上海合作组织信息安全合作：必要性、现状及前景*

张文伟

【内容提要】　信息安全问题已经成为上海合作组织成员国普遍面临的现实问题，直接影响到成员国的政权基础、安全稳定和未来发展。上海合作组织成员国在信息安全合作领域形成了高度的共识，并展开了一系列卓有成效的合作。上海合作组织在信息安全合作方面拥有广阔的合作空间和巨大的合作潜力。

【关 键 词】　上海合作组织　信息安全合作　“颜色革命”　“三股势力”

【作者简介】　张文伟，中国社会科学院研究生院博士生。

作为支撑上海合作组织发展的“两大车轮”之一，安全合作一直是上海合作组织发展的主要动力，也是各成员国开展务实合作的重要领域。上海合作组织成立以来，遵循循序渐进的安全合作原则，逐步由双边合作向多边合作发展，由传统安全合作向非传统安全合作拓展，合作领域和范围不断拓宽，合作的深度和层次不断提升，成为维护地区稳定与安全的一支重要力量。信息安全是非传统安全的重要组成部分，近年来，上海合作组织积极面对成员国在信息安全领域面临的一系列问题和挑战，形成利益共识，重视务实合作，取得了显著成果。

一　成员国在信息安全领域面临的问题

（一）西方不断借助互联网等媒体信息推动“颜色革命”

从2003年起，独联体地区发生了一系列所谓“颜色革命”的非正常政权更迭，在多个国家引发尖锐的政治冲突和社会对抗。在这些“颜色革命”的背后，明显可以看到西方支持的反对派滥用媒体，特别是通过互联网传播、制造和放大

* 感谢匿名审稿人提出修改意见，文中疏漏由作者承担。

矛盾，散播有关国家政权腐败、内讧等虚假信息，混淆民众视听，从而引发社会动荡。2005 年年初吉尔吉斯斯坦举行议会选举之前，美国积极向该国非政府网站、新闻出版和发行单位提供技术设备和资金支持，为从业人员提供专业培训，同时着力取消吉当局对非政府网站所设置的各种限制。吉反对派利用美非政府组织“自由之家”基金会资助的《MSN》等报纸不断爆料阿卡耶夫及其家人的奢华生活，激起民众对执政者的不满。据美国媒体披露，美国政府至少向《MSN》报提供了 7 万美元的资助，并安排该报在“自由之家”所属的印刷厂印刷出版。在“自由之家”基金会的资助下，《MSN》等报纸成车运往吉境内各地，免费向民众发放。最终，吉发生大规模骚乱并引发政权非正常更迭，阿卡耶夫本人则逃往国外①。2010 年 4 月吉再次发生骚乱，当局虽吸取上次“颜色革命”的教训，关闭了多家媒体网站，但欧洲安全与合作组织随即致函吉外交部部长，要求允许民众自由登录互联网、允许独立广播电台恢复播音。

2014 年 2 月乌克兰发生的政权更迭，是美欧策动“颜色革命”的又一次行动。反对派通过“脸书”、“推特”等互联网社交媒体组织游行示威活动，进行宣传鼓动，使街头抗议活动与社交网络保持线上的实时联动，放大了示威活动的效应，最终引发亚努科维奇政权垮台②。

不断发生的“颜色革命”引起上海合作组织成员国对本国媒体特别是互联网治理的关注和思考。乌兹别克斯坦议会下院信息与通信技术委员会主席朱拉巴耶夫在一次听证会上明确主张进一步加强对互联网空间的监管，认为某些外部大国正在针对乌发起“信息战”。2015 年 3 月 4 日，俄总统普京在俄内务部会议上表示，从非法街头活动到社交网络上的公开仇恨宣传，俄罗斯正成为“颜色革命”的目标③。2014 年 12 月，普京正式批准新版《俄罗斯联邦军事学说》，该文件首次正式写入信息空间安全，认为当信息安全威胁“阻碍俄联邦国家和军事指挥系统工作，破坏战略核力量和导弹预警系统、航天空间控制、核弹药存储设施和核生化医学药物工业或其他潜在危险设施职能”时，信息安全威胁被列为军事威胁，当“信息和通信技术用于军事政治目的，以实施违反国际法、破坏国家主

