MIN YING SHI DIAN | 民营视点

探寻新形势下网络安全发展之路——

新理念 新目标 新技术 新生态

本报记者 孙 琳

7月，骄阳似火，网络安全领域同样热度高涨。

7月2日至3日，以“构建安全可信的数字世界”为主题的2022西湖论剑·网络安全大会在杭州举行；7月13日，“2022年北京网络安全大会（BCS2022）”在北京召开。

新形势下，网络安全将朝什么方向演变？

随着数字化、网络化、智能化的深入推进，网络安全行业又该如何应势而变？在南北举行的两场网络安全行业盛会上，众多业界人士齐聚展开深入探讨，求解新形势下网络安全之道，共论未来网络安全之路。

新形势——网络安全问题更趋严峻复杂

数字技术飞速发展，已辐射到经济社会生活的方方面面，无论是在抗击新冠肺炎疫情、提供公共服务还是促进产业发展等方面都展现出强大作用。但与此同时，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁也日益凸显，有组织、有目的的网络攻击形势愈演愈烈，其中每一台设备、每一行代码都可能成为网络攻击的突破点。

工业和信息化部党组成员、副部长张云明在2022年北京网络安全大会上指出，当前世界大变局和产业大变革历史性交汇，以5G、人工智能等为代表的新一代信息技术与实体经济深度融合，安全风险加速传导、渗透、叠加、放大，网络安全形势挑战日益复杂严峻。

据SonicWall全球响应智能防御（GRID）威胁网络数据显示，仅2021年上半年已发现3亿多次勒索软件攻击未遂事件，同比增长151%。而我国2021上半年感染计算机恶意程序的主机数量约为446万台，同比增长46.8%。勒索病毒只是威胁网络安全的方式之一，网页被挂暗链、网站被植入后门、大流量DDoS攻击等现象屡见不鲜，而除了来自外网的攻击，终端设备也有可能受到病毒流氓软件、网络钓鱼、挖矿软件的攻击。

作为今年北京冬奥会第三方网络安全服务商，奇安信对网络攻击严峻形势有着更为直接的感受。据奇安信集团总裁吴云坤介绍，在北京冬奥会筹办前后800多天时间里，网络攻击超过3.8亿次，跟踪、研判、处置的涉奥关键网络安全事件就达105起。

除了如奥运会这样的重大赛事活动，基础设施也成为近年来网络攻击的重点对象，无论是追逐经济利益的黑客组织，还是谋求政治目的国家级黑客，都频现魅影，一旦出现网络安全问题都对国家以及个人带来巨大影响。正如俄罗斯网络安全厂商卡巴斯基公司创始人尤金·卡巴斯基所说，“复杂而且脆弱”也许是当下网络空间最贴切的形容。

新理念——传统被动应对式理念亟须更新

那么，面对如此复杂的网络安全新形势，如何筑牢网络安全新底线？多位与会人士表示，科技工作者和网安企业应摆脱传统被动式建设思路的束缚，不断拓展认知疆域，实践新理念、新思路、新方法、新技术，推动网络防御理念、防御体系、防御技术深度变革。

对此，奇安信集团董事长齐向东在接受记者采访时表示，“过去很长一段时期内，业界普遍认为网络安全不存在‘绝对安全’状态。大家常说，没有攻不破的网络，没有打不透的墙，网络安全攻防相长，漏洞是补不完的。在这种认知之下，很多企业在进行网络安全防护系统建设时，主要针对过去出现过的安全事故，采用相应的防护技术和产品。这样的防护系统却存在极大的安全隐患，因为过去没有发生，不代表未来不会发生。”

据国家互联网应急中心发布的数据显示，2021年上半年全国捕获恶意程序样本数量约2307万个，日均传播次数就高达582万余次。

中国工程院院士吴建平也指出，互联网连接着各种计算机系统以及嵌入式处理器、控制器，涉及海量虚拟信息环境。它们之间一经连接，产生数据交互便构成了不断扩展的拼图并难以分割。面对巨大体量的互联网系统，补丁式、外挂式网络安全防护方法的作用已非常有限。

面对网络安全新形势，变革已势在必行。“只有以‘零事故’为目标，努力穷尽所有可能风险，并一一进行防护，才有可能实现网络安全的万无一失。”在齐向东看来，可将“零事故”作为网络安全建设新目标。“以北京冬奥会为例，自2019年12月26日开始的800多天里，北京冬奥会累计抵御住了超过3.8亿次的网络攻击，最终实现了‘零事故’。”

