【当代政治】

“双轮驱动”:推进网络政治安全能力建设的新路径*

刘远亮 虞崇胜

摘 要:当今互联网时代,由于网络信息技术和政治体系的深度交融和互动,使得国家政治安全的内涵及影响变量等都发生了深刻变化,网络政治安全问题日益凸显。推进网络政治安全能力建设,既要着眼于诸种网络安全风险的防范,也要着眼于政治体系自身的积极建构,并将二者有机结合起来,从而实现“双轮驱动”的理想格局。实践中,既要坚持综合防范,通过不断强化网络治理提升网络安全风险防范能力,也要积极利用网络技术促进相应制度和体制的变革和完善,通过网络赋权增强政治体系内生政治安全能力。以“双轮驱动”推进网络政治安全能力建设,有利于形成维护网络政治安全的长效机制,更好地应对纷繁复杂的网络政治安全风险和挑战,促进国家长治久安。

关键词:互联网时代;“双轮驱动”;政治安全;网络政治安全能力

中图分类号:D630 **文献标识码**:A **文章编号**:1003-0751(2021)06-0014-07

近些年来,我国经济社会发展取得巨大成就的同时,国家安全问题受到越来越多的关注。党的十九大报告明确提出了“加强国家安全能力建设”的任务,并强调要“完善国家安全战略和国家安全政策,坚决维护国家政治安全”①。在国家安全能力建设中,政治安全能力建设是至关重要的内容。但在当今互联网时代,伴随多元化网络技术手段对政治的介入,国家政治安全的内涵及影响变量等都发生了深刻变化,网络政治安全问题日益凸显。本文在梳理既有研究成果的基础上,试图从政治体系的外部网络安全风险防范能力和自身的内生网络安全生长能力即“双轮驱动”的崭新视角,提出创新网络政治安全能力建设的新路径,借以应对纷繁复杂的网络政治安全风险和挑战,保障来之不易的改革发展稳定的大好局面。

一、文献回顾

网络技术变革及其广泛运用对国家政治安全产生了深刻影响,网络技术和国家政治安全的关系也因此成为学界热点研究议题,其中,如何实现网络政治安全是重要研究内容。对于该问题,目前学界的研究角度主要集中在如下方面。

1.网络信息安全角度

互联网时代,信息安全风险是政治安全风险的重要表现。②因此,从信息安全角度探讨网络政治安全治理成为许多学者的关注点。有研究者认为,我国信息技术还相对落后,给政治安全带来隐患。我们应转变观念,正视网络政治的出现和发展;加强立法,使政府上网和网上行政能够有法可依;加速构建覆盖全国的“政府网”;大力开发网络政治的技术人力资源以及充分利用网络加强国家意识形态的宣传。③有论者通过分析我国“信息边疆”安全面临的威胁,进而提出相应对策,包括加强网络安全防护措施和防范意识,提高网络管理水平,抵制不良信息的渗透,建立自己的信息阵地,加强对引进信息设备的有效管理和技术改造,建立专业信息部队,筹划信息

收稿日期:2021-03-13

*基金项目:国家社会科学基金一般项目“网络空间命运共同体与网络空间治理创新研究”(16BZZ080)。

作者简介:刘远亮,男,西北工业大学马克思主义学院助理教授、法学博士(西安 710029)。

虞崇胜,男,华中科技大学国家治理研究院特聘研究员,武汉大学教授(武汉 430074)。

战略，拓展“信息疆域”等。④也有学者提出，通过优化互联网治理模式，依法进行互联网治理，加强网络舆论引导，加强互联网内容管控，强化网络主体的自律，加强国际合作，健全互联网基础管理制度等措施维护信息安全，进而促进政治安全。⑤

