上海合作组织成员国保障国际信息安全政府间合作协定

上海合作组织成员国政府（以下简称“各方”）

注意到构成全球信息空间的信息通信新技术和新手段在发展和应用方面取得巨大进步；

对在民用和军事领域将这些技术和手段用于与维护国际稳定和安全相悖目的引起的威胁表示担忧；

认为国际信息安全作为国际安全体系中的一个关键因素具有重大意义；

深信各方在国际信息安全问题上进一步加深信任、加强协作是当务之急，符合各方利益；

注意到信息安全在保障个人和公民权利和基本自由方面发挥着重要作用；

考虑到联合国大会“从国际安全角度看信息和电信领域的发展”决议；

致力于遏制国际信息安全威胁，维护各方信息安全利益，构建和平、合作、和谐的国际信息环境；

希望建立各方开展国际信息安全合作的法律基础和组织基础；

商定如下：

第一条

术语和概念

为便于各方在本协定框架内开展合作，将使用商定的术语和概念，其清单见附件一《国际信息安全领域基本术语及概念清单》。该附件是本协定不可分割的一部分。

附件一在必要时，经各方商定后进行补充、明确和更新。

第二条

国际信息安全领域的主要威胁

根据本协定开展合作时，各方应以国际信息安全领域存在的下列主要威胁为出发点：

（一）信息武器的研制和使用，信息战的准备和实施。

（二）信息恐怖主义。

（三）信息犯罪。

（四）利用在信息空间的领先地位损害他国的利益和安全。

（五）传播破坏他国政治、经济和社会制度以及精神文化环境的信息。

（六）对全球和各国信息基础设施安全稳定运行的自然和（或）人为威胁。

各方对上述主要威胁的实质内容的共同理解见附件二《国际信息安全领域的威胁种类及其根源和特征清单》。该附件是本协定不可分割的一部分。

附件二可在必要时，经各方商定后进行补充、明确和更新。

第三条

主要合作方向

考虑到本协定第二条所述各种威胁，各方、其授权代表和根据本协定第五条确定的各方国家主管机构，在国际信息安全领域的下列主要方向开展合作：

（一）确定、协商并实施保障国际信息安全的必要的共同措施。

（二）建立对该领域出现的威胁的监测和共同应对体系。

（三）制定共同措施，完善国际法准则，限制威胁各方国防能力、国家和社会安全的信息武器的扩散和使用。

（四）打击以信息通信技术为手段的恐怖主义威胁。

（五）打击信息犯罪。

（六）为实现本协定目标，就保障信息安全开展必要的鉴定、调查和测评。

（七）推动保障全球互联网安全稳定运行和国际化管理。

（八）保障各方国家关键结构的信息安全。

（九）制定并实施有助于保障国际信息安全的共同信任措施。

（十）制定并实施统一政策和组织技术管理程序，实现在跨国信息交流中使用电子签名和信息保护。

（十一）就信息安全领域的各方国家立法交流信息。

（十二）完善国际法基础和实际合作机制，保障国际信息安全。

（十三）创造条件，以利各方国家主管机构为落实本协定相互配合。

（十四）在国际组织和国际论坛框架内就国际信息安全问题相互协作。

（十五）在信息安全领域交流经验，开展人员培训，举行工作会谈、会议、研讨会以及各方授权代表和专家论坛。

（十六）就本条所列主要方向开展合作问题交流信息。

各方或各方国家主管机构可协商确定其他合作方向。

第四条

合作基本原则

一、各方在本协定框架内进行合作并在国际信息空间开展活动时应遵循：此活动应当有助于社会和经济发展，符合维护国际稳定和安全的目的，遵守公认的国际法原则和准则，包括

和平解决争端和冲突、不使用武力、不干涉内政及尊重人权和基本自由，遵守地区合作原则和不侵犯各方国家信息资源的原则。

二、各方在本协定框架内的活动应符合各方享有的寻找、获得、传播信息的权利，与此同时应当考虑到此权利可能因国家和社会安全利益而受到法律限制。

三、各方平等享有保护本国国家信息资源和关键结构免受非法使用、非法干扰、包括免受信息攻击的权利。

一方不对其他方采取类似行动，对其他方实现上述权利给予支持。

第五条

合作主要方式和机制

一、在本协定生效后60天内，各方通过保存方相互交换负责落实本协定的各方国家主管机构信息，以及可就具体合作方向直接交流信息的联络渠道信息。

二、为研究本协定的执行情况，开展信息交流，分析和共同评估信息安全威胁，协商、确定和协调应对这些威胁的共同措施，各方将定期举行其授权代表及各方国家主管机构的磋商（以下简称“磋商”）。

