DOI:10.3969/j.issn.1009-6868.2016.01.002
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20151117.1506.006.html

网络空间安全面临的挑战及应对策略

Challenges and Countermeasures of Network Space Security

周延森/ZHOU Yansen
周琳娜/ZHOU Linna
(国际关系学院 信息科技学院,北京 100091)
(Department of Information Science and Technology, University of International Relations, Beijing 100091, China)

中图分类号:TP393.4 文献标志码:A 文章编号:1009-6868 (2016) 01-0005-005

摘要: 当前网络空间安全威胁包括:大规模分布式拒绝服务攻击,众多主机被境外结构控制,关键信息存储在非本国品牌服务器中,用户借助翻墙软件逃过监控等。提出了应对网络空间威胁的措施——自主可控与互联网应用创新,具体包括自主研发CPU和路由器等核心硬件以及操作系统和数据库等系统软件。认为下一代信息技术从内容的深度和广度挑战现存的网络空间,形成了新的安全威胁,这需要国家加快下一代网络的部署及研发。

关键词: 网络空间;空间主权;大数据;物联网;云计算

Abstract: The main security threats of network space include large scale distributed denial of service attack denial of service attacks; many hosts controlled by foreign institutions; key information stored in many foreign brand servers; and users with special software who can escape monitoring. The main measures to deal with space threats are self controlled and Internet application innovation, including 1) independent research and development of core hardware including CPU and router and 2) system software including operating systems and databases. The next generation of information technology from the depth and breadth of content challenges the existing network cyber, which forms a new security threat. This requires China to speed up the research and deployment of the next generation network.

Key words: network space; spatial sovereignty; big data; Internet of things; cloud computing

随着互联网应用不断深入,网络空间逐渐被视为继陆、海、空、天之后的"第5空间",成为世界关注的焦点和热点。网络在方便和丰富人们生活的同时,也使得网络攻击行为广泛存在。互联网的应用已深入到社会的方方面面,小到百姓的日常生活,例如网上购物和网络金融,大到涉及国计民生的行业,例如国家电网等。西方国家已将网络空间安全提升到国家战略高度予以重视,中国政府也非常重视网络空间安全。国家教育部最近将网络空间安全专业列为一级学科,这说明教育部门正在为国家网络空间安全提供强大可持续的人才储备。

从国家层面上看,为了适应网络安全空间面临的严重挑战和维护国家的网络主权安全,2014年中央网络安全和信息化领导小组正式成立,这为网络空间安全提供了强大的组织保证。习近平总书记说:"没有网络空间安全就没有国家安全"。这充分说明党和国家领导人高度重视网络空间安全,把网络空间安全提升到国家主权安全的高度[1]。

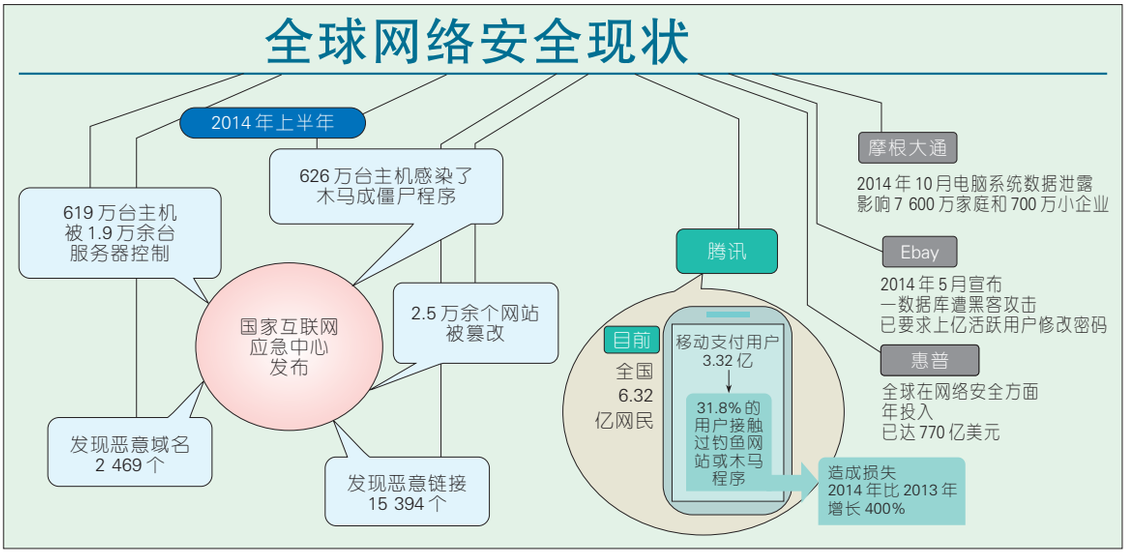
网络空间不是一个抽象虚拟的概念,而是实实在在存在于我们的生活当中。从物理结构上分析,网络空间主要由通信基础实施、部署在网络外围的计算机、移动智能终端以及各种提供共享资源的服务器等组成。此外,各种互联网应用和提供的服务都是网络空间重要的组成部分。

