

第五届“强网论坛”郑州开讲

院士专家畅谈“新时代、新空间、新发展”

7月10日,第五届“强网杯”系列活动在郑州高新区正式拉开帷幕。“强网论坛”作为本届活动的重要环节,聚集了来自国内网安领域的院士、知名专家和行业精英,围绕新形势下网络安全的现状、发展与变革进行前瞻性的探索与分享。

朱中梁、郭光灿、管晓宏、邬江兴、刘炯天、陆军、王承祥等多位院士及来自清华大学、上海交大、中科院信工所等一流网络安全学院建设示范高校专家学者、知名企业负责人等齐聚郑州高新区,共话网安产业现状及未来,共谋网安产业发展新思路。记者 孙庆辉

网络空间已经成为继陆、海、空、天之后的第五大主权空间

当前,网络空间已经成为继陆、海、空、天之后的第五大主权空间,网络安全已经成为国家安全的战略高地。网络安全专业是国家建设的重点专业,网络空间安全人才培养重要性日益凸显。“强网论坛”作为网信领域的一次盛会,交流合作、主题报告、高端对话是重要环节,主论坛中,来自国内网安领域的院士、知名专家和行业精英,围绕新形势下网络安全的现状、发展与变革进

行前瞻性的探索与分享。持续2天的“强网论坛”设置一个主论坛和11个分论坛,其中主论坛以“新时代、新空间、新发展”为主题,邀请院士、高端研发机构和知名企业负责人,以及一流网络安全学院建设示范高校专家共同参与,围绕网络空间国际交流与合作、网信智库建设、网络空间安全人才培养、网络安全前沿技术等方面开展高端对话。

主论坛上,中国工程院院士

邬江兴以《网络空间安全发展模式的变革》为题进行主旨演讲;中国工程院院士陆军以《量子计算机及应用》为题作主旨报告;安恒信息董事长范渊以《构建数字化转型下的网络空间对抗安全》为题进行主题分享;欧洲科学院教授王承祥以《6G无线信道研究进展与挑战》为题进行主题分享;国际著名密码学专家、上海交通大学教授来学嘉以《密码学与区块链》为题进行主题演讲。

网络安全人才缺口超150万 需从国家战略高度特事特办助力

当前,网络安全专业是国家建设的重点专业,网络空间安全人才培养重要性日益凸显。

7月10日下午,网络空间安全学科专业建设与人才培养论坛围绕当下学界、业界亟待解决的网络空间安全学科专业建设与人才培养展开,与会专家学者纷纷支实招、献良策。

针对我国网络安全人才培养的现状,北京电子科技学院副院长封化民谈到,总体来看,我国对网络安全人才的需求量在140万以上,社会对网络安全人才的需求量每年约2.5万人。而高校每年培养的网络安全人才不到1.5万人,短期网络安全人才供需矛盾依然突出。同时,网络安全师

资队伍、网络安全教材体系建设、网络安全实践教学、网络安全实习基地亟待加强。

国防科技大学教授苏金树认为,网络空间人才培养面临三个瓶颈问题,包括视角狭窄瓶颈、创新不足瓶颈、系统能力不足瓶颈。这就需要完善知识体系、掌握新规律、加强教与研结合。

那么,如何加强培养网络安全人才?封化民从产学研合作方面提出了几点建议,可以从搭建校企合作交流平台、推动人才培养模式改革、促进高等教育的内涵式发展等方面着力。

网络空间的竞争,归根结底是人才的竞争。在加快推进网络空间安全学科建设和人才培养方

面,中国工程院院士沈昌祥在论坛上指出,网络空间安全人才需求呈金字塔型,除需要基础研究型人才(重点大学)外,更需要大量的工程应用型人才(一般大学)和推广实用型人才(中、大专技校)。除此之外,更需要重视全民普及教育,重视对中小学生进行科普教育。

同时,沈昌祥院士强调,网络安全人才的培养更需要加强改革创新力度。从国家安全战略急需的角度,特事特办,加快填补网络安全150多万人才巨大缺口;加强组织,统筹规划全国网络空间安全学科专业建设,争创一流网络空间安全学院,做好网络安全普及教育。



专家陆军



专家邬江兴

5G 专网 将成为2021年5G应用先锋

5G不仅是通信时代的演进,更是整个社会的大变革。

随着新基建对5G应用的大力推进,在进一步加强个人用户体验的同时,面对各行业的5G专网技术突破是目前行业发展的重中之重。

什么是5G专网?目前发展形势如何?又该如何去部署?7月10日下午召开的5G/B5G垂直行业应用论坛,一一给出解答。

专网的概念并不是5G时代才出现的,早在3G、4G时代就已存在,专网就是为特定用户提供网络通信服务的专用网络,公网与专网的区别主要在于公网为社会大众服务,例如打电话、发短信、看视频等需求,而专网为特定对象服务。

中科院信工所研究员李凤华认为,5G专网有以下几大优势:部署范围区域化,可面向封闭式的使用场景;网络需求个性

化,对时延要求严苛、可靠性要求高、上行速率需求高、数据安全和隔离要求严格等,5G专网能实现灵活部署;可与现有IT网络实现兼容互通,网络能力、网络技术也将不断演进升级。“对于多数企业而言,5G公网与专网的融合部署可缩短建设周期,进而大大降低成本。”

国家有关部门多次要求行业内加快5G虚拟专网落地,打造高质量5G网络。运营商也不断在加大5G专网建设力度。论坛上,中国移动通信研究院高工郑庆国介绍,中国移动通过采用“核心网独立部署(分别面向ToC和ToB),无线共用为主按需专用,共用传输资源按需隔离”的方式组网,划分为优享、专享和尊享三个等级。目前,不少5G专网项目已经落地,为企业搭建智慧工厂专业体系,无论是生产效率和产品质量、还是安全性都得到了极大的提高。

计算机硬件安全 是网络空间安全最后一道关闸

网络安全已成为国家的基本国策和战略思想,而随着互联网、大数据、人工智能等新技术的不断发展,现代处理器的高性能、低功耗和智能化是行业追求的三大方向,因此带来了更多的处理器硬件安全隐患。

处理器作为计算机系统的底层硬件组成,其安全系数的保障直接涉及到计算机的安全性。

清华大学计算机科学与技术系教授汪东升在7月10日召开的“洞见”——漏洞分析技术论坛中,以《网络空间安全的最后一道关闸——浅谈处理器安全》为主题阐述了他的观点。

“许多漏洞都是由于技术行业长期以来对性能最大化的关注而产生的。要让我们的处理器速度更快,是以安全为代价

的,唯一真正的解决方法可能最终是放慢速度”。汪东升表示,计算机硬件安全是信息空间、安全空间的最后一道关闸,新的特性与新的技术出现,必然会带来安全问题。硬件追求的高性能、低功耗、智能化是未来趋势,硬件安全是关键!

此外,他还说明了因为追求高性能而产生的“熔断”和“幽灵”漏洞,以及它们带来的影响说明硬件漏洞是广泛存在的,同时解释了追求低功耗而产生“骑士@tsinghua”漏洞是如何进行攻击的以及它的危害。

论坛中,还有来自信息工程大学、武汉大学、西安交通大学等高校的教授从研究范式、生态安全、问题挑战、发展趋势等多个维度,共同探讨网络空间安全脆弱性的关键问题。