例行磋商由各方协商举行，通常每半年在上海合作组织秘书处或提出邀请的某一方境内举行一次。

任何一方均可提议举办非例行磋商，就会期、地点和议题提出建议，并与各方和上海合作组织秘书处就此进行协商。

三、本协定具体合作方向的务实合作由各方负责落实本协定的国家主管机构实施。

四、各方国家主管机构之间可签订有关的部门间协议，为具体方向的合作奠定法律和组织基础。

第六条

信息保护

一、如果公开某些信息可能损害一方国家利益，那么本协定的任何条款都不可被解释为任何一方必须承担提供信息的义务，或该条款构成为了合作而传递信息的依据。

二、各方在根据本协定进行合作时，对任何一方国家法律规定属于国家秘密的信息不予交流。如在某些具体情况下此类信息为履行本协定所必需，其传递和使用程序则由各方签订的相关协议规定。

三、对在本协定框架内合作中传递或生成的、根据任何一方国家法律不属于国家秘密的信息，如任何一方国家法律和（或）相关规定对其接触和传播进行限制，各方应给予此类信息必要的保护。

保护这种信息应根据该信息获得方的国家法律和（或）相关规定办理。没有该信息原始提供方的书面许可，不得公开或

转让这些信息。

这种信息应根据各方国家法律和（或）相关规定以适当形式进行标注。

第七条

费用

一、各方自行承担本方代表和专家参加落实本协定的相关活动的费用。

二、对于与落实本协定有关的其他费用，各方可根据国家法律视情商定其他经费原则。

第八条

与其他国际条约的关系

本协定不妨碍各方根据其参加的其他国际条约所享有的权利和承担的义务。

第九条

争议的解决

因本协定条款的解释和适用产生的争议，各方应通过协商和谈判解决。

第十条

工作语言

本协定框架内进行合作的工作语言是俄文和中文。

第十一条

保存方

上海合作组织秘书处是本协定的保存方。

协定正本由保存方保存。保存方在本协定签订后 15 天内向各方发送核对无误的协定副本。

第十二条

最后条款

一、本协定无限期有效，并自保存方收到第 4 份完成本协定生效所必需的国内程序的书面通知后第 30 天生效。对于协定生效后完成国内程序的其他各方，本协定自保存方收到相应的书面通知后第 30 天对其生效。

二、各方经协商，可通过签订补充议定书的形式对本协定进行修订。

三、本协定不针对任何国家和组织，生效后向所有赞同本协定宗旨和原则的国家开放，任何国家都可通过向保存方递交加入书的方式加入。对于新加入国，本协定自保存方收到所有缔约国和加入国同意其加入的书面通知之日起第 30 天生效。

四、每一方均有权退出本协定。退出方应向保存方提交书面通知，退出通知应至少提前90天提交。保存方在收到退出通知之日起30天内将该情况通报其他各方。

五、如本协定终止执行，各方应采取措施，充分保证信息安全以及协定终止前在本协定框架内业经商定但尚未完成的共同工作、项目和其他活动得以执行完毕。

本协定于二OO九年六月十六日在叶卡捷琳堡签订，正本一式一份，用中文和俄文写成，两种文本同等作准。

哈萨克斯坦共和国政府代表

中华人民共和国政府代表

吉尔吉斯共和国政府代表

俄罗斯联邦政府代表

塔吉克斯坦共和国政府代表

乌兹别克斯坦共和国政府代表

《上海合作组织成员国保障国际信息安全
政府间合作协定》附件一

国际信息安全领域基本术语及概念清单

信息安全——个人、社会、国家及其利益在信息空间处于受保护状态，免受威胁、破坏和其他负面影响。

信息战——两个或两个以上国家之间在信息空间进行对抗，旨在破坏对方的信息系统、信息运转和信息资源、关键结构和其他结构，动摇对方的政治、经济和社会制度，对其民众进行心理操控，破坏其社会和国家稳定，迫使该国做出有利于敌对方的决定。

