**陕西省互联网网络安全情况月报**

2019年3月 （第W003期） 总第65期

陕西省通信管理局

国家计算机网络与信息安全管理中心陕西分中心

目 录

[**1 情况综述** 1](#_Toc6395123)

[**2 安全事件分析** 1](#_Toc6395124)

[**2.1 木马、僵尸网络事件分析** 1](#_Toc6395125)

[**2.2 “飞客”蠕虫病毒事件分析** 3](#_Toc6395126)

[**2.3 网页篡改事件分析** 3](#_Toc6395127)

[**2.4 网站后门事件分析** 5](#_Toc6395128)

[**3 安全事件处置情况** 6](#_Toc6395129)

[**4 安全预警信息** 6](#_Toc6395130)

[**4.1 本月重要安全漏洞信息通报** 6](#_Toc6395131)

[**4.2 本月重要漏洞修补信息** 7](#_Toc6395132)

[**5 业界动态** 11](#_Toc6395133)

[**5.1 切实加强党对网信工作的领导 奋力开创网络强省建设新局面** 12](#_Toc6395134)

[**5.2 我省通信行业圆满完成“两会”期间通信保障任务** 13](#_Toc6395135)

[**5.3 我局与省工信厅联合举办中国西部工业信息化发展论坛** 13](#_Toc6395136)

[**5.4 我局赴北京市反电信网络诈骗犯罪中心学习交流** 14](#_Toc6395137)

[**5.5 中国网络社会组织联合会网络传播专业委员会在京成立** 15](#_Toc6395138)

1. **情况综述**

2019年3月，全省公共互联网网络安全状况整体评价为良。

本月，我省互联网基础设施运行平稳，全省范围内未发生关键基础设施运行安全重大事件，未发生网络安全重大事件。

通过国家计算机网络应急技术处理协调中心陕西分中心（简称“陕西互联网应急中心”，SNCERT）监测及电信运营企业、安全厂商、安全通报成员单位报送，省内被木马僵尸程序控制的主机（受控端）IP数为10,310个，较上月减少9.30%，占全国总数的2.15%；木马僵尸控制服务器（控制端）IP数为21个，较上月增加110.00%，占全国总数的1.11%；省内被篡改网页的网站数为29个，较上月减少3.33%，占全国总数的2.38%；省内被植入后门的网站数为65个，较上月增加209.52%，占全国总数的1.96%；省内感染飞客蠕虫的主机IP数为7,192个，较上月增加1.07%，占全国总数的3.48%。

1. **安全事件分析**
   1. **木马、僵尸网络事件分析**

2019年3月，CNCERT对木马僵尸的活动状况进行了抽样监测，发现中国大陆地区480,264个IP地址对应的主机被木马或僵尸程序控制。事件高发的三个省份分别为广东省（约占28.0%）、北京市（约占19.0%）、上海市（约占10.1%），分布情况如图1所示。

