国盟信息安全通报

2020 年 4 月 27 日第 214 期

全国售后服务中心

国盟信息安全通报

（第 214 期）

国际信息安全学习联盟

2020 年 04 月 27 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 419 个，其中高危漏洞 204 个、中危漏洞 182 个、低危漏洞 33 个。漏洞平均分值为 6.81。本周收录的漏洞中，涉及 0day 漏洞 190 个（占 45%），其中互联网上出现“D-Link DWL-2600 认证远程命令注入漏洞、Windscribe 权限提升漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4486 个，与上周（2497 个）环比增加 79%。

主要内容

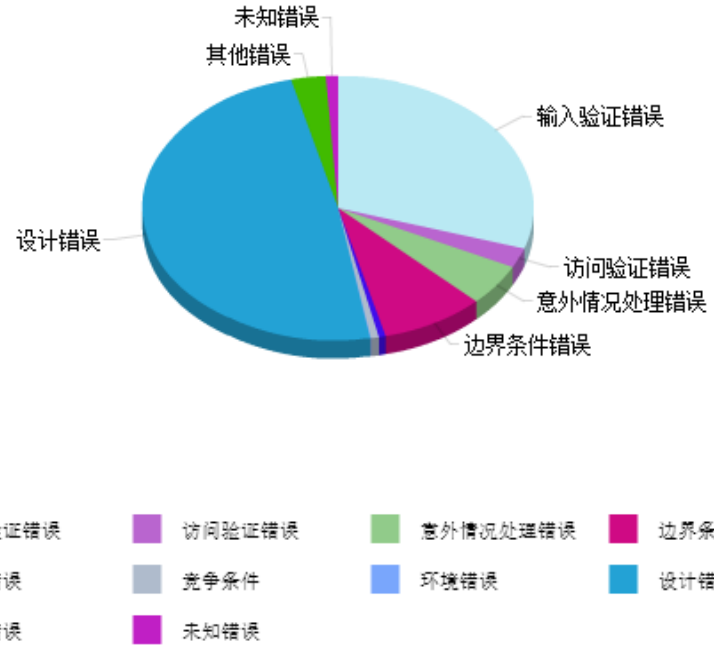
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

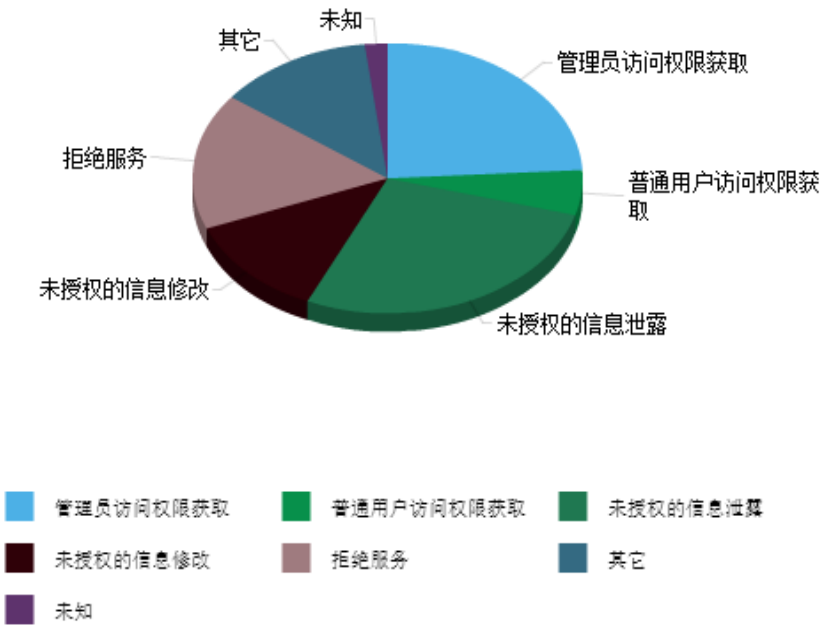
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 419 个，其中高危漏洞 204 个、中危漏洞 182 个、低危漏洞 33 个。漏洞平均分值为 6.81。本周收录的漏洞中，涉及 0day 漏洞 190 个（占 45%），其中互联网上出现“D-Link DWL-2600 认证远程命令注入漏洞、Windscribe 权限提升漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4486 个，与上周（2497 个）环比增加 79%。

二、安全漏洞增长数量及种类分布情况

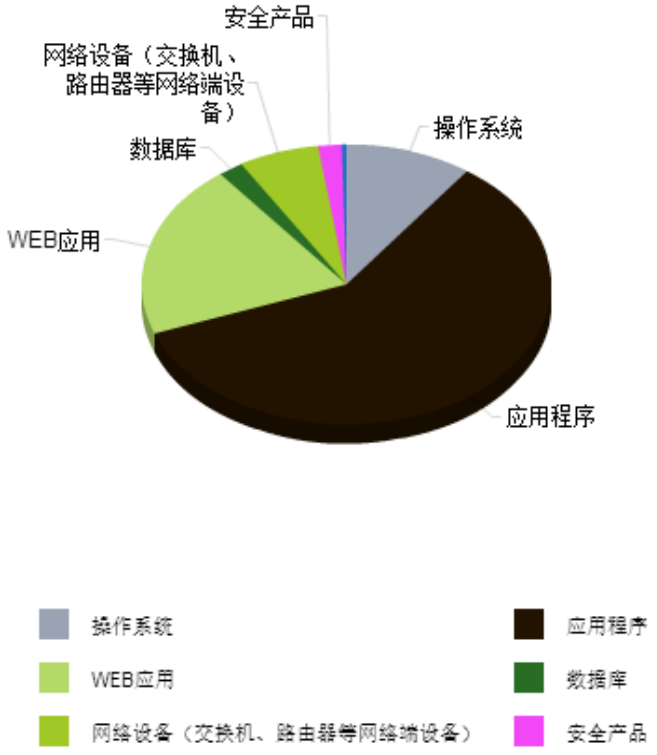
➢ 漏洞产生原因（2020 年 04 月 12 日—2020 年 04 月 26）



➢ 漏洞引发的威胁（2020 年 04 月 12 日—2020 年 04 月 26）



➢ 漏洞影响对象类型（2020 年 04 月 12 日—2020 年 04 月 26）



三、安全产业动态

➢ 习近平谈总体国家安全：把生物安全纳入国家安全体系

【编者按】“备豫不虞，为国常道。”坚持总体国家安全观，是习近平新时代中国特色社会主义思想的重要内容。习近平总书记围绕总体国家安全观发表了一系列重要论述，立意高远，内涵丰富，思想深邃。今年的 4 月 15 日是第五个全民国家安全教育日。新时代学习工作室带您回顾习近平总书记关于总体国家安全的重要论述。

坚持总体国家安全观

1、要坚持党对国家安全工作的绝对领导

要坚持党对国家安全工作的绝对领导，实施更为有力的统领和协调。中央国家安全委员会要发挥好统筹国家安全事务的作用，抓好国家安全方针政策贯彻落实，完善国家安全工作机制，着力在提高把握全局、谋划发展的战略能力上下功夫，不断增强驾驭风险、迎接挑战的本领。

——2018 年 4 月 17 日，习近平在十九届中央国家安全委员会第一次会议上发表重要讲话

2、人民安全是国家安全的宗旨，政治安全是国家安全的根本

坚持人民安全、政治安全、国家利益至上的有机统一，人民安全是国家安全的宗旨，政

治安全是国家安全的根本，国家利益至上是国家安全的准则，实现人民安居乐业、党的长期执政、国家长治久安……

——2018 年 4 月 17 日，习近平在十九届中央国家安全委员会第一次会议上发表重要讲话

3、国家安全是安邦定国的重要基石

有效维护国家安全。国家安全是安邦定国的重要基石，维护国家安全是全国各族人民根本利益所在。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。严密防范和坚决打击各种渗透颠覆破坏活动、暴力恐怖活动、民族分裂活动、宗教极端活动。加强国家安全教育，增强全党全国人民国家安全意识，推动全社会形成维护国家安全的强大合力。

——2017 年 10 月 18 日，习近平在中国共产党第十九次全国代表大会上作报告

4、要坚持国家安全一切为了人民、一切依靠人民

要坚持国家安全一切为了人民、一切依靠人民，动员全党全社会共同努力，汇聚起维护国家安全的强大力量，夯实国家安全的社会基础，防范化解各类安全风险，不断提高人民群众的安全感、幸福感。

——2016 年 4 月，习近平在首个全民国家安全教育日到来之际作出重要指示

5、下好先手棋，打好主动仗，做好应对任何形式的矛盾风险挑战的准备

推动创新发展、协调发展、绿色发展、开放发展、共享发展，前提都是国家安全、社会稳定。没有安全和稳定，一切都无从谈起。“明者防祸于未萌，智者图患于将来。”我们必须积极主动、未雨绸缪，见微知著、防微杜渐，下好先手棋，打好主动仗，做好应对任何形式的矛盾风险挑战的准备，做好经济上、政治上、文化上、社会上、外交上、军事上各种斗争的准备，层层负责、人人担当。

——2016 年 1 月 18 日，习近平在省部级主要领导干部学习贯彻党的十八届五中全会精神专题研讨班上发表重要讲话

6、安而不忘危，存而不忘亡，治而不忘乱

改革开放以来，我们党始终高度重视正确处理改革发展稳定关系，始终把维护国家安全和社会安定作为党和国家的一项基础性工作。我们保持了我国社会大局稳定，为改革开放和社会主义现代化建设营造了良好环境。“安而不忘危，存而不忘亡，治而不忘乱。”同时，必须清醒地看到，新形势下我国国家安全和社会安定面临的威胁和挑战增多，特别是各种威胁

和挑战联动效应明显。我们必须保持清醒头脑、强化底线思维，有效防范、管理、处理国家安全风险，有力应对、处置、化解社会安定挑战。

——2014 年 4 月 25 日，习近平在十八届中央政治局第十四次集体学习时发表讲话

7、保证国家安全是头等大事

增强忧患意识，做到居安思危，是我们治党治国必须始终坚持的一个重大原则。我们党要巩固执政地位，要团结带领人民坚持和发展中国特色社会主义，保证国家安全是头等大事。

——2014 年 4 月 15 日，习近平在中央国家安全委员会第一次会议上发表重要讲话

8、以人民安全为宗旨，以政治安全为根本，走出一条中国特色国家安全道路

当前我国国家安全内涵和外延比历史上任何时候都要丰富，时空领域比历史上任何时候都要宽广，内外因素比历史上任何时候都要复杂，必须坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，走出一条中国特色国家安全道路。

——2014 年 4 月 15 日，习近平在中央国家安全委员会第一次会议上发表重要讲话

维护重点领域国家安全

1、政治安全

办好中国的事情，关键在党。中国特色社会主义最本质的特征是中国共产党领导，中国特色社会主义制度的最大优势是中国共产党领导。坚持和完善党的领导，是党和国家的根本所在、命脉所在，是全国各族人民的利益所在、幸福所在。

——2016 年 7 月 1 日，习近平在庆祝中国共产党成立九十五周年大会上发表重要讲话

2、国土安全

维护国家主权和领土完整，实现祖国完全统一，是全体中华儿女共同愿望，是中华民族根本利益所在。在这个民族大义和历史潮流面前，一切分裂祖国的行径和伎俩都是注定要失败的，都会受到人民的谴责和历史的惩罚！中国人民有坚定的意志、充分的信心、足够的能力挫败一切分裂国家的活动！中国人民和中华民族有一个共同信念，这就是：我们伟大祖国的每一寸领土都绝对不能也绝对不可能从中国分割出去！

