密载体销毁中心，确保涉密载体流转的最后环节安全可靠。

联起来管，着力构建群防群治的“防护网”。一是建立军地协作机制。贵州省保密委员会将总队纳入核心秘密载体传递保障小组、保密工作第四协作小组、档案工作第五协作小组，每半年召开一次会议，互通信息，分析形势，研究对策；经常走访座谈，交流经验做法，取长补短，共同提高。二是建立联合检查机制。采取经常查与突击查、普遍查与随机查、专项查与综合查的方式，在对重大活动、重要时段、重点人员、要害部位进行检查的同时，建立联合检查机制，每年会同公安、国安、保密等地方单位，对营区周边保密环境进行检查，形成军地携手、齐抓共管的良好局面。三是建立联管联控机制。与省政府应急办、公安网监中心、三大通信运营商建立涉军舆情应急响应机制，将官兵的手机、QQ和微信号统一登记备案，实行全程管控，着力构建上下联动、军地齐管、群控群防的保密防范体系。■

责任编辑/徐 琛

大数据时代的公开与保密

中共中央政治局2017年12月8日就实施国家大数据战略进行第二次集体学习。习近平总书记在主持学习时强调，大数据发展日新月异，我们应该审时度势、精心谋划、超前布局、力争主动，深入了解大数据发展现状、趋势及其对经济社会发展的影响，分析我国大数据发展取得的成绩和存在的问题，推动实施国家大数据战略。4月22日，首届数字中国建设峰会开幕，习近平总书记在贺信中对加快数字中国建设作出重要指示。大数据战略背景下，对保密工作有何挑战？有哪些泄密风险？如何防范？政府信息公开与保密法律体系如何衔接、完善？本期聚焦国家大数据战略，对以上问题进行阐释。

大数据格局下的保密、泄密与防范

□李伟国

也许你已经习以为常，早上出门上班，手机告诉你到单位需要多长时间；也许你已经司空见惯，新闻客户端的头条都是你关心的话题；也许你已经不足为奇，各家电商向你推介准备入手消费品的打折信息；也许你已经见怪不怪，通讯软件将多年杳无音信的同桌推荐给你。可是！你并没有告诉手机，我的单位在哪，我想看哪些新闻，我需要哪些消费品，谁曾经是那个同桌的她。这就是大数据！短短几年时间里，我们自觉或不自觉、自愿或不自愿地产生着大数据，同时也被大数据所环绕、笼罩和支配。大数据颠覆了我们的生活方式，也对国家安全产生了巨大影响，国家秘密更是首当其冲。大数据模糊了密与非密的界限，打破了传统的定密习惯，改变了情报搜集的方式，也给反窃密防泄密提出更大的挑战。

大数据时代对保密范围和方式的挑战

随着传感网和物联网的快速发展，人、机、物三元世界高度融合引发数据规模几何式增长和数据模式极度多样化，网络化的大数据时代已悄然来到我们身边。大数据时代对于保密工作的直接挑战是，一些重要信息可保性急剧下降，关系国家安全的关键性数据亟须纳入保密管控。

1.原属于政府控制的一些重要信息可保性急剧下降

日本3·11地震期间，政府先向公众宣称放射程度没有那么危险，核辐射处于控制之中；随后，核反应堆墙体被冲垮，在冒着滚滚浓烟的画面下，政府欲盖弥彰仍称情况在不断好转。大数据时代，这种行为只能称之为作死，日本各地成千上万人自发上传盖革（Geiger）计数器（用于测量放射性污染程度）数据，通过Pachube平台对外发布，政府和东京电力公司的“人设”瞬间崩塌。在一个可以有效感知并能分享信息的世界中，将数据算法运用到大数据上，就不难对部分政府希望保密的事项进行推断和预测，这显然是对传统政府垄断重要信息的巨大挑战。舍恩伯格等在《大数据时代》中举例，美国劳工统计局每个月统计、公布消费价格指数（CPI），花费巨大且结果滞后。两位麻省理工学院经济学家通

随着传感网和物联网的快速发展，人、机、物三元世界高度融合引发数据规模几何式增长和数据模式极度多样化，网络化的大数据时代已悄然来到我们身边。大数据时代对于保密工作的直接挑战是，一些重要信息可保性急剧下降，关系国家安全的关键性数据亟须纳入保密管控。

过软件在互联网上每天收集50万种商品价格信息，通过大数据分析，就能比官方提前两个月发现通货紧缩的趋势。

对数据进行有选择性地屏蔽是政府控制信息的传统方法，大数据时代此法可能不再奏效。以“谷歌街景”作为类比来看，谷歌公司的图像采集车在很多国家采集了道路和房屋的图像以及大量备受争议的数据，德国民众强烈抗议这一行为，认为这些图片会帮助黑帮窃贼选择有利可图的目标。在巨大压力下，谷歌公司将一些房屋或花园的影像模糊化，但这种模糊化却起到了此地无银三百两的反作用。与之类似，如果政府试图屏蔽某些大数据库里的数据，则有可能引起相反的效果。

大数据格局下，要求政府重新审视需要保守的国家秘密范围，对于已不具有可保性的，及时从范围中剥离出去；对一些通过大数据分析有可能被准确预测，且确实关系国家安全的信息，要研究如何切断数据获取、分析和预测的途径，而不仅仅是将国家秘密信息放在保险柜中。

2. 一些关系国家安全的基础数据逐步显示出保密的重要性

大数据背景下，过去没有引起足够重视的一些数据，对国家安全的重大影响逐步显现。比如，过去我们对人种基因的安全重视不够，随着医疗大数据、基因大数据的快速发展，已直接关系国家存亡甚至种族延续；对垄断性电商销售数据的长时间汇总、分析，就有可能直接掌握各地区经济发展态势、居民购买力等重要信息。

此外，大数据将对涉密人员管理产生巨大影响。我们的通话、电子邮件、即时通讯信息等被加上时间印戳备份在通讯公司、软件公司的服务器中；我们在电商处买东西的偏好和支付能力被详细统计分析；我们的即时行踪被手机厂商完全掌握；甚至我们的音容笑貌都被各大街角和商场的摄像头实时捕捉并存储在网络上。可以说，每个人在大数据面前都是一丝不挂，当然也包括涉密人员，这就有可能对国家安全产生间接威胁。帕特里克·塔克尔在《赤裸裸的未来》中举例，2010年，美国罗切斯特大学研究员亚当·萨迪雷克组织了一项研究，如果锁定的目标关掉GPS，且不再发布含有地理定位的信息，能否对其准确定位？他们通过搜集目标朋友或亲属公开的推特信息，利用其中带有的定位标签，大数据分析预测目标的行踪准确率高达47%。2011年，萨迪雷克和研究员约翰·克鲁姆又组织了一项研究，他们雇佣了数百个受试者，让其随身携带追踪器。经对受试者及相关人员超过6年的监测，可以通过大数据分析，在80个礼拜或更久前预测受试者所在的位置，准确率高达80%。

可以想见，未来的保密已不仅仅是信息的保密，构成信息的基础数据的保密将会同等重要。这要求我们不仅仅考虑信息的保密，还要考虑在大数据分析条件下，哪些数据可能推测出相关信息。必要时，要通盘考虑对数据的保密管理要求和技术防范措施。

3. 一些大数据与国家安全的关联程度正在不断增强

总体国家安全观提出的国家安全体系，使得国家安全的外延得到进一步延伸。国家安全的概念不仅包括传统上的政治、军事、领土等国家生存安全的领域，还逐步扩大到包括文化、社会、科技等多个国家发展安全的领域；不仅包括传统安全领域，还包括非传统安全领域。在涉及国家发展安全方面，如经济安全、生态安全等，一定程度上依托于大数据安全；在非传统安全领域，如粮食安全、文化和意识形态安全、网络与信息安全等，都涉及或者包含大量的相关行业、部门、区域的大数据信息，而掌握这些信息，并由此进行梳理、整

合、分析，可以得到更有价值涉及国家安全的重要信息或者重要结论、判断。比如，我们对粮食安全的判断，可以基于耕地数据、气候数据、农业技术数据以及农产品市场数据、主要产粮国家经济政治数据等予以推断；我们对金融安全的判断，可以基于信息化背景下金融系统大数据的分析和研判。因此，大数据在一定程度上直接决定了很多国家安全领域重要信息的安全与否。

