# 新形势下移动终端安全需求和对策

## Security Requirements and Solution of Mobile Terminal under the New Situation

李兴新，郭晓花，侯玉华，陈礼波，旷　炜，齐　霄（中讯邮电咨询设计院有限公司，北京 100048）
Li Xingxin，Guo Xiaohua，Hou Yuhua，Chen Libo，Kuang Wei，Qi Xiao（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

**摘　要：**
在泛终端时代背景下，公众市场、政务安全市场及自身行业层面的终端安全形势更加复杂。国家倡导网络强国和技术创新积极应对移动终端行业安全问题，终端及安全企业立足核心关键技术，从基于应用的被动式信息安全防护、基于网络和大数据能力的预警式安全防护，逐步探索构建端云协同主动防御的安全防护体系，建设安全可信的移动网络空间。

**关键词：**
安全威胁；终端生态；防护；端云协同主动防御
**doi：**10.12045/j.issn.1007-3043.2021.06.017
**文章编号：**1007-3043（2021）06-0088-05
**中图分类号：**TN929.5
**文献标识码：**A
**开放科学（资源服务）标识码（OSID）：**

**Abstract：**
In the era of pan-terminal，the terminal security situation of public market，government security market and its own industry is more complex. The government advocates the network power strategy and technological innovation to actively respond the security needs of mobile terminal industry. Based on the core key technologies，terminal and security enterprises gradually explore and build a security protection system based on terminal and cloud coordination from application-based passive information security protection and early warning security protection based on network and big data capabilities. The final goal is to build a secure and trusted mobile cyberspace.

**Keywords：**
Security threats；Terminal ecology；Protection；Active defense of device and cloud collaborative

**引用格式：**李兴新，郭晓花，侯玉华，等. 新形势下移动终端安全需求和对策[J]. 邮电设计技术，2021（6）：88-92.

## 0 引言

伴随5G网络应用的普及和物联网的发展，移动智能终端从最初的以智能手机为主，逐渐向形态多样化、跨终端生态化的新阶段演进。

当前，世界政治经济形势正在发生深刻复杂的变化，从单纯的技术竞争变成国际政治经济斗争，信息安全也不再是单纯的个人问题，成为国家网络空间安全的重要组成部分，不仅仅关系到应用安全和行业安全，更成为国家战略安全的关键环节[1]。

收稿日期：2021-05-27

本文从终端生态所面临的相关安全挑战入手，论证了终端产业的安全需求和安全对策，并给出了安全建议。

## 1 移动终端发展新阶段

### 1.1 市场规模进一步扩张

伴随着设备广连接和终端智能化发展，智能手机渗透率进一步稳步提升，移动终端的形态向多样化、智能化的泛终端演进，市场规模大规模扩张。

整体上看，快速扩张的移动终端市场呈现以下几个显著特征[2]。

a）终端硬件性能大幅提升。终端芯片依旧遵循

着摩尔定论快速迭代发展，尤其是移动终端领域发展更为迅猛，且同时伴随着硬件成本下降，同价位终端设备中配置了更高性能的硬件，为提供更丰富的功能和性能做好准备。

b）终端操作系统发展迅猛。以iOS和Android为代表的智能手机操作系统继续高速迭代，同时面向物联网设备的轻型、实时操作系统走向前台，促进移动设备快速进入智能时代。

c）终端形态多样，类型丰富。在5G技术推动下，智能手机、智能机器人、智慧大屏设备、智能可穿戴设备、智能家居、智能医疗、智能车载智能终端等智能硬件蓬勃发展，智能终端产业链和市场规模同步放大，形成以智能手机为代表的泛智能终端体系。

d）终端数据规模急剧扩大。形态多样的智能终端是大数据的重要输入输出口。2020年中国连接设备的数量已超过80亿台，物联网市场产生数据已接近40 ZB，终端产生的收入和数据量呈现惊人的增长。中国物联网连接量与增速如图1所示[3]。