——2018 年 3 月 20 日，习近平在第十三届全国人民代表大会第一次会议上发表重要讲话

3、军事安全

我国正处在由大向强发展的关键阶段，前景十分光明，挑战也十分严峻，中华民族伟大复兴绝不是轻轻松松、敲锣打鼓就能实现的。军事斗争是进行伟大斗争的重要方面，打赢能

力是维护国家安全的战略能力。全军要强化忧患意识、危机意识、打仗意识，全部心思向打仗聚焦，各项工作向打仗用劲，尽快把备战打仗能力搞上去。

——2017 年 11 月 3 日，习近平在视察军委联合作战指挥中心时发表重要讲话

4、经济安全

建设现代化经济体系，必须把发展经济的着力点放在实体经济上，把提高供给体系质量作为主攻方向，显著增强我国经济质量优势。加快建设制造强国，加快发展先进制造业，推动互联网、大数据、人工智能和实体经济深度融合，在中高端消费、创新引领、绿色低碳、共享经济、现代供应链、人力资本服务等领域培育新增长点、形成新动能。支持传统产业优化升级，加快发展现代服务业，瞄准国际标准提高水平。促进我国产业迈向全球价值链中高端，培育若干世界级先进制造业集群。加强水利、铁路、公路、水运、航空、管道、电网、信息、物流等基础设施网络建设。坚持去产能、去库存、去杠杆、降成本、补短板，优化存量资源配置，扩大优质增量供给，实现供需动态平衡。

——2017 年 10 月 18 日，习近平在中国共产党第十九次全国代表大会上作报告

5、文化安全

牢牢掌握意识形态工作领导权。意识形态决定文化前进方向和发展道路。必须推进马克思主义中国化时代化大众化，建设具有强大凝聚力和引领力的社会主义意识形态，使全体人民在理想信念、价值理念、道德观念上紧紧团结在一起。要加强理论武装，推动新时代中国特色社会主义思想深入人心。深化马克思主义理论研究和建设，加快构建中国特色哲学社会科学，加强中国特色新型智库建设。坚持正确舆论导向，高度重视传播手段建设和创新，提高新闻舆论传播力、引导力、影响力、公信力。加强互联网内容建设，建立网络综合治理体系，营造清朗的网络空间。落实意识形态工作责任制，加强阵地建设和管理，注意区分政治原则问题、思想认识问题、学术观点问题，旗帜鲜明反对和抵制各种错误观点。

——2017 年 10 月 18 日，习近平在中国共产党第十九次全国代表大会上作报告

6、社会安全

发展是硬道理，稳定也是硬道理，抓发展、抓稳定两手都要硬。要坚定不移走中国特色社会主义社会治理之路，善于把党的领导和我国社会主义制度优势转化为社会治理优势，着力推进社会治理系统化、科学化、智能化、法治化，不断完善中国特色社会主义社会治理体系，确保人民安居乐业、社会安定有序、国家长治久安。

——2017 年 9 月 19 日，习近平在会见全国社会治安综合治理表彰大会代表时发表重要讲话

7、科技安全

我们不拒绝任何新技术，新技术是人类文明发展的成果，只要有利于提高我国社会生产力水平、有利于改善人民生活，我们都不拒绝。问题是要搞清楚哪些是可以引进但必须安全可控的，哪些是可以引进消化吸收再创新的，哪些是可以同别人合作开发的，哪些是必须依靠自己的力量自主创新的。核心技术的根源问题是基础研究问题，基础研究搞不好，应用技术就会成为无源之水、无本之木。

——2016 年 4 月 19 日，习近平在网络安全和信息化工作座谈会上发表重要讲话

8、网络安全

要理直气壮维护我国网络空间主权，明确宣示我们的主张。现在，各级领导干部特别是高级干部，如果不懂互联网、不善于运用互联网，就无法有效开展工作。各级领导干部要学网、懂网、用网，积极谋划、推动、引导互联网发展。要正确处理安全和发展、开放和自主、管理和服务的关系，不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力，把网络强国建设不断推向前进。

——2016 年 10 月 9 日，习近平在十八届中央政治局第三十六次集体学习时发表讲话

9、核安全

中国将继续加强本国核安全，积极推进国际合作，分享技术和经验，贡献资源和平台。中国将构建核安全能力建设网络，推广减少高浓缩铀合作模式，实施加强放射源安全行动计划，启动应对核恐怖危机技术支持倡议，推广国家核电安全监管体系。只要我们精诚合作，持续加强核安全，核能造福人类的前景必将更加光明。

——2016 年 4 月 1 日，习近平出席第四届核安全峰会并发表重要讲话

10、生态安全

生态环境没有替代品，用之不觉，失之难存。我讲过，环境就是民生，青山就是美丽，蓝天也是幸福，绿水青山就是金山银山；保护环境就是保护生产力，改善环境就是发展生产力。在生态环境保护上，一定要树立大局观、长远观、整体观，不能因小失大、顾此失彼、寅吃卯粮、急功近利。我们要坚持节约资源和保护环境的基本国策，像保护眼睛一样保护生态环境，像对待生命一样对待生态环境，推动形成绿色发展方式和生活方式，协同推进人民富裕、国家强盛、中国美丽。

——2016 年 1 月 18 日，习近平在省部级主要领导干部学习贯彻党的十八届五中全会精神专题研讨班上发表重要讲话

11、资源安全

全面促进资源节约集约利用。生态环境问题，归根到底是资源过度开发、粗放利用、奢侈消费造成的。资源开发利用既要支撑当代人过上幸福生活，也要为子孙后代留下生存根基。要解决这个问题，就必须在转变资源利用方式、提高资源利用效率上下功夫。要树立节约集约循环利用的资源观，实行最严格的耕地保护、水资源管理制度，强化能源和水资源、建设用地总量和强度双控管理，更加重视资源利用的系统效率，更加重视在资源开发利用过程中减少对生态环境的损害，更加重视资源的再生循环利用，用最少的资源环境代价取得最大的经济社会效益。要全面推动重点领域低碳循环发展，加强高能耗行业能耗管理，强化建筑、交通节能，发展节水型产业，推动各种废弃物和垃圾集中处理和资源化利用。

——2017 年 5 月 26 日，习近平在十八届中央政治局第四十一次集体学习时发表讲话

12、生物安全

要从保护人民健康、保障国家安全、维护国家长治久安的高度，把生物安全纳入国家安全体系，系统规划国家生物安全风险防控和治理体系建设，全面提高国家生物安全治理能力。要尽快推动出台生物安全法，加快构建国家生物安全法律法规体系、制度保障体系。

——2020 年 2 月 14 日，习近平在中央全面深化改革委员会第十二次会议上发表重要讲话（来源：中国共产党新闻网）

➢ APP 个人信息安全现状问题及应对策略

随着用户个人信息保护意识的觉醒，个人信息安全受到了前所未有的广泛关注，2019 年可以说是个人信息安全“崛起”的一年。中国信息通信研究院经过长期的检测分析发现， 我国移动互联网应用普遍存在隐私政策缺失、权限滥用、私自收集共享、强制定向推送等个人信息安全问题。要解决这些问题，提升 APP 个人信息安全能力，需要终端厂商、应用服务商、应用分发商、安全厂商全产业链的共同努力。

近年来，移动互联网应用（APP）的种类和数量呈爆发式增长，移动互联网应用作为收集用户数据的主要入口，强制授权、过度收集等侵害用户权益的现象层出不穷，明文传输、诱导下载等现象屡见不鲜，移动互联网应用引发的安全威胁和个人信息保护风险，逐渐成为国家和社会的关注焦点，进一步推进移动互联网应用安全和个人信息保护工作已势在必行。

APP 个人信息安全发展现状

在 5G 移动通信、大数据、物联网、人工智能等技术的推动下，我国移动互联网产业正

呈现垂直化、专业化和平台化趋势，对推动实体经济转型、促进经济社会发展起到了基础性的支撑作用。产业总体收入突破万亿元大关。然而，APP 在丰富大众数字生活的同时，也扩大了网络暴露面，带来了新威胁和新风险。

当前，企业通过 APP 收集用户数据的范围不断扩大，随着用户数据使用、共享、交易的不断深入，用户数据已成为企业发展的重要战略性资产。然而，企业安全意识和个人信息保护水平参差不齐，强制索权、过度收集、非授权转移共享、个性化展示和定向推送不规范、账户注销难等问题层出不穷，既严重威胁了广大人民群众的切身利益，又影响了企业的发展，甚至威胁国家的安全。

APP 个人信息安全常见问题分析

随着行业的发展及权益保障意识的提高，用户对移动互联网应用违规收集使用个人信息、过度索权、频繁骚扰等侵害用户权益的问题感受强烈。根据网络不良与垃圾信息举报受理中心数据显示，近年来，APP 用户个人信息安全相关投诉量急剧上升，投诉内容涉及个人信息收集使用规则、权限申请、个人信息收集、个人信息使用、个性化服务、账号注销等多个方面，其中几类问题尤为突出，账号注销难的比例高达 30%，私自共享给第三方比例为 21%，不给权限不让用比例为 14%，超范围收集个人信息比例为 11%，私自收集个人信息比例为 7%，过度索取权限比例为 7%，频繁申请权限比例为 1%。除了用户感受强烈的这些表象问题，还存在更深层次的成因，本文将对移动互联网应用常见的个人信息安全问题展开研究分析。

一是个人信息收集使用规则效果不佳。APP 应公开收集、使用规则，并明示收集、使用信息的目的、方式和范围。APP 使用规则通常以隐私政策形式呈现，是 APP 厂商向用户明示收集使用信息行为的主要途径。隐私政策缺乏，隐私政策内容不清晰、用词含糊、语义不清、冗长难懂、用户难理解，“霸王条款”限制用户权利，默认、强制用户同意隐私政策，侵犯用户选择权等都是目前的常态化问题。

二是强制、频繁、过度索权成为普遍现象。系统权限是终端操作系统赋予用户的应用管控能力，对于位置、录音、设备标识、通话记录等敏感信息的收集，用户可通过开启、关闭权限进行管控。然而部分应用不给权限不让安装、不给权限不让登录、不给权限不让使用某项无关业务，变相强制用户授权，为肆意收集个人信息大开方便之门。同时，提前申请权限或无业务功能申请权限；权限无关场景或服务下频繁申请权限，变相诱导用户授权等现象也逐渐成为新的关注点。权限问题是当前用户感受最强烈、最为集中的问题。

三是私自收集频发，超范围收集问题突出。用户数据作为企业发展的重要战略性资产，最大化收集是互联网应用发展早期的常见现象。个人信息收集使用规则中，常见缺乏告知，或者不明确告知收集使用个人信息的目的、方式和范围；有些 APP 在获得用户同意前，收集用户个人信息。或在非服务所必需或无合理应用场景情况下，超范围或超频次收集个人信息。还有些 APP 在登录时，将收集银行卡号、身份证号、人脸、指纹等敏感信息作为应用开启使用的前提条件，或通过积分、奖励等方式诱导用户输入相关敏感信息。

四是数据共享行为不规范，缺乏约束措施。大数据技术推动了 APP 的深度发展，数据的交易和共享应在明示并获得用户同意的基础上进行。有的用户数据共享行为未向用户明示；有的未经用户同意转移用户个人信息。有的 APP 在用户拒绝同意的情况下，依然转移用户数据至第三方；有的 APP 未对第三方数据共享行为进行安全评估，无法保障所共享用户数据在第三方使用时的安全。

五是无开启或关闭个性化服务选项。APP 未向用户告知并经用户同意的情况下，收集用户搜索、浏览记录和使用习惯等个性化特征，并将其用于定向推送服务或精准营销等。用户通常无法选择是否使用或接受个性化服务及定向推送。调查发现，84.42%的应用存在未经用户同意，强制接受个性化服务或精准营销的现象。

六是设置不合理障碍，账号注销难。APP 通过账号注册，提供更具价值的服务。为了留存用户，在注销环节设置各种障碍是常见现象。有的 APP 不提供账号注销服务，或应用声明提供账号注销服务，但注销入口难以寻找、注销功能无效或跳转到无关页面。有的 APP 在用户使用注销功能时，注销失败、无响应或超出注销承诺时限。有的 APP 设置指定方式、指定

地点等作为注销必要前提等。

APP 个人信息安全应对策略

提升 APP 个人信息安全能力，加强用户权益保护，需要全产业链的共同努力。

加强行业自律，明确企业主体责任。行业自律是用户个人信息保护的关键，也是企业可持续发展的内在基础。广大应用服务和应用分发厂商应主动适应个人信息保护和数据管理新形势新要求，严格遵守法律法规，贯彻落实个人信息收集使用规定，不断完善企业内部的个人信息保护和数据管理制度，持续优化用户隐私政策，并将个人信息保护的要求贯彻执行到规划、开发、运营等各个环节，切实有效维护好用户合法权益。

