防火长城

维基百科，自由的百科全书

防火长城（英语：**Great Firewall of China**，常用简称：**GFW**，中文也称**中国国家防火墙**或**防火长城**[1]，中国大陆民众俗称**防火墙**[2]、**功夫网**），是对中国政府在其互联网边界审查系统（包括相关行政审查系统）的统称。此系统起步于1998年[3]，其英文名称得自于2002年5月17日Charles R. Smith所写的一篇关于中国网络审查的文章《The Great Firewall of China》[4]，取与Great Wall（长城）相谐的效果，简写为Great Firewall，缩写GFW[5]。随着使用的拓广，中文“墙”和英文“GFW”有时也被用作动词，网友所说的“被墙”即指被防火长城所屏蔽。

目录

简介

一般情况下，防火长城主要指中国政府监控和过滤互联网国际出口上内容的软硬件系统，由服务器和路由器等设备，加上相关公司的应用程序所构成，构建类似美国的棱镜项目的大机制，因此防火墙不是中国特有的一个专门单位，实际上大多数国家也会创建网络监管，不过其他政府的管理仅止于金融洗钱、国际诈骗等犯罪行为，与中国的审查机制有着相当大的不同。它的作用主要是监控国际网关上的通讯，对认为不符合中共官方要求的传输内容，进行干扰、阻断、屏蔽。由于中国网络审查广泛，中国国内含有“不合适”内容的网站，会受到政府直接的行政干预，被要求自我审查、自我监管，乃至关闭，故防火长城主要作用在于分析和过滤中国境外网络的信息互相访问。中国工程院院士、北京邮电大学前校长方滨兴是防火长城关键部分的首要设计师[1][3][6][7]。

然而，防火长城对网络内容的审查是否限制和违反了言论自由，一直是受争议的话题。也有报告认为，防火长城其实是一种圆形监狱式的全面监控，以达到自我审查的目的[8]，许多人不希望发出的消息会被屏蔽而选择中性的讲法或不说出来。而中共当局一直没有正式对外承认防火长城的存在，如当有记者在外交部新闻发布会上问及互联网封锁等问题的时候，发言人的答案基本都是“中国政府鼓励和支持互联网发展，依法保障公民言论自由，包括网上言论自由。同时，中国对互联网依法进行管理，这符合国际惯例。”方滨兴曾在访问中被问及防火长城是如何运作的时候，他指这是“国家机密”。官方媒体公开发布的报道里曾涉及防火长城的监控，从侧面证明其的确存在[9][10]，但中国一直宣称是“依法管理”，而2015年1月《环球时报》则发布报道公开宣扬其存在。[11]

中国还有一套公开在公安部辖下的网络安全项目——金盾工程，其主要功能是处理中国公安管理的业务，涉外饭店管理，出入境管理，治安管理等，所以金盾工程和防火长城的关系一直没有明确的认定。

主要技术

封锁

域名解析服务缓存污染

原理：防火长城对所有经过骨干出口路由的在UDP的53端口上的域名查询进行IDS入侵检测，一经发现与黑名单关键词相匹配的域名查询请求，防火长城会马上伪装成目标域名的解析服务器给查询者返回虚假结果。由于通常的域名查询没有任何认证机制，而且域名查询通常基于的UDP协议是无连接不可靠的协议，查询者只能接受最先到达的格式正确结果，并丢弃之后的结果。用户若改用TCP在53端口上进行DNS查询，虽然不会被防火长城污染，但可能会遭遇连接重置，导致无法获得目标网站的IP地址。

IPv6协议时代部署应用的DNSSEC技术为DNS解析服务提供了解析数据验证机制，可以有效抵御劫持。

全球一共有13组根域名服务器（Root Server），2010年中国大陆有F、I、J这3个根域DNS镜像[12]，但曾因为多次DNS污染外国网络，威胁互联网安全和自由，北京的I根域服务器被断开与国际互联网的连接。[13][14]目前已恢复服务。[15]

- 从2002年左右开始，中国大陆的网络安全单位开始采用域名服务器缓存污染技术，使用思科提供的路由器IDS监测系统来进行域名劫持，防止了一般民众访问被过滤的网站。对于含有多个IP地址或经常变更IP地址逃避封锁的域名，防火长城通常会使用此方法进行封锁，具体方法是当用户从境内

向境内DNS服务器提交域名请求时，DNS服务器要查询根域名服务器，此过程会受防火长城污染。而用户不做任何保护措施直接查询境外DNS时，会受防火长城污染。
- 当用户从境外查询境内服务器（不一定是有效DNS服务器），结果也会被污染。

- 2010年3月，当美国和智利的用户试图访问热门社交网站如facebook.com和youtube.com还有twitter.com等域名，他们的域名查询请求转交给中国控制的DNS根镜像服务器处理，由于这些网站在中国被封锁，结果用户收到了错误的DNS解析信息，这意味着防火长城的DNS污染已影响国际互联网。[16]

- 2010年4月8日，中国大陆一个小型ISP的错误路由数据，经过中国电信的二次传播，扩散到了整个国际互联网，波及到了AT&T、Level3、德国电信、Qwest和西班牙电信等多个国家的大型ISP。[17]

- 2012年11月9日下午3点半开始，防火长城对Google的泛域名*.google.com进行了大面积的污染，所有以.google.com结尾的域名均遭到污染而解析错误不能正常访问，其中甚至包括不存在的域名，而Google为各国定制的域名也遭到不同程度的污染（因为Google通过使用CNAME记录来平衡访问的流量，CNAME记录大多亦为.google.com结尾），但Google拥有的其它域名如.googleusercontent.com等则不受影响。有网友推测Google被大面积阻碍连接是因为中共正在召开的十八大。[18]
- 2014年1月21日下午三点半，中国网站的.com域名解析不正常，网站被错误地解析至65.49.2.178，该IP位于美国北卡罗来纳州的Dynamic Internet Technology，即自由门的开发公司。据推测，可能是操作失误造成的事故。[19]
- 2015年1月2日起，污染方式升级，不再是解析到固定的无效IP，而是随机地指向境外的有效IP。刚开始只是对YouTube视频域名（*.googlevideo.com）进行处理，之后逐渐扩大到大多数被污染的域名。[20]这导致了境外服务器遭受来自中国的DDoS攻击，部分网站因此屏蔽中国IP。[21]

