个人使用 vpn"翻墙"是否违法？——基于规范性法律文件、案例以及相关计算机技术的分析与讨论

本文旨在分析“翻墙”行为的法律风险，并基于现行规范性法律文件和相关案例进行学术讨论。在分析相关法条时可能需要对部分计算机专业术语进行释义。但本文不涉及有关“翻墙”的任何技术指导或方法的具体介绍。

另，本文讨论的一切“XXX 合法与违法”问题，分析的主体都是“单纯访问境外网站”，不包括“访问、发布、传播违法有害信息”，后者当然属于违法犯罪行为，但这和翻墙行为没有任何本质联系，因为在境内网站也可访问、发布、传播违法有害信息。

在本文大致框架形成以前，我已查阅国内几乎所有关于“翻墙”的论文和文章，大部分探讨都存在着严重的问题，有些是法学常识性问题（或不讨论法律层面的问题），有些是计算机技术方面的常识性问题（常出现在法学类文章中）。

这是一个很有趣的现象——“翻墙”是一个同时牵涉法学和计算机技术的两个领域的跨学科问题。很多法学专家不了解技术；很多技术人员，也没有意愿探讨技术涉及的法律问题。这个疑难问题今天终于被我这个“既没学好法，又没学好计算机”的奇葩捡了漏。望两个学科的大佬们对于本文可能出现的纰漏予以指正！

如果你能完整阅读完这篇一万余字的文章（的第一章、第二章部分），你最大的收获，就是能够认识到某律所文章的部分段落（见下文引用部分）在论证中犯下的严重前提错误：

> 由于企业的“翻墙”行为既未使用合法的“国际出入口信道”，也未接入合法的“接入网络”，甚至未使用境内的“互联网络”，已经违反了《中华人民共和国计算机信息网络国际联网管理暂行规定》的规定，公安机关有权责令企业停止国际联网行为，同时给予警告，并处以 15000 元以下的罚款。

（在看完第四章的基础上），你将对“GFW”、“翻墙”等话题有更深入、更正确的认识，同时避免被不怀好意的人的类似观点（见下文引用部分）欺骗。

> 因为全球大部分根域名服务器都设立在美国，所以美国掌握互联网的底层，而中国必须建立 GFW 来保障互联网安全。这也是互联网 + 产业安全运转的重要基础。

本文论证的逻辑链如下：

国际出入口信道是物理信道，现行法只规定不允许非法架设物理信道——翻墙必定使用合法物理信道（主要在第四章展开论证）——翻墙不违法

本文的主要结论如下：

①“个人使用 vpn 等工具翻墙”的禁止性规定是不存在的，无论是从技术角度还是法律方面，访问境外网站和境内网站没有任何本质区别；

②一切翻墙行为都必须使用国家批准的合法国际出入口信道，因为全球互联网的本来面貌就是所有国家网络基建的互联互通（主要在第四章展开论证）；

③GFW 的运行基本原理是“网络攻击或入侵检测”（主要在第四章展开论证）；

④“翻墙”的基本原理是抵御“网络攻击或入侵检测”（主要在第四章展开论证）。

目录：

一、案例导入及相关材料真实性的检证

2018 年 12 月 28 日，广东韶关南雄市公安局对“翻墙”的朱某某作出行政处罚决定，理由为“擅自建立、使用非法定信道进行国际联网”，处以 1000 元人民币罚款，其处罚依据为《中华人民共和国计算机信息网络国际联网管理暂行规定》第六条、第十四条。

> 广东公安执法信息公开平台行政处罚决定书信息 韶雄公（网）行罚决字 [2019]1 号
> http://www.gdgafz.alldayfilm.com/bookDetail.html?type=1&id=1134323

笔者此前看到此新闻时一度是不相信的，但未曾料到，近日在检索过程中真的在官方信息公开平台查到了这一案件的处罚决定。但上图显示的“行政处罚决定书”拍摄样图并非来源于官方，且样图有很多可疑之处（法律文书课老师看到可能会被气哭），在此提前予以指出：

a. 样图中的文书格式非常极其不规范，正文字体大小悬殊、行距和字距不统一。表面上，该文书似乎是一份标准模板，横线是提前固定的，但细看便可发现，正文文字下划线与页面的边距不统一，因此这明显是在正文文字填写之后才事后加上“下划线”格式的。且文字没有统一边距；