依托公众监督，及时响应用户关切。公众监督是保障用户权益的重要渠道，也是约束企业行为的有效方式。应用服务、应用分发平台厂商应高度重视用户权益保障，秉承以用户为中心的思想，健全公众参与监督的机制，主动关注用户感受和体验，尊重并保障用户的投诉权，为用户举报投诉设置便捷的方式和渠道。

规范收集使用规则，落实告知同意。个人信息收集使用规则是用户了解 APP 用户个人信息收集使用的主要渠道，收集使用规则应包含信息收集的内容、目的、方式、范围、频次、保护措施。同时，个人信息收集使用规则应清晰、明确、完整、易懂。移动应用服务商应严格依照收集使用规则收集处理用户个人信息，并遵循告知同意原则，在收集用户个人信息前，明示并经用户同意。

规范信息共享规则，明确责任归属。为明确责任归属，增加信息可追溯性。移动应用服务商应制定清晰、明确的信息共享规则，在公开、转移、共享用户个人信息前，应先明示用户公开、转移、共享的内容、对象、用途等相关信息，征得用户同意后，方可公开、转移或共享信息。移动应用服务商应与共享、转移的信息接收方订立安全协议，明确各方信息保护责任，并督促落实。

规范推送及权限调用，加强用户可知可控。APP 通常是基于用户画像进行定向推送和精准营销，APP 的开发者应遵循用户可知可控的原则，进行最小化权限申请，并提供完善的个性化推送开关选项，以有效约束在未向用户告知或未以显著方式标示情况下，将收集到的用户搜索、浏览记录、使用习惯等个人信息用于定向推送或精准营销。

提高应用防护能力，保障用户合法权益。安全防护能力是移动应用保护用户个人信息的基础保障。APP 开发者应采取必要的手段保障应用的安全性和用户数据的机密性、完整性和可用性。应用服务开发者应将安全编码原则贯穿整个软件开发周期，采用高等级 API 和安全 SDK、适配最新操作系统及外部代码库，并对应用进行必要的安全加固，采用安全存储和传

输技术保障用户敏感信息安全，通过完善的身份认证机制保障通信过程安全。

规范平台信息声明，保证下载用户知情。应用平台信息声明是用户了解应用基本信息的重要途径。平台应向用户明示应用名称、功能描述、卸载方法、开发者信息、应用安装及运行所需权限列表等基础信息，明确告知用户应用收集使用用户个人信息的内容、目的、方式和范围。

完善安全审核职责，落实分发上架机制。应用分发平台审核机制是用户个人信息保护的重要关口。平台应审核开发者资质和应用相关信息，制定明确的上架要求并建立完备的检测机制，通过自动化检测和人工审核等手段，对应用收集使用用户个人信息的行为进行规范。并对应用进行跟踪监测和管控，定期对已上架的应用进行复查，发现问题立即下架。

健全投诉反馈渠道，配合监管落实规范。应用分发平台承担连接用户、应用及终端的桥梁责任，是用户个人信息保护工作的重要环节。应用分发平台应建立多种渠道，及时接收和反映用户的建议和投诉，并通过既定的规则流程，及时响应用户投诉和应用侵权审核情况。

加强多方沟通协调，强化产业协作体系。针对当前用户普遍关注的移动互联网应用用户个人信息安全问题，移动互联网产业界应积极响应产业诉求，加强终端厂商、应用服务商、应用分发商、安全厂商等多方面的沟通协调，在设备安全、应用安全、数据安全等多方面加强交流合作，共享技术经验，制定行业标准规范，强化产业协作体系，保障移动互联网应用用户个人信息安全。（来源:《质量与认证》杂志社）

➢ 短视频应用的隐私政策问题与对策研究

随着人工智能、5G 等互联网新技术、新应用的迅速发展，为互联网用户提供了更加便捷、简单的信息制作、发布和传播途径。信息借助 5G 高速传播技术，一经发布，即可实现瞬间扩散，对人们的生活方式和生活习惯带来巨大变革。与此同时，互联网用户个人信息保护成为国内外政策法规出台、标准研制的焦点。

短视频应用以其便捷的内容生成途径、生动的内容展现形式、简洁的内容传播方式，自出现起便逐步成为备受互联网用户青睐的移动端娱乐方式。随着短视频应用用户量逐步增长，其对于用户的个人信息保护早已被纳入政府监管范畴，而 2019 年年底出现的疑似某短视频应用草稿箱视频外传事件，更是将短视频应用的个人信息保护推向社会公众关注的焦点。

我国法律法规等对于个人信息保护的要求

2011 年以来，关于用户的个人信息保护相关法律要求逐步在各项法律法规、规范性文件中体现。近 3 年，我国在个人信息保护方面立法更加频繁，个人信息的法律保障也逐步完善和成熟。

目前，我国暂时未出台专门的个人信息保护法律法规，相关要求分散存在于《网络安全法》《中华人民共和国刑法修正案（九）》《电信和互联网用户个人信息保护规定》等法律、部门规章等文件中（见表 1）。总体而言，对于个人信息保护的有关要求，可以归纳为几个方面。

类型	发布年份（年）	名称	相关要求
法律	2015	中华人民共和国刑法修正案（九）	明确违反国家有关规定，向他人出售或者提供公民个人信息，窃取或以其他方法非法获取公民个人信息等三种情形属于违法行为，且规定了处罚方式
	2016	网络安全法	明确了个人信息的概念，规定了个人信息保护原则和网络运营者应承担的法律义务
	2017	民法总则	明确了自然人的个人信息受法律保护
	2018	中华人民共和国电子商务法	明确电子商务经营者从事经营活动，收集和使用用户的个人信息，应当遵守法律和行政法规有关个人信息保护的规定，履行个人信息保护等方面的义务，并按要求制定个人信息保护的平台服务协议和交易规则
部门规章	2011	规范互联网信息服务市场秩序若干规定	明确了互联网信息服务提供者收集、使用用户个人信息的收集、使用原则，并应妥善保管用户个人信息，以及个人信息泄露后的处理流程
	2013	电信和互联网用户个人信息保护规定	明确了电信和互联网用户个人信息的保护范围，收集、使用原则与规则，电信业务经营者、互联网信息服务提供者应采取的安全保障制度，以及电信管理机构对用户个人信息保护情况实施监督检查等，进一步规范电信服务、互联网信息服务过程中收集、使用用户个人信息的活动
	2019	儿童个人信息网络保护规定	规范了在我国境内的网络运营者通过网络从事儿童个人信息的收集、存储、使用、转移、披露等活动，应遵守正当必要、知情同意、目的明确、安全保障、依法利用的原则，同时，明确提出网络运营者针对儿童个人信息的专门性、特设性保护义务
司法解释	2017	最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释	在《网络安全法》的基础上进一步扩大了个人信息的定义范围，同时明确了侵犯公民个人信息刑事案件的认定标准和量刑标准

规范性文件	2016	移动智能终端应用软件预置和分发管理暂行规定	明确生产企业和互联网信息服务提供者的用户个人信息收集、使用原则和基本要求，并提出从事应用商店等移动应用分发平台服务的互联网信息服务提供者，应加强网络安全防护、加强对相关人员的教育培训，保障用户个人信息安全
	2016	移动互联网应用程序信息服务管理规定	明确移动互联网应用程序提供者应建立健全用户信息保护制度，明确了个人信息收集、使用原则和基本要求
	2017	互联网跟帖评论服务管理规定	明确跟帖评论服务提供者应建立健全用户信息保护制度，明确了个人信息收集、使用原则和基本要求
	2016	互联网信息搜索服务管理规定	明确互联网信息搜索服务提供者应落实主体责任，建立健全信息安全管理制度，并具有安全可控的防范措施
	2017	互联网论坛社区服务管理规定	明确互联网论坛社区服务提供者应落实主体责任，建立健全信息安全管理制度，并具有安全可控的防范措施
	2017	互联网用户公众账号信息服务管理规定	明确互联网用户公众账号信息服务提供者应采取必要措施，保护用户个人信息安全，并提出不得泄露、篡改等禁止情形
	2017	互联网群组信息服务管理规定	明确互联网群组信息服务提供者应采取必要措施，保护用户个人信息安全，并提出不得泄露、篡改等禁止情形
国家标准	2017	GB/T 35273《信息安全技术个人信息安全规范》	对于个人信息存在的安全问题，提出个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为要求

表 1 我国个人信息保护的相关条例和标准

（1）明确个人信息的定义、收集和使用原则，个人信息的收集和使用需遵循合法性、正当性和必要性。

（2）个人信息收集、使用应获得信息主体的明示同意，并明确告知其信息使用和收集的目的、方式和范围。

（3）明确个人信息收集方应尽的法律义务和禁止性情形，不得对收集的个人信息泄露、篡改、毁损；未经允许不得向第三方提供。

（4）明确安全保障措施要求，个人信息收集方需采取必要措施，建立健全用户信息保护制度，确保个人信息安全。

（5）明确信息主体申诉的权利，信息主体发现被收集的个人信息未按双方的约定收集、使用等，或被用于违背法律法规要求使用时，可要求解除授权并删除有关个人信息。

（6）明确提出个人信息收集方对儿童个人信息的专门性、特设性的保护义务。

截止到 2019 年年底，工业和信息化部开展 APP 侵害用户权益专项整治工作，对违规收集和使用用户个人信息、不合理索取用户权限、为用户账号注销设置障碍等方面进行重点整治，整治对象包含 APP 服务提供者和 APP 分发服务提供者，并对检查中发现的存在侵害用户权益行为且未按要求完成整改的 APP 进行通报。

短视频应用用户隐私政策分析

本文选取在华为应用市场、App Store 的拍摄美化、短视频、摄影与录像等多个分类用户下载量排名靠前，且位于热门应用榜单推荐的 3 款短视频应用，分析其用户隐私政策。3

款应用用户隐私政策基本体现了对于用户个人信息收集、使用和处理等环节的明示同意、有限收集和使用，按要求存储有关日志，终止服务时的匿名化处理，并设立专门条款，加强对未成年人的个人信息保护，但仍普遍或部分地方有待完善。

涉及应用内第三方的情况规则缺失或采用一揽子形式

（1）对应用内提供的第三方产品、服务或技术，未明确告知用户个人信息的收集、使用情况，缺少有效的制度保障措施和技术手段。

（2）用户一经勾选同意隐私政策，即表示同意将个人信息在本公司、公司的关联方、合作方之间进行共享，未给予用户充分的自主选择权利。

疑似过度收集用户个人信息

（1）以维护服务正常运行、保障账号安全为名，收集用户的设备型号信息、操作日志信息、网络质量数据等用户个人信息。

（2）以安全运行所必需为名，收集正在运行的进程信息、应用程序的总体运行、使用情况与频率、总体安装使用情况等。

（3）以节省网络流量为名，收集用户的网络运营商及种类、网络类型、Wi-Fi 名称等。收集信息的目的和收集信息的种类无明确关联关系，疑似过度收集用户个人信息。

未明确对用户个人信息的存储时限，取消授权或明示删除后的处理方式

（1）未明确用户个人信息存储时限，或条款中仅承诺存储时限符合法律要求和服务所需的合理必要期限。

（2）未明确提出用户取消授权或明示删除时的信息处理方式和方法，或仅提出对于此类信息做删除或匿名化处理，未提供更多其他信息。

部分条款表述存在模糊、泛化或倾向性用词

（1）多存在“难以与您的真实身份关联”“可能收集”等模棱两可的模糊表述。

（2）提出多种情形可豁免征得同意，即可收集和使用个人信息，但部分情形表述过于泛化、含糊，难以界定。

（3）提出去标识化处理、匿名化处理后的个人用户信息用于共享、优化产品和服务等情形，但无法界定被使用的个人信息是否达到条款中所述无法识别用户个人身份的标准。

（4）使用具有明显倾向性或引导性表述，引导用户授权个人信息，或暗示用户授权更多个人信息，即可获得更好的服务。

对策与建议

（1）规范应用内第三方产品、服务或技术对用户个人信息的收集、使用，并将其配备

的制度保障措施、技术手段等情况如实告知用户，允许用户自主选择是否共享个人信息或使用相应功能。

（2）遵循合法、正当和必要的原则，经用户明示同意后，有限收集用户个人信息，给予用户对应用内各个服务、功能的自主选择是否使用，以及共享个人信息的权利，尽量避免采用一次性打包授权的形式。

