编者按

数字经济正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。习近平总书记强调，我们要结合我国发展需要和可能，做好我国数字经济发展顶层设计和体制机制建设。要加强形势研判，抓住机遇，赢得主动。

“网络安全牵一发而动全身”“没有网络安全就没有国家安全”，要做强做优做大数字经济，就必须将安全放在第一位。如果不能保障数字安全，规模再大的数字经济，可能都会像是建在沙滩上的高楼——楼越高，风险越大。

在数字时代，由于对手、场景等发生了变化，数字安全面临新挑战，传统的应对之策已不奏效。我们必须尽快转变对数字安全工作的指导思想，用新的数字化思想应对新的安全挑战。为此，六位来自不同界别的全国政协委员就建立新时代的数字安全建言献策。

委员眼中的数字安全

全国政协委员、经济委员会副主任毕井泉：
应高度关注数字经济领域知识产权保护

近年来，以大数据、人工智能等新技术新业态为代表的数字经济，正在重组全球要素资源，重塑全球经济结构。2020年，我国数字经济规模已达到39.2万亿元，占GDP比重达38.6%，为经济高质量发展注入了新的活力，给数字领域的知识产权保护提出了新的要求。

多年来，中国互联网企业大多走的是“免费发展用户，有了用户以后做广告”的商业模式，而不是靠软件自身销售获利，根源是我们对软件的知识产权保护不够，这也导致很多基础性软件、专用软件很少有国内企业研究开发，而主要依靠国外厂商提供，这存在很大的安全隐患。只要这些软件受制于人，我们就很难做到数据的安全，也很难做大做强我们的数字经济。

鼓励软件的研发，就必须加强包括软件在内的知识产权保护，打击侵权盗版，努力营造一个使用正版软件的环境，激发企业自主创新，实现高水平自立自强，把发展数字经济自主权牢牢掌握在我们自己手中。

发展数字经济，首先要界定数据权属，保护数据所有者的权益。有了这个前提，才有数据开发和利用、数据流动和交易。数据所有人还要承担隐私保护的责任。与此同时，我们也要积极参与数字经济国际合作，鼓励数据跨境流动。要主动参与国际组织数字经济议题谈判，开展双多边数字治理合作，维护和完善多边数字经济治理机制。

企业是创新的主体。对于数字安全领域企业，应当实行“谁使用谁付费、谁委托谁付费”的原则，实现数字安全企业的可持续发展。

全国政协常委、提案委员会副主任赖明：
护航数字经济 做强做优数字安全是首位

今年1月，《求是》杂志发表习近平总书记重要文章《不断做强做优做大我国数字经济》。从标题我们就可以深刻体会到，我国要实现数字经济的高质量发展，不仅要“做大”，更要“做优”，最重要的是要“做强”。我国数字经济目前仍处在大而不强、快而不优的阶段，整体规模虽然已经比较“大”了，但是在结构上仍然欠“优”欠“强”。如，依赖互联网经济的“人口红利”，在一些日常生活领域方面做得比较多，但是在产业数字化等方面做得却远远不够，工业、农业数字化转型相对滞后，“消费端”较为成熟、“创新端”相对薄弱。据有关数据显示，2020年我国电子商务交易额达到37.2万亿元，2021年预计超过40万亿元。当然，不能简单地说我们卖东西就不“优”，但从国家层面而言，仅有这个“优”还远远不够，我们还要在结构优化强化方面下功夫。

值得关注的是，在数字经济的快速发展过程中，也出现了一些不健康、不规范的苗头和趋势，这不仅影响数字经济的健康发展，而且对国家经济金融安全等构成了威胁，必须坚决纠正和治理。如，在数字安全方面，可以说我们早年基本上处于“裸奔”状态。个人去了哪里、干了什么、喜欢什么、想看什么，这些信息在互联网上能轻易地被他人获得；尤其是对于企业甚至国家而言，“谁进来了不知道、是敌是友不知道、干了什么不知道”。“聪者听于无声，明者见于未形”，这种情况必须引起高度重视。

习近平总书记强调，“没有网络安全就没有国家安全”。近年来我国网络安全创新发展取得积极成效，网络安全法、数据安全法、个人信息保护法、《关键信息基础设施安全保护条例》等相继出台，人民群众拥有了更多获得感、幸福感、安全感。在新发展阶段，我们必须全面理解、科学把握、系统推进，统筹抓好发展与安全。如果没有国家安全，经济、社会、政治、文化等方面的发展都是一句空话。做强做优做大数字经济，必须将安全放在第一位，必须首先筑牢数字安全屏障。如果不能保障数字安全，数字经济就如建在沙滩上的高楼，稍微有个风吹草动就可能会倒塌。