2.具体的网络实践或网络技术运用角度

不少学者从具体的网络实践或网络技术角度分析网络对政治安全的影响，探讨如何通过优化网络实践或网络技术运用来促进政治安全。有学者强调通过优化公民的网络政治参与来维护党的执政安全⑥；有研究者提出通过加强互联网虚拟社区管理，促进国家政治安全⑦；有学者建议通过网络舆情的治理和引导以及网络舆情治理创新来维护国家政治安全⑧；还有的研究者提出通过建立网络谣言生态治理体系、提高信息主体网络政治素养、构建全过程安全风险防控体系、健全网络空间安全法制体系等途径进行综合施策，从而维护国家政治安全⑨；另有论者主张通过确保网络舆论的内容安全、制度安全、资金安全和技术安全，从而促进政治安全⑩；等等。

3.完善互联网领域的政策、法规和相关机制的角度

有学者建议在战略层面建立分级安全战略应对防线并重视战略目标的可实现性、改变国家安全战略的固化现象、重视国家软实力建设和巧实力应用；在方法层面明晰监管原则、理清政府职责、着力体制和规范创新、依法管理要实至名归；在实践层面应实施参与式监管、疏导式监管、激励式监管、低调无为式管理以及属地式监管。⑪也有学者从加强法治的角度分析网络安全治理，强调依法处理网络群体性事件，增强处理工作的依法性和科学性，从而维护社会的稳定与安全。⑫另有论者提出建立网络时代政治发展中政治功能平衡与政治文化凝聚的双规安全机制，前者包括权力制衡机制、必要的控制机制、协调机制等，后者包括意识形态安全机制、政治文化体系的动员机制、政治认同机制等。⑬等等。

通过上述梳理不难发现，在既有的研究文献中，尽管学者们的分析视角、研究方法、研究议题以及具体研究内容等都有所不同，但就其共同点来说，都凸显了互联网时代网络政治安全问题的特殊性。当然，既有研究也存在薄弱之处。比如，对于网络化境遇中网络政治安全的维护，学者们大都从防范的角度提出相应措施，而对政治体系内生安全机制的探讨不够。尽管也有学者从政治体制的角度作出探讨，提出大数据背景下构建政治安全的内生动力系统和外部防范系统，以有效维护国家政治安全⑭，但是，如何将两个方面有机结合进而提升网络政治安全能力，学界仍缺乏较为系统的分析。的确，诸多网络政治安全问题是人们对网络技术的运用而诱发的，但其根源并不在于网络媒介本身。加强网络安全风险防范是维护网络政治安全的重要内容，但它只是提升网络政治安全能力的一个方面，而更为根本的还在于政治体系自身的积极建构，通过“强身健体”而增强抵御各种网络政治安全风险的能力。所以，我们认为，推进网络政治安全能力建设，既要着眼于政治体系外部网络安全风险的防范，也要着眼于政治体系自身的积极建构。将二者有机结合，实现“双轮驱动”，是当前推进网络政治安全能力建设的必然选择。

二、“双轮驱动”推进网络政治安全能力建设的依据及意涵

1.提出“双轮驱动”的主要依据

唯物辩证法关于事物发展内因和外因相互关系的理论，是提出以“双轮驱动”推进网络政治安全能力建设的重要理论依据。根据其理论观点，一切事物运动、变化、发展的根本原因在于其内部的矛盾，但任何事物都不是孤立的，都与周围的事物互相联系、互相影响，而这种外部的影响、作用则是其发展的外部条件。正如毛泽东在《矛盾论》中分析指出的：“单纯的外部原因只能引起事物的机械的运动，即范围的大小，数量的增减，不能说明事物何以有性质上的千差万别及其互相变化，事实上，即使是外力推动的机械运动，也要通过事物内部的矛盾性。”⑮事物发展是由内因和外因共同推动的，内因是事物发展变化的内在原因，具有根本性；外因是事物发展变化的外部原因，即外部条件，这种外部条件最终是要通过事物内部原因才能起作用。对于一个国家来说，要维持其安全与稳定，防范外部的侵害无疑是必要的，但同时也需要国家内部的良好治理及自身的发展壮大。

从实践层面来看，着力防范化解重大风险是当前国家经济社会发展中面临的迫切任务，需要从外部和内部同时入手。一方面，加强防范，使国家免受外在安全风险的破坏；另一方面，增强自身免疫力，