当前,中国网络空间安全形势非常严峻。图1列出了2014年上半年中国网络空间安全现状的一些数据[2]。

1 网络空间安全面临的挑战

随着信息技术的迅猛发展和互联网的普及,特别是以微信、Facebook和LINE为代表的新一代即时通信软件的推广和普及应用,使得信息传播的速度、广度和实时性都达到史无前例。互联网应用正在深入到国家与社会的各个方面,同时也伴随着大量的不良信息以及恶意的网络行为,如计算机木马、拒绝服务攻击、垃圾邮件、恐怖主义视频以及泄露的党和国家机密信息等。网络不良信息和网络恶意行为不仅会造成重大的经济损失,而且会严重威胁国家的政治、经济、国防、文化等正常秩序,干扰人民群众的正常生活,甚至会因为恶意散发的网络谣言会引发国家与社会

收稿日期:2015-11-15
网络出版时间:2015-11-17
基金项目:自然科学基金(61170175)



◀图1
网络空间安全现状

动荡。由此可见，网络空间安全在国家主权安全中的地位和作用也越来越大[3]。

互联网已经成为党政机关和企事业单位获取信息的重要来源，来自于互联网的海量数据正成为各行各业做出正确决策的重要依据。因此在下一代网络空间中，针对海量数据基于数据挖掘算法和大数据处理技术以及云计算技术进行深度及时分析处理，是任何国家政府和企事业单位必须解决的关键问题。对大数据获取与智能处理是决定国家和社会发展的一个关键问题，是走出“有数据但无知识”困难局面的一个重要的突破口[4]。

（1）大规模分布式拒绝服务攻击

下一代网络IPv6只在网络层进行了深层次的改变[5]，传输层和应用层没有改变。因此，基于传输层的分布式拒绝服务攻击还会存在。据相关结构报告：中国大型的电子商务网站和提供搜索引擎服务的网站屡次遭到大规模的拒绝服务攻击（DDOS），例如天猫和京东等电网站都曾遭受过此类攻击，给网站的卖家带来巨大的经济损失；百度网站在过去几年也遭受此类攻击，由此导致众多用户无法使用搜索服务。

（2）众多主机和服务器受控制

中国众多的政府机关、企事业单位以及个人的服务器和主机遭到境外机构的控制。据国家互联网应急中心发布的数据显示：2014年，中国有650多万台主机因感染了木马病毒而被境外服务器控制，2万多个网站被篡改主页。这些被恶意控制的服务器和主机不仅泄漏了国家机密和私人隐私，而且成为境外机构发动分布式决绝服务攻击的帮凶[6]。

从这些攻击的源头上分析，我们发现大部分参与实际攻击的是这些被控主机，而实际上真正发起攻击的源头在其他一些国家。

（3）翻墙软件挑战信息监控

中国非常重视互联网内容的监管工作[7]，在国家多个关键的互联网接口处都有网络监控设施。但是，随着互联网翻墙软件的轻易获取，只要稍微懂得互联网技术的用户，就可以通过在计算机和手机上安装此类软件，突破网络监控，随意访问一些严禁访问的网站。例如，法轮功组织开发的无界限翻墙软件，能够在本地机器实现代理服务器的功能，通过该代理可避开监管，访问到大智慧等非法网站。另外，通过浏览器设置代理服务器的连接方式，能够完成网络攻击源IP地址的隐藏。因为在被攻击服务器的日志中总是留下代理服务器IP地址作为网络攻击行为源IP地址，除非各个国家政府之间进行互联网安全的协作，否则这种攻击行为难易完成源头的定位。