针对境外的IP地址封锁

原理：相比起之前使用的控制访问列表（ACL）技术，现在防火长城采用了效率更高的路由扩散技术封锁特定IP地址。正常的情况下，静态路由是由管理员根据网络拓扑或是基于其它目的而给出的一条路由，所以这条路由最起码是要正确的，这样可以引导路由器把数据包转发到正确的目的地。而防火长城的路由扩散技术中使用的静态路由其实是一条错误的路由，而且是有意配置错误的，其目的就是为了把本来是发往某个IP地址的数据包统统引导到一个“黑洞服务器”上，而不是把它们转发到正确目的地。这个黑洞服务器上可以什么也不做，这样数据包就被无声无息地丢掉了。更多地，可以在服务器上对这些数据包进行分析和统计，获取更多的信息，甚至可以做一个虚假的回应。这些错误静态路由信息会把相应的IP数据包引导到黑洞服务器上，通过动态路由协议的路由重分发功能，这些错误的路由信息可以发布到整个网络。这样对于路由器来讲现在只是在根据这条路由条目做一个常规数据包转发动作，无需再进行ACL匹配，与以前的老方法相比，大大提高了数据包的转发效率。但也有技术人员指出，从以前匹配ACL表到现在匹配路由表是“换汤不换药”的做法，依然非常耗费路由器的性能[22]。而且中国大陆共有9个国际互联网出口和相当数量的骨干路由，通过这种方法封锁特定IP地址需要修改路由表，故需要各个ISP配合配置，所以其封锁成本也是各种封锁方法里最高的。

一般情况下，防火长城对于中国大陆境外的“非法”网站会采取独立IP封锁技术，然而部分“非法”网站使用的是由虚拟主机服务提供商提供的多域名、单（同）IP的主机托管服务，这就会造成了封禁某个IP地址，就会造成所有使用该服务提供商服务的其他使用相同IP地址服务器的网站用户一同遭殃，就算是“内容健康、政治无关”的网站，也不能幸免。其中的内容可能并无不当之处，但也不能在中国大陆正常访问。

- 20世纪90年代初期，中国大陆只有教育网、中国科学院高能物理研究所（高能所）和公用数据网3个国家级网关出口，中国政府对认为违反中国国家法律法规的站点进行IP地址封锁。在当时这的确是一种有效的封锁技术，但是只要找到一个普通的服务器位于境外的代理然后通过它就可以绕过这种封锁，所以现在网络安全部门通常会将包含“不良信息”的网站或网页的URL加入关键字过滤系统，并可以防止民众透过普通海外HTTP代理服务器进行访问。

IP地址特定端口封锁

原理：防火长城配合上文中特定IP地址封锁里路由扩散技术封锁的方法进一步精确到端口，从而使发往特定IP地址上特定端口的数据包全部被丢弃而达到封锁目的，使该IP地址上服务器的部分功能无法在中国大陆境内正常使用。

经常会被防火长城封锁的端口：

- SSH的TCP协议22端口
- HTTP的80端口
- PPTP类型VPN使用的TCP协议1723端口，L2TP类型VPN使用的UDP协议1701端口，IPSec类型VPN使用的UDP协议500端口和4500端口，OpenVPN默认使用的TCP协议和UDP协议的1194端口
- TLS/SSL/HTTPS的TCP协议443端口
- Squid Cache的TCP协议3128端口

在中国移动、中国联通等部分ISP的手机IP段，所有的PPTP类型的VPN都遭到封锁。

2011年3月起，长城防火墙开始对Google部分服务器的IP地址实施自动封锁（按时间段）某些端口，按时段对www.google.com（用户登录所有Google服务时需此域名加密验证）和mail.google.com的几十个IP地址的443端口实施自动封锁，具体是每10或15分钟可以连通，接着断开，10或15分钟后再连通，再断开，如此循环，使中国大陆用户和Google主机之间的连接出现间歇性中断，使其各项加密服务出现问题。[23]Google指中国这样的封锁手法高明，因为Gmail并非被完全阻断，营造出Google服务“不稳定”的假象，表面上看上去好像出自Google本身。[24][25]

2014年5月27日起，几乎所有Google服务的80和443端口被封锁。[26]2014年12月26日起，Google数段IP被路由扩散封锁，直接导致GMAIL客户端所用的IMAP/SMTP/POP3端口也被封锁。[27][28]

无状态TCP协议连接重置

原理：防火长城会监控特定IP地址的所有数据包，若发现匹配的黑名单动作（例如TLS加密连接的握手），其会直接在TCP连接握手的第二步即SYN-ACK之后伪装成对方向连接两端的计算机发送RST数据包（RESET）重置连接，使用户无法正常连接至服务器。

这种方法和特定IP地址端口封锁时直接丢弃数据包不一样，因为是直接切断双方连接因此封锁成本很低，故对于Google的多项（强制）加密服务例如Google文档、Google网上论坛、Google+和Google个人资料等的TLS加密连接都是采取这种方法予以封锁。

从2015年初开始，RST重置已被实时动态黑洞路由取代。[29]

对加密连接的干扰

- 在连接握手时，因为身份认证证书信息（即服务器的公钥）是明文传输的，防火长城会阻断特定证书的加密连接，方法和无状态TCP连接重置一样，都是先发现匹配的黑名单证书，之后通过伪装成对方向连接两端的计算机发送RST数据包（RESET）干扰两者间正常的TCP连接，进而打断与特定IP地址之间的TLS加密连接（HTTPS的443端口）握手，或者干脆直接将握手的数据包丢弃导致握手失败，从而导致TLS连接失败。但由于TLS加密技术本身的特点，这并不意味着与网站传输的内容可被破译。[30]

- Tor项目的研究人员则发现防火长城会对各种基于TLS加密技术的连接进行刺探[31]，刺探的类型有两种：
  - “垃圾二进制探针”，即用随机的二进制数据刺探加密连接，任何从中国大陆境内访问境外的443端口的连接都会在几乎实时的情况下被刺探[32]，目的是在用户创建加密连接前嗅探出他们可能所使用的反审查工具，暗示近线路速率深度包检测技术让防火长城具备了过滤端口的能力。
  - 针对Tor，当中国的一个Tor客户端与境外的网桥中继创建连接时，探针会以15分钟周期尝试与Tor进行SSL协商和重协商，但目的不是创建TCP连接。

