在 2019 北京网络安全大会上的讲话

（2019-8-21）

很荣幸应邀出席“2019 北京网络安全大会”。

当今世界，信息革命已经带来了生产力质的飞跃，人工智能、机器学习、物联网、区块链和大数据等新技术正在改变我们的生活和未来。在网络时代，网络空间与物理世界深度融合，数字技术已深深嵌入到国际政治、经济、军事、文化、教育等各项活动中。历史告诉我们，每一次科技变革在推动世界进步的同时，也对世界各国的主权、安全、发展利益带来新的挑战。网络空间安全不但是国家安全的重要组成部分，而且已经成为维护世界和平的应有之义。

网络安全是全球性挑战，中国支持以联合国为主渠道为网络空间建章立制。当前，互联网治理由国家层面发展为国际层面的进程依然缓慢，分歧和争论远远多于共识与合作，这种情况令人忧虑。由于网络空间的开放性和国际性，加强网络空间治理的国际合作具有越来越突出的紧迫性。2015 年，中国国家主席习近平针对网络空间的发展与治理问题提出了“四项原则”和“五点主张”，这是中国关于互联网的安全与发展、关于网络空间国际治理的基本立场和主张。习近

平主席还指出，世界各国虽然国情不同、互联网发展阶段不同、面临的现实挑战不同，但推动数字经济发展的愿望相同、应对网络安全挑战的利益相同、加强网络空间治理的需求相同。各国应该深化务实合作，以共进为动力、以共赢为目标，走出一条互信共治之路，让网络空间命运共同体更具生机活力。

下面，我想着重谈几个问题：

1、中国一贯强调网络空间的主权属性，坚持国家在网络空间的合法权力。正如大家所知道的，《联合国宪章》确立的主权平等原则是当代国际关系的基本准则，覆盖国与国交往的各个领域，其原则和精神也应该适用于网络空间。尊重网络空间主权，就是要尊重一个国家在建设、运营、维护和使用网络以及在网络安全的监督管理方面所拥有的自主决定权。任何国家在网络空间都可以独立自主地处理内外事务，享有在网络空间的管辖权和自卫权以及平等参与网络空间国际治理的权利。

2、近 20 年来，网络军事化的进程逐步加快，网络空间已经成为国家间军事斗争的新疆域、战略竞争新的制高点。我最近看到一则报道：自 2010 年开始，北约每年都在爱沙尼亚的塔林举行代号为“锁盾”的网络安全演习。今年的演习场景设定于大西洋的一个

岛国，该国在国内大选期间遭到敌国大规模和系统性的“网络入侵”,电力电网系统、净水厂、4G 通信网络、海事预警系统等基础设施遭到网络攻击，民众舆论及选举进程受到操控,并导致国家发生了严重政治动荡。这个演习的目的是让北约各成员国真实感知网络威胁,在复杂、激烈的网络对抗环境下迅速形成民事和军事响应能力，以此加强北约内部及其与伙伴国的组织协同。由此可见，将网络空间设置为战场，已经成为不少国家军事准备的重要内容。这提示我们防止网络空间不断加剧的军备竞赛已经是重大的国际安全问题，国际社会对于防止网络空间冲突亟需达成共识。

3、当前，随着网络空间的不断拓展，网络与国家基础设施的结合日益紧密，与此同时，针对关键基础设施的网络攻击行为也日益增多，一些在传统互联网设备中并不会造成过大危害的漏洞，也有可能在关键基础设施中引发灾难性后果。关键基础设施是国家的核心要害，去年发生的乌克兰大停电和今年发生的委内瑞拉大停电都说明了这一点。因此，加强对关键基础设施的保护应当提上国际社会的重要议程。各国应当通过协商的途径达成共识，认定对于关键基础设施的网络攻击是战争行为，具有反人类的性质。各国应当通过立法和行政的手段，加强对关键基础设施的保

护。提供关键基础设施的设备厂商应当与传统网络安全厂商紧密结合，针对关键基础设施在部署、运行中的特点，研发具有针对性的防护软硬件，采取具有实效的保护措施。

4、维护网络安全对于高速发展的经济体而言具有尤其重要的意义。当前，互联网企业正如雨后春笋般不断涌现，互联网与传统产业的结合也日益紧密，因此，推动网络安全产业加快发展的任务也更加紧迫。网络安全产业的发展依赖于各国相关法律和制度、政策的支持，依赖于网络安全人才培养机制的规模和水平，依赖于人财物的投入。此外，加强网络安全教育，在民众中特别是企业家中树立网络安全意识十分必要。网络安全企业要寻求差异化发展，走互补融合之路，避免恶性竞争。

最后，我衷心希望与会的各位专家学者、工程技术人员将网络安全视为世界和平与发展的重要基石，尊重网络主权，加强国际合作，保护关键基础设施，努力推动网络安全产业的有序繁荣！