阅后即焚：GFW的前世今生，一部GFW之父方滨兴的发家史

From China Digital Space

标题的GFW之所以加上引号是因为，GFW是局外人起的绰号，它的真实称呼并非如此，但”GFW”也确实如实涵盖了这一在中国一贯隐晦而模糊的概念。

时间表

- 1998年9月22日，公安部部长办公会议通过研究，决定在全国公安机关开展全国公安工作信息化工程—”金盾工程”建设。

- 1999年4月20日，公安部向国家计委送交金盾工程立项报告和金盾工程项目建议书。

- 1999年4月25日，上万名法轮功练习者围攻中南海。

- 1999年6月，国家计算机网络与信息安全管理中心成立，局级事业单位。

- 1999年7月22日，中华人民共和国政府宣布法轮功妨碍国家安全和社会稳定，认定法轮大法研究会及法轮功为非法组织，决定予以取缔。

- 1999-2000年，在哈尔滨工业大学任教多年的方滨兴调任国家计算机网络与信息安全管理中心副总工程师。

- 1999年12月23日，国务院发文成立国家信息化工作领导小组，国务院副总理吴邦国任组长。其第一下属机构计算机网络与信息安全管理工作办公室设在已经成立的国家计算机网络与信息安全管理中心，取代计算机网络与信息安全管理部际协调小组，对”公安部、安全部、保密局、商用密码管理办公室以及信息产业部”等部门的网络安全管理进行组织协调。

- 2000-2002年，方滨兴在国家计算机网络与信息安全管理中心任总工程师、副主任、教授级高级工程师。

- 2000年4月20日，公安部成立金盾工程领导小组及办公室。

- 2000年5月，005工程开始实施。

- 2000年8月19日，大纪元时报创刊。

- 2000年10月，信息产业部组建计算机网络应急处理协调中心。

- 2000年12月28日，第九届全国人民代表大会常务委员会第十九次会议通过《关于维护互联网安全的决定》。

- 2001年，方滨兴”计算机病毒及其预防技术”获国防科学技术三等奖，排名第一。

- 2001年，方滨兴获国务院政府特殊津贴、信息产业部”在信息产业部重点工程中出突出贡献特等奖先进个人”称号，中组部、中宣部、中央政法委、公安部、民部、人事部等联合授予”先进个人”称号。

- 2001年1月19日，国家计算机网络与信息安全管理中心上海分中心成立，位于上海市黄浦区中山南路508号6楼。国家计算机网络应急技术处理协调中心上海分中心是工业和信息化部直属的中央财政全额拨款事业单位。

- 2001年4月25日，”金盾工程”经国务院批准立项。

- 2001年7月，计算机网络与信息安全管理工作办公室批准哈尔滨工业大学建立国家计算机信息内容安全重点实验室，胡铭曾、方滨兴牵头。

- 2001年7月24日，国家计算机网络与信息安全管理中心广州分中心成立，位于广州市越秀区建中路2、4号。

- 2001年8月8日，国家计算机网络与信息安全管理中心组建国家计算机网络应急处理协调中心，缩写CNCERT/CC。

- 2001年8月23日，国家信息化领导小组重新组建，中央政治局常委、国务院总理朱镕基任组长。

- 2001年11月28日，国家计算机网络与信息安全管理中心上海互联网交换中心成立。提供”互联网交换服务，互联网骨干网华东地区数据交换，数据流量监测与统计，网间通信质量监督，交换中心设备维护与运行，网间互联费用计算，网间互联争议协调”，位于上海市黄浦区中山南路508号。

- 2001年11月28日，国家计算机网络与信息安全管理中心广州互联网交换中心成立，位于广州市越秀区建中路204号。

- 2001年12月，在北京的国家计算机网络与信息安全管理中心综合楼开始兴建。

- 2001年12月17日，国家计算机网络与信息安全管理中心湖北分中心成立。

- 2002年，方滨兴任中国科学院计算技术研究所客座研究员、博士生导师、信息安全首席科学家。2002-2006年，方滨兴在国家计算机网络与信息安全管理中心任主任、总工程师、教授级高级工程师，升迁后任其名誉主任。