提高自身内生安全能力。只有将两个方面有机结合,才能更好地应对发展过程中面临的风险挑战,保障国家安全。

如今,互联网技术迅猛发展及其广泛运用对国家政治安全的影响日趋增强,以至于有论者认为“新媒体的发展让政治革命几乎唾手可得”⑯。然而事实证明,网络媒介并非许多国家政局动荡、政权颠覆的根本原因。近年来,诸多“颜色革命”发生的根源更多的还是这些国家政府自身内部的问题。⑰“打铁还需自身硬”。对我国来说,虽然互联网技术的飞速发展对国家政治安全有较大的影响,但它终究是一种外在影响变量,政治体系自身的变革和完善才是化解网络政治安全问题的根本。简言之,有效应对各种网络政治安全风险,既要防范因网络技术变革及其广泛运用而引发的诸多网络安全风险,又要重视政治体系自身的变革和完善。将二者有机结合,实现“双轮驱动”,是推进网络政治安全能力建设的必然选择。

2.“双轮驱动”的核心意涵

对于实现网络政治安全来说,防范网络安全风险无疑是十分重要的,但基于网络技术发展而催生的多元化网络信息传播渠道,以及难以控制的网络信息流等,使得诸多网络安全风险防不胜防。唯有政治体系自身不断变革和完善,增强对网络社会的适应能力,才能有效应对各种风险挑战。因此,要切实增强网络政治安全能力,必须“双轮驱动”,二者缺一不可。

其一,提升政治体系外部网络安全风险防范能力。按照《现代汉语词典》的解释,“防范”有戒备、防备之意,与之相近的概念有防御、防卫等,即在祸患发生之前采取措施对其加以预防。换言之,就是要借助特定方式或采取相应措施对将要发生的风险、危机或破坏进行防备,以阻止其发生或进一步扩大,力求将危害降到最低。如今,网络技术迅猛发展及其对政治的全方位介入,加之其因高度的开放性、互动性以及跨越国界的特征,打破了前网络时代信息传播的诸多限制,对国家政治安全构成了新的挑战。英国著名学者尼尔·巴雷特在其著作《数字化犯罪》中指出,如何防范和打击网络犯罪、维护网络安全,已对全世界的所有执政者提出挑战。⑱对我国来说,加强网络安全风险防范是实现网络政治安全的必然要求。习近平强调:“过不了互联网这一关,就过不了长期执政这一关。”⑲采取各种措施防范因网络运用而导致的各种威胁、挑战、破坏,切实提升应对各种网络安全风险的能力,加强网络安全保障无疑是网络政治安全能力建设的重要内容。

其二,提升政治体系内生网络安全能力。内生安全指的就是通过事物自身内部要素的优化重组,由此形成内在的安全能力。形成内生安全长效机制是适应外部环境变化,应对诸种风险和挑战,维持网络政治安全的根本保障。有研究者强调,纵观人类历史,虽然每一次政权更迭都有着复杂的外部原因和多种表现形态,如外敌入侵、自然灾害等,但就其内部原因而言,都与执政者的腐败有本质上的联系。⑳提升内生网络安全能力主要是从政治体系自身着手,加强政治建设,通过政治体系“祛除疾病”“强身健体”来抵御外部网络安全风险。虽然不排除各种防范手段的使用,但主要是以政治体系内部的积极建构来确保安全的,即“通过政治体系的持续自我进化来增强其活力和生命力”㉑,以达实现网络政治安全之目的。网络技术只是一种外部条件,它毕竟要通过政治体系内部原因才能起作用。政治体系充分利用现代网络技术促进自身变革和完善,不断增强自身抵御外部网络政治安全风险和威胁的能力,才能更好地适应网络社会变迁,促进网络政治安全。