信息基础设施——生成、创建、改造、传输、使用和存储信息的技术手段和系统的总和。

信息武器——为实施信息战所使用的信息技术、手段和方法。

信息犯罪——为达到非法目的在信息空间使用和（或）影响信息资源。

信息空间——与生成、创建、改造、传输、使用和存储信息有关的，包括对个人意识和社会意识、信息基础设施及信息本身产生影响的活动范围。

信息资源——信息基础设施，以及信息本身和信息流。

信息恐怖主义——为达到恐怖主义目的，在信息空间使用和（或）影响信息资源。

关键结构——国家的设施、系统和机构，对其施加影响则可直接危害国家安全，包括个人、社会和整个国家的安全。

国际信息安全——系指这样的国际关系状态，其在信息空间可防止破坏国际稳定、威胁国家安全和国际社会安全的行为发生。

非法使用信息资源——在无相应授权或违反有关规定、各方国家法律或国际法准则的情况下使用信息资源。

未经许可干扰信息资源——非法影响信息的生成、创建、加工、改造、传输、使用和存储过程。

信息安全威胁——在信息空间中危及个人、社会、国家及其利益的各种因素。

《上海合作组织成员国保障国际信息安全政府间合作协定》附件二

国际信息安全领域的威胁种类及其根源和特征清单

一、信息武器的研制与使用，信息战的准备和实施

该威胁根源：研制和发展信息武器，可对他国关键结构构成直接威胁，可能引发新的军备竞赛，这是国际信息安全领域的主要威胁。

其威胁特征：为准备和实施信息战而使用信息武器，干扰通信传输系统和防空、反导及其他国防设施的指挥系统，使一国在入侵者面前丧失防卫能力，无法行使正当自卫权利；破坏信息基础设施的运行，使他国的管理和决策体系陷入瘫痪状态；对关键结构造成破坏性影响。

二、信息恐怖主义

该威胁根源：恐怖组织或参加恐怖活动的个人，利用或针对信息资源进行非法活动。

其威胁特征：恐怖组织利用信息网络实施恐怖活动，吸收新成员；破坏信息资源，导致社会秩序混乱；控制或封锁大众传媒渠道；利用互联网或其他信息网络散布恐怖主义言论，制造社会恐怖和恐慌，以及对信息资源造成其他负面影响。

三、信息犯罪

该威胁根源：个人或组织为犯罪目的非法使用信息资源或未经许可干扰信息资源。

其威胁特征：潜入信息系统，破坏信息的完整性、可用性和保密性；故意制作、传播计算机病毒和其他恶意程序；实施拒绝服务攻击等破坏行为；破坏信息资源；侵犯公民在信息领域的合法权利和自由，如知识产权和个人隐私；利用信息资源和手段从事诈骗、盗窃、敲诈勒索、走私、贩毒、传播儿童色情等犯罪活动。

四、利用在信息空间的领先地位损害他国利益和安全

该威胁根源：由于各国信息技术发展不平衡，发展中国家和发达国家间的“数字鸿沟”有进一步加大的趋势。一些具有信息技术优势的国家蓄意限制其他国家发展和掌握信息技术，使信息技术处于弱势的国家面临严重威胁。

其威胁特征：对信息基础设施的软硬件生产实行垄断，限制他国参与国际信息技术合作，阻碍其发展，增加其对信息技术发达国家的依赖；在出口到他国的软件和设备中设置隐藏功能，控制和影响他国信息资源和（或）关键结构；控制和垄断信息技术和产品市场，损害他国利益和安全。

五、传播破坏他国政治、经济和社会制度以及精神文化环境的信息

该威胁根源：国家、组织、团伙和个人使用信息基础设施

传播破坏他国政治、经济和社会制度以及精神文化环境的信息。

其威胁特征：借助电子媒体（广播、电视）和其他大众传媒、互联网和其他信息交换网络散布：

歪曲他国政治和社会制度、内外政策、重要的政治和社会进程及其民众精神和文化价值的信息；

宣扬恐怖主义、分裂主义和极端主义的信息；

煽动民族、种族和宗教敌意的信息。

六、对全球和国家信息基础设施安全稳定运行的自然和（或）人为威胁

该威胁根源：自然灾害和其他危险的自然现象以及突然爆发或长期积累造成的人为灾难，可对国家信息资源产生大规模的破坏性影响。

其威胁特征：破坏信息基础设施的运行，导致关键结构、国家管理和决策系统不稳定，其后果直接关系国家和社会安全。