SCO打击网络恐怖主义的司法应对措施

赵宪伟　　最高人民检察院检察技术信息研究中心

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018　Beijing·China
（原“中国互联网安全大会”）

目录

上合组织成员国总检察长会议

范围 **成员国、观察员国、对话伙伴国等**

届别 **第15届**

作用 **重申了上合组织成员国携手打击利用现代信息和通信技术实施的犯罪的现实必要性和紧迫性；提出各成员国检察机关要加强双边和多边协调合作，加大力度应对信息安全领域犯罪的挑战和威胁，特别是坚决铲除涉“三股势力”犯罪在信息网络的生存土壤，共同维护本地区的和平稳定。**

中国倡议

一是依法及时打击、从严从重惩处发生在本国境内的网络犯罪，形成强大的威慑效应。特别是要加大对涉“三股势力”网络犯罪的打击力度，针对日益突出的“**恐毒合流**”问题加强分析研判，重点打击利用网络实施的涉恐涉毒等犯罪。

二是加强司法协助和交流，扩大惩治网络犯罪成果。各成员国检察机关要进一步加强**网络犯罪侦查取证，冻结、扣押并追回被非法转移的犯罪所得，引渡或者遣返在逃犯罪嫌疑人等方面的司法协助，加强情报交流，深入开展检察业务交流和培训，提升惩治能力，形成打击合力。**

三是坚持各方联动、标本兼治，从**经济、法律、技术、情报**等方面整体考虑，做好观念引导、立法规制、技术规范、情报支撑等基础性工作，铲除网络犯罪生存空间。

上合组织成员国总检察长会议

第十五届上合组织成员国总检察长会议，提出“**举办打击网络犯罪的国际合作实践活动**”。

2018年6月6—9日，俄罗斯联邦总检察院在莫斯科组织召开。

上合组织成员国总检察长会议

成员国 1 2 3 4 5 6

哈萨克斯坦、中国、吉尔吉斯斯坦、俄罗斯、塔吉克斯坦、乌兹别克斯坦、巴基斯坦、印度

观察员国 7 8

阿富汗、白俄罗斯、伊朗、蒙古

对话伙伴国 9 10

阿塞拜疆、亚美尼亚、柬埔寨、尼泊尔、土耳其、斯里兰卡

11

南非

目录

网络恐怖主义的模式和定义

模式

定义

网络恐怖主义的模式和定义

伊朗

一是滥用现代信息和通信技术来处理传统的恐怖主义行为

二是恶意利用现代信息和通信技术实现网络恐怖主义

恐怖分子使用新型通信工具作为媒体或业务交流的工具。

恐怖分子使用现代信息和通信技术进行渗透，访问和攻击未经授权的计算机系统和网络、传播病毒和恶意程序、侵入和破坏公共网络基础设施工程（如电子银行、医疗服务机构、运输系统、生产和能源网络、发电厂等）。

亚美尼亚

网络攻击具有恐怖袭击的特征，他们旨在灌输恐惧，从而完成政治和社会任务。

印度

网络恐怖主义是一种黑客行为，他通过锁定和污染计算机等行为，以限制国家或地区的安全外交关系。2015年，涉及该国的网络攻击案件同比增长16%。2017年4月至2018年1月，超过22000个印度网站被攻击（其中包括114个政府网站被黑客入侵）。

网络恐怖主义的模式和定义

网络恐怖主义的特征

宣传极端和恐怖主义思想、招募新兵、煽动实施恐怖活动、融资、培训、规划等。

2016年，白俄罗斯公民T在一所德国监狱中被激进化，制定了恐怖主义计划。回国后，在互联网上宣誓效忠”伊斯兰国”，并开始制造一种简易爆炸装置。2017年，被判处监禁12年。