① 孙壮志主编：《独联体国家“颜色革命”研究》，中国社会科学出版社 2011 年版，第 396 页。

② 潘斐斐、刘开国、张静、方兴东：《互联网在乌克兰冲突中的作用》，载《中国信息安全》2014 年第 7 期。

③ Владимир Путин принял участие в расширенном заседании коллегии Министерства внутренних дел. http：//www. kremlin. ru/events/president/news/47776

权、政治独立和领土完整的行动，对国际和平安全、全球和地区稳定带来威胁”时，它被视为外部军事危险，而“旨在破坏俄联邦信息基础设施的行为”则被视为内部军事危险”①。2014 年 10 月，塔吉克斯坦海外反对派组织“24 小组”利用“脸书”、“优图”等互联网社交网络，号召民众走上街头推翻拉赫蒙政权，引起当局高度重视。塔吉克斯坦当局为防止“广场革命”在塔上演，及时屏蔽了“脸书”、“推特”等多家社交网站，关闭 200 多家网站，控制互联网接入，甚至还一度中断了手机短信服务，最终迫使反对派取消了游行示威活动②。

境内外反华势力利用互联网积极输出西方的意识形态、政治制度、文化思想和价值理念，他们将网络作为煽动中国“颜色革命”的重要手段，通过持续、潜移默化的宣传战、舆论战，使国内的民族价值观念、意识形态和传统文化遭到严重侵蚀。同时，境内外敌对势力还利用互联网放大当前一些社会矛盾和问题，造成官方舆论和宣传被动。例如，2014 年下半年香港发生非法“占中”事件，西方媒体兴高采烈，美、英、法等国媒体迫不及待地将其冠名为“雨伞革命”，称其为“颜色革命”的香港版，一些国家还发出策应和支持“革命”的信号，其试图先搞乱香港进而搞乱中国的企图昭然若揭。

（二）“三股势力”利用互联网等进行传播，问题日益突出

信息技术的快速发展给恐怖分子在内的“三股势力”提供了更大的便利。互联网在社会政治经济生活中的作用越来越大，恐怖分子也越来越娴熟地利用其获取、传递信息，甚至直接通过其从事各种恐怖活动。据报道，“伊斯兰国”积极在“脸书”、“推特”等社交网站上传播极端思想。据塔吉克斯坦互联网管理中心人员称，目前“伊斯兰国”在社交网站上有 3 万多个账号用于传播极端主义思想，仅在“推特”上他们就有 1 300 万听众，而曼彻斯特足球俱乐部仅有 350 万听众，美总统奥巴马本人仅有 850 万听众③。

近年来，“三股势力”通过网络、电子载体等在上海合作组织成员国特别是中亚各国的青年人中加紧渗透并快速蔓延，不仅进行蛊惑人心的煽动宣传，还教唆制造爆炸装置，利用社交网络平台招募人员，甚至威胁发动恐怖袭击，成为破

① Военная доктрина Российской Федерации//Российская газета，30 декабря 2014.

② 丁晓星：《乌克兰危机对中亚地区的影响》，载《中亚国家发展报告 2015》，社会科学文献出版社 2015 年版，第 74 页。

③ Эксперты：Уроки ислама в школах – панацея от радикализма. http：//news. tj/ru/news/eksperty – uroki – islama – v – shkolakh – panatseya – ot – radikalizma

坏中亚安全稳定的一个重要因素。哈萨克斯坦官方认为，宗教极端主义传入哈境内最主要的途径是互联网①。2012 年年底，哈安全部门表示，哈西部一系列恐怖袭击事件的组织者和执行者主要是受了宣传恐怖主义和极端主义网站的影响，其中部分恐怖活动是“哈里发战士”的成员所为②。2013 年年初，一些哈萨克斯坦公民前往叙利亚参加“圣战”的视频在网上流传③。2014 年 11 月，“Daily Mail”网站播出一段名为《通向幸福之路》的视频，披露了在“伊斯兰国”军事训练营中有大批哈萨克斯坦儿童在接受宗教极端思想“洗脑”和恐怖暴力训练的事实。视频用阿拉伯语和哈萨克语两种语言解说④。乌兹别克斯坦宗教委员会称，“伊斯兰国”在乌播放关于乌极端分子在叙利亚“打胜仗”的视频，企图以此招募战斗人员。“沙特阿拉伯文化中心”等机构及其网站不仅散播极端主义言论，而且在网页上直接教授如何制造爆炸装置⑤。2011 年 4 月 23 日，宗教极端组织在网站上发布信息，称将针对塔吉克斯坦当局发动恐怖袭击。9 月 16 日，塔圣战组织通过网络散布呼吁该国穆斯林发起反政府及异教徒的恐怖袭击⑥。