筑牢数字安全屏障，既是技术命题，也是治理考题。对于如何做好数字安全方面的工作，有以下几个方面的建议：

一是要尽快提高全社会对数字安全重要性的认识。数字安全很重要，但不是所有人都认识到位，甚至有不少个人和单位不知道、不觉得这是一个重要问题，重发展轻安全、重建设轻防护，没有忧患意识、底线意识，这是非常危险的。“网络安全为人民，网络安全靠人民”，必须加大数字安全知识普及和教育，尽快提高全社会的数字安全意识。

二是要及时制订和完善数字安全配套法律法规。由于数字经济、网络社会发展速度非常快，相关法律法规相对滞后。要尽快提高我们的数字管理能力、治理能力和治理水平。随着网络安全的威胁来源和攻击手段不断变化，要做到关口前移，防患于未然，即使新问题出来后短时间没有法律法规可依，也要及时让监管跟上企业创新的步伐，以技术管技术，让数字经济发展步入正轨。

三是要及时出台一些财税方面的政策，支持数字安全企业做强做大，让它们有能力为中国数字经济发展护航。企业直接面向市场，处在创新第一线，让企业持续健康发展，既是企业家奋斗的目标，也是国家发展的需要。在数字安全方面实施更多的专项，增加更多的投入，无疑是值得的。

四是要鼓励核心技术、关键装备、重要软件的自主创新，充分发挥我国超大规模市场优势和新型举国体制优势，打好关键核心技术攻坚战，着力构建自主可控、安全可靠的信息技术体系，尽快实现高水平自立自强，把发展数字经济自主权牢牢掌握在我们手中。

全国政协委员、社会和法制委员会副主任陈智敏：
要尽快转变数字安全工作的思路

近年来，国家出台了一系列关于数据安全和网络安全的法律法规，包括网络安全法、数据安全法和个人信息保护法等，基本解决了网络安全和信息安全面临的突出问题，但还有两大问题需要解决。

首先要尽快转变数字安全工作的思路。现在的互联网安全保障机制、打击能力、作战体系、破案要素，都是围绕互联网自身安全进行的。这套思路虽然对过去以互联网安全、关键信息基础设施安全为主是有效的，但是在数字经济时代，维护数据安全的对手、场景、要素等都发生了变化，这套技战法已不完全适用。

因此，要尽快转变过去机械论的思维方式，用控制论、信息论和系统论思维，来考虑数字安全或者数据安全问题，从工作思路、领导指挥、力量组织、作战样式、体系协调、标准规则制定等方面做出调整。

与此同时，我们对数据的本质属性，对数据在数字经济社会中的地位作用，认识还需要深化。

第一，数据是信息文明时代或数字文明时代，一切科技革命和产业革命的基础。物联网、5G、区块链、人工智能等，全部建立在数据基础上。数据是一个基础性的基础。

第二，数据是信息文明时代或数字文明时代的战略资源和社会财富，是持续增长不可或缺的生产资料。我们对这个问题的认识，之所以很难形成共识，关键是思维方式没有完全从传统的工业文明和农业文明对财富的认识中走出来。

第三，信息文明时代，数据的本质属性是生产关系、经济关系、社会关系和人与人之间的关系。表面上是数据，实质上是各种关系，所以它涉及国家安全、政治安全和公共安全。

这“三个认识”不到位，带来的一个重大问题，就是数据权属问题。即数据应该归谁所有、归谁使用，生产出来的财富应该归谁拥有、应该如何分配。数据权属如果不明确，将带来了一系列的安全风险、挑战，甚至威胁。

数据权属这个根本性问题，已经到了必须回答的时候，回避不了、绕不过去了。特别是从消费互联网到工业互联网、产业互联网过渡的过程中，数据权属问题必须从法律上进行明确，必须回答好以下几个方面的问题：

第一，随着数据的无序生长，大量的数据分散掌握在各部门、各企业手中。谁可以收集、谁可以掌握、谁可以控制、如何使用，必须从法律层面予以明确。

第二，要采取措施防止数据垄断造成不公平竞争和数据资源的使用不充分。数据是战略性的基础资源，任何企业和平台对数据的采集，不得超过必要的限度。

在数据确权的过程中，必须遵循几个原则：第一，和人权、物权一样，数据权也是公民的基本权利；第二，国家对于数据具有发展、管理、调控、流向、境外审查、保护、依法处置等权力；第三，企业将孤立分散的数据开发出的有价值的产品，可以进入市场进行等价交换，国家应该保护企业的合法权益。