（3）严格遵守有限收集、使用用户个人信息的原则，仅收集为用户提供服务所必须的个人信息，并明确告知用户所收集的个人信息存储时限，以及当用户要求取消授权或终止服务时，对于已收集个人信息的处理流程与方式。

（4）进一步优化隐私政策文字表述，采用客观、清晰的描述形式，为用户详尽阐述个人信息的收集、使用和存储等情况。在更新隐私政策时，允许用户查看最近一次更新上一版本的隐私政策，并在更新后的政策中显著标注调整内容，确保更新后的隐私政策不削减用户依据已同意生效的隐私政策应享有的权利。（来源：中国信息通信研究院安全研究所）

➢ 顺应时代要求大力加强网络安全人才建设

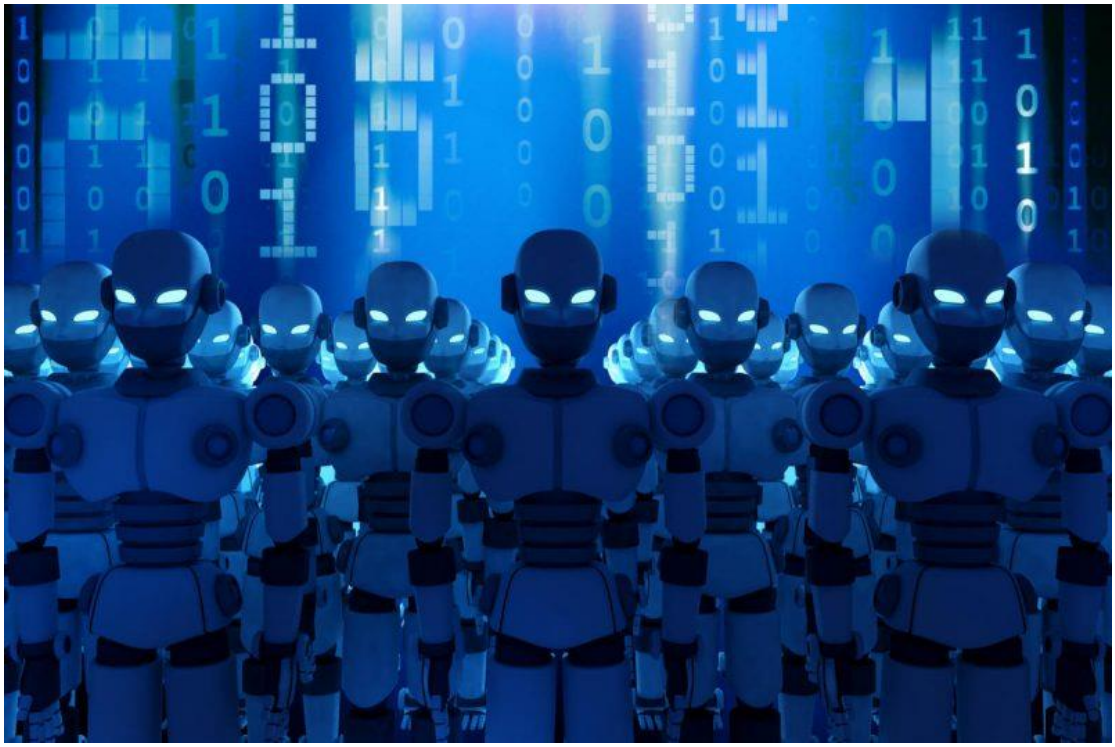
一、网络安全人才是经济发展和国家安全重要资源

人类社会经历了农业革命、工业革命，正在经历信息革命。数字化、网络化、智能化快速推进，经济社会运行与网络空间深度融合，从根本上改变了人们生产生活方式，重塑了社会发展的新格局。网信代表着新的生产力、新的发展方向。新一轮产业升级和生产力飞跃过程中，人才作为第一位的资源将发挥关键作用。

从全球范围来看，网络安全带来的风险正变得日益突出，并不断向政治、经济、文化、社会、国防等领域传导渗透。网络安全对国家安全牵一发而动全身，已成为国家安全体系的重要组成部分。网络空间的竞争，归根结底是人才竞争。信息化发达国家无不把网络安全人才视为重要资产，大力加强网络安全人才队伍的建设，满足自身发展要求和加强网络空间国际竞争力。建设网络强国需要聚天下英才而用之，要有世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队提供智力支持。在这个关键时期，能否充分认识网络安全人才和人才工作的重要性并付诸行动，关系着我们能否抓住信息化发展历史机遇，充分发挥中国人民在网络空间的聪明才智，实现网络强国战略的宏伟目标，推动实现中华民族伟大复兴中国梦。

二、国外网络安全人才队伍建设

随着信息技术快速发展，各国普遍将网络安全人才建设作为维护国家网络空间安全的核心需求。美国、俄罗斯、英国、德国、以色列、澳大利亚、日本、韩国等在网络安全投入上排名全球前列的国家都高度重视网络安全人才发展，把网络安全人才队伍建设列为国家的优先要务。



（一）世界网络强国高度重视网络安全人才建设

作为互联网的发源地和网络实力最强的国家，美国深谙网络安全人才的极端重要性，把公共领域和私营领域的网络安全人才队伍定位为保护美国国土安全和经济繁荣、确保美国竞争优势的基础。2010 年美国就启动了“国家网络安全教育（NICE）”计划，要求从专业人才、储备人才以及社会公众三个层面提升整个国家的网络安全能力水平。特朗普总统执政以后奉行“美国优先”的施政纲领，国家安全战略重新转向大国竞争，人才也成为其霸权护持的一项重要战略举措。为了维持美国在网络空间的绝对优势，特朗普政府提出了新的人才建设总目标，要在激烈竞争的网络空间“建设更有优势的网络安全人才队伍”，以避免敌对国家通过网络安全人才发展“威胁美国的长期竞争力”。

在网络空间“一超多强”力量格局下，其他信息化发达国家也普遍将人才建设作为网络安全战略中的重要组成部分。英国《国家网络安全战略（2016-2021 年）》要求政府将立即采取行动，解决关键的网络安全专业人士供需之间不断扩大的缺口，为该领域的教育和培训注入新的活力。澳大利亚《网络安全战略》提出要建设国家网络安全人员能力，指出人才是澳

大利亚实现其网络安全国家战略各项目标的基础。俄罗斯《国家信息安全学说》强调了信息安全保障人员欠缺的问题，要求发挥信息安全保障和应用信息技术领域人员的潜力。德国网络安全战略把联邦政府网络安全人事发展作为十大战略目标措施之一，要求进一步加强人员的培训，提升部门间人员合作。日本也制定了网络安全人才培养计划，设立“网络安全与信息化审议官”一职以统管人才培养工作，要求以东京奥运会为契机大力培养网络安全专家。

（二）国外网络安全人才建设的政策举措和启示

以美国为代表的发达国家在网络安全人才建设方面起步较早,在网络安全这一非传统领域培养专业人才进行了很多探索。从借鉴先行者经验的角度，有很多做法值得我们参考。首先美国对网络安全人才问题的重要性和紧迫性认识比较深刻，促使国会和联邦政府持续推出各种立法和行政手段进行应对。比如 FISMA 法案明确联邦政府部门负责人要对本部门的网络安全负总责，对安全岗位人员必须进行培训。美国由国家标准与技术研究院（NIST）牵头的国家网络安全教育（NICE）计划已经实施了十年，持续协调政产学各方面共同建设网络安全教育的生态网络。国家安全局（NSA）和国土安全部（DHS）主导的网络安全卓越学术中心（CAE）计划实施已有二十年时间，迄今已对 300 多所高校的网络防御、网络行动教学和研究能力进行了认定。即便如此，美国的人才危机意识依然很强，认为自己的人才缺口还在逐年增大。美国统计的网络安全岗位人才缺口 2017 年约为 30 万，到 2020 年已经超过 47 万。为此，美国政府责任署（GAO）已经连续二十年把网络安全人才问题列为联邦政府的一项高风险领域问题，要求未来还要进一步加大人才工作力度。

其次美国在人才建设方面秉承标准化思路，对各种分工的网络安全人员都有明确的教育培训、考核和管理的规范。比如美国标准与技术研究院于 2017 年发布了 SP800-181《国家网络安全人力框架》，对各类网络安全角色对应的任务，应该具备的知识、技能和能力都进行了给出了相应的描述。国防部所有承担信息保障职责的人员都需要根据国防部 8570 号令的要求进行培训和认证，六个月内拿不到资质的人员将无法承担相关岗位的工作。美国网络司令部最精锐的网络行动部队（CMF）更是制定了严格的网络安全培训与认证标准，对队伍进行训练并保持其战备状态。这些标准的背后是通过美国防务领域顶级的技术水平和深厚的网络安全产业基础来维系的，体现出的是美国对全频谱网络安全人才专业能力的洞察。各类人才标准互相关联和映射，体系性比较强，而且能够及时进行动态更新。通过标准化的方法，可以使高质量的人才培养模式得到复制和扩张，实现人才队伍的专业化和规模化发展。

三是注重保障重点领域的人才需求，美国在军队、政府部门制定了很多吸引人才、培养人才和留住人才的办法，启用了非常规手段优先解决重点要害部门的网安人才紧缺问题。例

如国防部、国家科学基金会（NSF）都针对高校设立了多项奖学金，吸引优秀的在校生攻读网络安全相关专业，鼓励其毕业后进入军队或政府部门工作。其中国防部的网络安全奖学金计划（CySP，原名信息保障奖学金计划 IASP）从 2001 年开始实施，截至目前已经提供了 9200 万美元的奖学金和教育资助经费。此外，网络安全人才短缺是各国都需要面对的难题，美国公共领域也需要同资本市场争夺高水平网络安全人才。美国军队和联邦政府部门都在设法使用一些破格用人、加强鼓励激励的措施。如，急需的网络安全人才可以通过非竞争性条件进行招聘，网络安全岗位人员破格提高薪酬和福利待遇等。

三、我国网络安全人才队伍建设

（一）网络安全人才培养具有优良传统和积累

我国的信息安全应用可以追溯至革命战争年代的密码工作。在信息安全人才培养方面，我国也有着悠久的历史。1959 年，西安电子科技大学就在钱学森的指示下在全国率先开展密码学研究。70 年代之前，已有专业性院校如军事院校设置信息安全相关专业，培养以密码学为主的技术人才。世纪交替之际，多所高校开始设立信息安全相关专业。1999 年，北京理工大学、西安电子科技大学等四所高校建立了信息对抗本科专业；2001 年，武汉大学建立了信息安全本科专业。与此同时，国家权威信息安全测评机构中国信息安全测评中心于 2002 年推出“注册信息安全专业人员（CISP）”，为党政机关、国家重要信息系统和基础信息网络的安全保障提供专业信息安全培训和人员资质认定。自此以后，我国信息安全学历教育和职业培训稳步发展，人才培养体系日趋完善。

（二）网络安全人才队伍建设进入快速增长期

党的十八大以来，国家就网络安全人才发展做出一系列重要部署，推出多项有力措施，取得了有目共睹的成就。网络安全学科专业设置、院系建设、学历教育方面取得突破性进展。目前，全国高校网络安全相关本科专业布点 233 个，网络安全相关专业建设院校超过 130 所。2018 年共招收本科生 9231 人，比上年增长 15.8%。共有 42 所高校成立了专门的网络空间安全学院或研究院；西安电子科技大学、东南大学、武汉大学、华中科技大学、北京邮电大学等 11 所高校入选一流网络安全学院建设示范项目。与此同时，针对网络安全专业人员的在职培训工作也取得了快速发展，中国信息安全测评中心 CISP 人员资质业务近年来每年增长速度超过 50%，累计培养信息安全专业人员数万人，为党政机关、通信、金融、能源、教育等重要行业持续输送信息安全骨干人才，已成为信息安全领域人才识别和能力评价的重要依据。