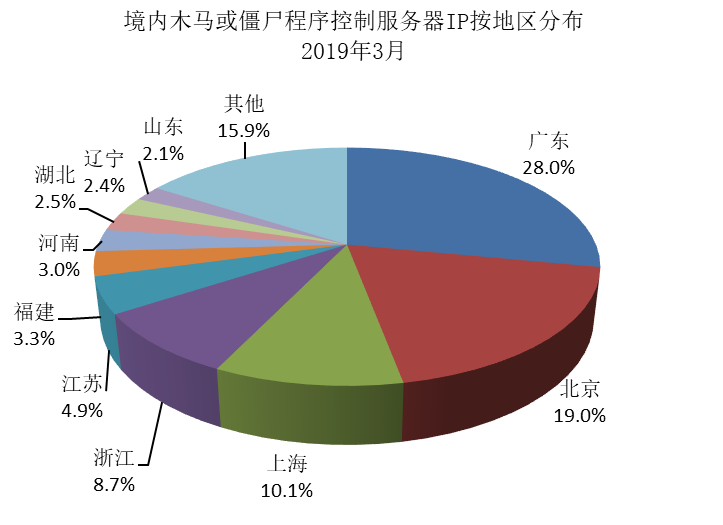


图1：境内木马或僵尸程序受控主机地区分布图

2018年4月-2019年3月境内木马或僵尸网络程序受控主机IP数量月度统计情况如图2所示。

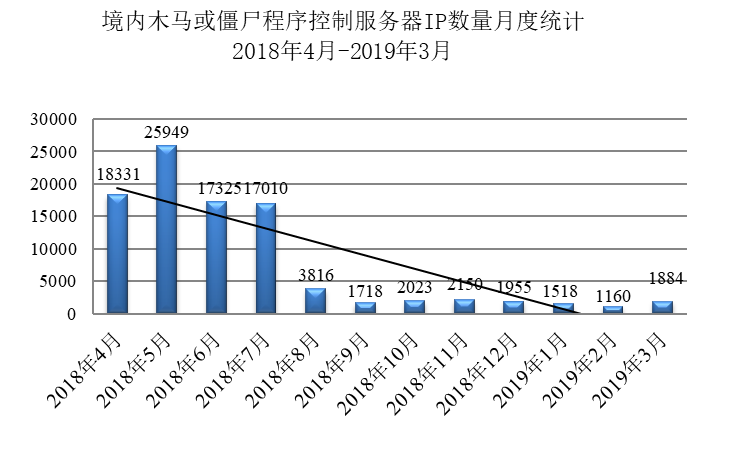


图2：境内木马或僵尸网络程序受控主机IP数量月度统计

2019年3月，陕西省有10,310个IP地址对应的主机被境内外黑客通过木马或僵尸程序控制，约占全国总数的2.15%，居全国第18位；有21个IP地址对应的主机被用作木马和僵尸程序控制主机与境外进行通信，约占全国总数的1.11%，居全国第17位。

* 1. **“飞客”蠕虫病毒事件分析**

2019年3月，CNCERT对“飞客”蠕虫的活动状况进行了抽样监测，发现境内感染“飞客”蠕虫的主机IP地址共206,950个。事件高发的三个省份分别为广东省（约占30.1%）、浙江省（约占8.0%）和北京市（约占7.3%）；其中陕西省7,192个IP地址，约占全国总数的3.5%，居全国第8位。其分布情况如图3所示。

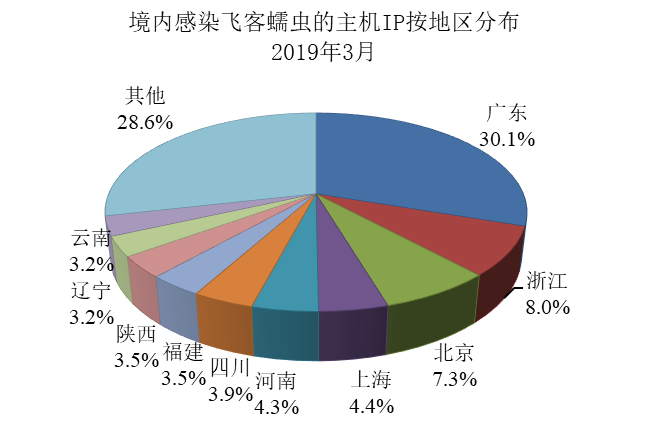


图3：境内感染飞客蠕虫的主机IP按地区分布图

* 1. **网页篡改事件分析**

2019年3月，CNCERT监测发现中国大陆地区被篡改网站1,220个，其中境内被篡改政府网站（.gov）数量为65个。被篡改网站分布情况如图4所示，最多的地区分别为广东省（约占34.9%）、北京市（约占18.4%）、上海市（约占8.0%）。

