通往创新之路

全国人大代表许立荣：全球供应链紧张状态下要为中小企业提供便利

本报记者 裴昱 北京报道

当全球新冠肺炎疫情给大部分行业的发展前景蒙上一层朦胧的阴影时，世界范围内的海运企业却交出了几乎是有史以来最亮眼的成绩单：丹麦全球航运巨头马士基（MAERSK）2021年全年实际利润240亿美元；中国央企中国远洋海运集团下属上市公司中远海控预计2021年净利润同比增长799.3%。

亮眼业绩的背后，是人们对全球供应链紧张状态的担忧。集装箱一箱难求、海运价格上涨，在过去的一年多时间中，成为中国外贸企业的主要压力之一。稳外贸与保持供应链稳定成为一个问题的“一体两面”。

十三届全国人大五次会议期间，全国人大代表，全国人大外事委员会委员，中国远洋海运集团有限公司原董事长、党组书记许立荣接受了《中国经营报》记者的专访。根据他的判断，在未来一段时间内，运力短缺的局面仍将持续。不过，他也告诉记者，包括中国远洋海运集团在内的航运企业，都在设法为中小企业订舱提供便利条件，以解决企业面临的实际困难。

许立荣相信，当疫情稳定下来、地缘政治因素影响逐渐消退后，全球供应链将重新回到稳定状态。“对于船东来讲，是不希望价格暴涨暴跌的。”在专访过程中，他向记者强调。

《中国经营报》：乌克兰局势给世界经济贸易造成了一定影响。如果当下的局面再持续一段时间，对航运和全球供应链会带来哪些影响？

许立荣：乌克兰出现紧张局势后，美国联合一些西方国家制裁俄罗斯。一方面，会对俄罗斯本国的经济、贸易、航运等带来影响，部分欧洲国家拒绝悬挂俄罗斯船旗的船舶停靠，部分港口禁止接载俄罗斯进出口货物，并加大对俄罗斯货物查验力度；部分国际大型班轮公司也宣布暂停俄罗斯货物的预订服务等。

另一方面，制裁实施后，还会对全球重要的港口、主要的航运企业，以及中转贸易带来影响。

当前油价上涨，创下十多年以来的新高，布伦特原油期货也创下2008年以来新高，这会增加所有航运企业的成本。如果按照这个趋势计算，对中远海运这样体量的公司来说，一年要增加80亿至90亿元人民币的燃油成本。对航运企业而言，接下来要考虑应对高油价的办法。

此外，俄罗斯和乌克兰是全球粮食和能源的重要出口国。乌克兰当前局势和西方国家对俄罗斯的制裁，会造成粮食和能源价格的进一步上涨，加剧通货膨胀，这对整个下游产业的影响是很大的。

这些地缘政治因素，可能在一定程度上改变贸易流向。从全球供应链的角度看，供需矛盾仍未解决，一些港口的拥堵情况可能还会加剧，航运运力紧张的局面仍将延续。这些影响才刚开始，慢慢地会逐步显现出来。

全国人大代表，全国人大外事委员会委员，中国远洋海运集团有限公司原董事长、党组书记许立荣

《中国经营报》：这些因素叠加，会造成航运价格进一步上涨的情况吗？

许立荣：航运价格处于历史高位是市场竞争的结果。疫情暴发后，供需矛盾更加突出，人工短缺导致供应链效率下降，使得全球的集装箱有效运力减少了17%～20%。然而，世界对中国制造的需求依然旺盛。据海关统计，今年前两个月，我国进出口贸易仍然保持两位数增长。同时，新船可能要到2023年下半年才能投入使用，这意味着今年基本没什么新增运力。而且，航运企业在经历了长时间的痛苦期后，在疫情出现的初期阶段，下新船订单也是比较谨慎的，不会像过去那样大规模造船，这些都是历史经验决定的。

对于船东来讲，是不希望价格暴涨暴跌的。在经历过这么多历史曲折后，我们更看重长期稳定的合同，保持航线稳定。去年和中远海运签订了一年合同的企业，基本不受运价上涨的影响。但是，在现货市场上，由于供需矛盾比较突出，一些中间环节进一步推高了价格；对比疫情开始前，主要船型的船舶租金已经涨了10倍多，加上一些没有航运背景的市场参与者加入，进一步推高了船舶租金，这些都会对客户最终支付的运价造成影响。