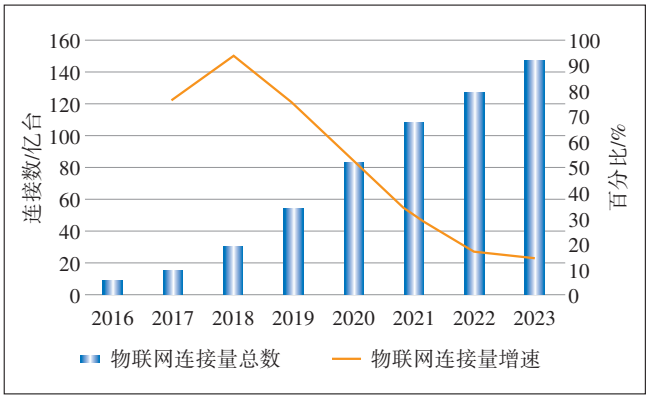


图1　中国物联网连接量和增速

## 1.2 移动终端生态构建

随着5G网络和商业模式的进一步成熟，移动终端从满足个人移动应用需求转向生态构建层面，业内厂商整合资源构建了智能家居、智能医疗、工业互联网、车联网等行业生态，推动移动终端进入一个崭新的发展阶段。在生态体系中，操作系统起到核心主导作用。鸿蒙产品发布中就描绘了分布式能力打造新硬件、新交互的全场景世界[4]，谷歌也紧急更新了其Fuchsia产品状态，可视作对鸿蒙的直接应对和正面竞争。

以智能手机领域的终端生态构建为例，华为基于鸿蒙全场景的、分布式优势，以鸿蒙操作系统为中心，构建了覆盖手机、电脑，以及更加丰富的物联网（IoT）设备的华为全场景生态。基于华为麒麟、鲲鹏、凌霄和鸿鹄等系列芯片，以鸿蒙系统叠加华为云服务能力，实现芯片到系统、到云端的统一。

小米生态链覆盖了从可穿戴设备（如智能手环）、家用机器人、智能家居、出行机器人到手机配件、VR、车载硬件等各类别智能硬件，整合了家庭场景、个人场景、AIoT智能生活场景，以智能手机、OTT大屏为主体构建了设备互联的智能生活全场景生态[5]。

面向生态构建的移动终端发展模式，可以向用户提供更良好的交互体验，还将进一步推动产业向集群化、规模化、标准化发展。

## 1.3 国际竞争加剧

2018年以来，中美贸易争端导致全球化趋势发生变局，美国利用其在技术和经济领域的优势，不断抛出所谓“实体清单”，打压中国科技发展，对移动终端产业发展产生极大影响。

移动通信市场是受影响较大行业之一。2018年前，中国手机企业发展迅猛，在全球市场占有率稳步提升。面对美国的直接打压，虽然中国企业迎难而上，积极调整产品布局，仍不可避免的出现波动。如图2所示，2020年华为手机全球市场份额减少2.9%，同比下降21.5%[6]。