俄罗斯自独立以来亦受到“三股势力”问题的袭扰。在第二次车臣战争中，车臣非法武装为获取外界支持，将车臣问题国际化，特别是积极利用“高加索中心”网站，用英、俄等语言进行舆论宣传，大肆列举俄军“暴行”，宣传宗教极端主义思想。2015 年 12 月 31 日，普京签署新版国家安全战略，将利用信息和通信技术煽动极端主义、恐怖主义和分裂主义、破坏政治与社会稳定的行为列为主要安全威胁之一。

随着中国关键基础设施对信息系统的依赖程度不断加强，互联网等新媒介也日益成为“三股势力”进行暴恐活动的重要平台和工具。“三股势力”利用互联网、手机和移动存储器等散布民族分裂主义思想，煽动民族仇恨。特别是“东突”分裂恐怖势力在境外建立数十家网站，加紧对内渗透，影响极大。2009 年 6

① Указ Президента Республики Казахстан от 24 сентября 2013 года №648 О Государственной программе по противодействию религиозному зкстремизму и терроризму в Республике Казахстан на 2013 – 2017 годы. http：//www. nomad. su/？a = 3 – 201310070036

② 《哈萨克斯坦官员称恐怖组织“哈里发战士”威胁哈安全》，新华网，2012 年 12 月 5 日。

③ 许涛：《关于上海合作组织应对全球和地区性突发事件的思考》，载《上海合作组织发展报告 2015》，社会科学文献出版社 2015 年版，第 51 页。

④ 同上，第 52 页。

⑤ 王宪举：《上海合作组织在乌克兰危机背景下如何发展》，载《上海合作组织发展报告 2015》，社会科学文献出版社 2015 年版，第 175 页。

⑥ 杨成：《上海合作组织政治与安全形势综述》，载《上海合作组织发展报告 2012》，上海人民出版社 2012 年版，第 51 ~ 52 页。

月韶关事件发生后，境外“三股势力”利用互联网将一起原本是工厂员工斗殴事件渲染为民族矛盾事件，呼吁在多地举行游行示威活动。7 月 5 日，分散在乌鲁木齐市区的数千名暴徒到处打砸抢烧，最终造成了一起惨痛的恐怖事件。2016 年 1 月，与“伊斯兰国”组织有联系的黑客首次攻击中国网站并鼓吹圣战。清华大学网站受到一个声明与“伊斯兰国”组织有联系的组织或个人的袭击，黑客将支持圣战的照片和音频贴到了清华大学教学门户网站上①。

（三）网络欺诈等问题导致俄中成为最大的网络犯罪受害国

上海合作组织覆盖着近 3 000 万平方公里的辽阔区域，占欧亚大陆总面积的五分之三。根据互联网数据统计机构 Internet World Stats 发布的数据，截至 2014 年年底，上海合作组织成员国共有网民 8 亿多，约占全球网民的 23.9%，互联网平均渗透率（网民数量占人口总数的比例）为 51.2%，略高于 46.4% 的全球互联网平均渗透率②。

国家	人口（万）	网民数量（万）	互联网渗透率
哈萨克斯坦	1 816	996	54.9%
中国	136 151	67 400	49.5%
吉尔吉斯斯坦	566	219	38.4%
俄罗斯	14 628	10 315	70.5%
塔吉克斯坦	819	143	17.5%
乌兹别克斯坦	2 920	1 271	43.6%
总体	156 900	80 314	51.2%

根据互联网数据统计机构 Internet World Stats 数据自制，其数据截至 2014 年年底。

上海合作组织成员国中，中俄两国网民更为活跃，移动网络用户众多。据中国互联网络信息中心统计，截至 2016 年 1 月，中国网民数量世界第一，其中手机网民规模达 6.2 亿。微信等移动即时通信工具使用人数众多，活跃度极高。如微信已覆盖 90% 以上的智能手机，每月活跃用户已达 6 亿，微信公众帐号总数超过 1 000 万个③。据俄罗斯社会舆论基金会的数据，在欧洲国家在线用户数量方