《中国经营报》：地缘政治因素对货物贸易和供应链的影响很大，航运企业该如何应对这些外部不确定性带来的影响？

许立荣：这些问题比较复杂，每家航运企业采取的措施可能都不一样，要根据自己的情况妥善应对。总体来说，有些共性的问题是大家都要想办法解决的，特别是成本上涨。面对油价高企，可以通过寻求清洁替代能源、优化采购策略和加油计划等方式应对。

《中国经营报》：美国洛杉矶港和长滩港的货物滞留费一再推迟征收，你认为，这一惩罚性的费用是否会真的收取？这对中国的出口企业和航运企业会有怎样的影响？

许立荣：美国的港口很清楚目前集装箱堆积的问题出在哪里，针对航运企业征收惩罚性费用并不能真正解决现在的问题。受疫情影响，美国国内劳动力短缺，陆路运输也受到影响，港口效率大幅度下降。虽然今年的情况比去年有所好转，但是没有很大的改变。

现在我们能看到，由于中国疫情防控效果明显，部分制造业回流中国，中国制造的优势还会充分显现，在未来一段时间内，运力短缺的局面仍将持续。可能要等疫情结束，回归常态，美国的政策也相应转变，提高港口效率，这些问题才会真正得以解决。

对航运企业来讲，一方面要加大长协合同的比例。另一方面，中远海运也响应国家稳外贸的政策，为中小企业提供了很多通道，比如开通网上订舱平台、开通中小微企业服务专线、举办中小微企业专场对接会，以及利用航运区块链技术提供无纸化放单服务，提升服务效率。

《中国经营报》：习近平总书记提出建设海洋强国，你认为应该如何扩大中国的航运话语权？

许立荣：谈到话语权，首先要明确一个问题，规模和垄断不是一回事。中远海运从综合运力上讲是世界第一，集装箱运力排世界第四，但是我们在中国进出口贸易中的集装箱承运量不足20%；在跨太平洋航线上，中远海运的市场份额排名第一，但是也只占16%。因为航运是全球监管最严厉的行业之一，单一市场份额超过30%就构成垄断，将面临全球监管机构的处罚。

航运企业要做大做强，首先要有规模，但这个规模不是垄断。规模的做大，要在符合法律和监管的要求下通过市场发展，这才符合我们国家海洋强国战略的要求。目前，我们走出了一大步，大企业要有引领作用，但还要在“做强”上继续努力。

全国政协委员周鸿祎：以能力导向代替合规导向，确保产业数字化安全

本报记者 裴昱 北京报道

在一切皆可编程、万物均要互联的当下，所有数字化场景所面临的安全问题，早已经超出了简单的网络安全的范畴，渐趋成熟的5G应用所推动的工业级、城市级的数据链接，让虚拟世界与现实世界联通，虚拟世界的攻击由此可以对物理世界产生伤害。

作为全国政协委员、360创始人的周鸿祎深知这一问题的重要性，他总是通过各种方式提醒，如今安全风险几乎遍布所有的数字化场景，已经突破了计算机安全、网络安全的范畴，上升为数字安全问题，监管部门、企业机构，甚至是社会个体，都必须意识到这种变化带来的重大影响。

全国政协十三届五次会议期间，周鸿祎接受了《中国经营报》记者的专访。他表示，数字化新技术、新应用的产生，导致简单安全问题升级为复杂安全问题，因此，要面向新型数字技术和应用场景，研究建设前瞻性的数字安全平台体系，企业则要以能力导向代替合规导向，夯实产业数字化的安全底座。

《中国经营报》：随着5G、AI等技术的发展，数字化的应用场景越来越广泛，你认为数字经济时代最大的安全挑战是什么？和过去有什么不同？

周鸿祎：进入数字化时代，首先明确一点，最大的安全威胁来自大型的网络攻击，小毛贼、小木马基本上还有，但不成气候。值得注意的是，数字化时代，这种网络攻击造成的威胁已从虚拟世界拓展到现实世界，对城市安全、产业升级、科技创新、社会稳定带来严重隐患。安全风险也已经突破计算机安全、网络安全的范畴，升级为数字安全。数字化有三个特征，即一切皆可编程、万物均要互联、大数据驱动业务，其本质是软件重新定义整个世界。在这种趋势下，虚拟世界与现实世界交织融合，过去针对虚拟世界的攻击会伤害到现实世界。还有大数据驱动业务，数据也可能变成被攻击的对象，过去数据主要起到存储的作用，现在数据一旦瘫痪，就意味着业务歇菜了。