目录

SCO应对网络恐怖主义的措施

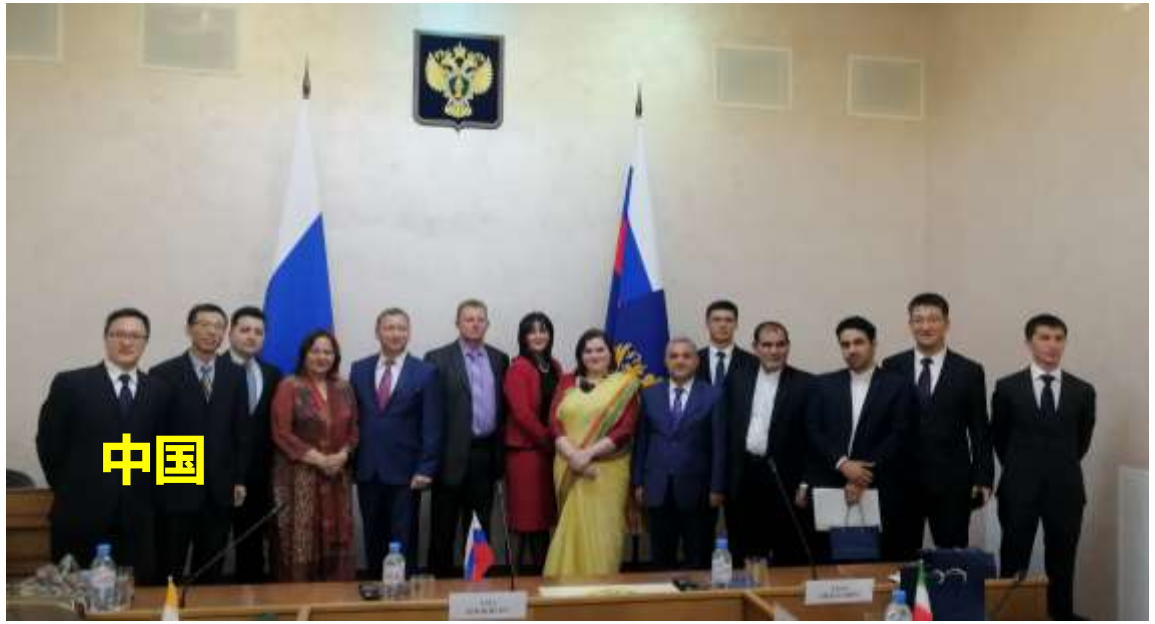
中国

印度

俄罗斯

南非

中国代表团发言主要内容



1、颁行《中华人民共和国反恐怖主义法》

2、刑法修正案（九），完善了对恐怖活动犯罪的规定，新增了五种恐怖主义犯罪

3、强化互联网服务提供者的网络安全管理责任，把常见的、带有预备实施犯罪性质的行为，在刑法中作为独立的犯罪加以规定，把打击互联网犯罪的节点前移。

4、严格规范互联网内容管理，对涉及极端宗教、恐怖主义、分裂主义等言论行为，及时依法进行处理。

5、中国执法机关及相关机构加强对网络和电子数据取证技术的研究。加强技术攻关，依法提取、固定证据，不断压缩信息网络支持暴力恐怖主义的空间。

印度

1、司法层面

2、执法机构建设

3、研究方面

4、其他方面

印度

1、在司法层面，印度政府为加大反恐的效率，不需要司法授权就可以拦截私人电话。

2、警方通过特殊手段截取的电汇、通信等，都可以直接在法庭上作为证据使用。

3、2000年就颁布了《信息技术法》。将所有的网络攻击行为，定义为网络恐怖主义行为。同时在惩罚上，从上限三年增加到终身监禁。

印度

2、成立网络调查局。2013年建成了集中式的中央监控系统（LIM），能够实时监控互联网流量、网络浏览和其他互联网活动。2014年建成国家情报网格（NETGRID）——更加集中的数据机构。计划建立国防网络局，专门用于实施网络战，作为武装部队的前驱和网络指挥。

印度

2014年，印度莫迪总理倡导制定了“有效利用基于空间技术的内部安全保障计划”，在此计划下建立了犯罪地图分析与预测系统（简称CMAPS），依托**海得拉巴高级数据研究所**，通过监控社交媒体与犯罪有关的新闻分析，可以进行犯罪模式识别、犯罪预测和警报、警察资源重新部署、犯罪热点分析等。

印度

印度自以为傲的反恐怖主义综合治理经验：立法、外交、社会经济倡议、军事、情报、技术、文化和民间社会倡议。

应用程序白名单制度

控制未经授权使用usb移动存储（类似我国的信息安全等级保护制度）

依托网络社区、覆盖全国的计算机应急相应小组

全球反恐数据库

俄罗斯

1、利用信息网络宣传恐怖主义意识形态，75%。

2、互联网游戏成为颠覆政权、宣扬恐怖主义的重要载体。

3、互联网社区”夺权“。

俄罗斯

1、如果组织或公民，在网上识别出这些信息，则通知检察官办公室，或者内政部、联邦安全局。

2、联邦通信监管局负责阻止网站

3、在阻止互联网资源之前，俄罗斯通信和媒体监管部门Roskomnadzor(俄罗斯联邦通信、信息技术和大众传媒监督局)，向通信运行商发送通知违反法律、建议自行删除信息。只有在未采取措施的情况下，才能阻止对该网站的访问。

俄罗斯

1、如果组织或公民，在网上识别出这些信息，则通知检察官办公室，或者内政部、联邦安全局。

2、联邦通信监管局负责阻止网站

3、在阻止互联网资源之前，俄罗斯通信和媒体监管部门Roskomnadzor(俄罗斯联邦通信、信息技术和大众传媒监督局)，向通信运行商发送通知违反法律、建议自行删除信息。只有在未采取措施的情况下，才能阻止对该网站的访问。

4、俄罗斯联邦检察机关与80多个国家开展此方面合作。

南非

1、面临严重的”金融圣战“威胁

2、技术层面上取得很大的突破

telegram、threema、tor、tutanota

目录

感受体会和建议

1、尽可能统一有关网络恐怖主义信息的识别，特别在法律层面上。

2、提高法律协助的效率，可以在取证协助支持上启动探索。

3、建立上合组织成员国检察机关打击网络恐怖主义犯罪专家交流机制，加强对跨国网络恐怖主义的研究。

4、国际和国家间专家交流常态化，培养地区和全球视野。


ISC
2018
ISC互联网安全大会
360互联网安全中心
谢 谢!
ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）