三、防范网络安全风险:网络政治安全能力建设的重要抓手

网络安全是政治安全的重要支撑,加强网络安全风险防范是网络政治安全能力建设的重要手段。在“百年未有之大变局”的时代背景下,我国既要防范网络技术与社会转型的交织而催生的各种网络安全风险,又要防范网络空间跨国信息流动所造成的渗透、颠覆和破坏等网络安全风险,从而在综合防范中促进网络政治安全。

1.增强网络政治安全能力必须着力防范网络安全风险

当前,我国仍处于社会转型期,虽然国家发展取得了显著成就,但同时也面临许多突出的矛盾和问题。要有效解决这些矛盾和问题,避免动荡局面的出现,根本途径是建立健全各项制度。但现实中各方面的制度尚处于完善之中,而且政府治理过程中也还存在这样那样的不足,于是各类社会风险不断

涌现。特别是随着网络社会的崛起,网络普及程度不断提高,各社会主体借助于网络参政议政广度和深度的变化及其影响力日趋增强,社会转型面临着新的变数。网络技术与社会转型的交织极大地增加了社会转型的安全风险,当然也考验着政治体系实现和维护网络政治安全的能力。

作为一种传播技术和沟通手段,互联网本身并无威胁性,关键是主体如何使用它以及要达成什么样的目的,而这决定着网络政治的样态,决定着网络政治活动是混乱还是有序;不同的网络政治样态又决定了其影响,特别是对国家政治安全的影响。[22]对于社会各主体来说,网络既可以用于参政议政,也可以成为其进行负面政治传播甚至进行犯罪的手段。诚如有学者所言,虽然从客观上讲,我国与“颜色革命”发生国在政治制度、经济状况、文化传统、社会结构等方面存在着较大差异,类似“颜色革命”的事件在我国发生的可能性不大,但我国与这些国家有着共同的社会主义历史渊源,又同处于社会转型期,社会内部存在着许多相似的社会问题和矛盾,所以同样存在着诱发“颜色革命”的潜在因素。[23]规避“颜色革命”的发生,防止因网络运用而对国家政权、主流意识形态、政治制度、政治秩序等造成的冲击和破坏,客观上需要对网络风险和挑战加强防范。

2.坚持对网络安全风险的综合防范

我国政府的许多权威文件如《国家信息化领导小组关于加强信息安全保障工作的意见》《2006—2020 年国家信息化发展战略》都强调对网络安全风险要坚持“积极防御、综合防范”的方针,即综合利用多种方式防范网络安全风险。对于网络政治安全能力建设来说,必须要对诸多网络安全风险实施综合防范,而统筹防范内部和外部网络安全风险则是必然要求。

其一,加强内部网络安全风险防范。截至 2020 年 3 月,我国网民规模为 9.04 亿,互联网普及率已达到 64.5%。网络普及率不断提高,其影响力也随之增强。对于网络政治安全而言,互联网络是一个必须受到特别重视的关键变量。多元化的网络信息、价值观念、意识形态等充斥着网络空间,加之负面的网络宣传和网络动员与现实社会矛盾的结合,很容易对现实社会政治秩序带来冲击。正因如此,各级政府对网络传播都保持着高度警惕,并通过诸多防范措施来应对网络风险。从关闭不法网站、删除不法信息,到对不法网络行为者进行严厉打击、针对特定网络安全问题开展相应的专项网络整治活动(如整顿网络大 V、网络谣言),从政府相关部门(公安、行政、网信等部门)对网络行为者的直接管控,到委托第三方(如网络服务提供商)进行删帖、过滤网络传播内容等,都是具体的防范举措。概言之,就是通过各种防范措施的实施来应对因网络技术变革与社会转型交织而带来的诸多挑战,消除或降低网络信息传播及网络行为的负面效应,以促进网络政治安全。