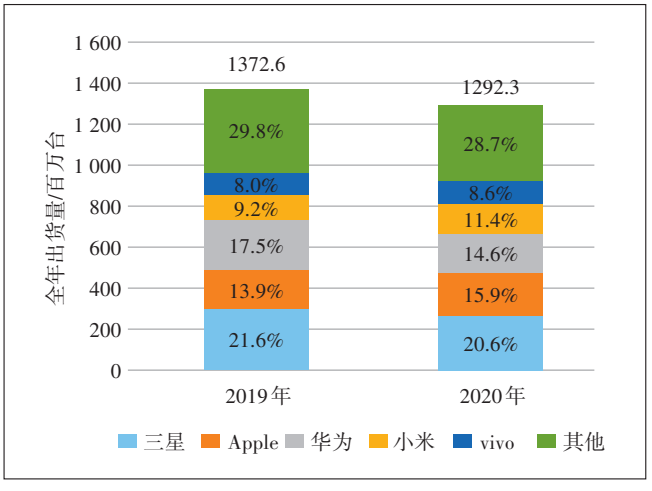


图2　2019—2020全球前五智能手机厂商及市场占有率

在通信领域，中国企业克服重重困难，推动技术和产品继续进步，在通信芯片、AI芯片、通信设备、信息安全等领域都有突出成果。

席卷全球的新冠疫情，也对移动终端领域的产业结构产生深远影响。先进制程的芯片制造成为竞争的焦点，各国纷纷布局并加大在芯片领域的投资和技术支持力度。

## 2 移动终端面临的安全威胁

### 2.1 公众市场

公众市场面临的移动终端安全威胁，排首位的仍旧是骚扰电话、诈骗电话、垃圾短信等通信欺诈行为。移动互联网恶意程序通过智能终端窃听用户通话，窃取用户信息，破坏用户数据，擅自使用付费业务，发送垃圾信息，推送广告或欺诈信息，影响移动终端运行，危害互联网网络安全。

移动互联网恶意程序数量逐年增长，持续侵犯广大移动用户的合法利益，具体如图3所示。

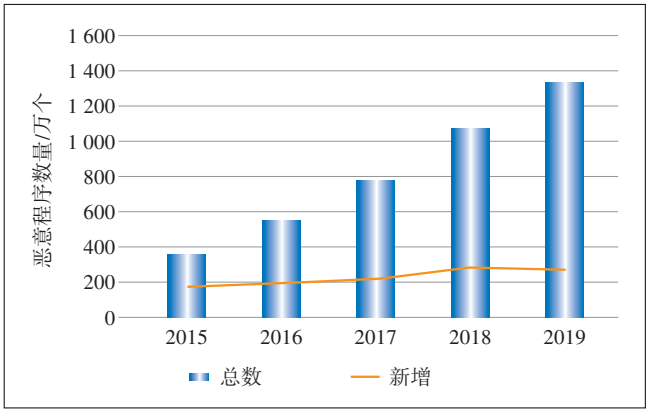


图3　我国移动互联网恶意程序规模趋势

### 2.2 政企安全市场

电子政务加速向数字政府转型是“十四五”期间数字化转型面临的重要任务，其中移动终端是重要载体，且其便利性对数字化转型有着显著的促进作用。其他如金融、能源、交通、公共事业以及工业信息化、电子商务、城市信息化等信息领域，对移动办公都有迫切的需求。相应的，移动办公的数据和业务安全问题是亟待解决的问题。

对政企行业移动应用的安全威胁，首先来自国际上涵盖军事、经济和科技等领域的网络安全博弈。2018年美国发布的《美国国家网络战略》[7]将中国视作网络安全方面的防范对象和竞争对手，国际网络空间长期走向博弈状态[8]。根据“棱镜门”事件暴露的信息，美国利用其互联网和信息技术优势，对各国实施了长期的网络监听和数据窃取，除了国家机密以及政府公务信息外，商业信息、个人信息都在美国监听之列，此类威胁使得涉及国计民生的领域和行业对信息安全需求迫切。

除了外部环境风险，数据泄露、技术漏洞、管理不善等因素也是造成我国网络安全环境形势严峻的重要原因。在显著进步的网络基础设施建设之外，网络信息安全的投入和建设明显滞后，对数据资产的重要性认知不足，存在着数据泄露风险；信息安全产业发展不到位，我国的信息化建设一定程度上还依靠国外技术，技术漏洞风险难以把控；以及工作中对信息安全的操作规程和管理规章执行不到位，社会的信息安全意识相对淡薄等。

### 2.3 终端产业安全

我国移动终端产业的关键器件和技术上仍受制于人，尤其是移动终端中涉及的硬件芯片和终端操作系统等产品对外部供应链依赖度较高。

移动终端的硬件芯片高度依赖苹果、高通、MTK、三星等外部厂商。以5G SoC芯片占有率为例，2020年第4季度中国5G手机芯片市场对外依赖度超过80%。由于华为受到美国制裁，预计这一比例还将继续提高。