（三）网络安全人才发展事业将释放巨大潜力

当前我国面临的网络安全威胁和风险日益严峻复杂，个人信息泄露、网络诈骗、网络攻击等事件与日俱增；通信、金融、能源、交通、水利、公共服务、电子政务等关键信息基础设施安全遭受威胁；网络失窃密事件时有发生。为避免巨大的经济损失和严重后果，各类企事业单位已不得不重视网络安全问题，不得不重视人才，以应对这些网络安全威胁和风险。与此同时，我国网络安全法律体系的逐步建立和完善，《网络安全法》及与之配套的一系列密码管理、关键信息基础设施保护、网络安全等级保护、网络安全审查、数据出境评估、个人信息保护、数据安全保护等重要法律法规政策的影响正在今后一个时期逐步显现。全社会向网络安全制度规范化过渡的过程中，人才的关键作用将日益突出。网络安全人才不到位，就无法满足相关法律法规政策的合规要求。根据工信部《关于促进网络安全产业发展的指导意见（征求意见稿）》制定的目标，我国的网络安全产业规模到 2025 年将超过 2000 亿。在未来的安全保障业务需求和政策法规合规需求推动下，网络安全人才建设的工作必将出现跨越式发展，进一步释放出巨大潜力。

四、当前网络安全人才建设存在的问题

我国无论是信息化还是网络安全的发展，整体来看都属于“后发”国家，网络安全人才队伍建设也存在较大的不足。中央网信办等六部门发布《关于加强网络安全学科建设和人才培养的意见》，认为“我国网络安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。”全国人大常委会在《网络安全法》实施后的首次执法检查报告中指出，“不管是经济发达地区还是相对落后地区，网络安全技术人才都比较匮乏”。此次检查发现，网络安全人才短缺的情况主要包括网络运营单位技术人才多侧重于使用和维护，风险监控、应急处置和综合防护能力不足；关键信息基础设施核心业务系统虽然安装了防护系统，但由于缺乏高水平的安全技术人才，产品难以有效发挥作用；不少政府门户网站没有专门的网络安全技术人才，网站管理人员没有接受过系统的网络安全技能培训；受到编制、职务、薪资等因素制约，网络安全主管部门专业人才也明显不足。

网络安全人才是民生急需和国家安全战略必争领域的重要资源，需要及时掌握人才现状，对存在的问题和短板进行分析研究。结合网络安全自身特点和网络安全人才发展规律，当前我国网络安全人才队伍建设还存在以下突出问题。

（一）网络安全从业人员全方位短缺

网络安全工作贯穿信息化建设的各个环节，无论是在数据、应用、系统、网络等工作层面，还是涉及规划、研发、建设、运营、管理、生产等业务流程，都需要有人承担网络安全

职责。但目前我国网络安全从业人员整体呈现全方位短缺的态势，一是网络安全人员规模总量不足，除专业安全服务企业、特大型企业集团，以及大型互联网企业建立有规模化的网络安全人才梯队外，多数单位的网络安全人员无法满足当前工作需要。二是大量信息安全工作以“非专职”方式完成，多数网络安全从业人员需要承担非安全内容的工作，政府机关事业单位里需要“身兼数职”的现象最为显著。三是各类安全工作角色均存在人才缺口，根据《中国信息安全从业人员现状调研报告（2018-2019 年度）》显示，在人才普遍短缺的前提下，从事安全建设和规划管理类的人才相对更加紧缺。

（二）信息安全职业化尚处于初级阶段

职业化是现代社会分工协作体系的结果，是行业发展到一定程度的标志。网络安全的职业化主要体现在对网络安全从业人员专业知识、能力和行为准则建立标准化规范，由专人专岗负责专门工作。我国《网络安全法》已对关键信息基础设施运营者“设置专门安全管理机构和安全管理负责人”做出了明确规定，同时鼓励其他网络运营者自愿参与关键信息基础设施保护体系。但目前网络安全的职业化总体来看还处在发展初级阶段。一是网络安全目前还没有统一的职业标准，对从业人员如何分级分类、应具备何种专业知识和能力水平等问题尚未建立标准规范，各用人单位的信息安全岗位设置和能力要求各行其是，差别较大。二是信息安全“人岗不匹配”情况普遍，专门的网络安全管理部门和岗位中的人员从事的不是网络安全工作，或是人员专业能力达不到岗位要求。三是社会对信息安全职业意识普遍不强，尤其是用人单位高层，或是对信息安全工作以及信息安全人才重要性的认知有待提升，或是对人才工作的重要性只有原则上的认同，在如何科学有效地加强信息安全队伍建设方面缺乏工作抓手。

（三）人员能力提升需求难以得到满足

战略性的人力资源管理核心在于把人看作重要的资产，通过教育培训等投入，持续提高其知识、技能和素质水平，更好地达成用人单位的业务目标。用人单位能否提供足够的培训、持续提升人才专业能力、帮助其完成自我价值实现，将在“引才”和“留才”中发挥越来越重要的作用。当前人员能力提升需求普遍难以得到满足，一是从业人员能力提升需求旺盛，新入职人员在学历教育之后普遍需要进行“二次培训”，已从业的人员也需要持续教育和终身学习。中国信息安全测评中心调研显示，当前从业人员最希望提升大数据安全、云安全、安全管理和渗透测试等方向的专业能力。二是从业人员期望获得专业资质，作为证明自己具备一定知识、能力和工作经验的凭证。调研数据显示未来一年内，有 83.7%的从业人员期望获得信息安全资质证书，其中希望获取 CISP 证书的人员占比最高，达到 68.9%。三是尽管从

业人员的学习热情很高，但用人单位教育培训投入不够，对信息安全人员普遍存在“使用多、培养少”的情况，用人单位资助从业人员接受职业培训的意愿和力度也不高。

（四）网络安全人才体制机制存在障碍

网络安全作为跨界、交叉、融合的非传统行业，唯有在鼓励创新发展的体制机制下，才能让人才的创造活力竞相迸发、聪明才智充分涌流。当前网络安全人才发展还存在一系列制度性障碍，一是对安全从业人员考核评价手段不足，信息安全工作不易直接量化考核，信息安全成果和价值难以直接得到体现。二是人员鼓励激励机制不健全，上升空间有限，从业人员难以得到与工作投入相匹配的职业回报。三是缺乏向关键领域的人才引导机制，从业人员在职业流动中对福利性因素和发展性因素均十分看重，但当前大量关键信息基础设施运营单位在“待遇引人”、“事业留人”等方面均面临挑战，甚至自有人才流失的现象也比较严重。

五、对策建议

网络安全是技术更新最快的领域之一，网络空间的竞争，归根到底是人才的竞争；建设网络强国，最关键的资源是人才。建议要以现有的学历教育和职业培训工作为基础，明确人才建设的总体战略方向，充分利用各种工作机制，最大限度地加强网络安全人力资源开发力度，为国家网络安全保障提供有力的人才支撑。

（一）建立体系化的网络安全人才发展规划

习近平总书记在 2018 年全国网络安全和信息化工作会议上提出，要研究制定网信领域人才发展整体规划，推动人才发展体制机制改革，让人才的创造活力竞相迸发、聪明才智充分涌流。总书记的指示高屋建瓴，体现了对网信人才重要性和当前重点任务的深刻认识。人才建设是长期性、战略性、基础性工作，建立网络安全人才发展整体规划至关重要。对国家网络安全人才发展全局进行系统性的超前规划部署，才能争取主动局面，建设具有全球竞争力的网络安全人才队伍，为网络强国建设夯实基础。

一是要构建网络安全国民教育和持续教育体系，为各类网络安全意识提升、基础教育、高等教育、职业培训、持续教育提供总体指导，为包括网络安全从业人员、后备人员以及普通公众在内的社会全体成员信息安全能力、防护技能的提升提供支撑。

二是统筹推进网络安全人才发展整体工作，通盘规划网络安全人才培养、管理和使用等各项工作，明确主要任务和阶段性目标，加快网络安全人才管理体制以及人员流动配置、培养开发、考核评价和激励保障等工作机制改革。

三是多主体协同共建网络安全人才生态，提高相关主管领导部门、产业界、学术界、科研院所、用人单位等相关各方的支持配合力度，有力整合资源，完善配套措施，形成推进合

力，共同构建良好的网络与信息安全人才发展生态。

（二）科学推进信息安全人才的职业化发展

在网络安全从业人员全方位短缺的严峻形势下，职业化手段有助于明确信息安全职业的正当性、改进网络安全教育培训的针对性、促进网络安全人才供需匹配、提升网络安全职业吸引力。但作为新兴的非传统领域，网络安全的职业化不宜对不同类型从业人员简单采用“一刀切”的职业许可方式进行管理。

一是要深入开展网络安全人才发展基础理论和前沿实践研究，探寻网络安全人才成长规律，形成科学的网络安全从业人员测评标准，作为安全人才职业化的发展依据，为制定人员教育培训目标、完善人才管理体系提供支撑。

二是要建立兼具相对稳定性和动态灵活性的网络安全知识体系，综合网络安全专业能力图谱中核心和通用的部分，维持一个相对稳定的基础知识体系；针对细分方向和前沿领域的部分，建立动态调整的知识子域，为网络安全职业化夯实基础。以 CISP 为例，其知识体系大约每三年进行一次更新，既维持了稳定的知识体系结构和主要知识要点，保障了培训体系的连贯性，同时能够及时反应网络安全新技术新应用的发展趋势，确保培训内容的时效性和实用性。为响应社会的迫切需求，CISP 根据技术发展趋势推出了安全开发、信息系统审计、渗透测试、大数据安全等十余个专业方向，为行业细分领域提供更加聚焦的专业培训内容，建立了日益丰富而全面的网络安全人才培养体系。

三是要推进权威机构的网络和信息安全专业人才资质认定工作，有公信力的机构开展资质认定工作能够有效证明从业人员具备了相应的专业知识和能力、工作经验和业绩以及较高的职业道德水平，从而为网络与信息安全人才评价考核、选拔任用、职业晋阶提供参考依据。CISP 经过多年的发展，已经建立了全面的知识体系、完备的教材体系、科学的培训方法、稳健的工作模式以及强大的师资队伍，成为行业内评价网络与信息安全专业人员综合能力的必备资质。

（三）着力提升网络安全从业人员规模能力

以经济社会发展和国家安全需求为导向，加强人才培养体系建设工作的前瞻性和针对性，建立贯穿网络安全从业人员学习工作全过程的终身教育制度，提高网络安全人才队伍的数量规模和整体能力。

一是加大教育培训投入和工作力度，既要利用好成熟的职业培训体系，快速培养网络安全急需人才；也要在基础教育、高等教育和职业院校中深入推进网络安全教育，积极培养网络安全后备人才；全面优化教育培训的内容、类别、层次结构和行业布局，着力解决网络安

全人才总量不足的突出问题。

二是分类施策建设网络安全人才梯队，对于社会对网络安全基层人员的需求，开展规模化培养，尽快解决当前用人需求；对于卓越工程师和高水平研究人才的需求，在工程和科研项目基础上加强专业化培训，打造网络安全攻坚团队和骨干力量；对于网络安全核心技术人才和特殊人才的需求，探索专项培养选拔方案，塑造网络安全核心关键能力。

三是结合领域特点推进网络安全教育培训供给侧改革，探索网络安全体系化知识更新与碎片化学习方式的结合、线下系统培训和线上交互培训的结合、理论知识理解和实践操作磨练的结合、金字塔层次化梯队培养和能揭榜挂帅的网络专才选拔的结合，加强专业资质测评在人才队伍建设中的引领和导向作用，创新人才培养模式，深化产教融合，贯通后备人才到从业人员的通道，推动各类学校、专业培训机构和企业通过校园教育、现代学徒制培训、任职培训、在职培训、岗位练兵、攻防竞赛、技术比武等方式，推动网络安全人才工作的高质量发展。