- 2002年1月25日，报道称：”国家计算机网络与信息安全管理中心上海互联网交换中心日前开通并投入试运行，中国电信、中国网通、中国联通、中国吉通等4家国家级互联单位首批接入。中国移动互联网的接入正在进行之中，近期可望成为第五家接入单位。”

- 2002年2月1日，国家计算机网络与信息安全管理中心新疆分中心成立。

- 2002年2月25日，国家计算机网络与信息安全管理中心贵州分中心成立。

- 2002年3月20日，多个国家计算机网络与信息安全管理中心省级分中心同时成立。

- 2002年9月3日，Google.com被封锁，主要手段为DNS劫持。

- 2002年9月12日，Google.com封锁解除，之后网页快照等功能被封锁，手段为TCP会话阻断。

- 2002年11月，经费6600万的国家信息安全重大项目”大范围宽带网络动态阻断系统”（大范围宽带网络动态处置系统）项目获国防科学技术二等奖。云晓春排名第一，方滨兴排名第二。哈尔滨工业大学计算机网络与信息内容安全重点实验室李斌、清华大学计算机系网络技术研究所、清华大学网格计算研究部杨广文有参与。

- 2003-2007年，方滨兴任信息产业部互联网应急处理协调办公室主任。

- 2003年1月31日，经费4.9亿的国家信息安全重大项目”国家信息安全管理系统”（005工程）获2002年度国家科技进步一等奖，方滨兴排名第一，胡铭曾排名第二，清华大学排名第三，哈尔滨工业大学排名第四，云晓春排名第四，北京大学排名第五，郑纬民排名第七，中国科学院计算技术研究所有参与。

- 2003年2月，在北京的国家计算机网络与信息安全管理中心综合楼工程竣工。

- 2003年7月，国家计算机网络应急处理协调中心更名为国家计算机网络应急技术处理协调中心。

- 2003年9月2日，全国”金盾工程”会议在北京召开，”金盾工程”全面启动。

- 2004年，国家信息安全重大项目”大规模网络特定信息获取系统”，经费7000万，获国家科技进步二等奖。

- 2005年，方滨兴任国防科学技术大学兼职教授、特聘教授、博士生导师。

- 2005年，方滨兴被遴选为中国工程院院士。

- 2005年，”该系统”已经在北京、上海、广州、长沙建立了互相镜像的4套主系统，之间用万兆网互联。每套系统由8CPU的多节点集群构成，操作系统是红旗Linux，数据库用的是OracleRAC。2005年国家计算机网络与信息安全管理中心（北京）就已经建立了一套384*16节点的集群用于网络内容过滤（005工程）和短信过滤（016工程）。该系统在广州、上海都有镜像，互相以十万兆网链接，可以协同工作，也可以独立接管工作。

- 2006年11月16日，”金盾工程”一期在北京正式通过国家验收，其为”为中华人民共和国公安部设计，处理中国公安管理的业务，涉外饭店管理，出入境管理，治安管理等的工程”。

- 2007年4月6日，国家计算机网络与信息安全管理中心上海分中心机房楼奠基，位于康桥镇杨高南路5788号，投资9047万元，”……是国家发改委批准实施的国家级重大项目，目前全国只有北京和上海建立了分中心，它是全国互联网信息海关，对保障国家信息安全担负着重要作用。”

- 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。

- 2007年12月，方滨兴任北京邮电大学校长。

- 2008年1月18日，信息产业部决定免去方滨兴的国家计算机网络与信息安全管理中心名誉主任、信息产业部互联网应急处理协调办公室主任职务，”另有职用”。

- 2008年2月29日，方滨兴当选第十一届全国人民代表大会安徽省代表。

- 2009年8月10日，方滨兴在”第一届中国互联网治理与法律论坛”上大力鼓吹网络实名制。

机构关系

国家计算机网络与信息安全管理中心（安管中心）是原信产部现工信部的直属部门。

安管中心与国家信息化工作领导小组计算机网络与信息安全管理工作办公室与国家计算机网络应急技术处理协调中心（CNCERT/CC，互联网应急中心）是一个机构几块牌子的关系。比如方滨兴简历中”1999-2000年在国家计算机网络应急技术处理协调中心任副总工”与”计算机网络应急处理协调中心”的成立时间两种说法就有着微妙的矛盾。实际上几个机构的人员基本一致。安管中心下属互联网交换中心与国家互联网络交换中心是不同的机构。各安管中心省级分中心一般挂靠当地的通信管理局。