齐向东将北京冬奥会网络安全工作经验概括为几个方面：以“数据驱动安全”的理念为指导，用自动化、智能化数据分析方法，快速发现网络攻击并溯源攻击者；以“内生安全”的工程方法建设系统，在可能产生攻击的所有网络资产上实现无死角防护监测，再通过监测数据的计算反过来驱动安全防护能力提升；以“经营安全”的理念深度运营，着眼于网络攻防的长期性、多变性、复杂性、突发性，持续增强认知能力、信任能力和安全能力。同时他还将“零事故”归纳为三个标准：业务不中断、数据不出事、合规不踩线。

“如果说过去追求网络‘绝对安全’还是停留在‘奢望’阶段，那么，北京冬奥会网络安全的‘零事故’则把梦想照进了现实。”在北京2022年冬奥会和冬残奥会组织委员会专职副主席、秘书长韩子荣看来，北京冬奥会的“零事故”经验为网络安全保障提供了有益参考。实践充分证明，只要将“零事故”作为目标，努力穷尽所有可能的风险，并一一进行防护，就能满足我们对“绝对安全”的无限追求。

新技术、新生态——守护网络安全

新理念新目标的实现最终还是需要技术的加持。与会人士普遍表示，网络安全行业只有始终将网络安全技术自主创新作为共识才能真正实现安全目标。

韩子荣就表示，“以北京冬奥会为例，只有制定实施全面网络安全战略，构建精细化的网络安全体系，才能夯实网络安全根基，也才能迎来北京冬奥会的成功举办，其中具有独立自主的网络安全技术以及系统体系对安全的保障至关重要。”

除了针对关键信息基础设施的网络安全防护，各类自主创新技术也正运用于网络安全保障的各个方面。据国家密码管理局副局长何良生在2022北京网络安全大会上介绍，从2011年至2021年的10年间，我国椭圆曲线公钥密码签名算法、SM3密码杂凑算法、SM4分组密码算法、ZUC序列密码算法、SM9标识密码算法均已成为ISO/IEC国际标准。“自立自强密码高水平的关键，在于密码基础理论引领研究的原创能力和密码关键核心工程与应用技术领先研发的攻坚突破能力。”

从安全趋势发展看，隐私计算作为重要底层技术近年来也备受关注。隐私计算技术以“原始数据不出域”“数据可用不可见”的方式，对多方数据进行模型计算，让数据价值有效流通，有效保障数据要素流通安全、可信、可控、可管、可溯。

而针对在新形势下如何全面提升网络安全行业的应对能力，通付盾创始人汪德嘉则提出，可将数据安全架构尽快升级到基于区块链与决策智能技术的Web3架构，以便基于区块链技术的分布式存储带来更高的安全性。同时他提出，分布式数字身份（DID）技术的应用也将会对数字安全领域产生深刻变革。“如传统Web2中心化的身份管控面临被黑客单点攻破的风险，基于区块链技术的分布式数字身份应用则会更加安全，对数据隐私的保护也更加全面。同时，分布式数字身份作为联盟链的核心技术，也为数据安全共享提供了更加完善的解决方案。”

总之，唯有不断地自主技术创新才能让网络安全一守到底成为可能。无论是冬奥“零事故”，还是关键信息基础设施安全检测评估安全保护，背后支撑的都是网安产业的持续创新和发展。

正如吴建平表示，为提升“安全性”，需要对涉及网络空间中的前瞻性、全局性、核心性技术问题进行预研和持续研究，针对软硬件领域的不同战略需求和特点，不断向下穿透，在基础理论和关键基础产品上不断壮大自主成果，构建出自主、可控、兼容、创新的互联网体系结构。

但不可否认，行业的技术创新离不开数字化安全新生态的共建共荣。对此，吴云坤表示，这既需要安全圈内的融合，也需要安全与信息化、业务的融合；既需要安全大厂、大平台的创新规划设计牵引，更需要细分领域的安全技术创新来填补空白。因此，面对严峻的网络安全态势，应进一步加强联合共治，强化新理念、新技术应用，筑牢安全屏障。

WEI YUAN SHUO HUA | 委员说话

以数字技术与实体经济深度融合建设全国统一大市场

骆沙鸣

当今世界，最稀缺的资源是市场。市场资源是我国的巨大优势，只有充分利用和发挥这个优势，不断巩固和加强这个优势，才能够为构建新发展格局提供雄厚的基础支撑。聚焦流通共享，以数据要素打通制约经济循环的关键堵点，促进商品要素资源在更大范围内畅通流动，可以加快建设全国统一大市场，全面推动我国市场由大变强。