当前，世界主要国家在数据主权上的博弈日趋激烈，发达国家相继推出“数据治国”战略并制定发展规划以赢得先机。对此，我们必须未雨绸缪、防患未然，在总体国家安全观的指引下，认真分析对国家安全可能造成重要影响的大数据安全，并有针对性地采取保护措施。

大数据时代的泄密风险

随着时代的发展，保密管理经历了针对纸质文件资料的“三铁一器时代”、针对电子文件资料的“涉密信息系统管控时代”。这些方式之所以有效，在于找到了纸质和电子文件资料泄露的风险点。大数据时代，泄密风险发生了质的变化，需要有针对性地研究。

1. 大数据时代国家重要信息的拥有者和发布者不断分散

过去，国家重要信息的拥有者和发布者主要是国家。大数据时代，信息的跨国流动已成为现实，政府不再是信息的唯一拥有者和权威发布者。全世界单独的个体被调动起来形成巨大的合力，足以打破政府对信息的控制。比如，在马航MH370失联事件发生后，美国数字地球公司通过Tomnod软件应用平台，提供其所汇集的失联区域数据和高分辨率卫星图像，邀请来自世界各地的科技志愿者搜索失联航班的任何迹象。该平台共动员了全球800万志愿者寻找失联航班，提供各类信息。不难预见，这种动员能力如果用于针对获取某个特定国家的国家秘密和重要情报，后果是不可想象的。据报道，美国数字地球公司最赚钱的业务，就是为美国情报界提供相关服务。该公司曾经在上述软件应用平台推出了一个名为“搜索挑战”的项目，要求志愿者利用其发布的高分辨率卫星图像，帮助搜索上千平方公里内的军事飞行器和车辆。值得玩味的是，这个搜索项目的目的并没有公布。

2. 大数据时代国家重要信息的存在方式发生巨大变化

从大数据发展态势来看，即将到来的世界是人、机、物融合的三元世界，机中有人、人中有机，物中有机、机中有物的世界已逐步走近我们。随着人、机、物的相互融合，对不同领域的大数据进行跨领域、集成式研究，就有可能推测和判断国家重要信息。比如，针对某涉密科研院所，通过对研究人员在互联网及数据库中的搜索记录进行分析，可能了解研究课题的主要方面甚至遇到的瓶颈问题；对该院所最近一段时间购买仪器设备记录进行分析，可能推断正在进行的课题研究方向甚至进展程度；对该院所研究人员、管理人员的电子邮件进行分析，可能发现有关项目的协作配套等信息；从该院所公开的外部人员来访报道进行分析，可能推测出项目委托方情况；如果可以幸运地侵入该院所实验设备构成的物联网中，获得产生的实验数据，据此判断项目进展情况就显得更加轻而易举了。也许单一来源的信息可能不会暴露国家秘密或重要情报，但如果像上述分析一样，可以将某个事件、某个人或者某群体的很多行为，从不同的独立角度聚集在一起时，信息就有可能被泄露，因为有关这个事件、这个人或者这个群体的数据已经足够多。传统以信息为主要形态的国家秘密或重要情报，在大数据时代发生质的改变。它们不仅简单地以文件、图片、资料的形式存在，还可以通过直接或者间接有关的大数据，经过细致的分析、推理和判断，描绘出其细致轮廓，甚至分毫不差。

此外，部分大数据自身就是重要的战略资源。比如，媒体频繁披露的境外机构、人员在我境内实施非法测绘活动，其目的就是获取我国家基础地理信息数据；再如，媒体曾报道美籍华人薛峰实施非法窃密活动的主要目标就是我油气资源数据。其他譬如气象数据、基因数据等，也是境外非法获取的重点目标。

3. 大数据时代获取国家秘密和重要情报的渠道不断增多

近年来，境外非法获取国家秘密和重要情报的方式日趋多样，大数据分析重要性显著上升。《参考消息》2014年11月24日报道，据美国情报系统的研究，所有情报中有90%来自公开渠道，只有10%是通过秘密管道获取。显然，大数据分析

功不可没。

观察各种复杂系统得到的大数据，直接呈现出来的往往是一个个孤立的数据和分散的链接，但这些反映相互关系的数据和链接整合起来就是一个网络。大数据往往以数据和链接背后复杂的关系网络予以存在。大数据分析给窃取国家秘密和重要情报提供了重要依循，通过对数据背后的网络进行查找、分析和挖掘，基于相互关系分析基础上进行预测即可获得或者推断有关信息。此外，对于已经获得的国家秘密和重要情报，还可以通过大数据分析的方式，印证信息的准确与否。比如，对于一些重大涉密会议、活动安排，可以通过组织人员、已知参加人员的即时通讯记录、电子邮件记录数据，有关机场、火车站的调度安排、警卫情况数据，宾客下榻酒店客房、餐饮准备数据等大概分析出会议、活动参加人员、行程、议题等内容，而不必一定拿到会议、活动安排方案。再比如，对于一些涉密的军队调动情况，通过相关地区的摄像头监控网络数据、有关机场或火车站的调度数据、有关军队饮食供应站情况数据，如果再增加一些沿途网民上传的照片、消息等数据，将会准确掌握军队调度的路线、规模甚至目的等重要信息。

4. 大数据分析获取国家秘密和重要情报成为常态

大数据分析不同于传统的逻辑推理研究，而是通过将海量碎片化的数据汇聚到一起，积少成多，再进行统计性的搜索、比较、聚类、分类等分析归纳，在碎片化的数据之间建立某种整体联系，就有可能挖掘出隐藏在大数据背后的重要信息。因此，大数据分析具备了从大量不敏感信息中发现国家秘密和重要情报的能力，日益成为境外情报机关搜集信息不可或缺的重要渠道。

美国国家安全局长期对全球通信系统和互联网进行大数据采集、挖掘和分析，从中搜集他国国家秘密和重要情报信息。斯诺登曝光的美国国家安全局实施的棱镜计划（PRISM），显示出美国情报机关较早便采用大数据分析方式获取情报，甚至可以说美国情报机关具有疯狂获取大数据的特殊癖好。棱镜计划监视范围很广，参与的公司包括微软、雅虎、Google、Facebook、Paltalk、YouTube、Skype、美国在线、苹果公司等；采集的数据范围很广，包括日志数据、社交网络数据、过程行为数据、传感网络数据、智能终端数据等，可以监控包括电子邮件、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料等信息。

台湾地区情报机关也在强化运用大数据分析方式获取大陆情报。2015年，媒体曝光了台“国安局”建构了运用大数据概念的“舆情监控系统”对大陆搜集情报，可同时搜集超过200个网站、1000个网页，并对海量网络数据进行自动分析、存取。据《环球时报》报道，早在2007年，台湾地区情报机关已对我政府和军队以及国防科研机构、军工企业网络实施大规模的网络攻击行动，受攻击单位遍及我绝大部分省、自治区、直辖市，还包括我十几个驻外机构。台湾地区网络间谍李芳荣案中被控制的电脑和网络达数百个，窃密内容涉及政治、军事、外交、经济、医疗卫生等多个领域。不难看出，此类网络攻击的动机就是窃取目标用户的海量数据，作为大数据分析窃密的基础。

大数据时代的风险防范

习近平总书记强调，要切实保障国家数据安全。要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。要加强政策、监管、法律的统筹协调，加快法规制度建设。大数据时代的到来，必将推动保密管理又一次产生新的革命性变革，直接对保密的方式、要求和标准产生质的影响。对大数据时代的泄密风险防范，我们必须进行深入研究，切实采取有效措施以应对这一重大变革。

1. 从过去的信息保密为主转变为数据、信息保密并重

数据是信息的载体，信息是数据的内涵。数据的价值不只限于特定的用途，它既蕴含我们所需要

习近平总书记强调，要切实保障国家数据安全。要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。要加强政策、监管、法律的统筹协调，加快法规制度建设。大数据时代的到来，必将推动保密管理又一次产生新的革命性变革，直接对保密的方式、要求和标准产生质的影响。