安管中心的主要科研力量来自”哈尔滨工业大学一定会兴盛”方滨兴当博导有一批学生的哈工大以及关系良好的中科院计算所，这两个机构是那三个国家信息 安全重大项目的主要参与者，之后还在不断吸引人才并为安管中心输送人才和技术。在方滨兴空降北邮之后，往安管中心输血的成分中哈工大的逐渐减少，北邮的逐渐增多。

CNCERT/CC的国内”合作伙伴”有中国互联网协会主办北京光芒在线网络科技有限公司承办的中国互联网用户反垃圾邮件中心，是个没有实权的空壳；国家反计算机入侵及防病毒研究中心、国家计算机病毒应急处理中心，是公安部、科技部麾下；违法和不良信息举报中心是国新办势力范围；国家计算机网络入侵防范中心是中科院研究生院的机构，同样直接支撑CNCERT/CC。

CNCERT/CC的应急支撑单位中民营企业最初领跑者是绿盟，后来绿盟因其台谍案被罢黜，启明星辰取而代之。而安管中心具有一些资质认证、准入审 批的行政权力，这可能是民间安全企业趋之若鹜的原因。不过，民营企业并未参与到国家信息安全的核心项目建设中，安管中心许多外围项目交给民企外企做，比如 像隔离器之类的访问限制设备外包给启明星辰以作为辅助、备用，或者在与他们在网络安全监测上有所交流。

GFW与金盾没有关系

敏锐的读者从时间表应该已经看出这样的感觉了。实际上，GFW与金盾就是没有关系，两者泾渭分明，有很多区别。

公安系统搞网络监控的是公安部十一局

GFW是“国家信息关防工程”的一个子工程,直接上级是国家信息化工作领导小组和信息产业部是政治局亲自抓的国防工程.这个工程主要监测发现有害网站和信息,IP地址定位,网上对抗信息的上报,跟踪有害短信息和及时进行封堵。 江泽民,朱镕基,胡锦涛,李岚清,吴邦国等多次视察该工程

“国家信息关防工程”包括 “国家信息安全管理系统 工程代号为005。还有国家信息安全016工程等等

GFW主要是舆情 情报系统的工具，而金盾主要是公安系统的工具。GFW的总支持者是负责宣传工作的李长春，和张春江 江绵恒 最初的主要需求来自政治局 政法委 安全部 610办 ；而金盾的总支持者是公安系统的高层人士，主要需求来自公安部门。GFW主外，作网络海关用；而金盾主内，作侦查取证用。GFW建设时间短，花费少，成效好；而金盾 建设时间长，花费巨大（GFW的十倍以上），成效不显著。GFW依附于三个国家级国际出入口骨干网交换中心从CRS GSR流量分光镜像到自己的交换中心搞入侵检测，再扩散到一些放在ISP那里的路由封IP，位置集中，设备数量少；而金盾则是公安内部信息网络，无处不在，数量巨大。GFW的科研实力雄厚，国内研 究信息安全的顶尖人才和实验室有不少在为其服务，比如哈工大信息安全重点实验室、中科院计算所 软件所 高能所 国防科大总参三部 安全部9局 北邮 西电 、 上海交大 北方交大 北京电子科技学院 解放军信息工程学院 解放军装甲兵工程学院 信产部中电30所 总参56所等等；另外几乎所有985 211高校都参与此工程 一些公司商业机构也参与某些外围工程项目如 Websense packeteer BlueCoat 华为 北大方正 港湾 启明星辰 神州数码也提供了一些辅助设备 中搜 奇虎 北京大正 雅虎等等参与了搜索引擎安全管理系统 在某些省市级的网络机房里，接入监控的部门就五花八门了，有安全、公安、纪检、部队，等等部署的设备也是五花八门 正规军 杂牌军洋外援各自为战.