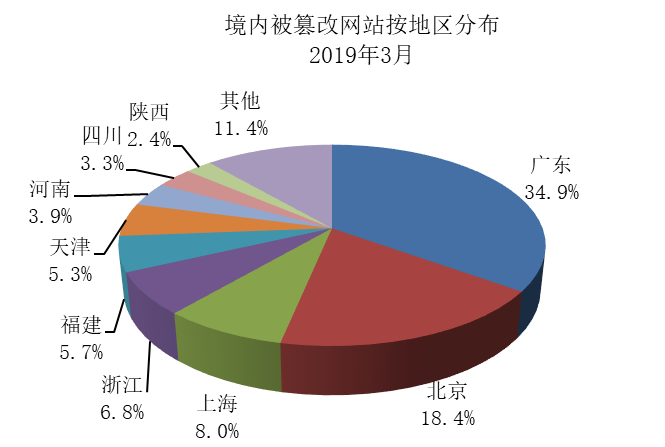


图4：境内被篡改网站按地区分布

2018年4月-2019年3月境内被篡改网站数量按月度统计如图5所示。

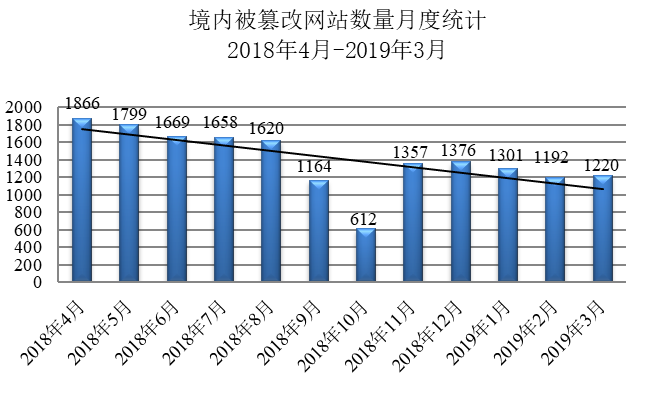


图5：境内被篡改网站数量月度统计

其中，2018年4月-2019年3月境内政府网站被篡改数量月度统计如图6所示。

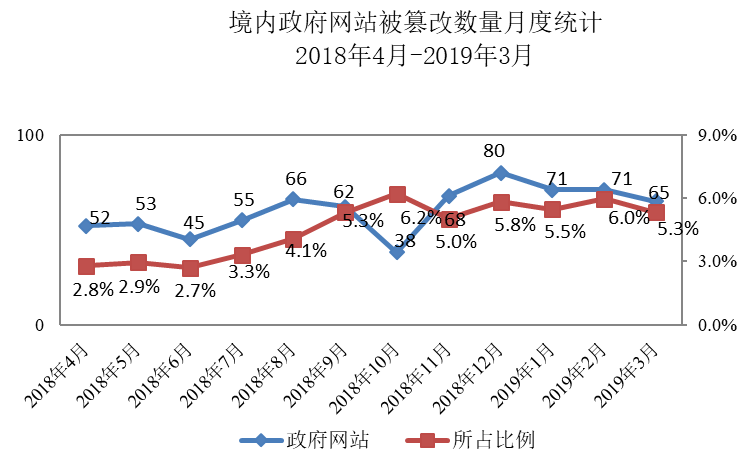


图6：境内政府网站被篡改数量月度统计

2019年3月，陕西省内被篡改网站数量29个，居全国第9位，约占全国总数的2.4%。

* 1. **网站后门事件分析**

2019年3月，CNCERT监测发现中国大陆地区网站被植入后门数量1,273个。网站被植入后门分布情况如图7所示，最多的地区分别为广东省（约占31.1%）、北京市（约占15.0%）和四川省（约占9.9%）。

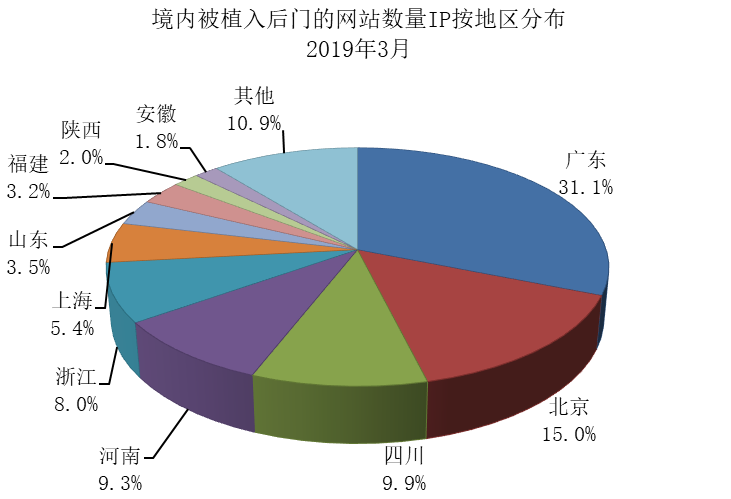


图7：境内网站被植入后门按地区分布

2019年3月，陕西省内监测发现网站被植入后门数量65个，约占全国总数的2.0%，全国排名第9名。

1. **安全事件处置情况**

2019年3月，SNCERT共协调处理各类网络安全事件16,135起，僵尸木马受控事件10,830起，控制事件38起，飞客病毒事件5,267起。政府网站安全事件14起，其中11个高危漏洞，3个网页篡改；高危漏洞包括弱口令5起，SQL注入漏洞2起，逻辑缺陷漏洞1起，目录遍历漏洞1起，SVN文件泄露1起，未授权访问漏洞1起；SNCERT及时向用户作了情况通报并指导用户进行系统修复，使事件及时得到处理。