- 切断OpenVPN的连接，防火长城会针对OpenVPN服务器回送证书完成握手创建有效加密连接时干扰连接，在使用TCP协议模式时握手会被连接重置，而使用UDP协议时含有服务器认证证书的数据包会被故意丢弃，使OpenVPN无法创建有效加密连接而连接失败。

TCP协议关键字阻断

原理：防火长城用于切断TCP连接的技术其实是TCP的一种消息，用于重置连接。一般来说，例如服务器端在没有客户端请求的端口或者其它连接信息不符时，系统的TCP协议栈就会给客户端回复一个RESET通知消息，可见RESET功能本来用于应对例如服务器意外重启等情况。而发送连接重置数据包比直接将数据包丢弃要好，因为如果是直接丢弃数据包的话客户端并不知道具体网络状况，基于TCP协议的重发和超时机制，客户端就会不停地等待和重发，加重防火长城审查的负担，但当客户端收到RESET消息时就可以知道网络被断开不会再等待了。而实际上防火长城通过将TCP连接时服务器发回的SYN/ACK数据包中服务器向用户发送的序列号改为0从而使客户端受骗认为服务器重置了连接而主动放弃向服务器发送请求，故这种封锁方式不会耗费太多防火长城的资源而效果很好，成本也相当的低。同时这种阻断可以双向工作，在中华人民共和国境外访问位于境内的网站时。如果在数据包头部出现部分关键字，连接也可能会被阻断。但是两者的关键词列表并不完全相同，比如在s.weibo.com中搜索“法轮功”连接会被阻断，搜索“六四”则不会，而在中华人民共和国境内访问境外网站时两者都会被阻断。

Firefox的“连接被重置”错误消息。当碰触到GFW设置的关键词后（如使用Google等境外搜索引擎），即可能马上出现这种画面。

本发明提供了一种阻断TCP连接的方法和装置；方法包括：保存各TCP连接的连接信息；所述TCP连接的连接信息包括该TCP协议连接的：客户端信息、服务端信息、请求方向TCP等待序列号和应答方向TCP等待序列号；抓取TCP数据包，找到该TCP数据包所属TCP连接的连接信息，根据所抓取的TCP数据包更新该连接信息中的请求方向TCP等待序列号和应答方向TCP等待序列号；如果所抓取的TCP数据包为需要阻断的TCP数据包，则根据更新后的、该TCP数据包所属TCP连接的连接信息生成RST数据包，并发送给该TCP连接的客户端和服务端。本发明可以进行准确而持续的阻断，从而能在大流量环境下的高效阻断非法TCP连接。[33]

- 针对HTTP协议的关键字阻断
  - 2002年左右开始，中国大陆研发了一套关键字过滤系统。这个系统能够从出口网关收集分析信息，过滤、嗅探指定的关键字。普通的关键词如果出现在HTTP请求数据包的头部（如“`Host: www.youtube.com`”）时，则会马上伪装成对方向连接两端的计算机发送RST数据包（Reset）干扰两者间正常的TCP连接，进而使请求的内容无法继续查看。如果防火长城在数据流中发现了特殊的内文关键词（如“falun”等）时，其也会试图打断当前的连接，从而有时会出现网页开启一部分后突然停止的情况。在任何阻断发生后，一般在随后的90秒内同一IP地址均无法浏览对应IP地址相同端口上的内容。同时这种阻断可以双向工作，在中华人民共和国境外访问位于境内的网站时，如果在数据包头部出现部分关键字，连接也可能会被阻断。两者的关键词列表并不完全相同，比如在境外使用s.weibo.com搜索“法轮功”连接会被阻断，并且90秒无法访问，搜索“六四”则不会，在中华人民共和国境内访问境外网站时两者都会被阻断。
  - 2010年3月23日，Google宣布关闭中国服务器（Google.cn）的网页搜索服务，改由Google香港域名Google.com.hk提供后，由于其服务器位于大陆境外必须经过防火长城，所以防火长城对其进行了极其严格的关键词审查。一些常见的中共高官的姓氏，如“胡”、“吴”、“温”、“贾”、“李”、“习”、“贺”、“周”、“毛”、“江”、“令”，及常见姓氏“王”、“刘”、“彭”等简体中文单字，当局实行一刀切政策全部封锁，即“学习”、“温泉”、“李白”、“圆周率”也无法搜索，使Google在中国大陆境内频繁出现无法访问或搜索中断的问题。2011年4月，防火长城开始逐步干扰Google.com.hk的搜索服务。2012年10月下旬起，防火长城使用更巧妙方式干扰Google搜索，部分用户在点击搜索结果链接跳转时一直被卡住，一直卡了6分钟之后客户端发送RST重置，然后页面一片空白。原因是链接跳转使用的是HTTP，用HTTPS跳转无影响。[34]

外部视频链接

Observations in mainland China (Chinese) (http://www.youtube.com/watch?v=vFAHKav2JZM)，YouTube

2012年Google搜索中国大陆之体验（中文版）(http://v.youku.com/v_show/id_XNDA1OTg4NDg0.html)，优酷网

- 干扰eD2k协议的连接
  - 从2011年开始，防火长城开始对所有境外eD2k服务器进行审查：当境内用户使用eD2k协议例如eMule使用模糊协议连接境外服务器时会被无条件阻断，迫使eMule使用普通方式连接境外服务器；同时防火长城对所有普通eD2k连接进行关键字审查，若发现传输内容含有关键字，则马上切断用户与境外服务器的连接，此举阻止了用户获取来源和散布共享文件信息，严重阻碍使用eD2k协议软件的正常工作。[35][36]

对破网软件的反制

因为防火长城的存在，大量境外网站无法在中国大陆境内正常访问，于是大陆网民开始逐步使用各类翻墙软件突破防火长城的封锁。针对网上各类突破防火长城的翻墙软件，防火长城也在技术上做了应对措施以减弱翻墙软件的穿透能力。通常的做法是利用上文介绍的各种封锁技术以各种途径打击翻墙软件，最大限度限制翻墙软件的穿透和传播。

同时根据中国大陆网民反映，防火长城现已有能力对基于PPTP和L2TP协议的VPN连接进行监控和封锁，这使得大陆网民突破防火长城的封锁变得更加困难。2015年起，防火长城加强对VPN的封锁，使iPhone用户无法使用VPN登录Facebook与Twitter账户。[37]

而每年每到特定的关键时间点（敏感时期）防火长城均会加大网络审查和封锁的力度，部分破网软件就可能因此无法正常连接或连接异常缓慢，甚至中国境内和境外的正常网络连接也会受到干扰：