而金盾的科研实力较弱，公安系统的公安部第三研究所信息网络安全研发中心、国家反计算机入侵与防病毒研究中心都缺乏科研力量和科研成果，2008年8月成立信息网络安全公安部重点实验室想 与哈工大的重点实验室抗衡，还特意邀请方滨兴来实验室学术委员会，不过这个实验室光是电子数据取证的研究方向就没什么前景，而且也没什么研究成果。GFW之父方滨兴没有参与金盾工程，而工程院里在支持金盾工程的是沈昌祥；实际上那个公安部重点实验室的学术委员会名单很是有趣，沈昌祥自然排第一，方滨兴因为最近声名太显赫也不好意思不邀请他，方滨兴可能也有屈尊与公安系统打好关系的用意。

GFW发展和状况

GFW主要使用的硬件来自曙光和华为，没有思科、Juniper，软件大部为自主开发。原因很简单，对国家信息安全基础设施建设，方滨兴在他最近的 讲话《五个层面解读国家信息安全保障体系》中也一直强调”信息安全应该以自主知识产权为主”。何况GFW属于保密的国防工程而且GFW没有闲钱去养洋老爷，肥水不流外人田。李国杰是工程院信息工程部主任、曙光公司董事长、中科院计算所所长，GFW的大量服务器设备订单都给了曙光。方滨兴还将安管中心所需的大型机大订单给李国杰、国防科大卢锡城、总参56所陈左宁三位院士所在单位各一份。所以GFW为什么那么多曙光的设备，GFW为什么那么多中科院计算所的科研力量，为什么方滨兴成为 中科院计算所和国防科大都有显赫的兼职，为什么方滨兴从老家哈尔滨出来打拼短短7年时间就入选工程院卢浮宫？就是因为方滨兴头脑灵活，做事皆大欢喜。

网上有人讽刺GFW夜郎自大，事实上这是盲目乐观，无知者无畏。GFW的技术是世界顶尖的，GFW集中了哈工大、中科院、北邮货真价实的顶尖人才， 科研力量也是实打实地雄厚，什么动态SSL Freenet VPN SSH TOR GNUnet JAP I2P Psiphon 什么Feed Over Email 算什么葱。所有的翻墙方法，只要有人想得到，GFW都有研究并且有反制措施的实验室方案储备。

比如说：串接式封堵 采用中间人攻击手段来替换加密通信双方所用的没有经过可信赖CA签名保护的数字证书网关/代理间的证书协调，在出口网关上进行解密检测也就是所谓深度内容检测 七层过滤 HTTPS 是需要认证的。客户端访问服务器时，服务器端提供CA证书，但有些实现也可以不提供CA证书那么对于不提供CA证书的服务器，防火墙处理很简单，一律屏蔽掉另外检测默认的CA发证机构，如果证书不是这些机构（Verisign、Thawte Geotrust）发的，杀无赦就是在客户端与服务器端进行https握手的阶段，过滤掉一切无CA证书或使用不合法CA证书的https请求。这一步是广谱过滤，与服务器的IP地址无关。

GFW主要是入侵防御系统，检测-攻击两相模型。

所有传输层明文的翻墙方案，检测然后立即进行攻击是很容易的事情；即使传输层用TLS之类的加密无法实时检测，那种方案面向最终用户肯定是透明的，谁也不能阻止GFW也作为最终用户来静态分析其网络层可检测特征。

入侵检测然后TCP会话重置攻击算是干净利落的手段了，最不济也能通过人工的方式来查出翻墙方 法的网络层特征（仅仅目标IP地址就已经足够）然后进行定点清除。

如果是一两个国家的敌人，GFW也能找到集群来算密钥。GFW是难得能有中央财政喂奶的科研项目。那些在哈工大地下室、中科院破楼里的穷研究生即使没有钱也能搞出东西来，现在中央财政喂奶，更是干劲十足了。

GFW什么都行，就是P2P没办法，因为匿名性太好了，既不能实时检测出来，也无法通过静态分析找到固定的、或者变化而可跟踪的网络层特征。就这样也能建两个陷阱节点搞点小破坏，而且中科院的242项目”P2P协议分析与测量”一直都没停。什么时候国外开学术会议还是Defcon谁谁发一篇讲Tor安全性的paper，立即拿回来研究一番实现一下，已然紧跟学术技术最前沿了。不过实际上，即使GFW这样一个中国最顶尖的技术项目也摆脱不了山寨的本性，就是做一个东西出来很容易，但是要把东西做细致就不行了。