① 《清华大学疑遭 IS 黑客网袭》，载《参考消息》2016 年 1 月 19 日。
② 数据来源于 http：//www. internetworldstats. com/
③ 《第 37 次中国互联网络发展状况统计报告》，中国互联网络信息中心，http：//www. cnnic. net. cn

面，俄罗斯是拥有最高网民指数的国家之一，在 2013 年夏季，俄罗斯每天至少上网一次的活跃用户数量为 5 220 万人。近几年来，俄移动上网用户人数急剧上升，目前手机网民已占网民总数的 40%。

开放性、匿名性和虚拟性的特点使得互联网空间成为犯罪滋长的沃土，俄罗斯与中国在网络犯罪受害国中占据头两名位置。俄罗斯是世界上发生恶意网络活动和网络犯罪行为最多的国家，网上公民隐私时常受到侵犯，基本上每种经济网络犯罪和政治网络攻击都在俄罗斯发生过。俄联邦储蓄银行第一副行长列夫·哈西斯称，2015 年网络犯罪导致俄罗斯损失约 10 亿美元。卡巴斯基实验室数据显示，俄罗斯网络罪犯在过去四年中从世界各地盗取的资金超过 7.9 亿美元。中国是互联网大国，也是受黑客攻击最大的国家。在中国，利用微信等即时通信工具发布涉暴、涉黄等违法信息，肆意传播诽谤和谣言信息的情况不时发生。一些不法分子还利用用户泄露的信息，实施精准的欺诈和敲诈，对公民信息和资金安全造成严重威胁。2015 年，全国公安机关侦办各类互联网违法犯罪案件 173 万起，抓获违法犯罪嫌疑人 29.8 万人[①]。根据案件数量、受害者数量、涉案金额、影响度和知晓度五个指标维度分析，当前中国互联网犯罪类型依次为网络诈骗、网络销售假冒伪劣及违禁品、网络窃取泄露个人信息、网络传播谣言、网络色情、网络攻击、网络赌博、网络侵犯知识产权、网络敲诈等。

二　上海合作组织信息安全合作现状

（一）成员国就网络治理达成共识

上海合作组织成员国在网络治理方面形成了高度一致的意见和看法，在历次峰会上通过了一系列涉及信息安全的宣言和文件，积极支持中国提出的网络管理倡议。

一是一致认为各国信息安全受到多方面威胁。在 2006 年 6 月 15 日上海合作组织成员国元首上海峰会上，与会各国元首一致指出，“各成员国在信息安全领域面临的具有军事政治、犯罪和恐怖主义性质的威胁，是需要立即采取措施共同应对的新挑战。责成成员国专家组在 2007 年本组织下次峰会前制定维护信息安

① 《今年以来我国公安机关已侦办网络违法犯罪案件 173 万起》，中国青年网，2015 年 12 月 16 日。

全的行动计划，其中包括确定本组织框架内解决这一问题的途径和方式”①。2014 年，元首理事会公报再次指出，“网络安全威胁依然是影响上海合作组织地区安全稳定的不利因素”②。

二是一致认为应当采取共同行动应对网络威胁。上海合作组织成员国元首在 2006 年峰会上发表了《上海合作组织成员国元首关于国际信息安全的声明》，将信息安全方面的威胁提升到与大规模杀伤性武器威胁相等的程度，并指出，“信息通信技术和当代威胁与挑战具有跨国性质，必须通过双边、地区和国际层面的合作，加大各国保障信息安全的力度”③。2014 年 9 月，上海合作组织杜尚别峰会宣言指出，“成员国愿在尊重国家主权和不干涉别国内政的原则基础上，共同努力建立一个和平、安全、公正和开放的信息空间。成员国将合作防止使用信息通信技术危害成员国政治、经济和公共安全、稳定以及人类社会生活道德基础，阻止利用国际互联网宣传恐怖主义、极端主义、分裂主义、激进主义、法西斯主义和沙文主义思想。成员国支持所有国家平等管理互联网的权利，支持各国管理和保障各自互联网安全的主权权利”④。