在智能手机操作系统市场，2019年iOS和Android市场份额占比合计已超过98%，几乎已完全垄断。

随着国际竞争形势走向政治化，我国整个移动终端产业面临显著的安全威胁，随时可能面临无芯片可用、无操作系统可用的困境。2021年4月，公开的美国国会代表的邮件中显示，考虑将对中国华为的许可禁令范围扩大至设计14 nm以下芯片的所有中国公司。此举将“锁死”中国大陆芯片先进产能扩张，使得终端厂商无法使用先进芯片，整个行业将陷入萎缩或休眠。

## 3 移动终端安全对策

### 3.1 国家战略层面

2018年4月，在全国网络安全和信息化工作会议上，习近平总书记提出了网络强国战略思想[10]，为解决移动终端安全威胁提供了纲领性指导。

建设网络强国是提升国家综合国际竞争力的必由之路，通过网络化和信息化带动现代化和市场化，引领再工业化，重构社会的生产力和生产关系，推动网络安全和信息化事业全面发展。业内预计在国家战略指导下的网络基础设施建设投资规模将突破3 000亿元，极大地推动5G、工业互联网等产业的快速发展，这是奠定我国未来数字经济的“硬件”基础。

网络强国战略要求加强与网络强国相适应的软硬件建设，进一步强调关键基础设施的安全，倡导推

进网络关键技术自主创新和关键设备国产化，着力实现关键技术自主可控，为维护国家安全、网络安全提供技术保障。在移动终端领域，推动实现在芯片技术、操作系统以及CPU等关键技术领域实现大的突破，以技术创新应对和解决移动终端的产业安全问题。

### 3.2 技术创新驱动产业发展

党的十九大以来，党中央全面分析国际科技创新竞争态势，深入研判国内外发展形势，针对我国科技事业面临的突出问题和挑战，坚持把科技自立自强作为国家发展的战略支撑，坚持把科技创新摆在国家发展全局的核心位置，全面谋划科技创新工作，牢牢把握建设世界科技强国的战略目标，充分发挥科技创新的引领作用，努力在原始创新上取得新突破，在重要科技领域实现跨越发展，推动关键核心技术自主可控，加强创新链产业链融合，加快建设科技强国，实现高水平科技自立自强。

在通信行业，我国从2G时代的一无所有、3G时代初登舞台、4G时代并跑，5G时代已经成为领跑者，这一步步发展与多年来持续加强核心技术研发密不可分。掌握核心技术是保障国家安全和终端产业安全的关键。

移动终端产业在芯片、操作系统、信息安全技术等方面的技术短板，必须且只能依靠核心技术的自主创新来解决。一方面业内厂商依托国家顶层设计和政策支持，整合优势资源，探索合作机制，持续迭代产品以适应不断发展的技术和使用需求，提升行业自主创新能力；另一方面，国家积极推动自主的芯片和操作系统等核心技术产品在重点领域的产业化应用。技术研发和产业应用互相促进，共同培育技术生态和应用生态，打造自主可控的移动终端产业链体系。

进一步的，还应鼓励和加强对终端安全架构的研究。建立主动防御的移动终端安全体系，结合自主芯片、自主操作系统等核心技术，共同构成我国独有的自主安全优势，保障重点领域、重点行业的安全，以全面的技术创新驱动移动终端信息安全产业的发展。

### 3.3 终端个人信息安全防护

经历多年的安全技术演进，围绕智能手机的终端个人信息安全解决方案已经逐步趋于完善。

针对骚扰电话、诈骗电话、垃圾短信等通信欺诈行为，工信部协调组织运营商和多个政府部门，已形成了通信技术层面预警与行政管理层面封堵相结合的联防联控机制，2020年通信欺诈数量已呈下降趋势，反欺诈工作已取得初步成效，相关安全形势回缓。