（四）持续优化网络安全人才发展整体环境

网络安全是信息技术的尖端领域，是智力最密集、最需要创新活力的领域。坚持以用为本、急用先行的原则，加快网络安全人才发展体制机制创新，制定适应网络安全特点的人才政策，让人才的创造活力竞相迸发，聪明才智充分涌流。一是提高各级党政领导干部的网安意识和网安人才意识，在干部培训中将网络安全作为必修课程，引导其积极适应时代要求，强化网络安全思维，提高对人才工作重要性的认识，真正尊重人才、爱才惜才，为人才发展创造良好条件。

二是加快创新网络安全从业人员评价激励机制，参考企业中激发网络安全人才活力效果最好的管理实践和经验，创新发展适应网络安全特点的薪酬制度、评价指标和鼓励激励措施，让网络安全人才价值得到尊重和体现，名正言顺地提高从业人员的经济待遇和社会地位。

三是建立重点领域网络安全人才引导和优先保障机制，采取特殊政策，完善配套措施，引导和鼓励网络安全人才向国家党政机关、要害部门、重要行业、关键信息基础设施运营单位流动，确保重点领域能够招得进、用得好、留得住网络安全高端人才和紧缺人才。（来源：《中国信息安全》杂志 2020 年第 4 期）

四、政府之声

➢ 国家网信办启动专项整治行动 严厉打击网络恶意营销账号

2020 年 4 月 25 日，中国网信网报道：今年 3 月以来，多个网络账号炒作“疫情之下的某国：店铺关门歇业，华商太难了”“多国渴望回归中国”“钟南山：5 月疫情将全面爆发”等“标题党”文章，散布虚假信息，造成极为恶劣的社会影响。针对这些问题，国家网信办有关负责人表示，部分网络账号为获取流量和广告进行恶意营销，有的无中生有造热点，引发社会恐慌；有的冒用权威人士名义，发布谣言误导公众；有的炮制耸人听闻标题，引发群体焦虑和不安；有的恶意篡改党史国史，鼓吹历史虚无；有的诋毁抹黑英雄烈士，消解主流价值观；有的大打色情“擦边球”，影响青少年身心健康；有的大搞“黑公关”敲诈勒索，侵害企业或个人合法权益。这些恶意营销行为扰乱了正常网络传播秩序，损害了广大网民利益，应该予以坚决打击。

该负责人还表示，按照国家网信办统一部署，近日北京、上海、广东等地网信部门积极作为，腾讯、新浪、今日头条、网易、趣头条等网站平台主动开展自查自纠，全面排查平台内网络账号恶意营销问题，集中清理相关违法违规信息，严肃处理涉及恶意营销的网络账号。据初步统计，已清理相关文章 6126 篇，关停账号 18576 个。

即日起，国家网信办将组织各地网信部门开展为期两个月的网络恶意营销账号专项整治行动，进一步聚焦突出问题，压实主体责任，加大惩治力度，对问题严重、影响恶劣的网站平台、网络账号及相关责任人依法依规严肃处置，并向社会公众通报处置结果。欢迎广大网民、媒体和社会各界积极参与，向网站平台和有关部门举报相关问题，携手营造清朗网络空

间。（来源：国家网信办）

➢ 银保监会回应“银行保险机构售卖数百万条客户信息”

2020 年 4 月 22 日，针对近期有报道称部分银行保险机构售卖客户信息达数百万条，中国银保监会副主席黄洪 22 日在北京回应说，被贩卖信息绝大部分系黑客伪造或拼凑。银保监会始终对侵害金融消费者权益、损害客户信息安全的行为坚持零容忍，一经发现将严肃依法查处，严厉打击。

黄洪当天出席国务院新闻办公室发布会时称，在上述报道之前两日，银保监会相关部门就已监测到不法分子在境外发布的售卖信息，并立即部署相关机构进行全面排查。随后，相关机构也陆续发表澄清声明。经查，被贩卖的信息绝大部分是黑客伪造或拼凑的。

他强调，银保监会高度重视银行保险机构网络安全工作，尤其把客户信息保护作为重中之重。近年来，已印发了一系列监管政策文件，要求银行保险机构认真贯彻落实个人信息保护方面的法律法规，加强客户隐私保护，对客户信息严格实行从采集到存储、销毁等全流程制度化管理。

此外，银保监会还建立了网络安全风险监测、风险预警、非现场监管、现场检查、监管评级等长效工作机制，把银行保险业客户信息保护工作纳入日常信息科技风险监管中。官方还不定期组织开展客户信息保护专项行动，银行业、保险业网络安全专项治理，指导监督银行保险机构加强网络安全风险排查整改。

黄洪表示，下一步，银保监会将继续坚持监管为民理念，进一步强化银行业、保险业网络安全监管，督促银行保险机构继续加大相关工作力度，进一步构建安全可靠的网络金融环境，切实保护好金融消费者权益。（来源：银保监会）

➢ 公安部公布十起侵犯公民个人信息违法犯罪典型案件

2020 年 4 月 15 日，公安部公布了 2019 年以来公安机关侦破的 10 起侵犯公民个人信息违法犯罪典型案件。

一、江苏南通公安机关侦破“20191023”“暗网”侵犯公民个人信息案

2019 年 10 月，江苏省南通市公安局网安部门工作发现，网民“wolinxuwei”多次在“暗

网”交易平台出售银行开户、手机注册等公民个人信息，数量高达 500 余万条。经查，“wolinxuwei”真实身份为林某。2019 年初，林某在“telegram”群组结识某公司安全工程师贺某，林某以 40 万元的价格从贺某处购得银行开户、手机卡注册等各类公民个人信息 350 余万条，并通过“暗网”销售给经营期货交易平台、推销 POS 机的费某、王某等人，非法牟利 70 余万元。11 月 12 日至 26 日，南通公安机关先后在上海、苏州、武汉等地抓获犯罪嫌疑人林某、费某等犯罪嫌疑人 11 名，查获公民个人信息 2000 余万条。

二、江苏南京公安机关侦破“4·2”“暗网”侵犯公民个人信息案

2019 年 4 月，江苏南京公安机关接到某单位信息中心报案，称该中心管理的南京市 1400 余万条居民社保数据被非法盗取，并在“暗网”内售卖。南京市公安局网安部门迅速查明盗取并在“暗网”上兜售社保数据的犯罪嫌疑人熊某及其上下线犯罪嫌疑人任某、薛某。经查，任某为江苏某计算机技术有限公司工程师，在为南京市某单位进行信息系统漏洞测试时，利用系统漏洞盗取了居民社保数据，后伙同在柬埔寨的违法犯罪人员熊某在“暗网”上销售。其中，熊某将 7 万条数据卖给了薛某。5 月 16 日，南京公安机关在柬埔寨警方配合下抓获犯罪嫌疑人熊某，后在境内抓获犯罪嫌疑人任某、薛某。

三、湖北武汉公安机关侦破吴某“暗网”侵犯公民个人信息案

2018 年 11 月，湖北武汉公安机关接到报案，称某汽车金融服务平台服务器被黑客入侵，包括身份证、手机号、家庭住址等情况在内的 30 余万条客户信息被盗取，被人以 1 比特币（时值 3.5 万元人民币）的价格在“暗网”上出售。武汉市公安局网安部门经过深入侦查，于 2019 年 1 月 22 日在四川成都抓获犯罪嫌疑人吴某。吴某交代其利用暴力破解手段非法获取涉案网站后台管理权限，盗取大量公民个人信息在“暗网”叫卖。

四、北京公安机关侦破高某“暗网”侵犯公民个人信息案

2019 年 6 月，北京市公安局网安部门工作发现，网民“yuhong”在“暗网”贩卖国内某银行 6.02 万条用户个人信息。北京市公安局网安部门缜密侦查，锁定犯罪嫌疑人高某。7 月 24 日，北京公安机关将高某抓获归案。高某交代其利用网站漏洞非法窃取了某银行等单位网站上存储的公民个人信息，截至被抓获，非法牟利 3 万余元。

五、江苏徐州公安机关侦破“12·21”侵犯公民个人信息案

2018 年 12 月，江苏省徐州市公安局网安部门工作发现，一网民在网上购买他人名下手机号码等公民个人信息。徐州网安部门以此入手，挖掘出一个以电信运营商、银行内部员工为源头的买卖公民个人手机信息、征信信息等信息的犯罪网络。2019 年 1 月 2 日，徐州公安机关组成 23 个抓捕组，分赴 20 余个省市开展集中收网行动，先后抓获嫌疑人 45 名，其

中电信运营商、银行等部门内部人员 20 余名，查获各类公民个人信息 43 万余条，冻结涉案资金 120 余万元。

六、河南开封公安机关侦破赵某等人侵犯公民个人信息案

2018 年 12 月，河南省开封市公安局网安部门工作发现，网民“夕阳红”通过微信群大肆贩卖手机机主姓名、财产信息、个人户籍资料等公民个人信息。公安机关侦查掌握了一个由多部门“内鬼”与外部人员勾结，层层倒卖公民个人信息至下游电信网络诈骗、暴力催债、网络赌博等违法犯罪人员的侵犯公民个人信息犯罪网络。开封公安机关历时 12 个月，辗转 20 余个省市，先后抓获犯罪嫌疑人 200 余名，其中，电信运营商、社区干部、物流行业等内部人员 80 余名、暴力催收人员 50 余名，打掉非法暴力催收公司 2 个，查获公民个人信息 1 亿余条，冻结涉案资金 1000 余万元。

七、山东济南公安机关侦破徐某等人公民个人信息被侵犯案

2019 年 3 月，山东济南公安机关接山东某高校学生徐某等人举报，称其与同学个人身份信息被他人非法收集用于注册实名手机卡出售。济南市公安局网安部门立即开展侦查工作。经查，济南某区联通公司某高校网点负责人葛某与其他高校网点业务员勾结，利用工作便利非法收集学生身份信息，开设实名手机卡后，向下游网络账号注册商、手机卡倒卖商刘某等人销售。刘某等人在销售手机卡的同时，使用“猫池”设备利用贾某、徐某等人提供的注册工具，通过接码平台大量注册、解封网络账号出售牟利。济南公安机关历时 6 个月，先后抓获庄某、刘某在内的犯罪嫌疑人 22 名，扣押“猫池”设备 163 台、手机卡 5 万余张，查获上述人员非法注册 QQ 号 150 余万个、新浪微博号 200 余万个、“12306”账号 100 余万个。

八、江苏连云港公安机关侦破梅某等人侵犯公民个人信息案

2019 年初，江苏连云港公安机关侦破一起搭建虚假炒股平台实施诈骗案。连云港市公安局网安部门随后顺线追踪，发现一条以证券公司内部人员范某等人为源头，层层倒卖股民信息至境内外网络炒股诈骗团伙的跨境侵犯公民个人信息犯罪链条，下游诈骗分子使用股民信息实施诈骗，涉案金额高达 2220 余万元。连云港公安机关据此先后抓获犯罪嫌疑人 53 名，包括某证券公司内部员工 2 名，查获股民信息 300 余万条。

九、贵州安顺公安机关查处杨某侵犯涉疫情公民个人信息违法案件

2020 年 1 月，贵州省安顺市公安局网安部门工作发现，一新浪网民在网上举报有人在微信朋友圈内大肆传播疫情防控重点人员信息。安顺网安部门立即开展网上侦查，查明该批涉疫情公民个人信息传播源头为安顺市天柱县某街道社区工作人员杨某，杨某在工作中获取

了社区疫情防控人员信息后向好友发送，造成相关信息在微信中迅速扩散，造成恶劣影响。安顺公安机关依法对杨某行政拘留 15 日、罚款 5000 元。

十、贵州黔东南州公安机关查处王某侵犯涉疫情公民个人信息违法案件

2020 年 1 月，贵州省黔东南苗族侗族自治州公安局网安部门工作发现，一份名为“新型冠状病毒感染肺炎防控重点人员台账”在互联网上大肆传播。黔东南州网安部门立即开展网上侦查，查明该台账由黔东南州凯里市某幼儿园员工王某在工作中获取，发布于小区微信群中，随后被层层转发，造成恶劣影响。黔东南州公安机关依法对王某行政拘留 12 日、罚款 5000 元。（来源：人民公安报）