的信息，也包罗我们尚未发现的信息。判断数据的价值需要考虑到未来它可能被使用的各种潜在方式，而非仅仅考虑它目前的用途。大数据时代告诫我们，不能把眼光仅仅局限在涉密信息的安全上，还要考量能够直接获得或者推测判断出涉密信息的基础数据的安全。要充分认识这些基础数据的基本价值和潜在价值。需要注意的是，大数据时代的一个突出特点是，非结构化数据的比例要远远高于结构化数据或半结构化数据。不论是结构化数据、半结构化数据，还是非结构化数据，这些数据都具有显性或者隐性的网络化存在，使得数据之间的复杂关系无所不在，一旦忽视其中的重要环节，就有可能导致重要情报的泄露。因此，大数据时代给我们的第一个挑战就是，对于关系国家安全和利益的数据进行准确的判断和筛选，既要注意各类结构化、半结构化数据，也需要考虑容易引起忽视的非结构化数据。

2.从过去的严防死守为主转变为预防为先、攻防结合

过去我们对国家秘密信息的保护，往往是通过切断或者减少信息传播的途径来实现的，比如知悉范围的最小化、信息设备的物理隔离等。大数据时代下，这样的方式显得力所不及。大数据分析的优势和缺陷是一致的，即通过大数据综合分析可以得到有效信息的前提是，用于分析的数据“噪声”比较少，即虚假或者无用数据相对较少。大数据分析的真正意义在于对数据进行分析之后产生的价值，因此数据的可靠性和准确性是实现价值的关键因素。关于大数据的一个普遍观点是，数据自己可以说明一切，数据自身就是事实。但是，成也萧何，败也萧何，如果对基础数据不仔细甄别，数据也会欺骗。正如由于网络刷单的存在，我们现在已经越来越难地从电商卖家的销售数量中判断该卖家的信誉和货品的质量；我们也很难通过点评网站上用户的点评，判断某家餐馆的菜品质量。因此，为了保护一些关系国家安全和利益的大数据，我们可以人为地制造“噪声”，使其无法或者很难从真假混杂的大数据中提取出有效的数据。通过伪造或者刻意制造的数据，可以引导分析者得到错误的结论，诱导分析者获取不实的信息。

3.准确、合理、有区分地判断数据的保密、共享与公开

大数据时代开启了一场寻宝游戏，不同的人对大数据的因果关系有不同的理解，不同的人也就可以在浩瀚的大数据中挖掘不同的宝矿。2015年8月，国务院常务会议通过《关于促进大数据发展的行动纲要》，提出要推动政府信息系统和公共数据互联共享，深化大数据在各行业创新应用。由此可见，通过大数据的共享共用，实现对各方面事业的巨大推动作用，是当前经济社会发展的一个重要着力点。恰当地控制大数据可能造成的危害和充分地利用大数据共享所产生的巨大成效，是摆在大家面前的一项重要抉择。在国家大数据战略背景下，需要我们认真地研究大数据互联共享可能造成的潜在危害，并根据实际妥善采取相应的方式，有效地控制这种危害的产生。要坚持大数据互联共享为原则，关系国家安全和利益的数据保密为例外，把必须保密的数据控制在最小的知悉范围，适当限制可能危害国家安全和利益数据的共享，密切关注公开的大数据并能在一旦发生危害国家安全情况下，采取必要的应急处置措施，这应当是我们面对大数据保密、共享与公开应有的态度。

习近平总书记强调，善于获取数据、分析数据、运用数据，是领导干部做好工作的基本功。各级领导干部要加强学习，懂得大数据，用好大数据，增强利用数据推进各项工作的本领，不断提高对大数据发展规律的把握能力，使大数据在各项工作中发挥更大作用。大数据时代的到来，对保密工作而言是挑战也是机遇，需要我们站在更高更广的层面，系统研究保密的范围以及保密工作的对象、方式，实现保密工作在大数据时代的转型升级。学好大数据这门必修课，应当成为每一位保密工作者的基本功。■

责任编辑/孙战国

大数据时代的公开与保密

大数据战略下政府信息公开与保密法律体系的完善

□黄道丽

大数据时代，信息已成为国家基础性、战略性资源，各国纷纷将大数据上升到国家战略层面。2015年，《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》首次把“推进数据资源开放共享”上升为“国家大数据战略”的组成部分。2016年，《国家信息化发展战略纲要》明确提出“构建统一规范、互联互通、安全可控的国家数据开放体系”，将安全可控作为国家信息公开顶层设计制度的三大基本要求之一。2017年12月，习近平总书记在中共中央政治局就实施国家大数据战略进行第二次集体学习时再次强调，实施国家大数据战略，要加强政企合作、多方参与，加快信息资源整合与开放共享，同时要切实保障“国家数据安全”。从讲话可以看出，大数据战略下的“国家数据安全”同时涉及关键信息基础设施安全、关键信息资源安全、企业信息和个人信息安全，并最终指向国家安全、社会公共利益及企业、个人合法权益。

政府信息公开与安全保密的立法现状

大数据是信息化发展的新阶段，发展与安全作为大数据战略之两翼，二者的辩证关系毋庸多言。保密法第四条明确规定，保密工作实行积极防范、突出重点、依法管理的方针，既确保国家秘密安全，又便利信息资源合理利用。法律、行政法规规定公开的事项，应当依法公开。这从另一侧面凸显了大数据“安全、发展”的二元价值特性，确立了政府信息公开与安全保密并重的基本原则。

除了保密法及其实施条例外，《国家安全法》《军事设施保护法》《刑法》等众多的行政法规、部门规章和司法解释均对保守国家秘密作出规范。目前，我国以2008年施行的《政府信息公开条例》及配套制度为原则，以保密法及其实施条例等为例外，共同构筑了政府信息公开的法律体系。

为了保障政府信息公开的同时避免国家秘密、商业秘密和个人隐私的不当泄露，平衡政府信息公开与安全保密的需求，《政府信息公开条例》第十四条确立了政府信息发布保密审查机制，要求行政机关应当建立健全有关制度，明确审查程序和责任，并在第三十四条进一步强调了行政机关不履行相关义务的法律责任。2010年11月，国务院办公厅发布《关于进一步做好政府信息公开保密审查工作的通知》，再次指出加强政府信息公开保密审查工作的必要性与重要意义，强调各地区、各部门要明确审查机构、落实审查职责、规范审查程序，做到审查工作有领导分管、有部门负责、有专人实施，同时加强督促检查。

政府信息公开保密审查作为信息发布前进行的一项内容甄别、确认和许可工作，是我国政府信息公开制度的核心机制与关键环节，决定了政府信息公开的限度和范围，属于机关单位自行开展的保密审查。保密法实施条例第三十二条，又明确了保密行政管理部门依法对机关单位执行信息公开保密审查情况进行检查，第三十八条进一步提出保密审查按照法定的职权和程序展开，以及科学、公正、严格、高效的要求，形成了对各机关单位自行保密审查的外部强制性补强。不

久前，复旦大学数字与移动治理实验室、新华网、提升政府治理能力大数据应用技术国家工程实验室联合发布了《2017中国地方政府数据开放平台报告》，根据相关信息披露，2012年以来，我国已有近20个地方政府陆续推出政府信息公开平台，并基于上述法律法规，基本完成了各级政府信息的基础公开要求。

法律适用与实践中的若干问题

政府信息发布内外部保密审查的规定构成了我国官方信息公开法律体系的一大特点，作为平衡我国政府信息公开和安全保密价值取向的制度设计之一，其在法律适用和落地实践中仍遇到了不少问题。

第一，机关单位内部自行开展的政府信息公开保密审查，缺乏有效的法律适用。除了《政府信息公开条例》外，目前在具体操作中可用的规定还包括国务院办公厅2010年发布的《关于进一步做好政府信息公开保密审查工作的通知》、2016年中共中央办公厅、国务院办公厅发布的《关于全面推进政务公开工作的意见》、2016年国务院办公厅发布的《〈关于全面推进政务公开工作的意见〉实施细则》等，均属于政策性文件，法律强制力相对不足。

第二，大数据的汇集与分析应用给实际的信息公开保密审查带来了更多挑战。不仅实时产生的、场景化特征明显的“热信息”被大量关注和搜集，如即时的位置状态、交易和浏览行为等，信息聚合与意外关联还使得较长时间之前的状态信息，即用于备份、灾难恢复、存档等的“冷信息”被持续激活和挖掘，通过有效叠加与精确应用，在很大程度上可能会给国家安全造成巨大威胁。而我国涉及大数据的若干指引、标准性文件仍在起草或征求意见阶段，指导标准的缺失加剧了保密审查标准的不确定性。在面对这类信息的保密审查时，容易形成过宽或过紧的不稳定态势和不可预期的风险结果。