（4）骨干网的高速交换机和路由器受控制

在互联网技术方面，美国遥遥领先于其他国家[8]，特别是在骨干网的基础通信设施方面。目前，中国骨干网的大部分通信设备主要由美国思科等公司提供。路由器配有独立IP地址，路由器人为设置的漏洞等，均会导致这些生产路由器的公司远程控制这些路由器。这些公司完全可以做到通过远程切断中国网络的通信服务。

（5）网络空间海量数据处理面临挑战

互联网空间中的大数据包含结构化和非结构化两种类型[9]。据互联网相关结构调查发现：在网络海量数据中，约20%的数据是结构化的，约80%是非结构化或半结构化的，并且非结构化信息增长率是结构化信息增长率的两倍。对非结构化数据的处理需要大数据处理核心技术，而目前这些技术掌握在西方国家手中。海量数据用现行的检测过滤技术无法做到实时检测，因此很多入侵者就可以利用这个漏洞进行浑水摸鱼式

的系列攻击。

目前网络上的加密软件体现出加密算法强度大、密码长度超长的特征，暴力破解面临严重挑战。

（6）基础设施面临瘫痪

随着社会重要基础设施的高度信息化，社会的“命脉”和核心控制系统有可能面临损坏和瘫痪。这主要有两点原因：

• 关乎国计民生的海量数据存储在非本国品牌的数据库服务器中。数据库系统软件主要有微软的SQL Server、甲骨文的ORACLE以及IBM的DB2以及SYBACE。目前，中国的主要银行、铁路、民航、社保和其他关乎国计民生的行业都离不开上述的数据库系统的支持。由于这些软件都不是开源的，因此我们对其存在的安全漏洞无从所知。这些数据库系统软件公司可以配合所在国政府轻易地删除或修改中国的核心数据，而这些数据的丢失则会引起社会的恐慌，从而达到“不战而屈人之兵”的效果。

• 涉及国计民生的大型服务器都是西方国家的品牌。美国的IBM、惠普等公司占据中国大型服务器80%以上的市场，目前涉及的主要行业为金融、交通和电力等。这些服务器具有强大的计算能力，每天都在为政府机关和企事业单位以及个人提供各种各样的金融和电子商务等日常服务。如果这些服务器受到远程控制的话，可以随时被切断服务。这将会导致整个社会的混乱。

（7）根域名服务器受控制

根服务器主要用来管理互联网的主目录。所有的根服务器均由美国政府授权的互联网域名与号码分配机构——ICANN统一管理。ICANN还负责全球互联网域名根服务器、域名体系和IP地址等的管理。

这些逻辑根服务器可以指挥Internet Explorer这样的Web浏览器和电子邮件程序控制互联网通信。自互联网成立以来，世界对根域名服务器的依赖性非常大，美国通过控制根服务器而控制了整个互联网。从理论上说，任何形式的标准域名要想被解析，按照技术流程，都必须经过全球“层级式”域名解析体系的工作，才能完成。层级式域名解析体系第1层就是根服务器，它负责管理世界各国的域名信息；在根服务器下面是顶级域名服务器，即相关国家域名管理机构的数据库，如中国的CNNIC。美国可以通过其控制的根域名服务器，随时切断中国对外的互联网服务。

（8）计算机和智能手机的核心部件受控制

CPU是计算机和智能手机的核心部件和主要计算单元。在PC端，CPU主要有Intel和AMD两大品牌；智能手机所使用的CPU都由高通公司提供。如果在这些CPU上植入木马，现存的任何检测软件都无法检测到此类硬件木马和病毒，并且它们可根据需要随时引发病毒，造成计算机系统停止工作。

操作系统是软件之母，所有其他软件的运行必须依附在操作系统正常工作的基础上。在PC端，目前主要品牌有Windows操作系统；手机操作系统主有IOS和Android。此外，现有的信息安全软件无法检测到存在于CPU之上的硬件木马，也无法检测到存在于操作系统核心模块的软件木马，但其他国家研制这些软硬件的公司可以轻易远程控制这些木马。

2 网络空间安全挑战的应对策略

针对上述网络空间安全的一系列挑战，我们提出了应对策略——自主可控与创新。具体包括以下几个方面。

（1）自主研制CPU

到目前为止，世界上90%以上的CPU芯片都由美国的Intel、AMD和高通公司控制。为了摆脱这方面的被动局面，中国现有的研发与生产CPU的公司需要进行整合，争取在未来5年设计出1～2款具有国际竞争力的CPU，特别要为军队和党政机关研发自主可控的CPU。中国应该在未来十年，投入更多的资金加强这方面的研究和设计，以摆脱有机无芯的被动局面。