数据的权属应该是全民共有共享。互联网的性质是互联互通，大数据共有共享，决定了大数据的权属是全民共有。而数据产生的经济效益也应全民共享，因此数据共有应该是国家代表管理，国家对数据统一调查，掌握其底数最为关键。

最后，应明确公民向国家和企业提供数据的义务，明确国家和各级政府公开相关数据的义务，明确数据在企业之间相互流动的规则和权益，明确数据产生的经济效益的分配方式，这样才能让数据在合规流动中发挥出最大价值。

全国政协委员、经济委员会副主任刘世锦：
数字安全问题研究要齐头并进

数字经济发展和数字安全相伴而生。在深入研究数字经济未来发展的同时，也要更加深入地研究数字安全问题。只有解决了数字安全问题，数字经济才能够做强做优做大，个人、企业、国家才能安全发展。

数字经济发展起来以后，把过去很多碎片化的东西通过网络连接起来，给我们带来了各种各样的便利，促进了社会的进步。与此同时，随着数字技术和实体经济的深度融合，城市数字化程度虽然越来越高，也在一定程度上导致城市的韧性下降。比如，在紧急状态下，某些大的冲击就会让城市断水断电断气。因此可以说，在数字技术推动社会进步的同时，也会导致城市的脆弱性增加。

我们常说，在数字经济的发展过程中，互联网犹如是一个通道，5G是一条高速公路，大数据则是原材料，云计算、云平台相当于仓储，人工智能利用数据生产出大量的新的、信息量更大、功能更强的数据。人工智能在不断演进升级，虽然整体能力现在还达不到人脑水平，但在有些方面，如计算能力等方面已经大大超越了人的能力。这方面的典型例证，就是AlphaGo轻而易举地就打败了围棋世界冠军。而人工智能发展到一定程度后，物理世界和数字世界高度融合，数字化渗透率、沉浸程度越来越高，也会带来一系列新的安全问题，都需要更多的关注和研究。

针对数字安全问题，一批信息安全企业作出了很多贡献，同时也要看到，做好数字安全工作方面需要长期、专注的投入和研究攻关，市场化的民营企业在这方面有着独特优势。可以预见，未来随着数字世界和实体经济的高度融合，数字安全问题会更加突出，因此应更多鼓励相关领域企业有意愿有信心推动数字安全方面的突破和创新。

值得关注的是，近年来国际数字贸易发展飞速，成为国际贸易和经济增长的新引擎。据测算，2020年我国可数字化交付的服务贸易规模达到了2947亿美元，占服务贸易总额的44.5%。预计到2025年，中国可数字化的服务贸易进出口总额将超过4000亿美元，占服务贸易总额的比重将达到50%左右。

在国际数字贸易中，一些已不经过海关或不完全按海关的原有程序在进行。很多规则不是国家事先制订出来，而是企业之间做交易的过程中自然形成的。在数字经济时代，数字贸易规则究竟应如何构建和实施，如何确保数字贸易规则的透明度及其在未来的可操作性，如何平衡个人隐私保护和跨境信息自由流动、保护知识产权，这些问题逐渐成为各大经济体谈判中的焦点问题，也需要进一步深度研究。

与此同时，我们还可以看到，在数字经济时代，传统物理意义上的国家边界正在弱化。那么，数字世界的边界究竟在什么地方，它的治理模式是什么，这些问题都亟待研究和探讨。

全国政协常委，中国税务学会副会长张连起：
国家应更多支持数字安全领域骨干企业

面对百年未有之大变局，我国必须统筹发展和安全，把安全贯穿到国家发展的各个领域和全过程，筑牢国家安全屏障。其中数字安全可以称为是数字经济的底座，只有做好了安全保障，我们的数字经济才能发展得更好、走得更快、走得更远。

习近平总书记指出，要完善数字经济治理体系。要重点加强数字经济安全风险预警、防控机制和能力建设，实现核心技术、重要产业、关键设施、战略资源、重大科技、头部企业等安全可控。

应让数字安全领域的一些骨干企业尽快成长起来，更多地承担起增强国家战略安全能力的责任。因此，国家应从战略高度更多更好支持这些数字安全领域的骨干企业发展起来，把数字安全产业链、价值链、创新链整合起来。

而数字人才作为数字经济的核心要素，在数字经济发展中起着重要支撑作用。数字人才质量、存量与储备量之争，已成为综合国力和区位竞争的重要方面。数字安全顶尖人才也是数字安全企业打造核心竞争力、实现高质量发展的关键。我们应更多聚焦数字安全企业、聚焦人才政策的激励和认定，出台更多相关激励政策，加快建设素质高、结构优的数字安全人才队伍。

