全国政协委员、正泰集团董事长南存辉：

推进混合所有制改革 保护中小股东权益

南存辉

本报记者 梁隽妤 许意强

“混合所有制改革，将会给民营企业带来很多机会，有品牌、有实力的民企参与混改，不仅有机会分享国企科技创新成果，还可以站上更高的发展平台，拥有更宽的视野。但是，在这一过程中既要保障国有资产的保值增值，还要保障非国有资本的权益”。

日前，全国政协委员、正泰集团董事长南存辉在接受《中国企业报》等媒体采访时提出，2017年以来，混合所有制改革正向纵深推进，并取得突破性进展。总体来看，重点突破、分层分类的国企混合所有制改革格局已形成。但是，当前混合所有制改革的关键是加强顶层设计，比如以“管资本为主”为方向，针对混合所有制经济发展出台专项法律法规。

立法保障 中小股东权益

据悉，南存辉希望可以建立混合所有制改革法律制度，建立完善的产权交易制度和平台，完善市场决定价格机制，让市场决定产权交易价格。在他看来，当前国企混改面临一些深层次矛盾和问题。比如清产核资与资产确权问题，国企混改前须做好清产核资，避免资产流失；中小股东权益保障问题，混改后企业股权多元化，不同决策机制间存在重大差异。

“只有更好地保护中小股东合法权益，才能消除各类所有制资本参与混改的顾虑。”南存辉表示，比如在混合所有制企业中，要强制性分红、强制性累积投票、分类计票、集体诉讼、内幕交易处罚等。进一步完善国有股减持立法，规范国有股减持的方式、程序与要求。按照“不因改制增加企业税收负担”的原则，完善国有企业改制重组税费等各项政策，避免对同一实际控制人所属的子企业重组征收高额税费。

今年政府工作报告中指出，支持民营企业发展。坚持“两个毫不动摇”，坚持权利平等、机会平等、规则平等，全面落实支持非公有制经济发展的政策措施，认真解决民营企业反映的突出问题，坚决破除各种隐性壁垒。在南存辉看来，民营企业要想在市场经济浪潮中大显身手，除了希望政府持续深化混改法律制度改革，同时还应该实施差别化金融监管并制定企业境外投资法。

企业境外投资 亟待有“法”可依

2018年以来，国有银行的流动资金贷款年利率均为4.8%以上，中长期项目贷款年利率均为5.9%以上，上下游供应链融资年利率均为8%以上。由于高利率且不能保障信贷规模，迫使企业去寻求其他更高成本的融资。由此，借贷利率上浮、融资成本增加、原材料价格上升，再加上人工成本增加等多重因素叠加，使得实体企业经营成本上升，利润下滑，不利于实体经济可持续发展。

对此，南存辉建议，一方面，金融去杠杆要避免“一刀切”，要有保有压，区别对待。比如，对“僵尸企业”和产能过剩行业一定要去杠杆，而对创新创业型企业则要在融资上给予倾斜，降低融资成本；另一方面，通过精准税收减免、补贴，对实体企业给予专项贷款利息补贴或退税优惠，减缓由欧美等国家降税带来的市场冲击。

面对越来越多中国企业“走出去”，南存辉认为迫切需要更强有力的法律保障，应该制定企业境外投资法。从总体上指导对外直接投资的企业境外投资，使中国的对外直接投资政策具有坚实的法律基础。比如，明确以国家为主导，与更多的国家签订双边或多边投资保护协定；鼓励国内企业对国际投资保险机构和保险规范的认知，用好用足国际投资保险额度；强化并规范公共保险机构政策性功能，鼓励中信保公司强化我国海外投资保险业务，设立多样化、针对性强的险种，实现与海外投资需求相匹配的保险范围。

今年全国两会，南存辉一共带来了14份提案，内容涉及新能源产业发展、混合所有制改革、金融投资、乡村振兴等多个方面。在每一份提案的背后，正是创业43载的南存辉对中国社会经济发展的思考，以及作为改革开放后第一代浙商对新时代发展的期盼。