当前，我国国内市场规模虽然已位居世界前列，商品市场规模优势明显，资本、技术、数据等要素市场规模迅速扩大，但仍然存在技术、数据和市场等“大而不强”现象，集中表现为市场发展不平衡，要素和资源市场发展相对滞后，市场分割问题尚未解决，商品和服务市场仍难以满足消费升级需要，市场体系长期存在制度规则不统一，要素资源流动不畅，超大规模市场对技术创新、产业升级作用发挥还不充分等问题，进而直接影响了我国市场功能的发挥。

而数字赋能主体实力不强、数字赋能客体动力不足、数字赋能原创能力不高、数字赋能传导机制不畅和数字赋能渗透程度不深，同样制约着全国统一大市场的快速建设。应加快数字技术与实体经济深度融合，发挥数实融合新优势助力全国统一大市场建设。

首先，应进一步强化数字赋能产业转型升级和实体经济高质量发展的作用，拓展数字赋能领域，提升数字赋能效益和全要素生产率，让市场数据资源配置效率和整体经济效率更高；同时打造丰富优质的数据平台、开放高能的算力平台和先进适用的算法平台，筑牢构建国内统一大市场的赋能之基；充分发挥工业互联网平台全要素、全产业链、全价值链的链接优势，实现更大范围的资源配置、更高效率的协作分工。

其次，数字技术在金融业的应用推动数字金融、普惠金融更好服务实体经济，完善多层次资本市场融资功能，形成全国统一的社会信用体系和市场监管体系。这样不仅能为更多创新型中小微企业增信，还能为大市场建设提供法治市场环境；同时可运用物联网和遥感技术掌握企业生产经营全链条“数字足迹”，提高信贷融资可得性、普惠性、渗透性，全面提升融资服务质量和改善消费环境。

此外，还可通过重点突破产权保护、市场准入、公平竞争、信用立法等构建全国统一大市场制度的基础，推动我国数据价值产品化、服务化，促进数据、技术、场景深度融合，满足全国各领域各产业数据需求和全国大市场建设的数据需求。如设立数据交易流通场所，探索数据治理新机制。充分利用大数据等技术手段，加快推进智慧监管，提升市场监管政务服务、网络交易监管、消费者权益保护、重点产品追溯等方面跨省通办、共享协作的信息化水平，进一步提升市场主体的信任度。

而针对中小企业，可立足内需，畅通循环，加强顶层设计和贯标工作，进一步完善中小企业数字化生态体系和统一大市场标准体系，建立更齐全的产业联盟、共享数据库与成果共享市场。以产业链、供应链、创新链、价值链构建更广泛的数据“朋友圈”，构建自信高尚、注重品质、自由公平的市场经济文化环境，营造更安全可靠的中小企业数字经济网络体系和数字贸易营销体系，有效降低全社会物流成本和市场交易成本，提高市场运营效率和资源配置效率。

总之，应努力构建一个“融合共建、协同共治、安全共享、创新共赢”的数字生态，建立城乡统一的土地和劳动力市场、数据市场、生态环境市场和要素资源市场，以深化政务数据与社会数据融合应用建设数字经济产业链和市场供应链为重点，推动数字技术与各产业深度融合，推动我国国内大市场数字应用场景更为丰富，释放更大的市场消费潜力，激活统一大市场活力。

（作者系全国政协委员，台盟中央常委、泉州市政协一级巡视员）

贷款利率下降0.35个百分点：

上半年普惠型小微企业再受益

本报讯（记者 王金晶）小微企业是国民经济的重要组成部分，融资支持是小微企业健康发展必不可少的一环。做好小微企业金融服务，是稳增长、调结构、稳就业、惠民生的重要举措，是监管部门服务实体经济、服务人民群众根本利益的重要体现。

近日，银保监会公布了上半年银行业保险业运行、普惠金融最新发展等情况。据介绍，截至6月末，我国银行业金融机构总资产360.4万亿元，同比增长9.6%；保险业总资产26.6万亿元，同比增长11.1%。其中，银行服务实体经济信贷投放力度加大。上半年，人民币贷款新增13.7万亿元，同比多增9192亿元，增速11.2%。

强化普惠领域金融供给，持续增量也在逐步扩面。据公布数据的显示，全国小微企业贷款余额55.84万亿元，其中普惠型小微企业贷款余额21.77万亿元，同比增长22.64%，较各项贷款增速高11.69个百分点；有贷款余额户数3681.33万户，同比增加710.02万户。上半年全国新发放普惠型小微企业贷款利率5.35%，较2021年全年下降0.35个百分点。