➢ 国家互联网应急中心发布《2019 年我国互联网网络安全态势综述》

2020 年 4 月 20 日，国家互联网应急中心（CNCERT）编写的《2019 年我国互联网网络安全态势综述》报告（以下简称“2019 年态势报告”）正式发布。为全面反映当前我国网络安全的整体态势，CNCERT 自 2010 年以来，每年及时发布前一年度网络安全态势情况综述，至今已连续发布 11 年，对我国党政机关、行业企业及全社会了解我国网络安全形势，提高网络安全意识，做好网络安全工作提供了有力参考。

2019 年态势报告立足于 CNCERT 网络安全宏观监测数据与工作实践，报告涉及 2019 年典型网络安全事件、网络安全新趋势及日常网络安全事件应急处置实践等内容。报告主要分为四个部分：

一是总结 2019 年我国互联网网络安全状况。

报告重点从拒绝服务攻击、APT 攻击、安全漏洞、数据安全、移动互联网安全、互联网黑灰产、工业控制系统安全等七个方面总结了 2019 年我国互联网网络安全状况。2019 年，我国在以上七个方面持续加大监测发现、治理处置力度并取得明显成效，但仍面临突出的风险与挑战。

二是预测 2020 年网络安全热点。

报告提出六点预测，认为国家关键信息基础设施安全、重要数据和个人信息保护、国家级网络对抗、精准网络勒索、远程协同安全风险、5G 等新技术安全将成为 2020 年网络安全领域值得关注的热点。

三是结合网络安全态势分析提出对策建议。

报告从强化关键信息基础设施保护、加快网络安全核心技术创新突破、提升数据安全管理和个人信息保护力度、壮大网络安全技术产业规模和网络安全人才队伍、扩大国内外网络安全合作五个方面，对进一步做好我国网络安全工作提出建议。

四是梳理网络安全监测数据。

报告从攻击来源、攻击对象、攻击规模三个维度，对恶意程序、安全漏洞、拒绝服务攻击、网站安全、工业控制系统安全等五个方面 2019 年我国互联网网络安全监测数据进行了梳理。（来源：国家互联网应急中心（CNCERT））

- **《2019 年我国互联网网络安全态势综述》报告**
- **全文：**https://www.cert.org.cn/publish/main/upload/File/2019-year.pdf

五、本期重要漏洞实例

➢ WordPress Search Meter plugin 输入验证错误漏洞

发布日期：2020-04-13
更新日期：2020-04-13
受影响系统：
WordPress Search Meter plugin <2.13.2
描述：

CVE(CAN) ID: CVE-2020-11548
WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。Search Meter plugin 是使用在其中的一个搜索内容记录插件。
WordPress Search Meter plugin 2.13.2 之前版本中存在输入验证错误漏洞。攻击者可利用该漏洞执行代码。
建议：

厂商补丁：
WordPress
目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：
链接：https://wordpress.org/plugins/search-meter/

➢ Oracle Weblogic WlsSSLAdapter 远程代码执行漏洞

发布日期：2020-04-16
更新日期：2020-04-16
受影响系统：
Oracle WebLogic Server 10.3.6.0.0
Oracle WebLogic Server 12.1.3.0.0
Oracle WebLogic Server 12.2.1.3.0
Oracle Oracle WebLogic Server 12.2.1.4.0
描述：

CVE(CAN) ID: CVE-2020-2798
WebLogic 是美国 Oracle 公司出品的一个应用服务器，是一个基于 JAVAEE 架构的中间件，WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 Java 应用服务器。
Oracle Weblogic WlsSSLAdapter 存在远程代码执行漏洞，攻击者可利用该漏洞通过 t3 协议或 iiop 协议发送精心构造的 Payload 达到远程代码执行效果。

建议：

厂商补丁：
Oracle
目前厂商已发布相关漏洞补丁链接，请关注厂商主页随时更新：
https://www.oracle.com/middleware/weblogic/index.html

➢ Microsoft 发布 2020 年 4 月安全更新

发布日期：2020-4-14
更新日期：2020-14-14
描述：

CVE(CAN) ID: CNTA-2020-0006
微软发布了 2020 年 4 月份的月度例行安全公告，修复了其多款产品存在的安全漏洞。受影响的产品包括：Windows 10 1909 & WindowsServer v1909（66 个）、Windows 10 1903 & WindowsServer v1903（66 个）、Windows 10 1809 & WindowsServer 2019（63 个）、Windows 8.1 & Server 2012 R2（39 个）、Windows RT 8.1（38 个）、Windows Server 2012（36 个）、Microsoft Edge (HTML-based)（2 个）、Internet Explorer（4 个）和 Microsoft Office-related software（22 个）。
利用上述漏洞，攻击者可绕过安全功能限制，获取敏感信息，提升权限，执行远程代码或发起拒绝服务攻击等。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题和摘要	最高严重等级和漏洞影响	受影响的软件
CVE-2020-1020	**Adobe Font Manager Library 远程代码执行漏洞** 当 Windows Adobe Type Manager Library 未能正确地处理构建的多主字体 Adobe Type 1 PostScript 格式时，Microsoft Windows 中存在远程代码执行漏洞。攻击者有多种方法可以利用此漏洞进行攻击，例如说服用户打开构建的文档或在 Windows 预览窗格中查看。	严重 远程执行代码	Windows 10 Server, version 1803 Server, version 1903 Server, version 1909 Server 2016 Server 2019 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0687	**Microsoft Graphics 远程代码执行漏洞** 当 Windows 字体库未能正确处理构建的嵌入字体时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。将帐户配置为在系统上拥有较少用户权限的用户可能比使用管理用户权限操作的用户受影响更小。 安全更新通过更正 Windows 字体库处理嵌入字体的方式来解决该漏洞。	严重 远程执行代码	Windows 10 Server, version 1803 Server, version 1903 Server, version 1909 Server 2016 Server 2019 Windows 8.1 Server 2012 Server 2012 R2

CVE-2020-0910	**Windows Hyper-V 远程代码执行漏洞** 当主机服务器上的 Windows Hyper-V 未能正确验证来宾操作系统上经过身份验证的用户的输入时，存在远程代码执行漏洞。要利用此漏洞，攻击者可以在来宾操作系统上运行构建的应用程序，这可能会导致 Hyper-V 主机操作系统执行任意代码。成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。 安全更新通过更正 Hyper-V 如何验证来宾操作系统用户输入来解决该漏洞。	严重 远程执行代码	Windows 10 Server 2019 Server, version 1903 Server, version 1909
CVE-2020-0938	**Adobe Font Manager Library 远程代码执行漏洞** 当 Windows Adobe Type Manager Library 未能正确地处理构建的多主字体 Adobe Type 1 PostScript 格式时，Microsoft Windows 中存在远程代码执行漏洞。对于除 Windows 10 以外的所有系统，成功利用此漏洞的攻击者都可以远程执行代码。对于运行 Windows 10 的系统，成功利用此漏洞的攻击者可以在 AppContainer 沙盒上下文中以有限的权限和功能执行代码。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 攻击者有多种方法可以利用此漏洞进行攻击，例如说服用户打开巧尽心思构建的文档或在 Windows 预览窗格中查看该文档。 更新通过更正 Windows Adobe 类型管理器库处理 Type1 字体的方式解决了该漏洞。	严重 远程执行代码	Windows 10 Server, version 1803 Server, version 1903 Server, version 1909 Server 2016 Server 2019 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0965	**Microsoft Windows Codecs Library 远程代码执行漏洞** Microsoft Windows Codecs Library 处理内存中对象的方式存在远程代码执行漏洞。成功利用此漏洞的攻击者可以执行任意代码。 利用此漏洞需要程序处理巧尽心思构建的图像文件。 此更新通过更正 Microsoft Windows 编解码器库如何处理内存中的对象来解决此漏洞。	严重 远程执行代码	Windows 10 Server, version 1803 Server, version 1903 Server, version 1909 Server 2016 Server 2019 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0969	**Chakra Scripting Engine 内存破坏漏洞** Chakra 脚本引擎处理 Microsoft Edge（基于 HTML）内存中对象的方式存在远程代码执行漏洞。该漏洞可能会破坏内存，使得攻击者可以在当前用户的上下文中执行任意代码。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 安全更新通过修改脉轮脚本引擎如何处理内存中的对象来解决该漏洞。	严重 远程执行代码	Edge (HTML based) ChakraCore
CVE-2020-0968	**Scripting Engine 内存破坏漏洞** 脚本引擎处理 Internet Explorer 内存中对象的方式存在远程代码执行漏洞。该漏洞可能会破坏内存，使得攻击者可以在当前用户的上下文中执行任意代码。成功利用此漏洞的攻击者可以获得	严重 远程执行代码	Internet Explorer 11

	与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 安全更新通过修改脚本引擎处理内存中对象的方式来解决该漏洞。		
CVE-2020-0931	**Microsoft SharePoint 远程代码执行漏洞** 当软件无法检查应用程序包的源标记时，Microsoft SharePoint 中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。 利用此漏洞需要用户将精心编制的 SharePoint 应用程序包上载到受影响的 SharePoint 版本。 安全更新通过更正 SharePoint 如何检查应用程序包的源标记来解决此漏洞。	严重 远程执行代码	SharePoint Foundation 2013 SharePoint Enterprise Server 2013 SharePoint Server 2019 Business Productivity Servers 2010 SharePoint Enterprise Server 2016

来源：

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Apr

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001

➢ Adobe ColdFusion 拒绝服务漏洞

发布日期：2020-04-15

更新日期：2020-04-16

受影响系统：

Adobe ColdFusion 2018

Adobe ColdFusion 2016

描述：

CVE(CAN) ID: CVE-2020-3767

Adobe ColdFusion 是一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言。

ColdFusion 2016，2018 在实现中存在输入验证漏洞，攻击者利用此漏洞可造成受影响应用拒绝服务。

<*来源：Jason Troy

链接：https://helpx.adobe.com/security/products/coldfusion/apsb20-18.html

*>

建议：

厂商补丁：

Adobe

Adobe 已经为此发布了一个安全公告（APSB20-18）以及相应补丁:

APSB20-18：Security updates available for ColdFusion

链接：https://helpx.adobe.com/security/products/coldfusion/apsb20-18.html

六、本期网络安全事件

➢ 旧金山国际机场证实其网站遭黑客入侵 员工密码或遭窃取

2020 年 4 月 14 日，旧金山国际机场已确认，其两个网站在 3 月份被黑客入侵，攻击者似乎已经访问了其员工和承包商的用户名和密码。该机场在 4 月 7 日的一份通知中证实，SFOConnect.com 和 SFOConstruction.com 这两个网站是 "网络攻击的目标"，黑客在这两个网站上 "插入了恶意的计算机代码，以窃取一些用户的登录凭证"。如果被窃取，这些登录凭证可能会让攻击者进入机场的网络。目前还不知道是否有任何额外的保护措施，如多因素认证等，以防止网络漏洞。

该通知还补充说："用户可能会受到这次攻击的影响，包括那些通过基于 Windows 操作系统的个人设备或非机场维护的设备从机场网络以外的 Internet Explorer 访问这些网站的用户。”

通知称，机场于 3 月 23 日将员工专用网站下线，并发布了强制重置密码的通知。现在两个网站都已恢复运行。旧金山国际机场的发言人没有立即发表评论。

攻击者利用现有的漏洞在网站上注入代码以获取输入的数据，如用户名和密码甚至信用

卡信息等，这种情况并不罕见。

两年前，英国航空的网站上有 38 万名客户的信用卡记录被黑客在其网站和移动应用上注入恶意代码，导致 38 万名客户的信用卡记录被盗取。这次攻击导致了欧洲历史上最大的数据泄露罚款--约 2.3 亿美元--这要归功于当时新出台的 GDPR 法规。（来源：cnBeta）

➢ 浙江一高校学生窃取出卖国家秘密，被判刑 5 年 6 个月！

2020 年 4 月 23 日共青团中央报道，近年来，境外间谍情报机关在网络上以求职招聘、学术研究、商务合作、交友婚恋等各种名义为掩护，巧言令色，欺骗、勾联我社会人员甚至在校学生窃取、出卖国家秘密。