- 3月上、中旬（中华人民共和国的“两会”召开期间、3月14日参见2008年藏区骚乱）
- 6月4日（参见六四事件）
- 7月上旬（7月1日建党节、7月5日参见乌鲁木齐七·五骚乱）
- 10月1日国庆节
- 中国共产党全国代表大会召开期间

间歇性完全封锁

间歇性封锁国际出口

从2011年5月6日起，中国大陆境内很多互联网公司以及高校、学院、科研单位的对外网络连接都出现问题，包括中国科学院。有分析指断网可能是因为防火长城已经具有了探测和分析大量加密流量并对用户IP地址执行封锁的能力，而各大机构的出口被封也在其中。具体表现为：当用户使用了破网（翻墙）软件后，其所在的公共网络IP地址会被临时封锁，所有的国际网站都无法访问，包括MSN、iTunes Store等，而访问国内网站却正常，但如果使用境外的DNS解析域名则将会由于DNS服务器被封锁导致无法解析任何域名，国内网站也会无法打开[38]。也有分析指，此举是中国当局在测试逐步切断大部分人访问国际网站的措施，以试探用户反应并最终达到推行网络“白名单”制，也就是凡没有在名单上的企业或团体其网络域名将不能解析，一般用户也无法访问[39]。而中共党机关报《人民日报》旗下的《环球时报》英文版则引述方滨兴指，一些ISP必须为自己的用户支付国际流量费用，因此这些公司“有动机”去阻碍用户访问国外网站。一位工信部官员说，用户碰到这些情况应先检查自己和网站的技术问题。[40][41]

境内骨干路由器间歇性阻断

2012年10月下旬，Google位于北京的服务器被国家级骨干路由器长时间干扰连接，包括中国大陆境内用户在内访问时返回“连接超时”错误，造成大量基于Hosts技术利用Google北京服务器作为反向代理访问Google服务的用户和软件无法正常使用，例如GoAgent。测试指出数据包经过部分国家级骨干路由器时被选择性丢弃，造成与服务器连接的丢包率飙升，甚至有部分用户反映被完全阻断与服务器之间的连接。

深度包检测

深度数据包检测（Deep packet inspection,DPI）是一种于应用层对网络上传递的数据进行侦测与处理的技术，被广泛用于入侵检测、流量分析及数据挖掘。就字面意思考虑，所谓“深度”是相对于普通的报文检测而言的——相较普通的报文检测，DPI可对报文内容和协议特征进行检测。

在中国大陆，DPI一度被ISP用于追踪用户行为以改善其广告推送业务的精准性，而最近则被国外视为防火长城城赖以检测关键词及嗅探加密流量的重要技术之一[42]。基于必要的硬件设施、适宜的检测模型及相应的模式匹配算法，防火长城能够精确且快速地从实时网络环境中判别出有悖于预期标准的可疑流量，并对此及时作出审查者所期望的应对措施。

华为公司曾被媒体指责涉及向伊拉克政府提供DPI所依赖的硬件支持以帮助后者开展网络审查工作[43]。

针对IPv6协议的审查

IPv6（互联网通信协议第6版）是被指定为IPv4继任者的下一代互联网协议版本。在IPv4网络，当时的网络设计者认为在网络协议栈的底层并不重要，安全性的责任在应用层。但是即使应用层数据本身是加密的，携带它的IP数据仍会泄漏给其他参与处理的进程和系统，造成IP数据包容易受到诸如信息包探测（如防火长城的关键字阻断）、IP欺骗、连接截获等手段的会话劫持攻击。

- 虽然用于网络层加密与认证的IPsec协议可以应用于IPv4中，以保护IPv4网络层数据的安全，但IPsec只是作为IPv4的一个可选项，没有任何强制性措施用以保证IPsec在IPv4中的实施。因为防火长城是挂载在国家级骨干路由器的旁路设备，而网络数据传输必须知道数据包来源地与数据包的目的地才能完成路由转发，故在IPv4协议时代实施的针对IP地址封锁技术和特定IP地址端口封锁技术依然对IPv6有效。
- 现阶段防火长城已经具备干扰IPv6隧道的能力[44]，因为IPv6隧道在用户到远程IPv6服务器之间的隧道是创建在IPv4协议上的，因为数据传输分片的问题或者端点未进行IPSec保护的时候很有可能暴露自己正在传输的数据，让防火长城有可乘之机干扰切断连接。
- 方滨兴在他的讲话《五个层面解读国家信息安全保障体系》中说：“比如说Web 2.0概念出现后，甚至包括病毒等等这些问题就比较容易扩散，再比如说IPv6出来之后，入侵检测就没有意义了，因为协议都看不懂还检测什么。”[45]
- 自2014年8月28日起，原先可以通过IPv6直连Google的中国教育网（CERNET）内试图通过https连接*.google.com.*等网页时，可能收到SSL证书错误的提示，其中以连接https://www.google.com.hk/几乎是每次连接均收到攻击，而其它连接例如https://ipv6.google.com/和https://accounts.google.com/也有受到攻击的报告，但攻击发生的概率相对较低。伪造的SSL证书显示其为google.com，颁发机构即为其本身，与真正的google证书不同，显示Google在中国教育网上受到中间人攻击（MITM attack）。[46][47]

对电子邮件通讯的拦截

正常情况下，邮件服务器之间传输邮件或者数据不会进行加密，故防火长城能轻易过滤进出境内外的大部分邮件，当发现关键字后会通过伪造RST数据包阻断连接。而因为这通常都发生在数据传输中间，所以会干扰到内容。也有网友根据防火长城会过滤进出境邮件的特性，查找防火长城部署的位置。[48]

2007年7月17日，大量使用中国国内邮件服务商的用户与国外通信出现了退信、丢信等普遍现象[49]，症状为：

- 中国国内邮箱给国外域发信收到退信，退信提示“Remote host said: 551 User not local; please try <forward-path>”
- 中国国内邮箱用户给国外域发信，对方收到邮件时内容均为“aaazzzaaazzzaaazzzaaazzzaaazzz”。
- 中国国内邮箱给国外域发信收到退信，退信提示“Connected to *.*.*.* but connection died.（#4.4.2）”
- 国外域给中国国内邮箱发信时收到退信，退信提示“Remote host said: 551 User not local; please try <forward-path>”
- 国外域给中国国内邮箱发信后，中国国内邮箱用户收到的邮件内容均为“aaazzzaaazzzaaazzzaaazzzaaazzz”。