三是一致认为应当对互联网进行有效的管理。2013 年 9 月，上海合作组织发表《比什凯克宣言》，称“成员国致力于以尊重国家主权、不干涉别国内政原则为基础，构建和平、安全、公正和开放的信息空间，反对将信息通信技术用于危害成员国政治、经济和公共安全的目的，阻止利用国际互联网宣传恐怖主义、分裂主义和极端主义思想，主张制定统一的信息空间国家行为准则”⑤。2015 年 12 月，中国在浙江乌镇举办第二届世界互联网大会，上海合作组织成员国领导人明确支持中方主张，即每个国家都有权在互联网管控领域上拥有自己的“主权”。梅德韦杰夫总理在会上发表演讲时表示，互联网应该是开放的，但必须对其进行管理，“任何国家都不能妄图成为世界互联网的全能管理者”。吉尔吉斯斯坦萨里耶夫总理在开幕式上致辞称，在协调立场的基础上，对利用和管理互联网形成共同立场非常重要。他还举例称，吉尔吉斯斯坦成立了总统直属的网络管理委员会，用来负责网络事务和信息通讯事务的管理和协调⑥。

① 《上海合作组织成员国元首理事会第六次会议联合公报》，华夏经纬网，2006 年 08 月 12 日。
② 《上海合作组织成员国元首理事会会议新闻公报》，新华网，2014 年 09 月 13 日。
③ 《上海合作组织成员国元首关于国际信息安全的声明》，http：//guoqing. china. com. cn
④ 《上海合作组织成员国元首杜尚别宣言》，新华网，2014 年 9 月 13 日。
⑤ 《上海合作组织成员国元首比什凯克宣言》，新华网，2013 年 9 月 13 日。
⑥ 《吉尔吉斯斯坦总理萨里耶夫：制定管理互联网的必要措施非常重要》，新华网，2015 年 12 月 16 日。

（二）组建国际信息安全专家组并开展有效合作

根据2006年6月15日的元首声明授权，上海合作组织成员国迅速组建了国际信息安全专家组，该专家组在上海合作组织的两个常设机构，即秘书处和地区反恐怖机构执委会代表的参与下，多次召开专家组会议，并在审议和研究成员国保障国际信息安全行动方面取得了显著成果。一是制定了保障各国信息安全的政府间协定。2009年6月15日，上海合作组织成员国在叶卡捷琳堡峰会上签署了《上海合作组织成员国保障国际信息安全政府间合作协定》，确定了成员国在上海合作组织框架内保障国际信息安全的途径和手段，强调各国通过双边、本组织内部和国际三个层面的合作，提高打击网络恐怖主义和网络犯罪、保障本国信息安全的能力，防止利用网络传播“三股势力”思想，防止个别国家利用网络干涉他国内政[①]。二是从专家层面上对各成员国在该领域的立法、信息安全领域现有和潜在的威胁，以及使用适当手段和方法来加以应对的前景进行比较分析，并就建立切实可行的威胁监控和协调行动机制提出相关建议。三是研究了国际信息安全领域的国际法基础、为加强上海合作组织成员国法治和安全对其加以完善的前景。2015年11月11～13日，在北京召开的上合组织国际信息安全专家组会议，强调上海合作组织通过的有关信息安全的所有文件对所有观察员国、对话伙伴国开放，研究在国际社会推进实施这些倡议的方法和前景。四是各成员国达成共识，在有关国际信息安全的问题上保持一致立场。

（三）举行成员国网络反恐演习

2013年9月20日，在俄雅罗斯拉夫市举行的上海合作组织地区反恐怖机构理事会第23次会议上，与会各方一致同意成立“上海合作组织地区反恐怖机构执委会和成员国主管机关预防和阻止使用或威胁使用电脑网络进行恐怖主义、分裂主义和极端主义活动的联合专家工作组”，该工作组由各国强力部门主管网络安全的专家组成，旨在促进上海合作组织成员国在打击“三股势力”网上活动等展开务实合作。2015年10月14日，上海合作组织成员国主管打击网络犯罪部门在厦门市举行代号为“厦门－2015”的网络反恐演习，这是上合组织首次举行的针对网络恐怖主义活动的联合演习。演习设定：某国际恐怖组织通过互联网在上海合作组织各成员国的网站、社交媒体中发布煽动“三股势力”的信息，潜