（2）自主研发操作系统

操作系统是计算机与智能手机的大脑，它们能够指挥多个进程协同和并发工作。经过中国计算机科学家多年的努力，在基于开源操作系统Linux的基础上，先后研发出红旗、银河麒麟和中国操作系统（COS）等，但目前这些系统在应用的广度和深度方面还有很多欠缺。中国应该制订操作系统研发的中长期国家计划，加大在操作系统研发方面的投入，特别是在手机操作系统方面。

（3）自主研制可控的服务器和大型数据库系统软件

服务器与国民经济息息相关[10]，关乎国计民生的数据都存放在大型数据库系统当中。因此，中国需要在未来十年，通过市场化等手段，加快国外知名品牌在高速服务器的核心技术转让。另外，还应该加强数据库等系统软件的研发和投入，组织1～2个核心科研团队，力争研发出具有市场竞争力的数据库系统。中国应该继续支持以山东浪潮为代表的生产大型服务器的高科技公司，在资金、市场等方面给予倾斜。

（4）使用国产品牌的路由器和交换机组织骨干网

目前，中国骨干网上的路由器和交换器主要由思科公司提供[11]。但是，随着中国国内以中兴通讯为代表的通信设备公司的崛起，中国应下定决心用国产的先进品牌逐渐替换非国产的品牌。为此，中国应该加大对这些产业的投入，在市场上加以引导，让大型的国有通信企业在采购设备中加大国产品牌的比重。

（5）加强互联网内容的管理以及控制

目前，以百度、阿里和腾讯为代

表的互联网公司在搜索引擎、电子商务和即时通信等新兴网络应用方面走在世界的前列。在带来可观的经济收入的同时也将大量的互联网数据留在了中国的服务器当中，减少了数据流量进入其他国家导致可能泄密的情况发生[12]。因此，中国需要通过扶持互联网新型应用，争取出现更多的大型互联网公司。

（6）大力支持目前中国的网络安全公司

中国网民的技术涵养近几年得到了很大的提高[13]，但是和西方发达国家相比，在网络安全意识方面还有一定的差距。另外，过去许多杀毒软件公司在升级病毒库时需要收取一定的服务费，许多用户不安装杀毒软件。上述这些因素都可能导致多达千万的中国的主机被其他国家机构与组织控制。以360为代表的新型网络安全公司，提供了一种全新的、免费的网络安全服务，使得中国大部分主机都安装了360的杀毒和防护软件，这些安全软件能够为用户提供绝大部分的安全服务，避免了更多的主机成为肉鸡。因此，中国应该加大以360为代表的网络安全公司的支持力度。

（7）部署根域名服务器于国际组织中管理

除了部分根域名服务器在欧洲与日本之外，大部分根域名服务器主要受控于美国商务部。由于美国参众两院的阻拦，美国迟迟无法将域名服务器转交给联合国等国际组织。随着信息技术实力的增强，广大发展中国家国家应该联合起来，要求美国交出根域名服务器的管理权限，将众多的域名服务器部署在一些发展中国家。中国应该在这个事件中起主导作用。

（8）建立国家级网络空间攻防专业技术队伍

中央网络安全领导小组的成立为网络空间的安全提供了组织上的保证，同时也还需要从技术上为网络空间的安全提供保障。中国应该整合国内所有研究网络空间安全的企事业单位以及科研院所，从中抽调精英，组建具有中国特色的网络安全部队，加强互联网翻墙软件的破译工作，对其他国家的代理服务器进行有效拦截。

3 下一代信息技术对网络空间安全的影响和应对措施

以下一代网络、物联网、大数据处理以及云计算为代表的新一代信息技术的最大特点就是促进了海量数据在更大范围的交流和超范围的信息共享[14]。新一代信息技术在给广大用户带来便利的同时，也给中国维护网络空间安全带来全新的挑战。