对完善法律体系的若干建议

信息化飞速发展导致信息公开面临的形势更加严峻复杂，管理难度日益加大，保密领域的“一法一条例”初步回应了信息安全保密的部分诉求。国家大数据战略下，构建安全可控的国家信息公开体系，须以法律法规或政策的方式确认信息属性，并为政府信息公开的全生命周期提供安全与行为规范。近年来，我国网络与信息安全保密的法治进程明显加快。2017年6月，国务院法制办公室发布《〈中华人民共和国网络安全法〉公开征求意见的通知》，针对信息化发展等新问题，对《政府信息公开条例》进行了修订。

随着新颁布的《国家安全法》《网络安全法》，以及2017年4月发布的《中华人民共和国密码法(草案征求意见稿)》，进一步体现出大数据发展与安全保密的平衡需要，再次将相关法律协调问题提上日程，以实现信息公开与保密法及其实施条例的衔接与映射。基于法律的稳定性要求，暴露出的问题亟须在法律法规征求意见、配套完善和落地实施过程中予以关注和解决。其中就包括如何应对大数据挑战，构建安全可控的国家信息公开法律体系，实现更精准的安全保密防护，更好地维护国家安全和利益；在《网络安全法》原则性规定仍在持续配套完善的情况下，要进一步强化政府信息公开涉及的机关单位网络安全保密职责；以及针对我国政府信息发布保密审查机制存在的主体较宽泛、标准不确定、程序不具体、审查责任不完备、外部监管介入时机与深度不明确等诸多问题，有待进一步完善。

值得注意的是，国家大数据战略下，政府信息公开也将不可避免地推动密码技术的进步和相应的立法升级。未来，《密码法》和其下《商用密码管理条例》等制度体系建设及监管策略的调整，也将为寻求政府信息公开，以强密码保障信息安全保密等提供更丰富的法律依据和工具选择。■

（作者系公安部第三研究所副研究员）

责任编辑/武 薇

BIG DATA

大数据时代的公开与保密

大数据时代 公开数据的泄密风险

□柳厅文 李全刚 时金桥

随着“人（人类社会）—机（信息空间）—物（物理世界）”三元的深度融合，数据规模呈爆炸式增长，且数据表现形式多样（包括文本、图像、视频、音频等）、异构多源、动态演变、真伪混杂。大数据时代，信息在网络空间发布、传播的渠道更加丰富多样，导致网络空间中的很多信息在未经过严格保密审查、未进行泄密隐患风险评估，或者未意识到信息情报价值的情况下随意发布。网络空间中非实名制场所和匿名场所的存在使得信息的源头追溯非常困难，使得敏感信息和高价值信息被公开的同时不承担追责的风险。另外，很多泄密信息和泄密事件的知悉者和目击者并不知道所看到的内容是涉密的，可能随手拍摄并记录下来传到网络空间。

大数据时代模糊了涉密数据和非涉密数据的绝对界限，碎片化数据、模糊化数据等传统意义上被认为安全的数据，在大数据时代也有可能引发泄密事件。将海量的碎片化、模糊化数据汇聚到一起，即使这些数据在公开之前经过了精心的脱密处理，通过深入的大数据关联分析，也可以洞察到隐藏在大数据表象背后的重要情报。

我国最著名的“照片泄密案”就是通过对公开数据关联分析发现情报的早期案例。日本情报人员根据《中国画报》和《人民中国》等刊登的王进喜照片和油田建设报道，准确地分析出大庆油田的位置、油田规模以及生产能力等关键信息。有了如此多的情报，日本人迅速设计出了适合大庆油田开采使用的设备。因此，当我国政府向世界各国征集大庆油田开采设备的设计方案时，日本人一举中标。一旦这些情报被用于打击摧毁的军事战略意图，后果难以想象。

2007年3月，美国海军部情报局发布了《中国海军2007》内部手册，其内容主要来自China’s Maritime Strategy,The Great Wall at Sea: China’s Navy Enters the Twenty-First Century，《中国国防白皮书》《中国海军百科全书》《海军大辞典》等国内外出版的公开资料。该手册共144页，分为16个章节。与传统的美国海军作战手册相比，手册中并没有各种舰船的清单和图解，但却详细介绍了中国海军的组织体制、领导层、政治工作制度、海军军事学术，以及海军的人力系统、部队训练、对外交往、武器装备等内容。

Bellingcat团队对2014年马航MH17空难事件的情报分析也是一个非常典型的案例。空难事件发生后，Bellingcat团队根据飞机失事地区的Twitter推文、Instagram照片、YouTube视频、Google地图等公开数据，快速分析出飞机是被俄制“山毛榉”导弹击落，以及导弹发射器的准确运输路线和时间，且空难事故后发射器最终进入俄罗斯境内，达到了与情报部门比肩的信

大数据时代将海量的碎片化、模糊化数据汇聚到一起，即使这些数据在公开之前经过了精心的脱密处理，通过深入的大数据关联分析，也可以洞察到隐藏在大数据表象背后的重要情报。

以美国为代表的信息优势国家意识到公开数据中蕴藏的情报价值和泄密隐患，非常重视通过大数据分析进行情报挖掘与泄密监测，力图实现“在任何国家、从任何语言”获取开源情报的能力，以支撑和强化美国在全球的霸主地位。目前，美国已建立了比较完善的开源情报工作体系。

息搜集和证实速度。2017年1月24日“东风—41”弹道导弹运输车出现在黑龙江街头的照片在互联网上引起广泛热议，一旦相关的报道、照片、视频、地图等公开信息被人聚合在一起进行类似马航MH17空难事件的情报分析，一些涉密信息和重要情报将不可避免地被泄露。

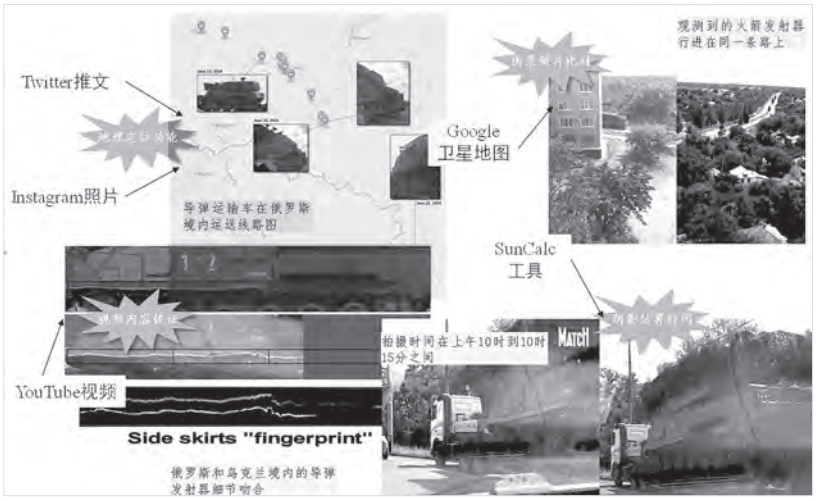
以美国为代表的信息优势国家意识到公开数据中蕴藏的情报价值和泄密隐患，非常重视通过大数据分析进行情报挖掘与泄密监测，力图实现“在任何国家、从任何语言”获取开源情报的能力，以支撑和强化美国在全球的霸主地位。目前，美国已建立了比较完善的开源情报工作体系。2005年美国国家情报主任办公室成立了开放源中心（Open Source Center,OSC），2006年又立法启动了国家开放源事业计划（National Open Source Enterprise,NOSE），专注公开信息的搜集、共享和分析，规定任何情报工作必须包含开源成分。美国广泛开展针对特定人群的情报收集任务，并将社交媒体、学术数据库等作为重要信息来源。

例如，2009年美国忧思科学家联盟（The Union of Concerned Scientists）发布的Anti-Satellite (ASAT) Technology in Chinese Open-Source Publications报告认为，虽然中国刻意减少反卫星导弹研发的透明度，但同时会在学术资源数据库中发表一些相关的技术和非技术报告，这给美国对中国ASAT技术的情报分析提供了丰富的信息来源。该报告分析了1971年至2007年的1486篇ASAT武器和技术相关的公开学术文献，这些文献来自328个科研机构的957名研究人员，发表在292种不同的中国期刊上。报告认为一些权威专家发表的文献中包含了一些非常具体有用的信息。此外，美国又非常重视对内部特定人群发布消息的规范和监测。2011年出版的《美国军队社交网络官方指导手册》针对美国军人浏览互联网，尤其是使用社交网络时对地理标注、隐私设置、视频发布等具体内容均有详尽的使用规范。