① 博·卡·努尔加利耶夫：《2008年上海合作组织的优先工作及成绩》，载《上海合作组织发展报告（2009）》，社会科学文献出版社2009年版，第13页。

伏在各成员国境内的恐怖分子受到指令拟实施暴力恐怖活动。上海合作组织地区反恐怖机构执委会在侦获相关情报后，立即启动联合网络反恐行动，协调各国发现、清除涉恐等有害信息，同时查明发布信息人员的身份信息、发布地点，迅速抓捕信息发布者，铲除了网络恐怖活动的威胁。通过此次演习，成员国一方面交流了本国打击网络犯罪的主管机关在打击利用互联网从事恐怖活动等行动中的工作流程、法律程序和组织技术能力，另一方面则进一步完善成员国相关部门在侦察并阻止利用互联网从事“三股势力”活动方面的合作机制，同时初步建立起了网络反恐的技术平台①。

（四）中俄两国积极开展上海合作组织框架下的双边合作

互联网产生于美国，将美国喻为“网络信息宗主国”毫不夸张。目前，全球网络空间处于极端失衡状态，80% 以上的网上信息来自美国。中俄两国开展信息安全合作，特别是“共同制定管理两国涉及网络安全、网络犯罪，当然还有公民在网上能做和不能做什么的互联网规则”② 对整个上合组织合作有着指导性、根本性意义。

中俄两国举行了多轮信息安全问题磋商，准备联合打击利用通信技术干涉国家内部事务、破坏国家主权、扰乱公共秩序和用于其他恐怖主义活动等犯罪活动。2015 年 5 月 8 日，中俄两国外长签署了《中华人民共和国政府和俄罗斯联邦政府关于在保障国际信息安全领域合作协定》。协定共 10 章，指出了国际信息安全面临的基本威胁，规定了中俄两国在国际信息安全领域开展合作的基本方向、基本原则、基本形式和机制，同时还明确了两国情报交换的保护原则、经费支出等。协定将利用信息通信技术破坏国际法普遍遵守的准则，如干涉其他国家内政、破坏主权和政治经济稳定、煽动民族间或教派间敌对情绪等，视为对国际信息安全领域的主要威胁。协定对中俄在保障国际信息安全领域开展合作的主要方向进行了操作性较强的具体规划，其中包括：在应对国际信息安全领域的威胁时采取一致立场，在打击利用信息通信技术从事恐怖主义和犯罪活动的行动中开展合作，在计算机应急响应、科研等领域开展共同行动，及时对国际信息安全中存在的或潜在的威胁进行情报交流，共同培训国际信息安全领域专家，交换相关专业的大学生、研究生或教师，在完善国际信息安全的国际法法律建设中展开协

① 《上合组织首次演练网络反恐》，新华网，2015 年 10 月 15 日。

② Chinese – Russian Relations Enter Cyberspace. http：//carnegieeurope. eu/strategiceurope/？ fa = 57014

作，在制定或采取必要的共同措施时加强互信。协定还承诺中俄双方互不进行黑客攻击。协定为中俄两国有关部门在国际信息安全领域开展对话和务实合作提供了法律和机制保障，表明两国在国际信息安全领域的协作到了一个新的战略性高度和水平[①]。2015 年 6 月，中俄政府专家组共同参加了联合国国际信息安全会议。此外，2015 年年底，俄罗斯互联网安全联盟（Лиги безопасного интернета России）和中国信息安全协会还签署了协议，双方专家将在信息战领域进行探讨研究，交流经验，实施打击网络攻击的联合演习，共同打击外来网络威胁。

（五）积极开展与联合国的合作

上海合作组织支持联合国在信息安全领域所做的相关工作，包括分析信息安全领域面临的威胁，以及为消除这些威胁而共同采取的措施，研究旨在加强全球信息和通信系统安全的相关国际构想等。成员国一致支持第 60 届联合国大会 2005 年 12 月 8 日通过的第 60/45 号决议、第 62 届联合国大会 2007 年 12 月 5 日通过的 62/17 号决议《从国际安全角度看信息和电信领域的发展》，并支持共同推动落实该文件中提出的各项建议。