对此，新浪的解释是“近期互联网国际线路出口不稳定，国内多数大型邮件服务提供商均受到影响，在此期间您与国外域名通信可能会出现退信、丢信等现象。为此，新浪VIP邮箱正在采取措施，力争尽快妥善解决该问题。”而万网客户服务中心的解释是“关于近期国内互联网国际出口存在未知的技术问题导致国内用户与国外通信可能会出现退信、丢信等普遍现象，万网公司高度重视，一直积极和国家相关机构汇报沟通，并组织了精良的技术力量努力寻找解决方案。”[50]

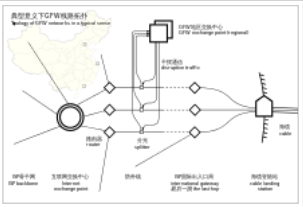
从2014年12月26日开始，有很多中国大陆网民反映说一度国内邮箱全部无法发信到Gmail。在此之前，国内一些用户可以通过IMAP、SMTP和POP3接收、下载邮件；而12月28日后，Gmail邮箱已经无法正常接收；据路透社报道Google旗下的Gmail业务已经被当局封锁。[51]

网络攻击

自2015年3月26日起至31日止，防火长城对GitHub发起旁观者攻击（英语：Man-on-the-side attack，主要针对运用GitHub服务做镜像的GreatFire和纽约时报中文版发动。[52][53][54]

硬件

据估计，防火长城可能拥有数百台曙光4000L服务器[55]。另外，思科公司也被批评参与了中国网络审查机制。


典型意义下GFW的线路拓扑

- 防火长城（北京）使用曙光4000L机群，操作系统为Red Hat系列（从7.2到7.3到AS 4），周边软件见曙光4000L一般配置
- 防火长城实验室（哈尔滨工业大学）使用曙光服务器，Red Hat操作系统
- 防火长城（上海）使用Beowulf集群。GFW是曙光4000L的主要需求来源、研究发起者、客户、股东、共同开发者。2007年防火长城机群规模进一步扩大，北京增至360节点，上海增至128节点，哈尔滨增至64节点，共计552节点。机群间星型千兆互联。计划节点数上千。
- 有理由相信防火长城（北京）拥有16套曙光4000L，每套384节点，其中24个服务和数据库节点，360个计算节点。每套价格约两千万到三千万，占005工程经费的主要部分。有3套（将）用于虚拟计算环境实验床，计千余节点。13应用于骨干网络过滤。总计6144节点，12288CPU，12288GB内存，峰值计算速度48万亿次。
- 2 GHz CPU的主机Linux操作系统下可达到600Kbps以上的捕包率。通过骨干网实验，配置16个数据流总线即可以线速处理八路OC48（一路OC48约2.5Gbps）接口网络数据。曙光4000L单结点的接入能力为每秒65万数据包，整个系统能够满足32Gbps的实时数据流的并发接入要求。有理由相信GFW的总吞吐量为512Gbps甚至更高（北京）。

会被过滤的网站

所有境外的网站都会受到关键词过滤的影响，故可能会出现暂时无法访问的情况。以下这些类型的网站被封锁的主要原因是因为其网站上发布中国政府不能接受的政治内容或未经国内政治审查过的新闻（比如中国2003年的SARS事件在中国政府揭露事实真相前关于SARS的相关报道和讨论）等方面的内容，有些综合性或技术性的网站只是含有少量的或可能牵涉到这些信息而被整体封锁。

被固定封锁或干扰的网站类型包括：

- 许多国际成人视频网站及大部分针对华人的色情论坛
- 所有涉及民运、法轮功、家庭教会、疆独、藏独以及不为中国共产党所控制或容许之宗教信仰的网站
- 大部分国际人权、保护记者及中国大陆维权组织的网站
- 台湾的大部分政府网站（如总统府、中央社等）
- 部分香港泛民主派和台湾政党网站（香港公民党、社民连，台湾民进党等）
- 大多数国际广播电台的中文网（如BBC中文网）
- 大多数香港、澳门和台湾的综合（门户/入口）网站中提供新闻的分站甚至与政治毫无关联的学术网站
- 部分港澳台及海外华人/留学生的热门论坛或讨论区
- 搜索引擎（雅虎香港hk.search.yahoo.com/search/和美国在线search.aol.com/aol/webhome等）
- 一些国际免费博客服务（如Blogger）
- 大多数港澳台的博客服务及社区类网站（如无名小站（关闭）等）
- 部分港澳台的免费在线电视台；部分海外提供Web 2.0或个人网站服务的知名或影响较大的站点
- 大多数视频类网站（如YouTube、Dailymotion、Vimeo、雅虎Video等）
- 大部分社交类网站（Facebook、Twitter、Google+等）
- 大多数天主教中文网站及部分基督教中文网站
- 博彩网站（如香港赛马会投注页面等）
- 香港及台湾的购物网站（如雅虎香港拍卖和奇摩拍卖、博客来、三民书局等）
- 部分个人网站和博客
- 大部分文件寄存网站（如Megaupload等）
- 大部分云计算文件寄存网站（如Dropbox和SugarSync等）
- 部分国际图片网站（如Flickr部分页面和Picasa网络相册等）
- 大部分免费服务器或主机（Yahoo! Small Business除首页外的全部IP和Google App Engine等）
- 大部分Twitter第三方电脑登录网站或客户端（如TweetDeck、Seesmic、推特中文圈等）以及API
- 大部分与Twitter相关的图片服务（如Twitpic、Img.ly、Yfrog、Twitgoo、ow.ly等）
- 大部分手机Twitter客户端（如Gravity、Socialscope、Snaptu等）
- 一些代理服务器或有提供类似突破网络封锁功能（VPN、SSH、网页代理等）的网站（如Hotspot Shield、Tor等）
- 部分RSS服务（如FeedBurner等）
- 手机浏览器Opera Mini国际版（Opera后自我审查使用大陆服务器）
- 诺贝尔奖多个官方网站、挪威广播公司（参见2010年诺贝尔和平奖）
- 维基百科的少量中文条目无法正常访问，而通过移动手机端查看词条可能出现完全无法连接的状况。（2015年5月19日起中文维基百科被完全屏蔽）[56]
- 顶级科学杂志《科学》的部分页面处于封锁状态，无法访问阅读某些页面的内容。
- 大部分由Google提供的有传播信息动机的服务（包括Gmail、Google云硬盘等，参见Google中国）