必须看到的是，目前我国在财税、金融等方面对数字安全企业的支持力度还不够，很多政策都是普惠性的，更多的是撒芝麻盐，不够点对点、不够精准。既然数字安全这么重要，建议应在财政、税收、购并、个人所得税等方面给予支持，让企业有更多的获得感。

比如，对于数字安全领域的龙头企业，可以率先出台一些点对点的政策，支持它们做强做大。比如引导国家主权基金、头部股权投资基金，加大对数字安全企业投资力度；综合运用贴息、奖补、增信等“组合拳”，让企业没有资金担忧，可以轻装上阵，专注于安全方面的创新发展；另一方面，作为信息安全企业，可在加大自主创新、抢占技术制高点、夯实自身“护城河”的同时，更多讲好数字安全的故事，要让更多的人知道做强做大数字安全企业的重要性和迫切性，从而为企业发展营造良好的氛围。

全国政协委员，360集团创始人周鸿祎：
应对数字安全挑战 国家需顶层规划

未来，数字化对安全带来的最大挑战是什么？我认为，这表现在：万物互联，一切皆可编程，数据将驱动业务，软件将重新定义世界。也许，在未来10年，所有企业都将转型为数字化企业，政府部门转型为数字化政府。数字经济将成为我国GDP的主要贡献者。

比如，以往汽车没有安装任何软件就可使用，但现在智能网联车主要是靠软件才可以运行。传统工业企业、关键基础设施，过去跟软件没有任何关系，现在工业互联网、关键信息基础设施都需要软件来定义、作用和使用。但与此同时，一切皆可编程后，一旦软件出现漏洞，就会出现不可避免被攻击的情况。

从这个层面来看，传统产业被数字化之后，被攻击的风险也会随之加大。如物联网打通了物理世界和虚拟世界，过去在虚拟世界里的犯罪、攻击，今天都可以通过物联网、工业互联网变成对物理世界的伤害。这几年，已经陆续出现了网络攻击造成工厂停工、医院停业、电力站停电的事件。而在360研究智能网联车后也发现，黑客会通过入侵智能网联汽车的云端、车企端操控汽车的运行，由此带来的巨大社会风险也许会超出我们的想象。

也许在未来，所有的公司都会变成互联网公司，大数据驱动业务，因此一旦数据遭到破坏，公司业务就会被迫停止，而对于数字政府来说同样面对巨大风险，未来政府部门的数据、关键基础设施的数据，都可能被攻击，从而造成服务中断或基础设施的停摆。

诚然，数字化给我们带来美好生活，但与此同时，我们不可否认这也会将整个世界置于一个更加脆弱的位置。可以预见，今后的网络犯罪，小蟊贼掀不起大风浪，但是两个新角色的登场，将对网络安全带来巨大的挑战。

首先是对手的变化。过去安全公司对付的是一些黑客、恶作剧、木马、盗号或者欺诈网站，都是小规模黑色产业。现在不仅出现了拥有先进网络专家的犯罪组织，而且各个国家还成立了专业的网络战部队。高级别对手进来之后，会催生网络攻击高级别技术的诞生和使用。像水电气等民生基础设施数字化之后，一旦遭到攻击带来的后果则不堪设想。

二是数字化场景变得更复杂。工业互联网、能源互联网、智慧交通、智慧城市、车联网等更多复杂的数字化场景可能遭到网络攻击。云计算、大数据、人工智能、区块链、物联网、5G通信等新技术的广泛使用，对网络安全提出了更大的挑战，传统的打补丁、“头痛医头、脚痛医脚”的解决网络问题的方法，已经很难应对数字化时代的网络安全问题。在新的数字化技术、数字化场景下，必须用新的数字化思想指导，提出新的战法，建立新的数字安全体系。

可以看到，随着数字技术和实体经济的深度融合，未来数字安全领域将面临更大的挑战。为应对这一严峻挑战，有四点建议：一是国家从顶层设计出发，把数字安全纳入新基建，超前布局和投资，打造国家级分布式安全大脑。二是以安全能力成熟度评估体系为抓手，推动安全从合规导向走向能力导向。三是参照集成电路行业，从税收减免、科研技术、项目资金等角度，打破体制机制和所有制限制，为数字安全企业攻克“急难关卡”技术提供综合支持，特别是为突破国外技术封锁和制裁提供定向扶持，打造数字安全体系。四是在涉及国计民生的重点行业、关键领域明确安全投入的占比，加大安全投入，带动更多社会资本进入。