美国启动了包括棱镜计划、上游计划在内的一系列项目，构建了具有YB级（字节）设计存储能力的大数据存储中心，以Accumulo为核心的大数据存储和处理系统，形成了完整的情报收集与分析框架和能力。美国通过直接读取微软、谷歌、苹果等网络巨头的数据库和监控骨干网网络流量，可以接触到互联网用户的电子邮件、聊天日志、搜索记录、网络社交等数据。这说明特定群体尤其是涉密人员的互联网言论和行为完全能够被汇聚在一起，通过碎片拼接似的关联分析即可以挖掘出其中隐藏的涉密信息。

可以看出，大数据时代公开数据中可能存在着极大的泄密隐患，已有的保密监管手段在应对这一新型的失泄密风险时面临新的挑战，因此亟须采取一系列措施来降低泄密风险和减少不必要的损失。■

责任编辑/孙战国



中国“窃取”美国知识产权？纯属诬蔑！

□本刊综合

连日来，中美贸易纠纷持续发酵。其中，保护知识产权成为美方挑起争端的借口之一，美国依据所谓“301调查”，污蔑中国“窃取”美国知识产权，指责中国“强制”美国企业转让技术。多位专家表示，这些指责纯属诬蔑、毫无事实根据。美方的所作所为严重违反WTO规则，是典型的单边主义和贸易保护主义。

事实一：这些指责没有任何实际证据

对外经贸大学中国世界贸易组织研究院院长屠新泉表示：这是一种妄想症，没有任何实际证据，完全是猜测。这个猜测来自哪呢？就来自中国近几年快速的技术进步，它觉得中国怎么能技术进步这么快呢？不合理。所以都是偷来的，都是从美国偷来的。

中国社科院世界经济与政治所国际贸易研究室主任东艳表示：美国“301调查”报告中用较大篇幅指责中国知识产权保护不力，依据的是美国政府行政部门(如司法部)或美国公司的单方面认定，还多处使用“据报道”“利益相关方认为”等来源模糊的说法，既缺少具有说服力的实际证据，也表露了美方对中国近年来在创新和知识产权保护成绩的无视。

事实二：中国创新成就一不靠偷，二不靠抢

事实上，中国在知识产权保护方面做出的努力有目共睹。世界知识产权组织发布的报告显示，中国是2017年《专利合作条约》框架下国际专利申请第二大来源国，中国国家知识产权局受理的发明专利申请量达138.2万件，超过美、日、韩以及欧洲专利局的总和。

多位专家表示，2017年中国研发投入占GDP的2.1%，成为仅次于美国的全球第二大创新投入国。

国家知识产权局保护协调司司长张志成强调：中国的创新成就一不靠偷，二不靠抢，是中国人踏踏实实干出来的。

事实三：技术转让是你情我愿的交易

指责中国强制或迫使美国企业转让技术更是无稽之谈。商务部国际贸易研究院副院长李钢表示：商业领域的技术合同是你情我愿的情况下达成的，如果说是一方强迫另外一方接受不平等条款，那么我相信这种技术合作是不可能达成的。所以我觉得美方的指责根本没有道理。

中国国际问题研究院常务副院长阮宗泽表示：中国没有任何法律规定外资或者外国公司必须向中国转让技术，企业之间的技术合作或技术转让是企业行为，是你情我愿的交易，政府不应该给予干预；如果有侵权的行为，可以诉诸法律手段。但是现在美国完全违背了WTO的基本精神和原则，违背了自己向WTO作出的有关承诺，采取单边措施，企图对中国发起大规模的征税活动。所以，美国是国际规则的破坏者，中国是国际规则的捍卫者。

中国驻英国大使刘晓明指出：美方无视中国不断加强知识产权保护的事实，其所作所为不仅严重违反WTO规定，是典型的单边主义和贸易保护主义，也是赤裸裸的“傲慢与偏见”。■

责任编辑/李 杰

脸书泄密 告诉我们什么

□郝耀鸿　王立金

3月中旬，美国《纽约时报》披露，美国社交网站Facebook（脸书）近5000万用户的个人信息遭到一家名为剑桥分析公司的泄露，该公司可能以这些数据为基础预测并影响了全球多地政治活动中公众的选择。尽管脸书公司首席执行官马克·扎克伯格3月21日在脸书个人主页发表声明，承认公司在保护用户数据方面犯了错误，并承诺将采取措施应对，但仍无法消除人们对安全问题的深刻忧虑。4月11日，马克·扎克伯格在出席美国参议院司法与商务委员会、众议院能源与商务委员会听证会时表示，打击Facebook平台上干涉选举的行为将是他今年“最高优先权”任务之一。

据Facebook称，共约8700万用户的数据可能被泄露出去，而且平台上大多数人的公开档案信息可能也被抓取。随着脸书“泄密门”丑闻持续发酵，网络时代，个人信息泄露问题再次被推上风口浪尖。那么，这些个人信息是怎么泄露出去的，又会造成什么影响？

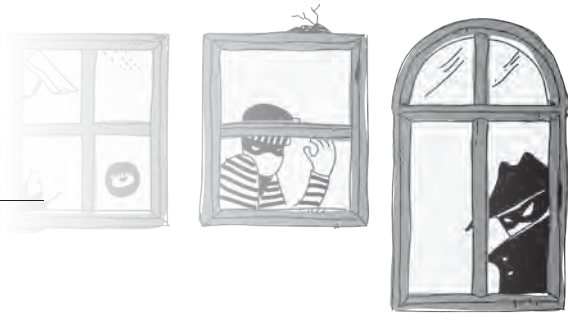
回顾这次风波，除了Facebook和剑桥分析公司的问题外，用户个人的安全意识不强也是其中因素。剑桥分析公司通过开展有偿的网络调查，诱导用户按照链接地址下载公司指定的App应用，当用户下载并安装该软件应用时，后台会默认申请查看该用户Facebook资料的权限，如果用户没有仔细浏览就点击“同意”，那么，其所有社交平台上的个人信息包括好友信息就会被“一网打尽”。正是这样，最终酿成几千万用户资料信息的泄露。

那么，剑桥分析公司拿这些用户的个人信息数据做什么呢？据悉，剑桥分析是一家大数据分析公司，千万不要小瞧这家公司的实力，通过大数据挖掘、分析和处理，该公司甚至试图在2016年美国总统大选和英国“脱欧”投票中影响投票者。也许有人会问，剑桥分析公司是怎样影响如此重大的国际事件的？没错，靠的就是这些被大量泄露的个人信息数据，例如，用户性格、习惯、兴趣、宗教信仰、政治倾向等。对民众个体而言，这些信息看似都微不足道，但是一旦汇聚起来，积少成多，积流成海，就会成为有价值的数据，被拿来进行分析预测，甚至倾向诱导，影响范围及程度将远远超乎想象。

个人信息保护是一个老生常谈的话题，那么，此次事件又带给我们哪些警示？一是要警惕App安装中的“隐私条款”。2016年6月28日，国家互联网信息办公室发布的《移动互联网应用程序信息服务管理规定》明确规定，移动互联网应用程序（App）开发商必须在安装时，向用户明示信息收集使用的目的、方式和范围，并且必须经得用户同意，否则将视为侵权行为。但是，如果我们在安装时未提高警惕，App开发商又加入了不合理的授权申请，那么必将埋下信息泄露的种子。例如，某款手电筒App，安装时居然要求授权调用通信录查看、摄像头开启，甚至定位功能，因此，大家一定要特别关注App的安装提示，看到不合理要求，一定要勾选去掉。二是不要随意参与网络测试。此次事件中剑桥分析公司对用户信息的窃取正是通过这种方式。目前，互联网上有很多网站和小程序提供在线测试，如“测测你的前世今生”“测测你的心理年龄”“测测你的工作发展”等，这些测试经常需要用户提供个人基本信息，如姓名、生日、手机号码、工作性质、习惯喜好等，这些信息一旦被获取，经过专业的数据分析，完全可以拼凑出完整的个人情况，那么，你在不经意间也就“裸奔”于世了。■