3.1 下一代信息技术对网络安全的影响

（1）下一代网络技术

下一代网络超快的网速为信息的交互带来极大的方便，但加密机制也给网络侦控带来了深远的影响。过去，国家机关可以借助网络监听技术，从不法分子的网络通信中获取犯罪证据；现在，对下一代网络存在的海量信息的监测，肯定会漏掉部分重要的敏感信息。由于通信协议中有强大的加密功能，大量的通信信息采用加密的方式，因此采用常规的监听和破解手段无法实现对加密信息有效的破解。如果敌对分子利用通信协议中的加密技术而导致信息加密无法破解，这就会给国家安全带来一定的危害。

（2）云计算

云计算是未来信息技术的一个重要发展方向。目前，云计算核心技术主要由美国几大IT巨头控制，包括核心的数据处理和海量数据的存储技术[15]。

目前，中国在云计算中心的建设发展没有国家统一的规划，发展有些混乱，如地方政府纷纷建设云计算平台，但因缺乏大数据处理的核心技术支持，导致云计算应用能力不够，缺乏业务数据。因此，中国应该制订科学合理的规划，对全国的云计算平台进行资源整合，构建具有自主核心技术、大规模的和具有核心竞争力的云计算平台，确保国家的核心数据能够留在本国的云计算中心进行处理。

另外一个问题就是云计算中心数据存储的安全。由于云计算的操作系统、数据处理技术以及存储的核心技术都在美国IT巨头手中，如果云端存在漏洞和后门，就无法确保在云端的数据安全。

（3）物联网技术

物联网基于下一代网络技术提供的通信服务和云计算中心提供的强大运算能力。物联网打破了之前网络通信的信息来源，目前其主要信息来源是人与物之间的交互信息。通过链路层的一些新创的通信协议，能够实现将地球上需要监控的实体信息联网，从而将原来虚拟的互联网空间变成了可感知的真实世界[16]。

基于美国IBM主导的“智慧地球”战略，其目的就是利用IBM掌握的核心技术资源，不断推出基于互联网的新技术、新产品和新应用。该战略的核心就是要建立网络社会，将现实世界的所有活动全部纳入互联网管理。随着现实生活对互联网的依赖，美国不仅可以掌握中国经济、政治、军事的信息，甚至可以随时实施信息干预和制裁。这不仅意味着中国的产业和经济安全无法得到保障，还意味着政府的执政能力也将受到来自美国IT巨头的严重挑战。

物联网的应用使得最为封闭的电力网络也进入了互联网时代。由于电力网络关乎百姓的日常生活和国民经济的生产活动，如果电力网络遭到攻击，会给国民经济造成重大的损失。

（4）智能手机即时通信软件的相关应用

智能手机作为移动互联网终端

的重要组成部分，可以作为下一代信息技术研究的重点。传统基于PC机之上的QQ、微博等通信软件和互联网应用，正在被智能手机上的即时通信软件和其他APP所替代。以朋友圈和公众微信号为代表的应用能够大面积传播各种未经证实的信息，容易引起社会的恐慌，还有可能引发群体性事件。

3.2 应对策略

下一代信息技术对网络空间安全影响的应对策略主要有以下几个方面。

（1）加快下一代网络通信基础设施的部署

下一代网络技术在通信协议方面主要基于IPv6技术，并对网络层协议进行重大的改变。如果不借助过度技术，IPv6和IPv4则无法在网络层进行兼容。目前只在高等院校和科研院所存在着一些IPv6的信息孤岛。中国应该对下一代网络骨干网的建设投入巨额资金，争取在“十三五”期间完成大中城市基于下一代网络骨干网的建设，让中国在下一代网络的建设中走在世界大国的前列。

通过下一代网络的建设，能够让中国拥有足够多的独立IP地址，以推进物联网的应用。另外，通过下一代网络的建设还可以扶持以中兴通讯为代表的众多高科技网络通信公司，自主研发出高性能的下一代高速路由器和交换器，抢占世界市场。

（2）自行研制云计算的核心技术

云计算技术在中国方兴未艾，虽然中国拥有众多的云计算中心，但是这些中心缺乏核心的云计算技术，包括计算技术和存储技术。中国应该整合现有的云计算平台，为研发云计算核心技术提供开发、测试与实验提供可靠强大的平台。