具体来看，产业数字化已经深入各行各业，安全风险遍布所有数字化场景。互联网发展进入下半场，主题是产业互联网，主角是政府和传统企业。随着产业数字化的发展，安全风险也遍布关键基础设施、工业互联网、车联网、能源互联网、数字政府、智慧城市等各大场景。由此，数字化的安全威胁已经超越虚拟世界，延伸到了现实世界，影响国家、国防、经济、社会乃至人身安全。去年，美国最大的油管公司遭受勒索攻击，导致18个州进入紧急状态。

数字化新技术、新应用的产生，会导致简单安全问题升级为复杂安全问题。随着大数据、云计算、人工智能等大量新技术的使用，除了网络安全外，还面临着大数据安全、云安全、供应链安全、区块链安全等一系列新的复杂安全挑战。以大数据安全为例，360公司每年接到并处理的勒索攻击事件多达4000余起，受害企业面临着重要数据资产被盗和泄漏的严重后果，轻则造成业务停顿，重则被迫缴纳巨额赎金。

《中国经营报》：中国出台了《数据安全法》《个人信息保护法》等法律法规，你认为这对数据安全能起到多大的保护作用？

周鸿祎：《数据安全法》《个人信息保护法》等法律法规施行，不仅对掌握数据的互联网企业有影响，也将对正在进行数字化转型的政府、传统企业产生巨大影响，因为未来数字化的主角就是它们，智慧城市、智能汽车和工业互联网等都将由数据驱动业务。因此，所有相关企业都要尽到保护数据安全的义务与责任。

首先，要明确自己所处行业属性以及核心业务是否涉及关键信息基础设施，如果涉及，则需要从严执行《网络安全法》《数据安全法》，并开展以《网络安全等级保护条例》《关键信息基础设施安全保护条例》为基础的安全管理工作，所有工作都要留痕记录。

其次，对于涉及关键信息基础设施的企业在申请海外IPO或者已经完成海外IPO的要定期开展数据安全审查，提交相关材料，涉及任何数据跨境传输的行为要申请通过后再进行。

全国政协委员、360创始人的周鸿祎

再次，个人信息收集是国家管控的重点，相关企业需要按照《个人信息安全规范》《个人信息保护法》《数据安全法》等相关法律法规进行数据安全治理工作。

最后，相关企业要结合自身业务所处的行业、城市的细分要求开展相关数据安全审查工作。

《中国经营报》：近几年，国家在网络安全、数据安全上的投入不断扩大，你如何评价这种投入和效果？

周鸿祎：国家这两年的投入确实在加大。在总体安全观的指引下，安全相关法规密集出台，政策体系不断完善。从个人信息保护到关键信息基础设施安全保护，从网络安全审查到大数据安全管理，涵盖数字安全各个领域的重要制度相继建立。

从产业角度看，近年来网络安全产业体系逐步建立，产业规模井喷式发展，随着我国新型基础设施建设的全面铺开，新技术新场景驱动的安全需求与日俱增。信通院数据显示，2020年我国网络安全产业规模达到1729.3亿元，较2019年增长10.6%。2021年产业规模约为2002.5亿元，增速约为15.8%。

同时，安全企业综合实力显著提升。一是从事安全的企业越来越多，已经达到近3000家，年新增200多家；二是我国安全企业的国际影响力日渐加深，在漏洞挖掘、攻防竞赛、技术认证等方面认可度逐渐提升。

我认为网络安全的市场还有很大空间。目前的投入大部分用来买硬件，也有一部分钱买了软件。但网络安全的实战和对抗能力是非常重要的，现在还要解决大数据安全的问题、解决云安全的问题，所以要引入一些专业的服务团队，同时国家要对数字化安全体系进行规划。

《中国经营报》：企业如何在越来越严格的数据安全监管环境下实施经营行为，达到合规与效率的平衡？

周鸿祎：我们必须认识到，未来大数据不仅是重要的生产资料、生产资源，也是重要的攻击对象，一旦数据遭到攻击，企业、机构业务就将停摆。现在，国家在这方面也做好了立法的准备，企业要根据相关法律法规、标准规范要求，采用相应的制度、技术手段和产品保护数据安全，这既是对国家和社会运行负责，也是对企业机构自身负责，这里面包含以下几个要点：