而一些知名的门户入口类、技术类、购物类、慈善类网站也经常被封锁，或被干扰得时断时续：

- SourceForge的项目站点托管服务（vhost，IP封锁）
- 数据访问和开源社区GitHub站点（由于抗议已解封）
- FreeBSD（已解封）
- 编程语言Python官方网站（python.org/download，已解封）
- 域名注册机构Go Daddy（已解封）
- 国际慈善组织乐施会香港网站（已解封）
- 国际知名的互联网电影数据库（IMDB，已解封）
- 购物网站Amazon.com（已解封）
- 国际门户及搜索服务网站雅虎（含地区性网站雅虎香港和雅虎奇摩的大部分服务）
- 微软Bing（已解封）

至于国际媒体几乎无一例外被封锁过，一般英文媒体在大陆召开高层会议或发生较大敏感事件会被短暂封锁，台湾泛蓝媒体（如联合报、中国时报、中天电视和中华电视公司等）有时会被短暂解封，其他大部分海外中文媒体会被长期封锁或干扰（有部分能打开首页，但无法点阅新闻内容）：

- CNN和BBC的网站（英文版主页解封，部分内容被定点封锁）
- New York Times和纽约时报中文网长期处于无法访问状态
- 在线的免费电视台直播网站及其客户端（如Livestation和TVUnetworks）
- 香港（含香港公营媒体香港电台）、澳门、台湾、新加坡、马来西亚的电台、电视台和中文报章的官方网站

防火长城对在中国大陆各ISP设置的黑名单基本上是同步和一致的，但有个别网站会有差别，例如：

- 中国移动封锁Google的图片、文件服务器域名*.ggpht.com及*.googleusercontent.com，图片搜索及诸多Google服务不能使用或出错。移动也封锁了HTC手机（含外国/港/台行货）天气预报服务器（AccuWeather提供）htc.accuweather.com，而联通和电信可以正常更新。

北京奥运与防火长城

据法新社报道，中国政府曾讨论是否在北京奥运会期间放宽防火长城的屏蔽范围[57]。在奥运前夕，曾一度被限制访问的Blogger、《中国时报》、《明报》等网站陆续被解除封锁，中文维基、BBC中文网和大赦国际网站等网站在8月1日亦被证实解封[58]，但部分被禁网站仍然未被解禁，包括“法轮功”网站、“西藏流亡政府”网站以及和“六四事件”相关的网站[59]。《齐鲁晚报》报道，有外国媒体指责中国政府违背先前全面开放互联网的承诺，奥组委发言人孙伟德表示，奥运期间将提供媒体“充分”的网络使用权，但外国记者上网不会完全不受限制。根据中国的法律，不得通过互联网传播违反法律的信息，如宣扬法轮功，以危害国家利益。希望媒体尊重中国“有关法律法规”。但文中没有解释为何众多与法轮功完全无关的新闻机构、博客、社交和视频网站也无法访问。[60]国际奥委会新闻委员会主席高斯帕也表示，国际奥委会一些官员和中国当局已达成协议，同意中国封锁一些被认为是敏感的、与奥运无关的网站[61]。

奥运会结束数月后，中国政府对海外新闻网站的封锁又重新开始。至2008年12月，重新被封锁的网站包括德国之声、BBC、美国之音、法广、澳广、加拿大广播电台等新闻机构的中文网站。此外，根据总部在美国的非盈利维权组织“自由之家”16日发布的新闻稿，这次遭中国政府封闭的还有一些被视为敏感的网站，包括无国界记者、《亚洲周刊》和《明报》等。中华人民共和国外交部发言人刘建超表示，中国总体上是采取对外开放的政策，但是中国和其他国家一样，对于网站还是要依法做必要的管理，某些网站确实存在违反中国法律的事情[62]。有评论认为，当局此次收紧舆论控制是为了防止经济危机进一步转化为社会与政治危机[63]。