全国政协委员、360集团董事长兼CEO周鸿祎：

网络安全漏洞管理问题多，人才缺口大

周鸿祎

本报记者 许意强

“漏洞是网络安全的命门，重视不够、修复不及时，就会引发各种网络安全问题。”

日前，首次当选全国政协委员的360集团董事长兼CEO周鸿祎告诉《中国企业报》等媒体，当前，中国在网络安全漏洞管理方面存在对漏洞不重视、修复不及时，缺少具体的漏洞修复管理细则和处罚机制等问题。此次他专门带来三份提案，包括《关于强化网络安全漏洞管理的提案》、《关于鼓励政企单位上报网络攻击信息的提案》和《关于完善网络安全人才培养体系的提案》。

工业互联网 面临新的安全问题

工业互联网作为新一代信息技术与制造业深度融合的产物，已经成为工业现代化、发展实体经济的关键支撑，其安全问题对国家经济社会发展至关重要。对此，周鸿祎说，“近年来，工业互联网的发展使得现实世界和网络世界深度联通，导致网络空间的攻击穿透虚拟空间，直接影响到工业运行安全，并扩散、渗透到城市安全、人身安全、关键基础设施安全，乃至国家安全，造成的后果日益严重”。

如今，工业互联网的重要性使其成为网络攻击的重要目标。据悉，2017年发生的“永恒之蓝”勒索病毒事件，就造成我国众多工业企业中招，给经济社会带来了严重影响。工业互联网是一个新兴融合领域，面临新的安全问题。

尽快建立漏洞管理 全流程监督处罚制度

虽然我国《网络安全法》已经正式实施，并规定网络运营者的安全义务以及相应的追责，但对网络安全漏洞管理还没有执行细则。此外，缺少严格的监督执行和处罚机制，对未及时修复安全漏洞的单位无法及时发现和予以处罚。

比如，2017年5月12日WannaCry勒索病毒事件爆发，微软公司早在当年3月就已发布相应安全漏洞补丁，但中国很多单位却一直没有打补丁，导致近30万台主机和电脑被感染。直到今天，360公司还能监测到我国每天仍有近千台电脑感染此勒索病毒。

周鸿祎建议，为强化网络安全漏洞管理，降低被攻击风险，提高我国网络安全防护能力，要建立漏洞管理全流程监督处罚制度，尽快制定覆盖网络安全漏洞发现、审核、披露、通报、修复、追责等全流程的管理细则，强制要求漏洞必须及时修复，对漏洞修复时间以及违规处罚措施予以明确规定。

同时，还要强制执行重要信息系统上线前漏洞检测，对涉及国计民生、国家关键信息基础设施的重大信息系统工程和项目，在其上线运行或交付使用之前，应强制要求进行网络安全漏洞的自检和备案。同时，国家网络安全主管部门应对上线系统进行抽检，发现问题及时整改。

再者，要强制召回存在重大网络安全漏洞产品。对于可能导致大规模用户隐私泄露、人身伤害或者影响民生服务、关键基础设施正常运行的软硬件产品，尤其是物联网、智能汽车等产品，应借鉴汽车行业的做法，对存在重大网络安全漏洞的产品实施强制召回，避免造成更大的损失。

网络安全人才 培养体系亟待完善

尽管近年来，国家网络安全人才培养取得重要进展，但与打造网络强国对人才的需求规模相比还存在较大差距，网络安全人才培养体系亟待完善。当前我国网络安全人才缺口巨大。据教育部有关机构和专家预测，当前我国网络安全人才缺口达70万，到2020年将急剧增加到140万。并同时存在着高校人才培养难以满足网络安全实战需求、网络安全职业培训质量有待提高、网络安全从业人员缺乏必要的职业技能鉴定等方面的问题。

周鸿祎建议，要通过大力支持网络安全企业设立相关教育培训机构、开展网络安全学科联合建设、把网络安全纳入职业技能鉴定体系等方式，全面加强网络安全人才建设。