运营商积极履行反欺诈的职责，整合并利用自有通信资源和能力，基于网络数据，通过诈骗网址识别、APP应用分析与识别、黑灰产框架特征萃取等分析研判能力，面向互联网诈骗、电话和短信诈骗等全业务场景，为人民群众提供识别预警和全网封堵服务，有效解决电信诈骗等社会性难题。运营商反欺诈系统的框架如图4所示。

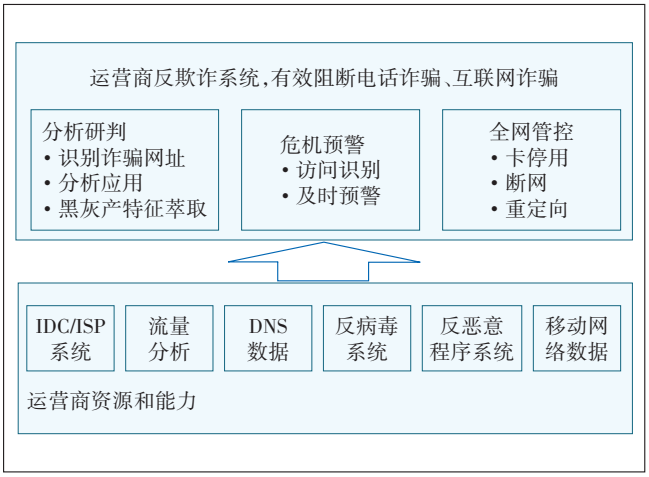


**图4**　运营商反欺诈系统框架

针对木马、病毒等移动互联网程序，通信和互联网厂商已推出多款功能全面的手机管家类安全应用，实现病毒查杀、漏洞扫描、自启动管理等功能，并支持系统优化、数据清理等辅助功能，基本可满足普通用户对个人信息安全防护的需求。

个人信息安全防护应是技术手段与个人安全意识的结合，在部署网络安全防护、终端安全管理的同时，还应提高个人防范意识，提高个人安全能力水平。

### 3.4 构建端云协同的主动防御安全防护体系

现有面向公众的终端安全防护手段，无法满足政企等涉及民生和国家安全等领域的安全需求。加强主动安全防护体系研究和建设，通过“端”与“云”有效协同，建立统一的整体加密与安全防护体系，达到主动防御的高阶安全能力保障，积极响应和对抗不断衍生的未知性风险。

端云协同主动防御的安全防护体系涵盖移动终端使用过程中的各个环节。终端侧建立硬件层、操作系统层、应用层等多个层面的安全防护，云端围绕云安全和平台安全部署数据和业务的安全服务，端云协

同达到端到端加密、数据安全存储、远程安全管控、应用系统安全保障等防护。图5是端云协同防护体系示意图。

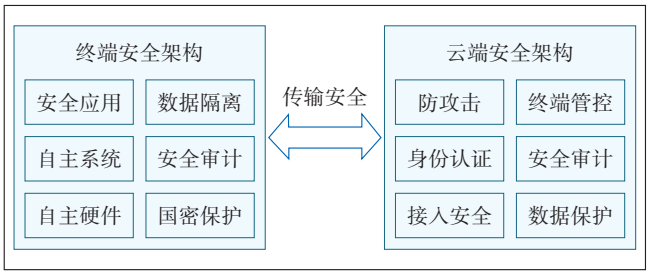


**图5**　端云协同整体加密的安全防护体系示意图

整体安全防护体系，包含以自主硬件和自主操作系统为基座的移动终端，叠加基于国密技术的加密和隔离机制，整合利用云端资源及能力，建立打通端侧、平台侧的安全的全业务流程。

终端侧致力于打造对应用和数据的可信执行环境TEE，以终端架构性安全设计实现端侧全方位防护。终端防护贯穿了硬件平台、智能终端操作系统和安全应用的设备架构，并通过应用国密加密芯片对数据在存储和传输过程中的加密保护提供加固防护，通过对数据生成、使用和传输各环节的隔离和审计保障数据安全，并部署使用硬件级加密保护机制、安全启动和防刷机保护机制等。

