找准战略定位，拥抱“互联网+”

明确能干什么、不能干什么，找出自身特色、优势和方向，做到差异化发展，才能顺利登上“互联网+”的技术巨轮

第三届世界互联网大会召开在即，“互联网+智慧医疗”“互联网+物流”“互联网+出行”“互联网+普惠金融”成为重要议程。“互联网+”成为时代热词，我们到底该如何迎接它？“互联网+”与实体经济能如何互动？我们又如何与“互联网+”时代安全对接？

“互联网+”已经被作为国家战略行动计划提出，各地政府和创业企业都在行动起来抢占风口。雷厉风行，映照着互联网时代的速度，但也要避免一种错误倾向：面对新事物缺乏战略定力，盲目从事、一哄而上，速度情结严重。要顺利登上“互联网+”的技术巨轮，既要认真学习吃透国家对于“互联网+”战略行动计划的精神，把握好方向，掌握政策和法律法规，更要冷静思考，做好自身战略定位。明确自身在“互联网+”中能干什么、不能干什么，找出自身特色、优势和方向，摸清市场的需求及自身的供给能力，才能做到差异化发展，在某领域、某些业务培育出竞争优势。

“互联网+”时代最大的特征是随时随地、快速高效、简捷方便的数据分享，这种虚拟属性又无时无刻不指向实体经济。数据爆炸时代，互联网中存储着海量的数据信息，如果不与实体经济结合，不为实体经济所用，只会是冗余的垃圾。实体经济是互联网发展的基础，推动支持实体经济的发展，则是“互联网+”发展的旨归。“互联网+”是实体经济快速发展获取数据信息的工具和平台，实体经济可以通过互联网大数据更精准地把握本领域的运行现状及未来发展。“互联网+”的未来价值，正在于它与实体经济的优势互补、相互促进，将激发许多现有产业的潜力。反之，如果“互联网+”发展实践脱离了对这组共生关系的深刻把握，便会让“互联网+”沦为“空中楼阁”。

“互联网+”时代，网络安全风险也在积聚。如何保障网络安全，已经成为“互联网+”时代安全到来的重要战略支点。在10月份中央政治局第三十六次集体学习时，习近平总书记就强调“要维护网络空间安全以及网络数据的完整性、安全性、可靠性，提高维护网络空间安全能力”。近来一系列的互联网电信诈骗案件，更以血的教训给出了风险提示。随着“互联网+”的不断推进，网络安全问题与种类必然增多，只有严阵以待才能行稳致远。

几天前，网络安全法通过审议，这对于维护我国网络空间主权和安全、社会公共利益以及促进经济社会信息化健康发展，具有里程碑意义。立足“互联网+”，保障网络数据信息安全和运行畅通是治理的底线，是第一位的。因此，我们不仅要将网络安全纳入国家安全战略规划，做好全国一张安全网的顶层设计，将网络安全系统产品及基础设施纳入国家重点工程与“互联网+”同步建设、发展和管理，也要及时制定、修改和完善网络安全管理的相关法律法规，明确主体责任。此外，为了拧紧“互联网+”时代安全阀，国家可建立“网络安全技术+网络安全管理有机融合的安全保障体系”以及“网络社会安全管理与现实社会治理有机融合的安全保障体系”，实现安全保障的双轮驱动。

“互联网+”的发展，是技术创新的迸发，也是长期持续的历史进程，各地在发展的过程中要有功成不必在我的胸襟。在自身战略定位上要清晰有序、有舍有得，让虚拟经济与实体经济共生共荣，更要让网

络安全体系严丝合缝。