责任编辑/徐　琛

Facebook寓言



□大 力

在地球村，有个FB地产公司，打造了一个名叫Facebook的免费社区，房子白住并附送金牌管家服务，吸引到了世界上最大的客户群体，入住者达20亿。但FB毕竟不是慈善机构，于是考虑如何把用户资源商业变现问题。它先是在社区投放广告，再推出高端物业收费服务，然后又与第三方公司合作，允许他们进社区淘金。这个模式居然达成共赢：FB成为最赚钱最有影响力的公司之一，入住者在社区享受各式各样且多是免费的服务，而第三方公司也通过提供个性化服务迅速发展起来。整个社区基本上维持了和谐、欢乐、繁荣的大好局面，直到有一天，来了一个心理学家团队。他们通过入户调查和调阅物业资料，取得重大研究成果。这些成果卖给了另一家咨询分析公司，而后者利用这些成果影响了地球村某大家族的家长选举结果。媒体披露此事后立刻引起轩然大波。各大家族首先不干了，影响选举结果已经碰触了这个世界已有规则的红线，台面上的诉求是家族里每个成员的隐私权保护问题，台底下的担忧是这些社区居民是你一个商业公司统治还是我家族统治的问题。居民也不干了，谁让你把我的资料给别人分析的，我的政治倾向都能分析出来，还有什么隐私是你不知道的。于是FB公司老板出来又是赔礼又是道歉，承诺加强监管严格控制，保证以后不出现类似事件……

故事没有结尾，因为现实中Facebook用户信息泄露事件还处于发酵之中，也许故事永远都不会有结尾，因为关于用户隐私泄露的事件，这不是第一次，也不是最后一次。

事件爆发以来，Facebook股价已从2月的历史高点应声下跌，累计超过20%。这一结果在一定程度上代表了人们对互联网经济和技术的恐慌。

为什么会恐慌？请看媒体的报道：剑桥大学心理学家科甘与剑桥咨询公司于2013年开发了一款“这是你的数字化生活”的应用，经用户授权后收集年龄、住址、性别等个人信息，平时参与的活动以及在社交网络中发表、阅读的内容等。一共有约27万人下载，再加上公开收集的用户信息，共涉及5000万用户的数据。剑桥咨询在收集到上述数据后，分析出了用户的行为模式、性格特征、价值观取向等，以便针对特定用户推送竞选广告。

在互联网时代，每个人都成了透明人。曾经只有国家相关部门才能够保管和合法阅读的个人档案，在这个时代化身为网络用户画像，直接向全社会公开了，而且内容之详细、分析结论之精准远远超过以前的个人档案资料。孟子说，羞恶之心，人皆有之。当互联网和大数据剥下人们最后一块遮羞布的时候，赤身裸体出现在网络空间的人们当然会感到恐慌和不安。

这样的个人隐私信息泄露的后果有多严重呢？从两年前发生的徐玉玉被电信诈骗案就可见一斑：骗子提前获得了徐玉玉的个人信息，之后冒充教育局、财政局工作人员，骗取其学费共计9900元，直接导致徐玉玉死亡。

Facebook事件只是暴露出互联网上用户隐私泄露的冰山一角，整个互联网生态的基本规则就是数据换免费、隐私换便利。从这个意义上讲，国内外其他互联网巨头的用户数据保护并不见得比Facebook好多少，更别提多如牛毛的中小微互联网公司了。

互联网的技术基础是共享，商业模式是免费。目前暴露出来的问题是技术的迅猛发展和商业模式的快速迭代与政府监督管理的能力滞后之间的矛盾造成的。要想从技术角度彻底解决用户隐私保护问题似乎并不现实，只能以管理手段为主。这就要求各国政府尽快推进网络空间立法，全面建章立制，并且加强监管和执法力度，使曾经的法外之地——网络空间全面置于法治之下，如此才能建立起清朗和谐的网络社会，保障互联网技术最大程度地为人类服务。■

责任编辑/满 宁

延伸阅读：

国内互联网大佬如何看待用户信息泄露?

马云

近日，阿里巴巴董事局主席马云在博鳌亚洲论坛发表讲话时，被问到最近几周脸书发生的用户隐私泄露问题。马云起初并没有正面回答，只谈到高级管理层人员应该承担起责任，立刻着手研究解决该问题。后来，他还表示，他不会因此问题对脸书作出任何评价，因为在15年前，脸书也没有预料到会有这样的事件发生，大家不能因为这件事情，就否定这家公司存在的价值。但是，他也提出："现在的确是我们应该解决它的时候了。"马云认为，在解决此问题的方案中，最重要的便是尊重数据，尊重安全，尊重隐私。最后，马云称他对此问题持乐观的态度，并相信这个问题终将会被解决。

无独有偶，近日，百度总裁张亚勤也回应了对脸书泄密事件的看法："我们在百度有一个非常明确的立场，安全和隐私是我们做其他一切事情的先决条件。"此前，百度CEO李彦宏在中国发展高层论坛2018"新时代的中国"发言表示："我们也非常重视隐私问题，以及数据的保护问题，用户信息安全保障是所有互联网公司的生命线，我们有责任保护用户信息安全不被侵犯。在过去几年中，中国也越来越认识到这个问题，也在加强相关法律法规的建设。比如，用户在电商、购物网站上的习惯、关注的品类等等信息，有助于网站为用户提供更贴心、更高效的服务。中国的消费者在隐私保护的前提下，很多时候是愿意以一定的个人数据授权使用，

张亚勤

李彦宏

去换取更加便捷的服务的。因此，我们需要在保障用户信息安全和运用用户数据为之提供更好服务之间，找到更好的平衡点。当然，这一切都要遵循一定原则，要在保障用户数据权益的基础上，用这些数据让所有人受益。"

目前，BAT（三大互联网公司百度、阿里巴巴、腾讯）中，腾讯还没有对脸书泄密事件发表任何看法。其实，由于微信、QQ等腾讯软件同脸书旗下的产品一样，都属于社交应用，过去一直饱受争议。2017年底，腾讯CEO马化腾在接受采访时就表示："在腾讯平台，每一天有超过10亿张的照片上传，节假日可能甚至有二三十亿张照片，绝大部分都是人的脸，尤其是中国人的脸。腾讯有一个更强大的能力就是，几乎掌握了每个中国人过去十几年来的面容变化，因为很多人从年轻开始，就一直在腾讯的平台上传照片，所以甚至可以预测其老的时候是什么样子。"

马化腾

（根据互联网内容整理）

事 件
Event

朴槿惠一审被判处24年有期徒刑

4月6日，韩国首尔中央地方法院对前总统朴槿惠“亲信干政”案作出一审宣判，裁定朴槿惠收受贿赂、滥用职权、泄露公务机密等16项罪名成立，判处她24年有期徒刑，并处罚金180亿韩元（约合1.06亿元人民币）。

法院认定朴槿惠向乐天集团会长辛东彬索贿70亿韩元、向SK集团索贿89亿韩元等行为属实，构成犯罪。认定朴槿惠滥用总统职权，与其好友、“亲信干政”案核心人物崔顺实合谋强迫大企业向Mir财团和K体育财团出资，严重侵犯企业经营自由，罪名属实。认定朴槿惠通过青瓦台前秘书郑虎成向崔顺实泄露青瓦台文件，泄露公务机密罪名成立。

朴槿惠当天并未出席审判，法院表示朴槿惠通过首尔看守所提交了拒绝出庭的事由书。当天法院以该案受到韩国民众高度关注，直播有利于保障公众知情权和公共利益为由，允许对审判全程进行电视直播。

美国前联邦调查局副局长因泄密被开除

3月16日，美国司法部部长塞申斯宣布，立即开除前联邦调查局副局长安德鲁·麦凯布。塞申斯在一份声明中说，这一决定基于内部监察和纪律部门的建议，并援引内部调查报告称麦凯布在未经授权情况下向媒体泄密并且不够坦诚。

据内部调查报告，麦凯布被指未经授权向《华尔街日报》记者泄露该部门有关对前国务卿希拉里·克林顿“邮件门”调查和对克林顿基金会调查的机密信息，并误导调查人员。麦凯布随后发表声明说，自己有权通过办公室与媒体分享信息，并否认误导调查人员，称上述决定不仅是对他个人名誉的诋毁，也是对联邦调查局、执法部门和情报人员的污蔑。