2011 年 9 月 12 日，上海合作组织四个成员国，即中、俄、塔、乌常驻联合国代表共同提交了《信息安全国际行为准则》，其目的主要在于推动各方签署“限制甚至禁止在特定情况下使用网络武器”条约。这是国际社会首次就网络和信息安全的国际规则提出比较系统、比较全面的文件，但没有得到西方国家的正面回应。2015 年 1 月 9 日，上海合作组织六个成员国常驻联合国代表再次联名提交《信息安全国际行为准则》更新草案，并呼吁各国在联合国框架内对该问题展开进一步讨论。该更新草案结合形势变化，吸纳了国际社会的合理意见建议，内容更趋全面平衡。目前，该文件已成为联合国的正式文件。

（六）当前合作中存在的问题及难点

尽管近年来上海合作组织在信息安全合作方面取得了较为显著的成果，但随着合作的深入，也暴露出一些问题。一是上海合作组织信息安全合作很多方面还局限在每年元首峰会的宣言以及各种会议文件中，总体上形式多于内容。在中方的积极倡议下，网络反恐演习仅举行了一次，尚处在起步阶段。二是已经签署的有关信息安全合作的文件没有得到认真贯彻和落实，有时还出现以文件落实文件

① 《中俄签署国际信息安全合作协定》，中新网，2015 年 5 月 12 日。

的现象，直接影响到组织的工作效率，这对上海合作组织自身发展也产生了不良影响。不少专家学者认为，如果上海合作组织务实合作没有进展，将出现组织“论坛化”、“空心化”现象。三是相关机制运行还不够到位，一些成员国有时仍借故不出席或者降低规格出席各种会议。

造成上述问题的主要原因有以下几点。一是信息安全合作与其他非传统安全合作不同，具有一定的敏感性和特殊性。上海合作组织成员国国家大小差别巨大，经济水平发展参差不齐，科技能力强弱明显，个别成员国网络从业人员和技术水平相对较低，对信息安全合作存在一定的顾虑，制约了信息安全合作的全面深入发展。二是各国的网络管理体制和相关法律法规不尽相同。如我国目前参加上海合作组织信息安全专家组会谈时通常由外交部牵头，公安部、国防部、互联网信息管理办公室等派员参加，俄方则以联邦安全总局牵头。三是各成员国对互联网的关注度有所差别。一些成员国更多关注如何消除互联网上对本国的负面消息和新闻，一些成员国则将互联网上的斗争提高到“网络战”的高度。

三　加强上海合作组织成员国信息安全合作的几点思考

（一）以新安全观引导成员国信息安全合作

上海合作组织提出了以对话求合作，以合作促安全，以发展谋安全为主旨的“上海精神”，即“互信、互利、平等、协商、尊重多样文明、谋求共同发展”，新安全观成为指导上海合作组织安全合作的指导理论。上海合作组织成立以来，依据“上海精神”在传统安全领域及非传统安全领域均开展了广泛而务实的合作，确保了地区的安全与稳定。信息安全作为非传统安全中的新的、重要的组成部分，事关各国国计民生以及国际安全与稳定，上海合作组织成员国在该领域有高度的共识。信息和网络空间没有国界，易于被犯罪分子利用，仅仅依靠一国的法律根本无法进行规范和管理，在没有一致认可的边界，难以划定统一标准的信息空间中加强合作，对各国在相互平等、相互信任的基础上加强协作提出了更高层次的要求。在上海合作组织信息安全今后的合作中，应当向各成员国充分阐释新安全观的内涵，并对在恪守“上海精神”的原则下，如何防止由于遵守协商一致原则而带来的因一个成员国反对而造成整个组织无法就问题达成一致的现象的发生进行深入研究。