其二,加强外部网络安全风险防范。跨国信息流动向来都是影响国家政治安全的重要因素,而基于多元化网络传播载体而进行的各种跨越国界的政治信息流动对国家政治安全的威胁则更为严重。一方面,网络空间为恐怖主义、分裂主义、极端主义势力及法轮功等邪教组织开展跨国破坏活动提供了便利条件,直接影响国家政治安全。比如各种网络恐怖主义活动,它正是以网络攻击为主要形式,具有跨国性、隐蔽性、成本低、破坏性大等特征,而且与传统恐怖主义相结合,往往能以非常低的成本对社会带来极其严重的危害,对国家政治安全也会构成直接冲击。[24]另一方面,以美国为首的西方国家往往利用网络对我国进行窃密、诋毁、攻击和意识形态渗透,进一步增加了网络政治安全的风险。2013 年轰动全球的“棱镜门”事件充分说明了这一点。实践中,比如内容过滤和审查、技术控制、设置防火墙等,是维护网络安全的客观需要。

3.通过网络治理提升网络安全风险防范能力

加强网络治理,不断提升网络安全风险防范能力,是推进网络政治安全能力建设的重要任务。

其一,严肃处置违法和不良网络信息。在社会转型期,在原有沟通和表达机制还不健全的情况下,网络已成为人们政治表达和互动的主要通道,其政治参与和政治表达的热情得到了空前释放。问题是,伴随现实社会中的矛盾、问题在网络空间的呈现,各种违法和不良网络信息也随之出现。比如,网络空间各种谣言、虚假信息特别是错误思想观点的大肆传播,会逐步消解人们既有的政治认知基础;各种形式的抹黑、丑化党的领导和社会主义制度的言论,极力歪曲党史国史的言论,违背宪法及否定四项基本原则的观点,以及历史虚无主义、自由主义等错误思潮,直接影响网络意识形态安全;一些网络推

手、“大 V”的恶意炒作,有意放大社会矛盾,制造负面舆论,煽动群众对党和政府的不满的言论,不仅会影响社会安全稳定,还会直接影响人们对党和政府的政治信任。正因如此,强化网络治理,严肃处置各种违法和不良网络信息,净化网络生态,就自然成为网络政治安全能力建设的重要内容。

其二,有效应对外来各种网络安全威胁。网络空间存在的跨越国界的负面政治信息流动,网络犯罪,特别是通过网络渠道进行思想文化渗透等,增加了网络政治安全治理的难度。《国家网络空间安全战略》明确提出,利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权,以及大规模网络监控、网络窃密等活动严重危害国家政治安全和用户信息安全。所以,我国要防范、制止和依法惩治境外势力利用网络进行渗透、破坏、颠覆、分裂活动。推进网络治理,需要从技术、制度、法治、网络产业发展等方面全面发力,以提升防范网络安全风险的能力。为此,必须“筑牢网络安全防线,提高网络安全保障水平,强化关键信息基础设施防护,加大核心技术研发力度和市场化引导,加强网络安全预警监测,确保大数据安全,实现全天候全方位感知和有效保护”[25]。概言之,就是要通过强化网络治理,提高政治体系抵御外来各种网络安全风险的能力,进而确保网络政治安全。

四、增强政治体系内生能力:网络政治安全能力建设的根本方策

防范网络安全风险对于网络政治安全至关重要,但要从根本上消除网络威胁,增强政治体系在网络社会的适应能力,则需要政治体系通过自身的变革和完善而“祛除疾病”“强身健体”。加强政治建设,增强政治体系内生网络安全能力,是互联网时代切实提升网络政治安全能力的根本方策。

1.内生安全:一种积极的网络政治安全理念

当今时代,互联网技术已经渗透到社会生活的方方面面,网络空间已成为一种全新的交流互动空间,但人们对许多网络政治安全问题的认识仍然存在偏差,以至于过分强调通过技术层面的控制来确保政治体系的安全与稳定。应该看到,诸种网络政治安全问题实际上是现实社会的政治安全问题借助于网络通道的一种对称性反映,要切实消除网络安全风险,一定的网络规制是必要的,但仅靠网络技术层面上的控制和防范是远远不够的,它并不能从根本上消除社会转型过程中所累积的矛盾和问题。内生安全正是强调通过政治体系内生安全机制的生成来确保网络政治安全,也就是说,要通过政治体系内部的结构功能的调整和优化来应对各种网络政治安全风险,通过自身的发展壮大来增强其网络政治安全能力,因而是一种内源性安全。

