世界数字巨头的监管。2020 年 12 月，欧盟委员会提交了两部新数字法案：《数字服务法》和《数字市场法》，对在欧盟境内运行的社交媒体、在线市场和其他在线平台进行监管。欧盟委员会称：这两部法案是其制定欧洲数字十年计划的核心。

在欧盟看来，美国属于“数据保护不完全国家”，欧盟对该国互联网巨头的监管是重要的工作。这些公司一旦被欧盟认定为通过损害竞争对手为自己谋利，可能将被迫出售在欧洲的业务并支付数十亿美元的罚款。此外，欧盟还公布了为美国微软和谷歌等公司制定的搜索排名方面的规则，要求它们增强该项业务的透明度。

美国马里兰州巴尔的摩市的科洛尼尔管道运输公司的一处燃油供给设施，5 月 7 日至 12 日，该公司因遭受勒索软件攻击，暂停其在美国东岸的关键输送业务。美国罕见地向勒索组织妥协，一次性付出了 500 万美金的代价以恢复被攻击的系统。。

惠志斌向《新民周刊》记者表示：现有的网络空间治理的国际体系存在很多不足。西方基于政治同盟治理与政治的意识形态的绑定，实际上在网络空间往往是无效的，有大量的议题超越传统政治的壁垒而产生。同时，新兴力量的崛起，包括发展中国家在内的新兴力量希望参与到全球网络空间治理中，但目前来看，他们还没有足够的力量这样做。

他提出，在当前的新形势下，网络安全治理有如下几个重点议题：

首先是人工智能，这是未来网络空间中，基于智能化算法的话题。在经济、生活、社会、政治、军事等背景下，如何出台对人工智能安全伦理系列的研究，将共同推动治理方面的工作。

其次是物，关键基础设施的保障，这是基于智能化的关键基础设施。目前，关键基础设施物联网的体系面临巨大的威胁，我们如何通过全球国家间、企业间等各方协同的治理，保障人类共同依赖的关键基础设施，是治理中非常严峻的问题。

然后是国际网络安全面临的“两进两出”与“长臂管辖”的挑战。

“两进”是禁止外国的网络安全相关产品进入本国市场，同时禁止相关的外国资本进入。而随着智能网络空间时代来临，只有互联网技术产品在确保安全时相互渗透才更有利于网络空间的发展。

“两出”是禁止本国的互联网核心技术出口，禁止本国数据出境。数据是最有效的资源，各个国家争夺资源时，如何在保障国家、企业和个人多个层面的隐私和安全的前提下有效促进数据的流动，而不是一禁了之，这也是重要的议题。

以美国为代表的“长臂管辖”模式则希望在他国的数字世界建立起有利于自身的壁垒，改变“数字地缘”。

在惠志斌看来，各国通过各自建立网络安全领域的法律法规体系来与对方博弈，这种难以达成共识的现状可能需要较长的时间才能改变。以上的议题，需要以建设人类命运共同体的理念来逐渐解决。

而对于跨国互联网企业而言，如何在各国网络安全监管政策不一致的情况下合法合规地经营，这是它们面临的最大挑战。

个人信息如何保证安全？

当下，用户在享受数字化便利的同时，也要将自身大量的数据提供给互联网平台，拥有大量用户信息的平台就拥有了核心竞争优势。在互联网发展早期，用户数据仅仅包括浏览记录、行动轨迹、发布内容等较为分散和笼统的信息。随着移动互联网的发展，智能终端的个性化定制服务开始普及，用户似乎不得不提供更多的数据以换取更加智能化的便捷服务，其中不少是涉及个人网络安全的隐私信息。