一是建立数据安全治理体系，委派高管牵头负责数据安全治理工作，根据《数据安全法》等法律法规的监管要求开展自身数据分类分级工作，对企业数据实施分类分级管理，分类分级结果与数据存储、权限、脱敏、开发等措施挂钩，实现体系管理。

二是建立以数据为中心、覆盖全生命周期的数据安全防护体系。在数据全生命周期的各个阶段部署关键的安全保护措施，确保各个环节的数据可管可控。

三是定期开展风险评估和数据安全成熟度评估，并通过实网攻防以及安全应急响应演练，及时改进公司中存在的风险，一旦发生安全事件后能及时响应，并做出最合适的反应措施，从而把损失降到最小。

四是建立健全全流程数据安全管理制度，组织开展数据安全教育培训，增强员工数据安全意识，提高企业自身数据安全能力。

《中国经营报》：在现在的数字化体系下，数据安全、网络安全已经不是一个简单的主体可以实现的，从国家和企业的角度来讲，你认为有哪些保护网络安全、数据安全的建议？

周鸿祎：第一，要瞄准产业数字化新场景，同步规划建设行业数字安全体系，保障传统产业数字化转型。未来，所有传统行业都将被数字化重塑，产生工业互联网、能源互联网、车联网等产业数字化新场景。我建议相关行业主管部门把建设行业数字安全体系纳入产业数字化的整体规划，推动各行业龙头企业建设以安全大脑为核心的数字安全体系，以能力导向代替合规导向，夯实产业数字化的安全底座。

第二，要面向新型数字技术和应用场景，研究建设前瞻性的数字安全平台体系。当前，人工智能、区块链、量子计算等新技术不断进步，数字货币、自动驾驶、元宇宙等新应用不断兴起，带来不可预知的安全风险，传统网络安全缺乏成熟的应对经验。建议相关部门采取“揭榜挂帅”的方式，鼓励企业、研究机构、高校共建数字安全平台，例如，依托国家新一代人工智能开放平台、大数据开放协同实验室等，牵引带动行业创新数字安全体系。

第三，可以以城市为主体，由政府统筹打造城市级数字空间安全基础设施和应急体系，保障经济社会稳定发展。城市作为经济、人口的集中地，未来将集聚全国80%的GDP和人口。俄乌冲突等现实案例已证明，城市已成为网络战的首选战场，也是维护国家数字安全的主阵地。一旦城市的政府服务、关键基础设施群遭受网络攻击，就会让城市业务停摆、经济停滞。

值得注意的是，过去城市并非数字安全的建设主体，讲究“谁建设谁负责”，大大小小的企业、单位都靠自己来应对网络安全问题，缺乏统一的数字安全感知、应急、指挥体系。因此，我建议以城市为主体，由政府统筹打造城市级的数字空间安全基础设施，建设城市的“数字安全医院”，包括城市级的统一感知系统、应急系统和指挥系统，做到及时发现、快速响应、联防联控，为各单位输出安全基础服务，为政府服务和关键基础设施群正常运营保驾护航。

第四，还可以开展对开源代码的系统性漏洞挖掘，构建开源代码的安全风险评估机制。当前，全球范围内90%以上的云服务器操作系统、80%以上的移动操作系统都基于开源软件。我国银行、能源、国防、医疗、电力等重要行业运行的系统大量使用开源软件。

但是，开源软件由于生态开放，存在着大量的安全漏洞等风险，如果被恶意利用，足以撼动我国关键信息基础设施的安全。建议监管机构通过安全社区、挑战赛等形式，鼓励各方力量开展对开源代码的系统性漏洞挖掘，掌握安全隐患，并对关键信息基础设施和重要信息系统开展普查，摸清开源软件使用情况“家底”，精确掌握其类型、协议、来源等基础信息，进行系统漏洞挖掘，布局安全风险管理。

第五，还应该建立软件企业安全责任制，明确软件企业承担起开源软件的全生命周期安全管理。建议有关部门明确要求开源软件企业有义务对所使用的开源代码进行漏洞审查，建立企业安全响应中心，提高开源软件的安全管理能力。