就性质定位而言,内生安全强调经由对网络技术的积极利用来促进政治体系自身不断优化,增强其适应网络社会以及抵御网络政治风险的能力,它属于一种积极的网络政治安全理念。积极安全包括多方面内容,不仅是态度积极,更是行为积极;不仅是手段的积极,更应当是目的的积极;不仅是体制的积极,更应当是效果的积极。[26]内生安全正是通过政治体系自身的积极构建来促进网络政治安全,“以发展促安全”是其显著特点。这种主要通过政治体系自身的积极建构来促进网络政治安全的路径选择,可以从根本上增强政治体系应对各种网络风险的能力。

2.利用网络技术促进政治体系变革和完善

在网络化境遇中,政治体系面临的重要挑战就是如何对自身进行“重塑”,对其结构、功能不断进行适应性调整,从而增强适应能力以确保自身的安全。有学者认为,就目前甚至就将来一段时间看,不论对中国还是对中国共产党而言,互联网与其说是一种障碍,不如说是一笔财富。[27]从另一个角度看,互联网也可能是现代政治的福音,“由网络所开发和聚积的新政治资源和能量,既是补充现有政治资源匮乏之源泉,也是改造既有政治框架的动力和工具”[28]。强调内生安全,就是要利用网络技术来促进既有相关体制机制的完善,促进政治建设,使其成为驱动网络政治安全能力建设的重要因素。固然,互联网是一把双刃剑,但它作为一种全新的生产力方式以及由此而导致的生产关系的变革,对人类社会发展的促进作用是占主流的,关键是如何更好地利用它来为人类社会发展服务。对网络政治安全能力建设来说道理亦然。唯有充分利用网络技术,挖掘其积极价值,发挥其在解决社会转型发展中各种社会矛盾和问题上的作用,并促使政治体系不断完善,增强在网络社会的适应性,才能更好地确保网络政治安全。

在互联网发展早期,曾有学者指出:“当电脑和

网络被广泛应用于政治参与后,它必将推动公民与政府官员直接对话,提高民意在政府运作中的分量,从而在很大程度上改变未来政治参与的结构与模式。”[29]应该说,这种预测是准确的。如今,网络技术已然成为人们参政议政的重要平台,它改变了既有的政治表达和参与模式,以及权力和权利关系。强调内生安全,正是顺应网络社会的特点及其特殊运行逻辑、增强政治体系适应能力的现实要求。相反,如果不能积极利用网络技术促进政治体系自身的完善,以及发挥网络技术在推进社会转型发展中的功能,要增强政治体系在网络社会的适应能力并维系政治安全将会无比艰难。因此,应对网络社会的异质化发展以及网络技术的多元化运用而带来的政治风险和挑战,确保网络政治安全,政治体系增强本身的适应能力至关重要,这就需要其在转变诸多传统安全观念基础上,伴随网络社会及网络技术发展而不断调整自身,对其制度、体制等加以完善,以增强其生机和活力。

3.通过网络赋权增强网络政治安全能力

在互联网时代,网络赋权已成为全新的发展动力,对于政治体系增强网络政治安全能力至关重要。现如今,不同的主体都可以借助于特定的技术手段自由表达思想、交流信息、实现权利、影响政治过程,于是就形成了所谓的虚拟政治、在线政治等新的政治形态。而且网络空间也是一个“公共平台”,没有任何一个主体或机构能像对待传统媒体一样对其多元化的交流渠道进行完全垄断和控制。然而,这并不意味着网络空间与现实社会没有关联,是一种绝对的“虚拟存在”。事实上,它是一种“虚拟的真实存在”:一方面,网络空间的行为主体都是现实的主体,不论是政府、社会组织,还是公民个人,都是在现实社会中真实存在的;另一方面,网络空间所反映的矛盾和问题都根源于现实社会,其有效解决有赖于现实社会相关制度和体制的运作。虽然从直观上看网络空间是虚拟的,但不同主体借助于它进行互动的过程及其后果却是真实的,网络空间的互动在本质上仍是一种真实的社会互动。[30]正是在这种虚拟与现实的有机互动中,网络赋权成为显著特点。通过利用网络技术赋能政治体系,成为推进网络政治安全能力建设的有效方式。