1. **安全预警信息**
   1. **本月重要安全漏洞信息通报**

2019年3月，CNCERT收到的来自国家信息安全漏洞共享平台（CNVD）报告的漏洞数量1,132个，其中高危漏洞343个、中危漏洞689个、低危漏洞100个，其中0day漏洞538个，可远程攻击漏洞1,005个。

2018年4月-2019年3月CNVD收录漏洞按月统计情况分布如图9所示。

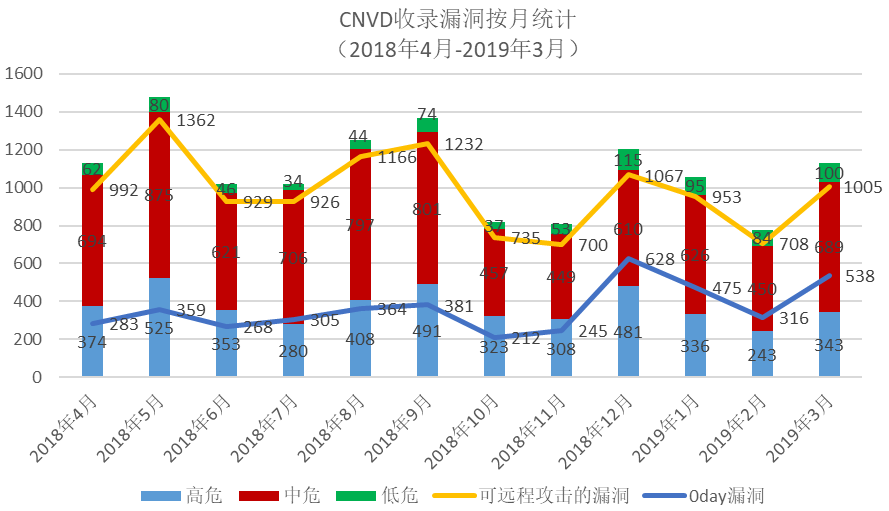


图9：CNVD收录漏洞按月统计情况

2019年3月CNVD收录漏洞按类型统计情况分布如图10所示。

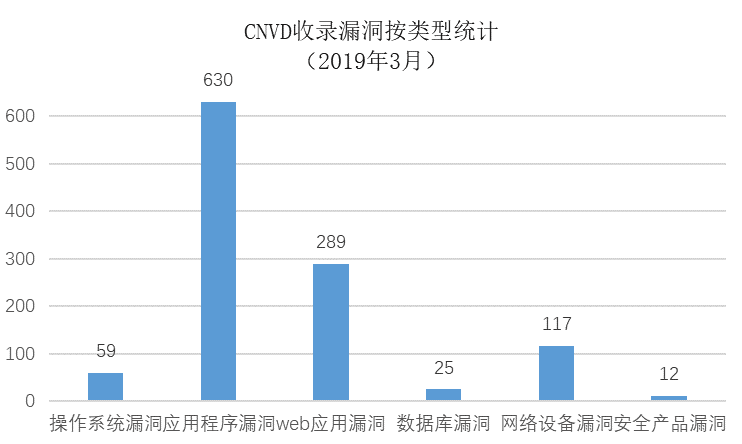


图10：CNVD收录漏洞按类型统计情况

2019年3月，国家信息安全漏洞共享平台（CNVD）收录漏洞的补丁总数594个，其中高危漏洞补丁177个、中危漏洞补丁366个、低危漏洞补丁51个。

* 1. **本月重要漏洞修补信息**

**（一）EDK2缓冲区溢出漏洞**

EDK2是一套基于UEFI和PI规范的跨平台固件开发环境。

EDK2的系统固件中存在缓冲区溢出漏洞。攻击者可利用该漏洞提升权限和造成拒绝服务。

目前，厂商已发布了漏洞修复程序。

补丁连接：

ttps://github.com/tianocore/edk2

**（二）Eclipse Jetty拒绝服务漏洞**

Eclipse Jetty是Eclipse基金会的一个开源的、基于Java的Web服务器和Java Servlet容器。

Eclipse Jetty 9.3.x版本和9.4.x版本中存在拒绝服务漏洞，攻击者可利用该漏洞造成拒绝服务。

目前，厂商已发布了漏洞修复程序。

补丁链接：

https://bugs.eclipse.org/bugs/show\_bug.cgi?id=538096

**（三）Apple macOS Mojave Bom安全绕过漏洞**

Apple macOS Mojave是美国苹果（Apple）公司的一套专为Mac计算机所开发的专用操作系统。Bom是其中的一个字节顺序标记（Byte Order Mark）组件。