不过可能有人就疑问，为什么GFW什么都能封但又不真的封呢？我的这个翻墙方法一直还是好好的嘛。其实GFW有它自己的运作方式。GFW从性质上讲 是纯粹的科研技术部门，对政治势力来说是一个完全没有主观能动性的工具。GFW内部有很严格权限管理，技术与政治封装隔离得非常彻底。封什么还是解封什 么，都是完全由上峰决定，党指挥枪，授权专门人员操作关键词列表，与技术实现者隔离得很彻底，互相都不知道在做什么。所以很多时候一些莫名其妙的封禁比如 封freebsd.org封freepascal.org（可能都联想到freetibet.org），或者把跟轮子的 GPass八杆子打不着的”package.debian.org/zh-cn/lenny/gpass” 列为关键词，都是那些摆弄着IE6的官僚们的颐指气使，技术人员要是知道了都得气死。

方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中讲一个立足国情的原则，说：”主要是强调综合平衡安全成本与风险，如果风险不大就没有必要花太大的安全成本来做。在这里面需要强调一点就是确保重点的，如等级保护就是根据信息系统的重要性来定级，从而施加适当强度的保护。”

所以对于小众的翻墙方式，GFW按照它的职能发现了也就只能过一下目心里有个底，上峰根本都不知道有这么一种方式所以也根本不会去封、GFW自己也没权限封，或者知道了也懒得再花钱花精力去布置。枪打出头鸟，什么时候都是这样。

目前的状况是对于敏感数据能通过封锁基本上就是安全的，否则就被过滤掉了，对于庞大的网络数据用人来分析是不可能的，敏感数据只能基于过滤技术根据数据流里面的一些特征来发现，目前的解密技术对于庞大数据流量和加密技术想使用解密的方法是不可能实现的，只要加密数据流没有可识别的特征，过滤技术就不会有任何记录和反映，因此过滤技术是无法真正实现网络封锁的，因此必需加入新的参数，它们选择了量，即保存你的一段时间的数据。

现在的破网方法用的比较多得是动态网，无界，花园，等等，由于接点相对来说是有限的和可知的，因此保存一段时间的数据就有了意义，由于使用破网软件的人很多，不可能人人都抓，可以根据量来区分出重点，和经常使用破网软件的人，当然你可已通过代理来连接这些可知接点来解决这个问题，破网软件也提供了这样的方法，但是通过代理联接可知的接点的请求还是可能被截获的方滨兴一个人把GFW崛起过程中的政治势能全部转化为他的动能之后就把GFW扔掉了。

现在GFW是平稳期，完全是清水衙门，既没有什么后台，也无法 再有什么政治、资金上的利益可以攫取，也无法再搞什么新的大型项目，连IPv6对GFW来说都成了一件麻烦事情。方滨兴在他最近的讲话《五个层面解读国家 信息安全保障体系》中也感慨道：”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……”

GFW 一直就没有地位，一直就是一个没人管的萝莉，国新办、网监、广电、版权、通管局之类的怪蜀黍都压在上面要做这做那。所以方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中也首先强调一个机制，”需要宏观层面，包括主管部门予以支持。”所以，想解封网站，不要去找GFW本体，那没用，要去找GFW的上峰，随便哪个都行。而ISP就根本跟GFW没关系了，都不知道GFW具体搞些什么，起诉ISP完全属于没找到脉门。

不过GFW现在还是运行得很好，工作能力还有很大潜力可挖，唯一害怕的就是DDoS死撞墙。GFW的规模在前面的时间表里也有数字可以估计，而且 GFW现在的网站封禁列表也有几十万条之多。网络监控和对MSN YMSG ICQ等IM短信监控也都尽善尽美。GFW在数据挖掘和协议分析上做的还比较成功多媒体数据如音频 视频 图形图像的智能识别分析 自然语言语义判断识别模式匹配 p2p VoIP IM 流媒体 加密内容识别过滤 串接式封堵 等等是将来的重点不过GFW也没有像机器学习之类的自组织反馈机制来自动生成关键词，因为它 本身没有修改关键词的权限，所以这种技术也没必要，况且国内这种技术也是概念吹得多论文发得多实践不成熟。现在GFW和金盾最想要的就是能够从万草从中揪 出一小撮毒草的数据挖掘之类的人工智能技术。