在互联网时代,社会治理已表现出了新的趋势,即正从线下治理转向线上线下协同治理,网络赋权的重要性日益凸显。对于网络政治安全治理来说,一方面,必须借助于网络通道了解多元化的社会诉求,发现矛盾问题,走好网络群众路径,营造良好网络空间生态;另一方面,则需要通过现实社会的政策调整及制度体制的优化和完善更好地解决人们在网络空间反映的问题。正如习近平所强调的,“各级党政机关和领导干部要学会通过网络走群众路线,经常上网看看,了解群众所思所愿,收集好想法好建议,积极回应网民关切、解疑释惑。善于运用网络了解民意、开展工作,是新形势下领导干部做好工作的基本功”[31]。他进一步指出:“我们必须科学认识网络传播规律,提高用网治网水平,使互联网这个最大变量变成事业发展的最大增量。”[32]互联网是政府与社会间加强政治沟通、实现良性互动的优越平台,是化解分歧、弥合裂痕的桥梁,也是创新社会管理、完善治理体系的重要方式,更是增强政治信任、强化政治认同的全新形式,对于网络政治安全具有非常重要的促进作用。以网络赋权促进政治体系变革,逐步完善或创新相应制度机制,形成维护网络政治安全的长效机制,才能更好地保障网络政治安全。

五、结语

防范化解重大安全风险是我国当前经济社会发展中必须高度重视的问题,对此,我们既要有防范风险的先手,也要有应对和化解风险挑战的高招;既要打好防范和抵御风险的有准备之战,也要打好化险为夷、转危为机的战略主动战。具体到网络政治安全能力建设来说,既要着眼于防范诸多网络政治安全风险和挑战,又要着力于政治体系自身的变革和完善。前者强调的是如何对网络加强治理,以使政治体系免受外在网络风险和威胁的破坏;后者强调的是政治体系内部的积极建构,即从政治体系自身着手寻求诸多网络政治安全问题的根源及其相应解决路径和方法。推进网络政治安全能力建设,二者缺一不可,实现“双轮驱动”,既是一种必然选择,也是不同于以往的创新路径。

不可否认,对网络媒介施以严格规制,是规避网络媒介自身信息传播负面政治影响的要求,是防止网络空间与现实社会不良互动引发消极政治后果的需要,也是应对网络空间跨国信息流动潜在政治威胁的重要方式;但作为一种反应性策略,它难以从根本上消除网络政治安全威胁,更何况多元化的移动

终端、多元化的互动和交流平台、多元化的信息传播媒介形式以及网络传播的即时性和网状扩散模式等,这都使得网络安全风险防不胜防。所以,如果一味地强调网络管控,进而通过加强网络风险防范来化解网络政治安全风险则是不现实的。而要从根本上确保政治体系的安全稳定,则需要政治体系自身的积极建构,通过积极利用网络技术不断促进政治体系"强身健体",进而增强内在的抵御诸种网络政治安全风险的能力。一言以蔽之,将政治体系外部网络安全风险防范机制与内生网络安全生长机制有机结合,二者相辅相成和相互促进,才能有助于形成维护网络政治安全的长效机制,从而更好地应对诸种网络政治安全风险和挑战,维护网络政治安全,促进国家长治久安。