参考文献

1. ^ **1.0** **1.1** 全国人大代表、北京邮电大学校长方滨兴：实施过滤计划慎用在线更新输入法 (http://www.cnii.com.cn/20080623/ca615907.htm). 中国信息产业网. 2010-03-11 [2010-03-18].
2. ^ 环球时报：防火墙带给中国互联网哪些影响 (http://tech.163.com/15/0128/14/AH26MQKQ000915BF.html). 环球时报. 2015-01-28 [2015-01-28].
3. ^ **3.0** **3.1** Great Firewall father speaks out (http://english.sina.com/china/p/2011/0217/360409.html). Global Times. [2011-02-18] （英文）.
4. ^ （英文）Great Firewall of China (http://archive.newsmax.com/archives/articles/2002/5/17/25858.shtml)，2008年1月30日新增。
5. ^ （简体中文）百度日本站被GFW屏蔽疑与色情内容有关 (http://media.people.com.cn/GB/40606/5617000.html)，人民网（有百度员工指出这是百度自我审查屏蔽内地用户，GFW并没有封锁，详见南方人物周刊：百度搜不到的与索取到的 (http://tech.163.com/08/1203/18/4S8QT3EA000915BF.html)）
6. ^ 李永峰. 网民披露方滨兴是GFW之父国庆前夕中国网络再次收紧 (http://www.yzzk.com/cfm/Content_Archive.cfm?Channel=nt&Path=2240658332/39nta.cfm). 亚洲周刊. 2009-10-04, **23** (39) [2009-09-25] （中文（繁体））.
7. ^ 方滨兴的墙内墙外 (http://www.infzm.com/content/92480). 南方周末. [2013-07-18] （中文（中国大陆））.
8. ^ （英文）JR, Crandall; Zinn D, Byrd M, Barr E, East R, ConceptDoppler: A Weather Tracker for Internet Censorship (http://www.cs.unm.edu/~crandall/concept_doppler_ccs07.pdf) (PDF), Computer and Communications Security, 2007 [2007-09-13]
9. ^ 区域经济规划密集亮相下半年步伐或继续加快 (http://news.xinhuanet.com/fortune/2011-07/07/c_121633462.htm). 新华网>新华财经. 2011年07月07日08:30:55.
10. ^ 听美国专家揭秘中国互联网瘫痪的原因 (http://tc.people.com.cn/n/2014/0126/c183175-24232291.html). 人民网通信频道. 2014年01月26日11:19.
11. ^ 防火墙给中国互联网哪些影响：成就本土行业崛起 (http://tech.huanqiu.com/internet/2015-01/5524442.html). 环球网. 2015-01-28.
12. ^ （英文）Asia Pacific Root servers (http://www.apnic.net/community/support/root-servers/root-server-map)，亚太互联网络信息中心
13. ^ DNS污染问题发生后中国根服务器被关 (http://internet.solidot.org/article.pl?sid=10/03/28/1135236). Solidot. 2010-03-28 [2011-02-10].
14. ^ After DNS problem, Chinese root server is shut down (http://www.itworld.com/networking/102576/after-dns-problem-chinese-root-server-shut-down). IT World. 2010-03-26 [2011-05-19].
15. ^ Root Server Technical Operations Assn (http://www.root-servers.org/). [2014-01-25].
16. ^ China censorship leaks outside Great Firewall via root server (http://arstechnica.com/tech-policy/news/2010/03/china-censorship-leaks-outside-great-firewall-via-root-server.ars). Ars Technica. 2010-03 [2011-05-19].
17. ^ A Chinese ISP Momentarily Hijacks the Internet (http://www.pcworld.com/article/193849/a_chinese_isp_momentarily_hijacks_the_internet.html). PC World. 2010-04-09 [2011-05-19].
18. ^ http://internet.solidot.org/internet/12/11/09/1044237.shtml (http://internet.solidot.org/internet/12/11/09/1044237.shtml). 2012-11-09 [2012-11-09].
19. ^ http://www.zhihu.com/question/22572025/answer/21822396
20. ^ 防火长城使用有效IP投毒DNS，其中包括色情网站IP (http://www.solidot.org/story?sid=42606). 2015-01-09.
21. ^ 遭DNS投毒DDoS攻击的服务器屏蔽中国IP (http://www.solidot.org/story?sid=42803). 2015-01-23.
22. ^ 深入了解GFW：路由扩散技术 (http://gfwrev.blogspot.com/2009/11/gfw_05.html). 2009-11-05 [2011-07-07].
23. ^ 翻墙专题：Google掉包问题 (http://www.rfa.org/cantonese/features/hottopic/feature_firewall_google-03112011105810.html?encoding=simplified). RFA. 2011-03-11 [2011-03-21].
24. ^ DAVID BARBOZA; CLAIRE CAIN MILLER. *Google Accuses Chinese of Blocking Gmail Service* (http://www.nytimes.com/2011/03/21/technology/21google.html). 纽约时报. 2011-03-20.（英文）
25. ^ Google accuses China of blocking Gmail (http://www.google.com/hostednews/afp/article/ALeqM5jmrkAJR9GaN2lv47rhrSivK_Lp1A?docId=CNG.59c9179dd6dee0a41928bcf240caa589.491). 法新社. 2011-03-21 [2013-03-18].
26. ^ 2014年中国大陆屏蔽谷歌服务事件 (https://zh.wikipedia.org/wiki/2014%E5%B9%B4%E4%B8%AD%E5%9B%BD%E5%A4%A7%E9%99%86%E5%B1%8F%E8%94%BD%E8%B0%B7%E6%AD%8C%E6%9C%8D [2014年5月27日].
27. ^ Gmail被中国完全屏蔽 (http://blog.caijing.com.cn/expert_article-151623-78153.shtml). [2014-12-29].
28. ^ 社评：中国出于安全考虑“封”Gmail不可信 (http://opinion.huanqiu.com/editorial/2014-12/5313832.html). [2014年12月30日].
29. ^ GFW此次升级的原理推测 (http://www.chinagfw.org/2015/01/gfw.html). [2014年1月14日].
30. ^ 翻墙专题：安全加密登入的方法 (http://www.rfa.org/cantonese/features/hottopic/feature_firewall_https-03182011112056.html?encoding=simplified). RFA. 2011-03-18 [2011-03-21].
31. ^ Knock Knock Knockin' on Bridges' Doors (https://blog.torproject.org/blog/knock-knock-knockin-bridges-doors). Tor. [2012-01-10].
32. ^ China's Great Firewall Tests Mysterious Scans On Encrypted Connections (http://www.forbes.com/sites/andygreenberg/2011/11/17/chinas-great-firewall-tests-mysterious-scans-on-encrypted-connections). [2011-11-17].
33. ^ 专利号2009100850310, 《一种阻断TCP连接的方法和装置》, http://www.cpquery.gov.cn/txnQueryBibliographicData.do?select-key:shenqingh=2009100850310, 2015-5-25查阅.
34. ^ 防火墙可能采用了更巧妙的方式干扰Google搜索 http://it.solidot.org/article.pl?sid=12/10/31/0510237
35. ^ 翻墙OK »关于GFW审查eD2k协议的相关内容汇总 (http://fqok.org/?p=3176). [2012-11-29].
36. ^ chengr28. 小盆友的可考证处：（In 2012-11-28）关于eD2k服务遭审查 (http://chengr28.blogspot.com/2012/11/in-2012-11-28ed2k.html). [2012-11-29].
37. ^ Cao Siqi. *Foreign VPN service unavailable in China* (http://www.globaltimes.cn/content/903542.shtml). 环球时报. 2015-1-23 0:23:01.（英文）
38. ^ 中国网警“修理”翻墙网民中科院也被牵连 (http://www.chinese.rfi.fr/%E4%B8%AD%E5%9B%BD/20110517-%E4%B8%AD%E5%9B%BD%E7%BD%91%E8%AD%A6%E2%80%9C%E4%BF%AE%E7%90%86%E2%80%9D%E7%BF%BB%E5%A2%99%E7%BD%91%E6%B0%91%E4%9 RFI. 2011-05-18 [2011-05-18].