Apple macOS Mojave 10.14.4之前版本中的Bom组件存在安全漏洞。攻击者可借助恶意的应用程序利用该漏洞绕过Gatekeeper检查。

目前，厂商已发布了漏洞修复程序。

补丁链接：

https://support.apple.com/zh-cn/HT209600

**（四）多款Apple产品WebKit逻辑缺陷漏洞**

Apple Safari等都是美国苹果（Apple）公司的产品。Apple Safari是一款Web浏览器，是MacOSX和iOS操作系统附带的默认浏览器。Apple iOS是为移动设备所开发的一套操作系统。Apple tvOS是一套智能电视操作系统。WebKit是其中的一个Web浏览器引擎组件。

多款Apple产品中的WebKit组件存在安全漏洞。攻击者可借助恶意的网站利用该漏洞在其他网站的上下文中执行脚本。

目前，厂商已发布了漏洞修复程序。

补丁链接：

https://support.apple.com/zh-cn/HT209599

**（五）多款Apple产品WebKit内存错误引用漏洞**

Apple Safari等都是美国苹果（Apple）公司的产品。Apple Safari是一款Web浏览器，是MacOSX和iOS操作系统附带的默认浏览器。Apple iOS是为移动设备所开发的一套操作系统。Apple tvOS是一套智能电视操作系统。WebKit是其中的一个Web浏览器引擎组件。

多款Apple产品中的WebKit组件存在内存错误引用漏洞。攻击者可借助恶意制作的Web内容利用该漏洞执行任意代码。

目前，厂商已发布了漏洞修复程序。

补丁链接：

https://support.apple.com/zh-cn/HT209599

**（六）SAP ABAP远程权限提升漏洞**

SAP ABAP是一款运行于NetWeaver（为SAP应用提供开发和运行环境的应用平台）中且基于ABAP高级编程语言和Java编程语言的应用服务器。SAP ABAP存在远程权限提升漏洞，远程攻击者可利用该漏洞提升权限。

目前，厂商已发布了漏洞修复程序。

补丁链接：

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=503809832

**（七）SAP Business One信息泄露漏洞**

SAP Enterprise Financial Services是德国思爱普（SAP）公司的一套企业财务服务解决方案。

SAP Business One存在信息泄露漏洞，攻击者可利用该漏洞获取可能有助于发起进一步攻击的敏感信息。

目前，厂商已发布了漏洞修复程序。

补丁链接:

https://www.securityfocus.com/bid/105307,https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2458

**（八）GitLab目录遍历漏洞**

GitLab是美国GitLab公司的一款使用Ruby on Rails开发的、自托管的、Git（版本控制系统）项目仓库应用程序。该程序可用于查阅项目的文件内容、提交历史、Bug列表等。

GitLab（社区和企业版本）11.4之前版本中存在安全漏洞。攻击者可利用该漏洞读取任意报告。

目前，厂商已发布了漏洞修复程序。

补丁链接：

https://about.gitlab.com/2019/01/16/critical-security-release-gitlab-11-dot-6-dot-4-released/

**（九）Foxit Reader越界读漏洞**

Foxit Reader是中国Foxit公司的一款PDF文档阅读器。

Foxit Reader处理PDF文件存在越界读漏洞，允许远程攻击者利用漏洞提交特殊的文件请求，可获取敏感信息或使应用程序崩溃。

目前，厂商已发布了漏洞修复程序。

补丁链接：

https://www.foxitsoftware.com/support/security-bulletins.php

**（十）QNAP QTS空指针解引用漏洞**

QNAP QTS是QNAP NAS智能操作系统，基于Linux，旨在提供高性能应用程序和服务，以满足您文件共享、存储管理、备份、虚拟环境、多媒体、监控等方面的需求。