麦凯布认为自己被开除的原因在于，他证明了总统特朗普曾试图施压前联邦调查局局长科米结束“通俄门”调查的说法以及他在出席国会听证会时力挺科米。

台湾地区初审通过“国家机密保护法”修正草案

3月14日，台湾地区“立法院”司法法制委员会初审通过了所谓的“国家机密保护法”修正草案，明文规定“涉密人员”退离职后，出境管制期限仅能延长、不得缩短，管制时间最长可达6年。而初审条文也将中国大陆及港澳等地区列入规范的范畴内，意味着未来若向大陆及港澳地区泄露、交付台方机密，可处3年以上、10年以下有期徒刑，泄露“绝对机密”者，加重其刑二分之一。

现行台湾地区的“国家机密保护法”规定，“涉密人员”退离职后，3年内出境须经审核；泄露或交付台方机密者，处1年以上、7年以下有期徒刑。

申请赴美签证拟提交社交媒体个人信息

3月30日，美国联邦政府公布的文件显示，国务院拟规定美国签证申请者提交社交媒体用户名等多项个人信息。

根据该规定，签证申请者被要求提供过去5年在指定社交媒体平台上的个人信息；申请者也可以自行选择提供非指定社交媒体平台上的个人信息。此外，签证申请者还被要求提供过去5年曾使用的电话号码、电子邮箱地址、国际旅行记录以及是否曾违反移民法、是否曾被驱逐出境、是否有家庭成员参与恐怖主义活动等信息。美国国务院表示，现面向公众征集对新规定的意见，即日起为期60天。新规定施行前须得到美国行政管理和预算局批准。

据报道，此前美国只要求需要接受额外审查的签证申请者提供社交媒体、电子邮件和电话号码等个人信息，此规定将适用于几乎所有美国签证申请者。

苹果公司修改隐私控制政策：允许用户彻底删除账号

3月30日，据彭博社报道，苹果公司表示将在未来几个月内更新其管理Apple ID的网页，允许用户下载苹果公司所持有的本人所有数据。该网站更新后，还将具备修改个人信息、暂时停用账号和彻底删除账号等功能。

该功能还将允许用户下载存储在各个应用程序和服务中的个人数据，比如，用户可以下载所有存储在“通讯录”“日历”“照片”等应用中的数据或Apple Music中关于音乐偏好的数据。这些选择将在5月初率先对欧洲用户开放，之后在其他国家将陆续推出。在此之前，用户虽可以进行类似的操作，但通常只能联系苹果公司按要求进行。

据了解，苹果公司制定新的隐私控制政策，旨在符合欧盟新的隐私保护法规《通用数据保护条例》，该法规将于2018年5月25日正式开始实施。

面 孔
Face

凯莉安·康威

4月3日，美国知名政治记者罗纳德·凯斯勒的新书《特朗普的白宫：改变游戏规则》面市，该书爆料，白宫的“头号泄密者”正是总统资深顾问凯莉安·康威。

凯斯勒说：“特朗普2016年竞选总干事、现任白宫顾问康威泄露给媒体的信息比其他任职于白宫的人都多，不但多次泄露内幕消息，更曾造谣中伤他人，并对特朗普的女儿伊万卡和女婿库什纳也很不屑。所以如果你在想为什么白宫会泄露这么多秘密，康威这个白宫第一号大嘴巴就是其中一个原因。知情人士表示，他们多次见到康威给媒体朋友发怼同事或泄密的短信。”

现年51岁的康威毕业于乔治·华盛顿大学法学院，早年经营民调公司，曾为美国前副总统丹·奎尔、前众议院议长金里奇和现任副总统彭斯等不少知名政客提供服务。

叶夫根尼·尼库林

3月29日，捷克宪法法院决定，向美国引渡遭国际刑事警察组织通缉、涉嫌对美国多家企业发动网络攻击的俄罗斯“黑客”叶夫根尼·尼库林，当天尼库林被解送美国。

尼库林现年29岁。2016年10月，捷克警方与美国联邦调查局合作，在捷克首都布拉格一家餐厅逮捕了他。尼库林去年在美国加利福尼亚州遭起诉，受到涉嫌2012年侵入社交媒体“领英网”、德罗普博克斯公司官方网站等指控。依照“领英网”的说法，尼库林窃取了超过1亿用户密码，导致这家社交网站不得不协助大批用户重置密码。

言 论
Viewpoint

审判流程信息公开以“依法”“必要”为限度

审判流程信息公开不必盲目地以“点多”“量多”取胜，而应以“依法”“必要”为限度。审判流程信息公开不是毫无原则的一律公开，根据司法解释第十二条，涉及国家秘密以及法律、司法解释规定应当保密、限制获取的审判流程信息，不得通过互联网公开。其中，国家秘密关乎国家安全和利益，此类审判流程信息不宜在互联网流转，如果法律、司法解释并未禁止当事人获取，则可以通过互联网以外的途径向当事人公开。

在划定国家秘密以外的其他不得公开的审判流程信息范围上，第十二条并未直接列举而是援引法律、其他司法解释，随着未来法律、其他司法解释内容调整，不公开范围也会随之改变，这样的条文设计增强了司法解释的适应能力。司法解释将不公开范围严格限缩在“有法可依”的前提下，最大限度压缩了解释空间，可以有效杜绝“选择性公开”现象。

——3月16日，最高人民法院发布《关于人民法院通过互联网公开审判流程信息的规定》，最高法审管办负责人接受《法制日报》记者采访时表示

“愿意用隐私交换便捷”颠倒了逻辑和因果关系

虽然现实中，用户确实享受了便捷，“放弃”了隐私，但不合理的现实不能推导出相应的逻辑正确性。为用户提供便捷并由此赚取利润是互联网公司存在的前提，不代表提供便捷必须以用户放弃隐私为前提，更不代表人们“愿意用隐私交换便捷”。如果打着“中国人愿意用隐私交换便捷”旗号肆意侵犯用户权益，显然低估了用户的智商和容忍度。“愿意用隐私交换便捷”的论调颠倒了逻辑和因果关系，忽视了孰轻孰重。必须强调，尊重并严格保护个人信息不被非法获取、利用是互联网社会的基本原则。互联网企业应认识到这一点，不以提供便捷服务为幌子过度收集、利用隐私，以至于出现大数据“杀熟”这一荒唐现象。

——3月28日《北京青年报》，“要看到‘愿意用隐私交换便捷’的逻辑错误”，作者史洪举

数字
Digit

130

3月26日，美国宣布驱逐60名俄罗斯人，称他们以外交身份做掩护从事间谍活动，其中包括俄驻西雅图领事馆48名“已知情报官”和12名常驻联合国代表团成员。总统特朗普同时下令关闭俄驻西雅图领事馆，理由是领事馆位置靠近美国一座潜水艇基地和飞机制造商波音公司。同一天，德国、波兰和法国等至少16个欧洲联盟国家宣布驱逐俄方外交官。加拿大、乌克兰、挪威、阿尔巴尼亚和马其顿等国跟随。截至27日，加上英国，至少23个国家对超过130名俄方外交官下逐客令，这是1991年“冷战”结束以来最大规模集体驱逐事件。

232，301

4月5日，美国总统特朗普要求美国贸易代表办公室依据“301”条款，额外对1000亿美元中国进口商品加征关税，中国对此坚决反对。在这场中美贸易摩擦中，有两个高频数字：“232”和“301”。所谓“232”调查，是指美国商务部根据1962年《贸易扩展法》第232条款，对特定产品进口是否威胁美国国家安全进行的立案调查。所谓“301”条款则是美国《1974年贸易法》第301条的俗称，通常而言，是美国贸易法中有关对外国立法或行政上违反协定、损害美国利益的行为采取单边行动的立法授权条款。

2111

近日，日本外务省、经济产业省、总务省、国土交通省等中央政府职员共计2111人的邮箱地址和密码被盗并在网上出售。目前尚未发现实际危害，但负责监视网络攻击的日本“内阁网络安全中心”于4月3日对所有政府机构下发紧急通知以引起注意。专家指出，除了向某个特定政府部门的职员发送假邮件，使其感染病毒并盗取机密信息外，还有一种危险的攻击是伪装中央政府职员进行诈骗及发起网络攻击。