网络侧安全能力包括针对设备的网络接入提供身份认证和接入安全管理，针对终端业务连接和交互提供加解密、云数据保护、业务安全审计，针对专用移动终端的设备管控等，集中打造云端的安全能力平台。

针对安全传输需求，运营商的5G安全专网可构筑统一开放的网络安全能力，为垂直行业客户提供各类安全服务：通过对网络中的密码算法、5G认证协议和安全知识库等安全资源的抽象和封装，为加密传输业务提供认证服务、信用服务、入侵检测等，使其高效安全地实现信息安全服务；通过开放安全资源池，以网络切片技术和边缘计算为基础，引入全新的AI、大数据分析、主动防御等技术，实现对垂直行业网络的深层次安全加固。支持按需定制的5G网络，进一步提升了运营商移动安全服务能力。

运营商基于端云协同、主动防御的设计理念，以自有的通信业务为载体，面向政企行业推出了安全通信业务，并以此为基础形成移动安全OA、视频会议、终端管控等一系列安全办公应用，融合安全终端和安全云端资源，逐步形成了针对移动办公行业需求的端云协同安全体系。

## 4　结束语

移动终端行业从面向个人的智能手机发展到面向政企行业的业务终端，并呈现生态化发展趋势，其安全影响到信息、行业甚至国家安全。因此，持续研究移动终端的安全威胁问题并探索行之有效的解决方法，营造安全的移动互联网环境，助力安全可信的网络空间建设是每个中国企业的使命和责任。业内厂商应以自主芯片平台、自主操作系统、国密算法等自主技术为基础、基于端云协同主动防御的安全设计理念、建立复杂网络下的主动防御体系，建立可信认证的网络信任体系，并融合5G网络技术和5G行业应用，建立产业安全标准体系，形成移动信息安全领域核心技术和安全产品解决方案。

**参考文献：**

[1] 李剑，杨军. 网络空间安全导论[M]. 北京：机械工业出版社，2021.
[2] 黄伟. 智能终端产业发展特点及趋势研究[J]. 信息通信技术，2014(2)：19-25.
[3] 智研咨询. 2020-2026年中国物联网行业市场现状调研及市场发展前景报告：R795326[R]. 深圳：智研咨询集团，2019.
[4] 鸿蒙官网. 鸿蒙介绍[EB/OL]. [2021-03-03]. https://www.harmonyos.com/cn/home/.
[5] 小米官网. 产品介绍[EB/OL]. [2021-03-03]. https://www.mi.com/.
[6] 国际数据公司(IDC). 2020年全球手机市场份额报告[EB/OL]. [2021-03-15]. https://www.sohu.com/a/447256652_100288184.
[7] 唐纳德·特朗普. 美国国家网络战略[EB/OL]. [2021-03-12]. https://www.sohu.com/a/255504169_468736.
[8] 神州数码信息安全. 解读特朗普《国家网络战略》[EB/OL]. [2021-03-12]. https://www.sohu.com/a/258562333_464012.
[9] 国际数据公司(IDC). 2020年手机季度跟踪报告[EB/OL]. [2021-02-20]. https://xueqiu.com/4917815737/167886646.
[10] 习近平. 习近平出席全国网络安全和信息化工作会议并发表重要讲话[EB/OL]. [2021-03-22]. http://www.gov.cn/xinwen/2018-04/21/content_5284783.htm.

**作者简介：**
李兴新，工程师，硕士，主要从事移动终端信息安全、终端操作系统相关研究工作；郭晓花，工程师，硕士，主要从事移动终端信息安全相关研究工作；侯玉华，硕士，高级工程师，主要研究方向为移动信息安全、终端操作系统；陈礼波，高级工程师，硕士，主要从事政企创新业务规划、光通信网络规划咨询设计工作；旷炜，工程师，硕士，主要从事安全平台相关研究工作；齐霄，工程师，硕士，主要从事移动安全相关研究工作。