QTS 4.3.5 build 20181013、4.3.4 build 20181008、4.3.3 build 20180829、4.2.6 build 20180829及更早版本存在空指针解引用漏洞，远程攻击者可利用该漏洞导致NAS媒体服务器崩溃。

目前，厂商已发布了漏洞修复程序。

补丁链接：

https://www.qnap.com/zh-tw/security-advisory/nas-201811-22

1. **业界动态**
   1. **切实加强党对网信工作的领导 奋力开创网络强省建设新局面**

陕西省委网络安全和信息化委员会会议28日在西安召开。陕西省委书记、省委网络安全和信息化委员会主任胡和平强调，要深入学习贯彻习近平总书记关于网络强国的重要思想，加强党对网信工作的领导，加快网络强省建设，为新时代追赶超越提供有力支撑。

省长、省委网络安全和信息化委员会副主任刘国中，省委副书记、省委网络安全和信息化委员会副主任贺荣出席会议。

胡和平指出，十八大以来以习近平同志为核心的党中央高度重视网络安全和信息化工作，习近平总书记提出一系列新思想新观点新论断，为我们做好新时代网信工作提供了根本遵循。要学懂弄通做实习近平总书记关于网络强国的重要思想，站在树牢“四个意识”、坚定“四个自信”、坚决做到“两个维护”的高度，深刻认识做好网信工作的极端重要性和现实紧迫性，推动网络强国战略在陕西落地生根。

胡和平强调，要建立网络综合治理体系，加强网上正面宣传，加快媒体深度融合发展，唱响主旋律，传递正能量，营造清朗的网络空间。要筑牢国家网络安全屏障，强化数据资源安全管理，加强关键信息基础设施防护，推进网络安全态势感知能力建设，做大做强网络安全产业，严厉打击各类网络违法犯罪行为，牢牢掌握网络安全主动权。

胡和平强调，要抢抓网信事业发展重要战略机遇期，坚持产业数字化和数字产业化两手齐抓，大力发展数字经济，加快网信军民融合发展，推动政务信息化建设，深入实施信息惠民工程，以信息化助力陕西高质量发展。要提高信息化条件下党的领导水平和执政能力，加快构建省市县三级网信工作体系，打造高素质网信干部队伍和专业人才队伍，为网信事业发展提供坚强保障。

会议审议了中共陕西省委网络安全和信息化委员会《工作规则》及办公室《工作细则》等文件，研究了有关事项。

* 1. **我省通信行业圆满完成“两会”期间通信保障任务**

2019年3月3日到3月15日，全国“两会”在北京顺利召开。为确保今年“两会”期间我省通信网络安全畅通，按照工信部要求，我局组织各基础电信企业精心准备、周密部署、团结协作，全力做好“两会”通信保障工作。

各基础电信企业按要求认真制定“两会”期间通信保障方案，加强对通信枢纽、互联网数据中心、传输干线等重点部位的“四防”工作，对重要业务采取“双活”或“多活”架构以及负载均衡、自动倒换等措施，确保关键系统安全稳定运行。会议召开期间，各企业严格落实7×24小时值班及领导带班制度，有关负责人、联络员24小时保持联络畅通，同时加强对网络运行状态的监测，及时处置各类突发事件。

“两会”期间，我省各基础电信企业累计投入保障人员6,718人次，保障车辆2,270台次，油机2,992台次，在全省通信行业的共同努力下，我省网络运行平稳，通信畅通，圆满完成 “两会”通信保障任务。

* 1. **我局与省工信厅联合举办中国西部工业信息化发展论坛**

3月15日，中国西部工业和信息化发展论坛在西安曲江举办。本次论坛由我局和省工信厅联合举办，我局党组书记、局长高彩玲出席论坛并致辞。

本次论坛以落实国务院《“十三五”国家信息规划》、《关于深化“互联网+先进制造业”发展工业互联网的指导意见》等政策，贯彻中共陕西省委关于全面深化改革扩大开放推动新时代追赶超越发展的决定精神为指导，以“助力西部发展工业信息化，建设内陆改革开放新高地”为主题，共设嘉宾致辞、产业报告、前言课题、主题报告、案例分享、互动答疑等环节，为期一天。