100万

4月4日，由公安部起草的《公安机关互联网安全监督检查规定》向社会征求意见。《规定》明确，互联网服务提供者和联网使用单位窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，应当依照网络安全法予以处罚，即由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

1000万

美国总统特朗普上任之初要求白宫高级幕僚签署“保密”协议，近日，《华盛顿邮报》披露了这份“保密”协议草稿。根据该协议，未经授权泄露“机密”信息，每次违反协议，要向联邦政府上缴1000万美元罚款。协议草稿把“机密”信息定义为幕僚“任职期间了解或有权限获悉的所有不公开信息”，同时规定该协议在特朗普卸任后依然有效。知情者表示，特朗普之前的历任美国总统曾同样痛斥泄密者和揭丑书籍，但从来没有要求幕僚签署“保密”协议。

13个未接电话

□冷 定

“丁零零……”

腊月二十八日傍晚，天色渐渐暗淡，我驾车在拥堵的芙蓉路上缓慢地“爬行”着，车窗外寒风凛冽，但想到明天即将开启的春节休假模式，堵车的烦恼早已被轻松化解。此时，骤然响起的手机铃声却打断了我对假期的憧憬。

低头一看：88***820的号码映入眼帘，这不是研发中心涉密计算机机房的电话吗？我暗自忖度。

下班前，按保密管理要求，我作为保密办主任，与公司领导一道对办公楼和保密要害部门部位逐个进行了巡查，要求相关负责人落实好节日期间的安全保密防范措施，对保安值班巡逻情况也进行了布置落实，还检查调试了涉密计算机机房的红外入侵报警系统，最后将所有要害部门部位贴上了封条。

“这时候应该没人在机房了，谁会给我打电话呢？”想到此，我立即按下了接听键。“喂……喂”，接连四五声，电话那头始终无人回应。想到涉密计算机机房电话是与机房外的办公电话并线，见没人回答，我有些疑虑地挂断了电话。

“丁零零……”5分钟后，手机再度响起，还是尾数820的座机，“喂……喂”，依然无人应答。

难道涉密计算机机房出问题了？一种不祥的预感向我心头涌来。

机房的红外入侵报警系统一直正常运行，一旦有人非法闯入或在未撤防的情况下进入，设置的报警电话每隔5分钟就会分别向我、机房管理员和保安值班室发送信号。虽然平时也有工作人员用机房外并线的办公座机给我打电话，但连续两次对方无人应答却是第一次发生。

我立刻给保安值班室拨去电话。“嘟嘟……”电话占线中。1分钟后，我再次拨打，还是占线。

我赶紧找到保安队长手机：“张队长，你赶快去研发中心大楼看看，涉密计算机机房一直在向我报警……”

“我们保安值班室电话也响个不停，接起来就是没人说话，已经派人去机房查看了。”张队长答道。

尾数820的座机仍每隔5分钟就拨来。我一边焦急地调转车头，向公司方向驶去，一边与研发中心联系，请他们速派人来公司会合。

“冷主任，研发大楼门窗完好、封条未动，没发现问题。”张队长的电话更加重了我的疑虑。

18：55分，我抵达公司，向张队长询问了有关情况，并对研发大楼外围再次进行了检查。研发中心同志赶到后，我们撕去封条，打开楼门，直奔位于顶层的涉密计算机机房。

铁门，完好！铁窗，完好！红外入侵报警系统，工作正常！

我们把所有可能出现问题的地方逐个排查了一遍，均未发现问题。奇怪的是，撤销红外入侵防护后，尾数820的座机仍在向我报警，已有13个未接电话！

问题究竟出在哪？我们又联系了系统安装人员。

“这套系统是从天花板的吊顶里布线，如果外围没有问题的话，线路老化、接触不良的疑点最大。”对方负责人的一句话提醒了我们。

向值班电工借来梯子和强光手电后，研发中心的同志爬到天花板预留的出风口，仔细查看起来。

“是不是线路被拽断了？”顺着老鼠爪印，他对电缆线逐段进行排查。

“仔细看看有没有咬噬的痕迹？”我和张队长提醒他。

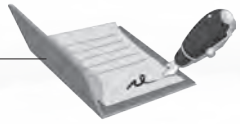
“找着了，这里有个断点！”他兴奋地叫起来。

晚上9点，拖着疲惫的身体，我饥肠辘辘地回到了家。窗外万家灯火，不时冲上云霄的礼花尽情地渲染着节日气氛。我不由得长舒一口气：终于可以安心过年了！■

（作者系湖南博云新材料股份有限公司保密办主任）

责任编辑/武 薇

我和保密“那些事儿”



□李思源

2014年7月，结束了4年风华正茂、挥斥方遒的大学时代，我走出“象牙塔”的大门，步入神圣的工作岗位。初来乍到，面对一切事物都感到那么新鲜而又陌生。虽说我是档案管理专业出身，常与文件资料打交道，且实习经历较丰富，但是谈及保密，那可还真是“大姑娘坐花轿——头一回”。

相识·心存敬畏严律己

我所在的党委办公室是单位的核心枢纽，需要承上启下、联系左右、协调各方，工作千头万绪、繁杂琐碎。因为经常接收涉密文件，所以刚到机要文书岗位不久，我就被定为涉密人员。回想起那时的心情——既兴奋又忐忑，脑海中不断掠过谍战剧里地下党员坚决捍卫组织秘密的情景，仿佛自己也成为了他们中的一员，一股自豪感油然而生。

带着愉悦的心情投入工作，然而现实却让我明白，做一名合格的涉密人员并没有想象中那么轻松。填表登记、审查备案、轮训学习、上机考试，每个环节都要一丝不苟，虚心对待。通过学习，我开始体会到涉密人员身上肩负的重大责任。尤其是看到那些泄密违纪人员受到法律严惩时，我的内心受到了极大冲击：有的人是为了牟取私利，但更多的却是无心之失！一时疏忽或是信念动摇都可能铸成大错，给国家和人民带来无法挽回的损失。几轮学习后，我顺利通过了保密考试，心中不由对保密工作者产生了仰慕与崇敬之情。

熟知·衣带渐宽终不悔

保密工作无小事。自从成为一名真正的涉密人员，保密意识就注入了我的血液：在日常收发传阅涉密文件时，严格践行登记管理制度；开展保密自查时，仔细梳理查摆问题；召开保密会议时，屏蔽手机信号，认真做好记录；落实涉密人员教育培训时，主动联系讲师，不断改进授课内容……

一分耕耘，一分收获。从一无所知到独当一面，我的胆识在摸索中成长，经验在磨炼中积累，知识在工作中丰富。

与保密朝夕相处的日子，疲惫渐渐舒缓成流溢于唇边齿间的轻歌浅唱，我彻底爱上了这份工作。有时它很枯燥，在保密自查工作中需要聚精会神，沉下心来逐条对照检查；有时它很刻板，人员变动、新增、借调或离岗离职时，手续一样也不能省略；有时它很严苛，借阅处理涉密文件时哪一个环节都不能少，培训考试差1分都不算过。

潜移默化中，我也开始养成“爱较真”的习惯：审批签字不全，不能办理借阅手续；涉密文件逾期未还，我会一天好几个电话追着要；迎接保密巡查，我尽忠职守、求真务实，一份份材料准备到深夜，逐项核查落实整改。严谨的态度锻造出过硬本领，缜密周全的材料、从容不迫的表现，让我们单位在保密抽测检查中连续两年被评为优秀等级。这来之不易的喜人成绩，或许就是对我工作最大的肯定吧。

回首·吾将上下而求索

岁月翩跹，我在保密工作岗位已有4年光景。蓦然回首，相识可谓胆战心惊，熟知可算命中注定。光阴荏苒，我与保密工作的交集渐渐融汇成点、连线，继而成面。

这一路走来，踏着荆棘却又花香弥漫。感谢保密工作给予我人格上的陶冶与锤炼，让我可以从淡泊中明志，在宁静里致远。现在，保密意识已成为我生命中不可或缺的存在，而这份信念也将与我同行，鞭策我勇往直前。

我相信，将至的岁月里，我和保密工作会碰撞出更加美丽的故事。路漫漫其修远，吾将上下而求索。在这个平凡的岗位上，我会继续坚持不懈地追求与拼搏，努力实现自己的人生价值，将毕生的光和热都奉献给我所钟爱的事业。■

责任编辑/齐 琪