2019 年 3 月，在校大学生庄宇在“舟山全职兼职普工”QQ 群中寻找兼职。一位成员主动申请添加庄为 QQ 好友，并向其提供“某军港附近地图信息采集和沿街商铺拍摄”的兼职工作，要求“每天工作 3 小时，一周工作 3 天，日工资 200 元”。

庄宇按对方要求，将个人简历、定位信息和微信收款码通过 QQ 发送给对方，先后 8 次应对方要求前往小区楼顶制高点、公园及医院附近，拍摄我国事目标及附近街道店铺、路况等，每次拍摄 100—200 张照片，通过邮箱发送给对方。庄宇还应境外间谍情报人员要求，通过网上购买长焦镜头观测及租船出海抵近观察等方式，先后 10 次赴我某海军舰队实施预警观察搜集。在此期间，境外间谍情报机关还对庄宇进行了安全培训，要求以“观察记录为主、拍照为辅”的方式搜报军舰舷号。

2019 年 12 月，舟山市中级人民法院以为境外非法提供国家秘密罪判处庄宇有期徒刑 5 年 6 个月，剥夺政治权利 1 年。

大家在发现国家秘密泄露时该如何做呢？公民在日常工作生活中应提高警惕注意发现，哪些危害国家安全的活动？具体如下：

- 一些可疑人员未经批准到内部作调查，进行科技、经济、企业等情况搜集。发现这种情况不能随意提供，并向当地公安机关或国家安全机关报告。
- 警惕境外电台、电视、网络等传媒的煽动、造谣。
- 一些境外组织和人员经常出现在我国事、保密单位周边，乘机盗取秘密情报和信息。如遇有可疑人员要立即报告。
- 一些有境外背景的组织和个人，利用一些群众不满情绪，煽动与政府对抗。遇到这些情况，应立即报告。

发现国家秘密已经或可能泄露时，我们应当采取哪些措施？具体如下：

- 拾获属于国家秘密的文件、资料和其他物品，应当及时送交有关机关、单位或保密工作部门。
- 发现有人买卖属于国家秘密的文件、资料和其他物品，应当及时报告保密工作部门或者国家安全机关、公安机关处理。
- 发现有人盗窃、抢夺属于国家秘密的文件、资料和其他物品，有权制止，并应当立即报告。
- 发现泄露或可能泄露国家秘密的线索，应当及时向国家安全机关举报。

任何组织和个人发现危害国家安全的情况和线索，均应及时向国家安全机关、公安机关举报。（来源：共青团中央）

➢ 美 CDC/世卫组织等机构的近 2.5 万电子邮件地址和密码遭泄露

2020 年 4 月 23 日，据外媒报道，在当局处理像 COVID-19 这种威胁生命的疾病时，最糟糕的事情之一就是安全漏洞。而现在这样的事情已经发生，因为不明身份人士公布了近 25000 个电子邮件地址和密码，这些电子邮件地址和密码来自不同的组织，包括美国疾病控制与预防中心(CDC)、盖茨基金会、美国国立卫生研究院（NIH）、世界卫生组织（WHO）和世界银行。

目前还不清楚这些机构遭黑客入侵的时间，也不清楚谁对入侵事件和信息的传播负责，但结果还是令人担忧。其中一些密码仍然可以被用来访问电子邮件地址。监视网上极端主义和恐怖组织的 SITE 情报组告诉《华盛顿邮报》，这些电子邮件的登录信息在周日被共享。到了周一，这些邮件已经被极右极端分子用来进行黑客攻击和骚扰。

"新纳粹分子和白人至上主义者利用这些名单，在他们的活动场所中积极发布这些名单，"SITE 的执行董事 Rita Katz 说。"极右极端分子利用这些数据，在分享新冠病毒大流行的阴谋论的同时，还呼吁开展骚扰运动。这些所谓的电子邮件凭证的分发只是整个极右分子长达数月的行动的另一个部分，目的是将 COVID-19 大流行病武器化。"

这些信息最初出现在 4chan 上，然后被转移到 Pastebin 上，然后又出现在 Twitter 和 Telegram 上的极右极端主义账户上。最大的一批电子邮件地址属于 NIH（9938 个），其次是 CDC（6857 个）、世界银行（5120 个）和 WHO（2732 个）。

澳大利亚网络安全专家 Robert Potter 表示，一些 WHO 的电子邮件地址和密码组合是真实的。"他们的密码安全性令人震惊，"Potter 说，关于泄露的 WHO 凭证，他说。"有 48 人用'密码'作为他们的密码。其他人用的是自己的名字或 ‘changeme’。” Potter 表示，世卫组织的信息来自于 2016 年的一次黑客攻击。目前还不清楚其他凭证的来源，也不清楚是谁能够获得这些凭证。其中一些可能是从暗网购买的。

新纳粹组织一直在利用这些信息传播和助长 COVID-19 的阴谋论。有一个团体说，这些邮件地址的数据 "证实了 SARS-COV-2 实际上是人工合成的病毒"，这也是目前流传的新冠病毒阴谋论之一。世卫组织最近表示，这种新型冠状病毒是动物源性的，没有任何迹象表明 COVID-19 病毒是在实验室里合成的。（来源：互联网综合整理）

➢ 山东胶州 3 人泄露 6000 余人医院就诊信息，被行政拘留

2020 年 4 月 19 日，青岛市胶州中心医院因出现当地居民在医院就诊期间感染新冠肺炎而备受关注，一份出入这家医院的人员名单在微信群里被广泛转发有多名网友在青岛胶州政务网咨询“微信群朋友圈流传一份胶州市接触中心医院人员名单，姓名电话住址身份证号都很详细，然后就骚扰电话诈骗电话不断……”。青岛市公安部门 19 日通报，泄漏信息的 3 人被拘留。

此前，胶州市公安局在线答复称：针对该市民提出的泄露信息源头问题，我局正在侦办中，坚决打击泄露个人信息行为。

警方通报如下：

4 月 13 日，胶州市民的微信群里出现中心医院出入人员名单信息，内容涉及 6000 余人的姓名、住址、联系方式、身份证号码等个人身份信息，造成了不良社会影响。胶州市公安局发现后迅速展开调查。经查：叶某(男，29 岁，胶州市李哥庄镇人)工作中将接到的随访人员名单信息转发至所在公司微信群，该群内的姜某(男，24 岁，胶州市李哥庄镇人)将名单信息转发至家人群，其家人又继续转发传播。张某(女，57 岁，胶州市里岔镇人)工作中将接到的随访人员名单信息转发至家人微信群，其家人又继续转发传播。以上 3 人的行为，造成中

心医院出入人员名单在社会上被迅速转发传播，侵犯了公民的个人隐私。依据《治安管理处罚法》的相关规定，公安机关依法对叶某、姜某、张某给予行政拘留的处罚。

警方提醒：公安机关提醒各社会单位和个人在做好疫情防控工作的同时，要采取有效措施加强对公民个人信息安全的保护，防止公民个人信息泄露，损害群众合法权益，造成不良社会影响。对于泄露秘密信息特别是个人隐私的行为，公安机关将依法予以严厉打击。（来源：青岛日报）

➢ 百度网盘道歉：默认用户加入“激励计划”占带宽

2020 年 4 月 19 日，有网友发现百度网盘会默认开启“用户激励计划”，会占用上传带宽和本地存储空间而引发争议。2020 年 4 月 20 日晚间百度网盘官方昨日晚公开道歉，并对客户端做了紧急更新。

百度网盘回应：

近期，百度网盘在 PC 端上线测试的“用户激励计划”收到了很多网友的反馈，感谢每一位用户的批评和建议，这对我们持续优化百度网盘的用户体验非常重要。首先，对于百度网盘默认 PC 端用户加入用户激励计划，我们深表歉意，并紧急开发了新的版本。明天(4 月

21 号)发布的百度网盘 PC 端新版本，将对“用户激励计划”的全部用户做取消处理。同时，也请大家放心，用户激励计划使用的是点对点(P2P)传输技术，可以改善用户在线观看视频的体验和移动端下载速度。P2P 传输技术已非常成熟并广泛采用，安全性完全有保障。最后，对于百度网盘给大家带来的困扰再次说声对不起，也请大家继续监督百度网盘，我们将继续努力，为大家提供值得信赖的网盘服务。

据悉，在之前的百度网盘 Windows PC 版的客户端中，有一个“用户激励计划”的选项，号称可提升 PC 用户体验，并根据用户的活跃度和使用情况，奖励相应的积分，可兑换不同奖品。如果每日持续贡献 1MB/s 带宽、5G 空间、7 小时在线时长，预计每月可获得 1000 积分(1000 积分可兑换爱奇艺 VIP 月卡等奖品)。

然而，有用户抱怨称被默认加入该计划，其默认操作有偷偷使用用户宽带的嫌疑。有网友直言：“用 P2P 没啥事，但问题是没让我们进行选择，直接默认开启。”此外，该默认选项在 PC 端隐藏得太深，也因此导致不少用户不满。

但更有问题的是，百度并未明确告知这会占用最高 1MB/s 的上传带宽，用于给其他用户传输文件，同时还会占用最多 5GB 的本地空间，而且是默认开启的，也不会给用户下载带来任何提速效果。

百度网盘官方表示，对此深表歉意，并紧急开发了新的版本，将对“用户激励计划”的全部用户做取消处理。据最新版本 Windows v6.9.3.1 显示，更新日志中称“修复了一些体验问题，提升稳定性”，实测发现用户激励计划选项依然存在，但默认已经关闭。

还没更新百度网盘的建议去更新吧!对于不方便更新的用户，可点击设置—传输—高级设置，将“用户激励计划”关闭即可。（来源：互联网综合整理）

➢ 两名工程师泄露 5G 核心技术文档 被判刑

2020 年 4 月 24 日报道，2002 年至 2017 年 1 月，黄某瑜就职于中兴通讯公司，担任过射频工程师、无线架构师等职务。2008 年 4 月至 2016 年 10 月，王某就职于中兴通讯公司西安研究所，担任过 RRU 部门研发工程师等职务。2014 年，黄某瑜接受了某研究所 5G 有源天线原型机的技术外包项目。

黄某瑜将项目挂靠在深圳森博兴业科技有限公司，与上述研究所先后签订了 4 份合同，合同总金额为 235 万元。黄某瑜将该项目交给王某负责技术落地，研发完成后按合同

约定，分阶段向研究所交付了一台 5G 有源天线原型机和相关技术文档，并在 2015 年到 2017 年期间，分 5 次收取了 235 万元。经鉴定，王某交付和发送的技术文档，与中兴通讯公司的文档具有同一性。

经鉴定，这些文档属于不为公众所知悉的技术信息。中兴通讯公司制定了多个保密制度，与员工签订《保密协议》《信息安全承诺书》，并对这些技术信息采取了保密措施。这些信息的评估值为人民币 430 万元。

2019 年 6 月，深圳市南山区检察院以黄某瑜、王某涉嫌侵犯商业秘密罪向法院提起公诉。同年 12 月，深圳市南山区法院判决被告人黄某瑜、王某构成侵犯商业秘密罪，均被判处有期徒刑三年，缓刑四年，并处罚金人民币 15 万元。两被告人认罪认罚，均未上诉。

检察官介绍，案件办理过程中，检察机关了解到黄某瑜在中兴通讯公司工作 10 余年，系公司通讯技术领域的专家级人才，其在 2016 年离职，创立深圳希某某田公司进行无人机图像传输技术自主研发，公司拥有多个发明专利，属于国家级高新技术企业。因涉本案导致公司经营困难。

中兴公司反馈，黄某瑜在工作期间为公司作出了很大贡献，离职创业后没有使用到中兴公司的技术，只要黄某瑜认罪悔罪并赔偿损失，公司愿意对其谅解。经过释法说理，最终两被告人赔偿了中兴通讯公司损失，并取得谅解。检察机关及时建议侦查机关对两名被告人改变强制措施，深圳希某某田公司得以继续经营，有效避免了“案件办了，企业垮了”。该案为国内首宗涉 5G 技术侵犯知识产权犯罪案。（来源：澎湃新闻）

信息安全意识产品服务

021-33663299