高彩玲在致辞中指出，当前全球经济社会发展正面临全新挑战与机遇，发展工业互联网成为世界各国推进工业经济转型发展的共同选择。我国具有发展工业互联网的良好产业基础和巨大市场需求，在党中央、国务院的高度重视下，我国工业互联网发展已从概念普及进入实践深耕阶段。陕西省的工业互联网发展与发达省市之间还存在较大差距，目前仍处于初期阶段，具有相当大的发展潜力，需要我省政府、企业、高校、研究院共同努力，让工业互联网为陕西经济高质量发展提供新支撑，为陕西制造业转型升级提供新动能，为陕西数字经济发展开辟新蓝海。高彩玲表示，我局将牢牢把握工业互联网发展的历史机遇期，加快陕西省工业互联网标识解析二级节点和工业互联网安全预警平台建设，引领我省工业互联网发展向更优环境、更快速度、更高目标迈进。

据悉，本次论坛涉及各设区市工信主管部门两化融合、装备制造相关负责同志，在陕协会、学会、高校、研究院所、企业代表等，共计700余人参加。

* 1. **我局赴北京市反电信网络诈骗犯罪中心学习交流**

当前，通讯信息诈骗正逐渐从电话诈骗转向网络诈骗，呈现许多新的特点，防范打击通讯信息诈骗依然是一项紧迫而重要的工作。为适应反诈工作新形势，3月初，我局作为省打击治理电信网络新型违法犯罪工作联席会议成员单位组织我局及省公安厅、中国人民银行西安分行、省银保监会一行人员，前往北京市反电信网络诈骗犯罪中心进行交流。

北京市反诈中心充分运用人工智能、大数据、互联网+的方法手段，搭建预知、预警、预防平台，着力构建“打击、防范、整治、宣传”四位一体的工作格局，不断提升打击防范治理电信网络诈骗犯罪的能力水平，取得显著成效。

我局在此行中与北京市反诈中心工作的同志就防范打击通讯信息诈骗工作的心得进行了交流，下一步我局将继续按照职能职责全力协助省反诈中心工作，一如既往的以新时代的担当精神，进一步完善制度机制，完善反诈系统功能，向互联网反诈扩展，强化用户个人信息安全保护，提高技术防范和打击能力，为反诈工作提供有力支撑，坚定维护人民群众切身利益。

* 1. **中国网络社会组织联合会网络传播专业委员会在京成立**

为加强中国网络社会组织联合会的专业工作力量，提升服务业务主管单位网上宣传引导工作的能力水平，3月4日下午，中国网络社会组织联合会网络传播专业委员会成立大会在京召开。

中央网信办副主任、国家网信办副主任刘烈宏，全国人大社会建设委员会副主任委员、中国网络社会组织联合会会长任贤良出席会议并讲话。

刘烈宏指出，当前，舆论生态、媒体格局和传播方式正在发生深刻变化，新闻舆论工作面临新的挑战和机遇。我们要因势而谋、应势而动、顺势而为，深入研究网络传播规律，加快推动媒体融合发展，牢牢掌握舆论场主动权和主导权。中国网络社会组织联合会网络传播专业委员会的成立恰逢其时、责任重大。

刘烈宏强调，网络传播专委会各成员单位要加快推进媒体融合发展；要增强脚力、眼力、脑力、笔力，更好履行网络媒体的职责使命；要着眼全媒体时代的新形势新任务，推进网上宣传理念、内容、形式、方法、手段等创新。他要求，网络传播专委会团结凝聚好业界、学界资源和力量，特别是近百家成员单位的力量，助力网上宣传引导工作，推动形成网上网下同心圆，让正能量更强劲、主旋律更高昂。

任贤良表示，中国网络社会组织联合会自去年5月成立以来，在业务主管单位国家网信办的关心支持下，积极开展网络传播领域相关活动，不断强化新媒体阵地意识，大力营造昂扬向上、健康有序的网络舆论环境，推动网络社会组织成为网上正能量传播的重要力量。任贤良要求，网络传播专委会作为中国网络社会组织联合会成立的第一个专业委员会，要积极开展工作，发挥带头示范作用，扣好中国网络社会组织联合会事业发展的第一粒扣子。

会上公布了网络传播专业委员会2019年十项重点活动，进行了交流发言。

中央网信办网络新闻信息传播局、网络社会工作局，中国传媒大学主要负责同志，以及网络传播专委会首批成员单位代表等100余人参加会议。