（二）切实加强地区反恐怖机构的作用

上海合作组织内，除秘书处外，仅有的一个常设机构即地区反恐怖机构。在打击“三股势力”、贩毒、跨国犯罪等活动中，地区反恐怖机构越来越认识到，“三股势力”等利用互联网开展极端思想宣传、人员招募、暴恐技能培训等破坏活动，已成为地区反恐怖机构当前工作的重点。地区反恐怖机构由各国内务、公安、安全、军队等强力部门代表组成，在执法安全领域形成了执委会、理事会以及安全会议秘书、公安内务部长会议及多个专家会议机制，在今后的信息安全合作中，应当切实发挥地区反恐怖机构作用，在安全合作目标进一步具体化的基础上，协调各方建立工作机制，联合采取共同措施。可适时提出建立上海合作组织网络安全中心，该中心可设于地区反恐怖机构之下，亦可作为独立机构设在某个中亚成员国境内，为各成员国在信息安全方面开展实质合作打下基础。同时依靠地区反恐怖机构或网络安全中心，制定举行网络反恐演习计划，将网络反恐演习搞成类似上海合作组织框架内的、机制化的联合军事演习。

（三）进一步发挥中俄两国的优势

在上海合作组织成员国中，中亚四国对信息安全管理尚处在起步阶段，以被动屏蔽网站为主。如 2014 年，哈萨克斯坦便关闭了 700 家宣扬极端主义的网站[①]。2015 年，在互联网上公布有哈萨克斯坦儿童受训视频后，哈又关闭了 500 多个网站[②]。在信息安全斗争中，发挥优势，主动出击方有可为。中俄两国在法律构建、技术装备方面具有较强的优势，面对可能的信息安全威胁，中俄更需要在达成共识的基础上，共同予以应对。俄罗斯是最早意识到信息威胁可能危害国家安全的国家，多年来，俄针对美拒绝在国际场合讨论网络安全做了持续不断、针锋相对的工作，并最早提出了对网络进行国际法规范的要求。早在 1998 年 12 月，俄罗斯便向联合国“裁军与国际安全委员会”递交名为“从国际安全的角度来看信息和电信领域的发展”的有关网络军备控制决议的草案。2005 年 12 月，联合国首次以 177：1 的绝对多数通过俄罗斯再次向联合国递交的该决议草案，表明国际社会在信息安全领域的合作取得了突破性的进展。来自 15 个国家

① 肖斌：《基于数据分析的中亚及外高加索国家社会经济发展》，载《中亚国家发展报告 2015》，社会科学文献出版社 2015 年版，第 92 页。

② Джихад приближается к Средней Азии. http：//mignews. com/news/disasters/world/100115 _ 202946 _ 77254. html

的专家组成了从国际安全的角度来看信息和电信领域的政府专家组[①]。而从全球互联网产业格局看，中国拥有广大的市场和产业基础，目前在互联网顶级域名管理权可展开实际操作意义争夺的只有中国和美国。在今后的信息安全合作中，中俄应发挥各自优势，共同抵制美国为维护其自身国家信息网络安全而推行的“双重标准”，联手打破美国的国际“信息垄断”行为。

（四）对各成员国信息安全机制和法律法规进行有效对接

上海合作组织六个成员国中，中亚四国与俄罗斯有着近 70 年的共同历史，形成了难以割断的密切联系。中亚国家在独立之后，虽然在许多方面努力体现自己的独立性，但在国家机构设置、法律法规建设方面仍与俄保持了相当程度的一致，加之苏联解体之后，俄一直致力于独联体的发展建设，在独联体内形成了颇为成熟的合作机制。而中国在国家机构设置和法律法规等方面与其他五国有较大不同。如俄罗斯与中亚各国均设有安全会议机制，统领强力部门，而中国则无类似机构。俄罗斯与中亚各国均在 20 世纪 90 年代制定有《反恐法》、《军事学说》等法律法规文件，而中国于近期才通过了《反恐法》。不同执行力的机构设置、不同衡量尺度的法律法规制约了成员国信息安全合作的实质性、深入性开展。为进一步深化上海合作组织信息安全合作，建议相关部门组织力量尽快对成员国相关法律法规进行研究，同时明确信息安全的主管机关，为上海合作组织成员国建立更加密切、高效、实质的合作关系奠定基础，从而使各成员国在有效对接的基础上开展合作。此外，应当加大成员国执法部门间在信息安全合作中联合打击行动和线索通报的力度，开展一系列的打击跨国犯罪联合行动。

（责任编辑　陆齐华）

① 《“从国际安全的角度来看信息和电信领域的发展”研究丛刊》，豆丁网。http：//www. docin. com