39. ^ 中国网络国际访问频故障　温水煮蛙测试断外网反应？ (http://www.rfa.org/mandarin/yataibaodao/wang-05122011111956.html). RFA. 2011-05-12 [2011-05-18].
40. ^ Theories abound for overseas web access troubles (http://china.globaltimes.cn/society/2011-05/656234.html). 环球时报. 2011-05-18 [2011-05-19].
41. ^ 方滨兴教授回应国外网站不能拜访事件 (http://internet.solidot.org/internet/11/05/18/1423227.shtml). Solidot. 2011-05-18 [2011-05-19].
42. ^ Internet Filtering in China in 2004-2005: A Country Study (https://opennet.net/studies/china). Open Net Initiative. [2014-12-31].
43. ^ Special Report: How foreign firms tried to sell spy gear to Iran (http://www.reuters.com/article/2012/12/05/us-huawei-iran-idUSBRE8B409820121205). Reuters.
44. ^ （In 2012-11-20）关于近日IPv6隧道被阻断连接 (http://chengr28.blogspot.com/2012/11/in-2012-11-20ipv6.html). 2012-11-08 [2012-11-08].
45. ^ 方滨兴院士解读国家信息安全保障体系（转载） (http://www.miit.gov.cn/n11293472/n11295344/n11297007/12425553.html). 中华人民共和国工业和信息化部. 2009年 [2011-03-21].
46. ^ 谷歌在中国教育网遭国家级中间人攻击 (https://zh.greatfire.org/blog/2014/sep/authorities-launch-man-middle-attack-google). greatfire.org. 2014年9月4日.
47. ^ 知名网站遭遇SSL中间人攻击 手法很熟业务很忙 (http://it.people.com.cn/n/2014/1021/c1009-25874921.html). 2014年10月21日.
48. ^ 找出GFW在Internet的位置，全面分析国内到国外邮件受阻的原因 (http://web.archive.org/web/20101028163039/http://www.chinaunix.net/jh/14/838622.html) - ChinaUnix.net
49. ^ 无耻的GFW，测试GFW工作原理 - MDaemon Server - 邮件服务器-邮件系统-邮件技术论坛（BBS） (http://www.5dmail.net/bbs/thread-167860-1-1.html)，日期为2007年7月6日，有网友在此抱怨GFW的封锁
50. ^ （简体中文）万网关于海外邮件通信问题的进展通告 (http://web.archive.org/web/20110510051404/http://www.net.cn/service/a/zytz/200707/2312.html)
51. ^ Gmail blocked in China (http://www.reuters.com/article/idUSKBN0K70BD20141229). Reuters. 2014-12-29.
52. ^ 陈晓莉. GitHub遭遇史上最大规模DDoS攻击，反中国网路防火墙专案被锁定 (http://www.ithome.com.tw/news/94872). iThome (台北). 2015-03-30 [20150411]（中文（台湾））.
53. ^ 萧菁菁. GitHub日前被网路流量塞爆　疑似大陆利用防火长城展开DDoS攻击 (http://www.digitimes.com.tw/tw/dt/n/shwnws.asp?id=0000419181_NYC23CLN7WZQ6S2B3CPHY). 台北. 2015-03-31 [2015-04-11]（中文（台湾））.
54. ^ 申铧. 针对GitHub的攻击已经停止 (http://www.rfa.org/mandarin/Xinwen/1-04032015110250.html). 自由亚洲电台. 2015-04-03 [2015-04-11]（中文（简体））.
55. ^ 中国GFW预作新技术储备用大奖赛招徕人才（图） (http://www.rfa.org/mandarin/yataibaodao/GFW-06082010100521.html). 自由亚洲电台. 2010-06-08 [2010-06-09].
56. ^ 中文维基百科被屏蔽 (http://www.solidot.org/story?sid=44125). solidot. 2015-05-19 [2015-05-19].
57. ^ China may relax Internet curbs during the Olympics: official (http://afp.google.com/article/ALeqM5hFYStst6HwRUp0__2m1K7q8pq0eA). Google - 法新社. 2008-02-05（英文）.
58. ^ 胡锦涛接受外国媒体记者采访 (http://news.bbc.co.uk/chinese/simp/hi/newsid_7530000/newsid_7536600/7536670.stm). BBC. 2008年8月1日 [2008年8月1日]（简体中文）.
59. ^ 奥运前夕中国解禁国际特赦网站 (http://news.bbc.co.uk/chinese/simp/hi/newsid_7530000/newsid_7536700/7536710.stm). BBC. 2008年8月1日 [2008年8月1日]（简体中文）.
60. ^ 外媒指责中国政府未兑现奥运期间网络自由承诺 (http://2008.sina.com.cn/2008-08-02/0616139429.shtml). 齐鲁晚报. [2008-08-31]（中文（简体））.
61. ^ 北京奥组委：外国记者上网不会完全不受限 (http://2008.zaobao.com/pages1/focus080731a.shtml). 联合早报. 2008-07-31（中文（新加坡））.
62. ^ China 'bans BBC Chinese website' (http://news.bbc.co.uk/2/hi/asia-pacific/7785248.stm). BBC. 2008年12月16日 [2008年12月16日]（英文）.
63. ^ 中国再屏蔽外国敏感网站引发争议 (http://www.voanews.com/chinese/w2008-12-17-voa42.cfm). VOA. 2008年12月17日 [2008年12月17日]（中文（简体））.
64. Blue的炫影. “连接被重置” (http://www.scribd.com/doc/31081416/%E5%A4%A7%E8%A5%BF%E6%B4%8B%E6%9C%88%E5%88%8A-%E8%BF%9E%E6%8E%A5%E8%A2%AB%E9%87%8D%E7%BD%AE). 译言. 2008-03-24 [2008-08-29]（中文（中国大陆））.

外部链接

- （英文） Chinese bloggers run the gauntlet of forced registration, censorship (http://www.ojr.org/ojr/stories/050621glaser/)
- （英文） Website Test behind the Great Firewall of China (http://www.websitepulse.com/help/testtools.china-test.html), WebSitePulse
- （简体中文） GreatFire.org (https://zh.greatfire.org/)
- （简体中文） 入侵防御系统的评测和问题 (http://www.chinagfw.org/2009/09/gfw_21.html)
- （简体中文） 阅后即焚：“GFW” (http://web.archive.org/web/20100507065344/http://freemorenews.com/2009/08/30/burn-after-reading-gfw/)（又名GFW的前世今生）——匿名作者
- （简体中文） 深入理解GFW：内部结构 (http://gfwrev.blogspot.com/2010/02/gfw.html)

参见

- 大炮_(中国网络审查)
- 中华人民共和国网络审查
  - 中华人民共和国审查词汇列表
  - 中华人民共和国被封锁网站列表
- 突破网络审查（俗称“翻墙”或“破网”）
  - 代理服务器
  - VPN
  - hosts文件
- 中国大陆封锁维基媒体事件
- 禁止网络盗版法案（SOPA，美国提出类似机制的法案）
- 方滨兴
- 和谐社会
- 第五权