今年以来，银行业金融机构聚焦重点领域精准发力，改进贷款服务方式，缓解小微企业融资周转难、缺抵押、期限错配问题，从公布的数据来看，6月末小微企业续贷、信用贷、中长期贷款余额分别同比增长29.46%、30.11%、17.22%，个体工商户贷款余额6.74万亿元，同比增长18.25%。

从银行业金融机构信贷资产情况来看，质量基本稳定，风险抵补能力整体充足。6月末，银行业金融机构不良贷款余额3.8万亿元，不良贷款率1.77%，较年初下降0.05个百分点；保险业务也保持平稳发展。1—6月，保险公司原保险保费收入2.8万亿元，同比增长5.1%。保险业赔款支出与给付累计7768亿元，同比增长3.1%。

解决小微企业融资难、融资贵问题，需要发挥各方合力，坚持不懈、久久为功。据悉，下一步银保监会将继续引导银行业等金融机构加大服务小微企业力度，努力实现小微企业金融服务高质量可持续发展。

YE JIE GUAN CHA | 业界观察

筑牢数字安全长城新举措：我国数据跨境有法可依

本报记者 孙 琳

“据测算，2021年我国大数据产业规模达1.3万亿元，逐渐步入高质量发展阶段。”在近日举行的第五届数字中国建设峰会新闻发布会上，据工业和信息化部信息技术发展司副司长王建伟介绍，近年来工业和信息化部出台了《“十四五”大数据产业发展规划》，加快信息基础设施建设，开展行业示范应用，打造产业集群，取得了积极进展。其中，我国数据资源极大丰富，总量已位居全球前列。

数据作为数字经济的核心要素，不仅成为企业竞争力的核心，也成为国家之间争夺的重要战略资源。而随着数字经济的蓬勃发展，数据跨境活动日益频繁，数据处理者的数据出境需求也快速增长。但同时，由于不同国家和地区法律制度、保护水平等的差异，数据出境安全风险也相应凸显。“数据跨境活动既影响个人信息权益，又关系国家安全和社会公共利益，亟须建立健全数据跨境管理规则”的声音由来已久。

近日，国家互联网信息办公室正式公布《数据出境安全评估办法》（以下简称《办法》），就个人信息和重要数据的出境安全评估管理措施提供具体的法律解决方案，明确了数据出境安全评估的目的、原则、范围、程序和监督机制等具体规定，并明确指出数据出境活动主要包括“数据处理者将在境内运营中收集和产生的数据传输、存储至境外”以及“数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用”。

在国家工业信息安全发展研究中心总工程师黄鹏看来，《办法》立足维护国家安全和社会公共利益、保护个人信息权益，构建了我国数据出境安全评估的制度，将事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障了数据依法有序自由流动。

相关行业企业也对《办法》的及时出台给予肯定，“《办法》的出台不仅对网络安全法、数据安全法、个人信息保护法等法律法规中‘出境数据安全评估’规定作了进一步细化落实，也进一步规范了数据出境活动。《办法》实施后，相关监管要求和细则将更加明确，对于相关企业来说对数据安全的整体建设思路也会更加清晰。”明略数据相关负责人表示，明确监管细则后，企业也亟须补短板，做到优先保障数据安全基础防护。

更值得一提的是，评估决定2年有效期的规定可以保障企业参与全球数字经济建设的持续性和连贯性。《办法》第十四条明确安全评估结果有效期为2年，意味着数据处理者可以申报2年内对特定境外接收方的数据出境计划，极大方便企业开展连续性数据出境业务，促进全球数字经济发展。

对此，中国科学院科技战略咨询研究院系统分析与管理研究所副所长、研究员孙晓蕾认为，面对复杂的国际形势，我国出于维护自身数据安全的需要，对于数据出境，不仅对数据处理者，还要对数据接收者进行管理是极其必要的。特别是，境外接收方所在国家或者地区的数据安全保护政策法规及网络安全环境对出境数据安全的影响，以及境外接收方的数据保护水平是否达到我国法律、行政法规规定和强制性国家标准的要求，应是评估重点。

显然，数据跨境流动已成为数字经济时代的数据价值最大化的必然趋势。业界普遍表示，值得期待的是，在企业意愿和市场需求刺激下，数据安全服务市场或将迎来更大市场发展空间。