注释

①㉓《习近平谈治国理政》第3卷,外文出版社,2020年,第39、311页。②黄新华、何雷:《国家治理现代化进程中的政治安全风险研究》,《探索》2015年第4期。③胡建、文军:《网络与国家安全》,贵州人民出版社,2002年,第92—96页。④季正矩、王瑾:《国家至要:当代国家政治安全新论》,重庆出版社,2006年,第196—203页。⑤张显龙等:《全球视野下的中国信息安全战略》,清华大学出版社,2013年,第287—298页。⑥安云初:《网络政治参与促进执政安全的路径选择》,《湖南农业大学学报》(社会科学版)2008年第6期。⑦曾润喜、徐晓琳:《国家政治安全视角下的中国互联网虚拟社会安全》,《华中科技大学学报》(社会科学版)2012年第2期。⑧舒刚:《基于政治安全的网络舆情治理创新研究》,武汉大学出版社,2018年,第222—223页。⑨李昊青:《面向政治安全的网络谣言生态治理研究》,《现代情报》2018年第10期。⑩黄斌:《网络时代的舆论安全与政治安全》,《广东社会科学》2018年第6期。⑪蔡文之:《网络传播革命:权力与规制》,上海人民出版社,2011年,第244—255页。⑫严茂丰:《关于网络群体性事件处置法治化的思考》,《公安研究》2014年第4期。⑬蔡翠红:《网络时代的政治发展研究》,时事出版社,2015年,第273页。⑭徐霞、邵银波:《大数据背景下国家政治安全机制研究》,《学校党建与思想教育》2018年第4期。⑮《毛泽东选集》第1卷,人民出版社,1991年,第302页。⑯吴强:《互联网时代的政治涨落:新媒体政治前沿》,《国外理论动态》2015年第1期。⑰王存奎:《中亚地区"颜色革命"的性质与原因探究》,《国际关系学院学报》2006年第4期。⑱[英]尼尔·巴雷特:《数字化犯罪》,郝海洋译,辽宁教育出版社,1998年,第6页。⑲《习近平关于文化建设论述摘编》,中央文献出版社,2017年,第42页。⑳刘建飞:《中国特色国家安全战略研究》,中共中央党校出版社,2015年,第45页。㉑胡象明、罗立:《系统理论视角下政治安全的内涵和特征分析》,《探索》2015年第4期。㉒刘远亮:《网络政治安全内涵探析》,《中南大学学报》(社会科学版)2016年第6期。㉓赵永华:《大众媒体与政治变迁——聚焦独联体国家"颜色革命"》,中国书籍出版社,2013年,第244页。㉔熊光清:《中国网络社会治理与国家政治安全》,《社会科学家》2015年第12期。㉕㉛《习近平谈治国理政》第2卷,外文出版社,2017年,第382、336页。㉖余潇枫:《安全治理:从消极安全到积极安全——"枫桥经验"五十周年之际的反思》,《探索与争鸣》2013年第6期。㉗吕增奎:《执政的转型:海外学者论中国共产党的建设》,中央编译出版社,2011年,第337页。㉘杨凤春:《互联网是现代政治福音》,《人民论坛》2007年第14期。㉙李斌:《网络参政》,中国社会科学出版社,2009年,第211页。㉚夏学銮:《网络社会学建构》,《北京大学学报》(哲学社会科学版)2004年第1期。

责任编辑:文　武

"Double-Wheel Drive": A New Path to Promote the Construction of Network Political Security Capacity

Liu Yuanliang　　*Yu Chongsheng*

Abstract: In today's Internet era, due to the deep integration and interaction of network information technology and political system, profound changes in the connotation and influence variables of national political security have taken place, and the problem of network political security is becoming increasingly prominent. To promote the construction of network political security capacity, we should not only focus on the prevention of various network security risks, but also the active construction of the political system itself, and combine them organically, so as to realize the ideal pattern of "double-wheel drive". In practice, we should not only improve the ability of network security risk prevention by strengthening network governance, but also actively use network technology to promote the reform and improvement of corresponding systems, and strengthen the endogenous political security ability through network empowerment. To promote the capacity-building of network political security by "double-wheel drive" is conducive to the formation of a long-term mechanism to maintain network political security, better deal with the complex risks and challenges of network political security, and promote the long-term stability of the country.

Key words: internet era; "double-wheel drive"; political security; network political security capability