（3）制订基于物联网技术的“互联网+”的战略工程

在国家“十三五”规划中，主推“互联网+”战略工程。在中国经济转型过程中，物联网技术能够为“互联网+”工程提供强有力的支撑平台和技术保证。

（4）对智能手机的即时通信进行有效管控

对基于智能手机的即时通信软件推行实名制，对朋友圈和公众号的的发布信息进行实时监控，对敏感的关键词进行有效过滤与实时预警，防止不良信息的广泛传播。

（5）从国家战略的高度重视下一代信息技术标准的制订

制订下一代信息技术通信与应用标准，例如移动通信5G技术和移动支付标准等，能够为中国经济带来巨额的收入。例如，美国高通公司通过标准和专利，每年高达80亿美元的利润。

（6）大力支持国家下一代信息技术自主创新支撑体系

推进国家高等院校和科研院所协作建立下一代信息技术自主创新体系和标准，并建立下一代信息技术研发和测试平台，为中国下一代信息产业的发展和应用提供强有力的物质支撑。

以应用推进下一代技术向广度和深度二维方向发展，以应用推进技术的发展，推进更广泛的用户的应用，使得技术发展与用户的应用进入良性循环，这是所有信息技术强国的必由之路。

4 结束语

网络环境的复杂性、多变性，以及信息系统的脆弱性，决定了网络空间安全威胁的客观存在。随着中国的日益开放，网络空间安全监管的加强和保护屏障的建立变得不可或缺。网络空间安全是涉及中国经济发展、社会发展和国家安全的重大问题。通过自主可控和创新才能从技术上应对网络空间安全面临的威胁与挑战。中国应该从战略高度重视下一代网络技术对网络空间主权的威胁与挑战，并采用相应的技术与政策及时应对。

参考文献

[1] 丁禹, 逯志安, 焦建伟. 2014年网络空间安全问题综述与展望[J]. 通信安全与信息保密, 2015, (2): 16–21
[2] 田力加, 王光厚. 中国网络空间安全现状研究[J]. 山西大同大学学报, 2015, 29(2): 12–14
[3] 廖东升, 石海明, 郭勤, 等. 全球视阈下的网络空间国家安全战略[J]. 湖南社会科学, 2013, (6): 43
[4] 何德旭, 饶云清, 王智杰. 金融安全网: 基于信息空间理论的分析[J]. 经济理论与经济管理, 2011, (2): 69–78
[5] 王世伟. 论信息安全、网络安全和网络空间安全[J]. 中国图书馆学报, 2015, (2): 72–84
[6] 惠志斌.我国国家网络空间安全战略的理论构建与实现路径[J]. 中国软科学, 2012, (5): 22–27
[7] 彭长艳. 空间网络安全关键技术研究[D]. 长沙: 国防科学技术大学, 2010
[8] 林伟. 空间网络技术的研究与实现[D]. 成都: 电子科技大学, 2012
[9] 张钢. 网络空间安全问题探讨[J]. 科技信息, 2013, (5): 96–97
[10] 方兴东, 张笑容, 胡怀亮. 棱镜门事件与全球网络空间安全战略研究[J]. 现代传播: 中国传媒大学学报, 2014, 36(1): 115–122
[11] 雷璟. 网络空间攻防对抗技术及其系统实现方案[J]. 电讯技术, 2013, (11) : 1494–1499
[12] 董淑英. 探究网络空间的自主构建与管理[J]. 信息安全与通信保密, 2013, (9): 47–52
[13] 王鹤鸣. 网络安全新政一实体战争与网络战争的突袭[J]. 信息安全与通信保密, 2011,(7): 15–16
[14] 胡连宛.中国网络安全面临严峻挑战[J]. 决策与信息, 2012, 330(5): 4–8
[15] 曲成义. 网络空间安全保密对抗态势和应对策略[J]. 电讯技术, 2012, (4): 6–7
[16]童淑英. 物联网与网络空间安全[J]. 河北省科学院院报, 2011, (3): 77–81

作者简介

周延森，国际关系学院信息科技学院信息安全教研室主任、副教授；主要研究方向为网络通信及安全、智能手机应用及安全；先后主持完成10多个校级项目；发表论文10余篇。

周琳娜，国际关系学院信息科技学院常务副院长、电子与通信工程学科组和警务科技学科组组长，国家百千万工程人才，国家重点领域创新团队负责人；主要研究方向为信息安全、数字取证、多媒体信息处理等；先后申请和主持了国家自然科学基金等重点项目共4项，获得国家科技进步一、二等奖各1项，获国家技术发明奖1项，获得省部级科技进步奖30余项；出版专著3本，发表SCI、EI检索论文30余篇。