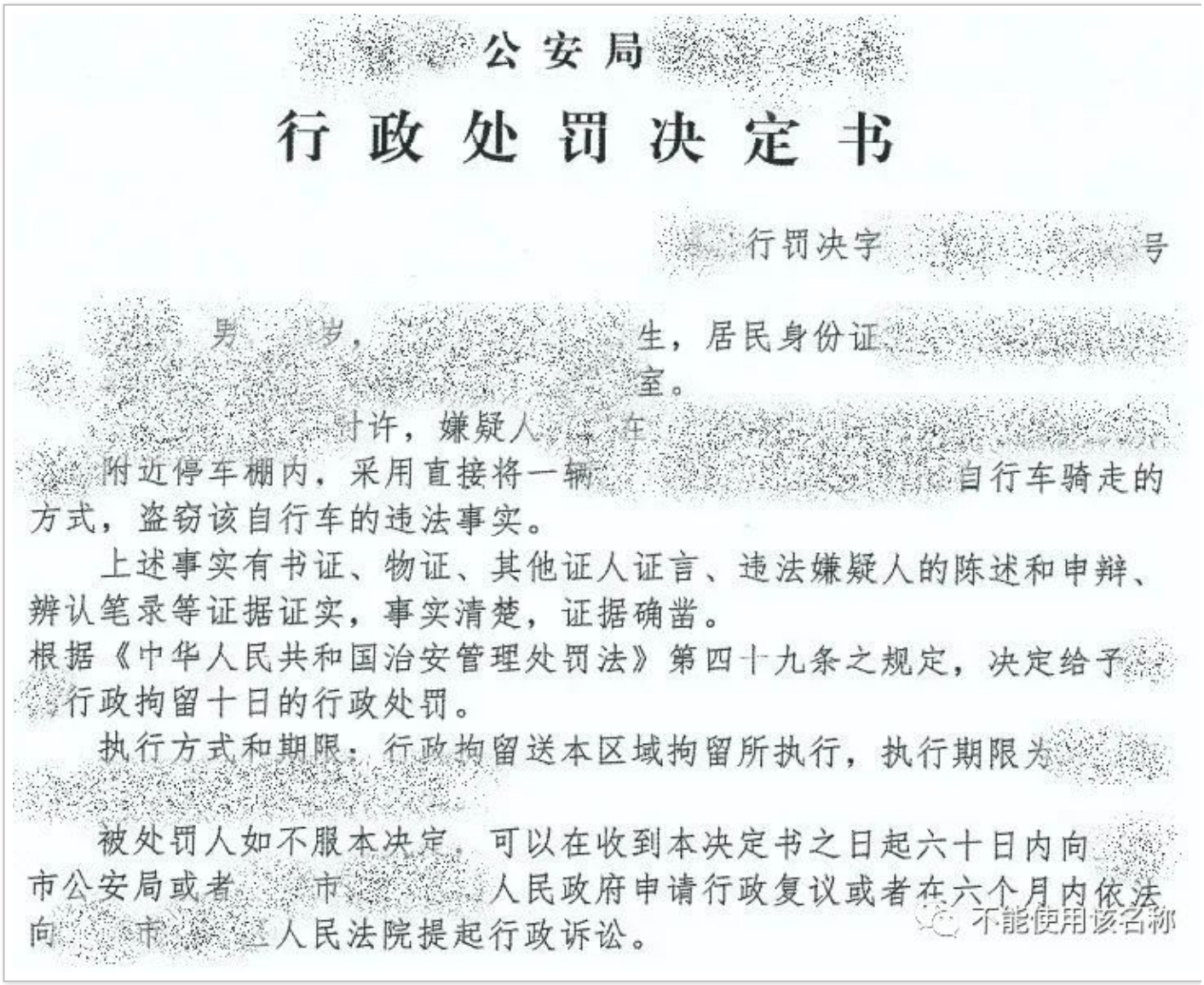
b. 在“现查明”的正文部分，“‘蓝灯’（Lantern Pro）软件 APP”中的“软件”和“APP”系表意相同的两个名词，此处连用存在语病，十分怪异；

c. 在内容部分，“且最近一周的登陆次数为 487 次”并没有相应的证据材料予以佐证。首先，行政相对人不可能记住自己使用 vpn 的连接次数，因此该数据不可能从询问笔录中反映出来。

其次，手机 app 本身并不会保存每天的连接次数，也没有日志的功能；

此外，即使该数据在手机和 app 内部以日志的形式保存，行政机关也不可能靠妄加猜测突然检查朱某某的手机，而是只可能使用远程手段（例如公安机关远程监控系统、电信运营商的举报或直接向运营商收集用户访问境外 ip 地址相关信息），但这样的证据并没有在此份决定书样图中反映出来，所以在证据层面是可疑的。

另附一份我在实习期间曾经手的一份行政处罚决定书的模板（关键信息已经隐藏）。从图中可见，基层机关行政处罚决定书的格式和行文要求是非常高的。而前后两相比较，可以看出前一份处罚决定书颇有些山寨的味道。



公安局

行政处罚决定书

行罚决字 号

男 岁， 生，居民身份证 室。

经查，嫌疑人 在 附近停车棚内，采用直接将一辆 自行车骑走的方式，盗窃该自行车的违法事实。

上述事实有书证、物证、其他证人证言、违法嫌疑人的陈述和申辩、辨认笔录等证据证实，事实清楚，证据确凿。

根据《中华人民共和国治安管理处罚法》第四十九条之规定，决定给予 行政拘留十日的行政处罚。

执行方式和期限：行政拘留送本区域拘留所执行，执行期限为

被处罚人如不服本决定，可以在收到本决定书之日起六十日内向 市公安局或者 市 人民政府申请行政复议或者在六个月内依法向 市 区人民法院提起行政诉讼。

不能使用该名称

当然，上述文书所反映的问题并不必然证明其为刻意捏造，因为笔者对于不同地区基层行政机关的法律文书和执法水平差异并不了解，但至少上述缺陷会降低该材料的可信度。

二、法条分析及相关专业名词释义

上述行政处罚案件的处罚依据如下:

> 《中华人民共和国计算机信息网络国际联网管理暂行规定》（国务院令第 195 号）（1996 年 1 月 23 日）
>
> 第六条　　计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行建立或者使用其他信道进行国际联网。
>
> 第十四条　违反本规定第六条、第八条和第十条的规定的，由公安机关责令停止联网，给予警告，可以并处 15000 元以下的罚款；有违法所得的，没收违法所得。
>
> 北大法宝 【法宝引证码】 CLI.2.13908 （现行有效）

> 关于发布《计算机信息网络国际联网出入口信道管理办法》的通知（邮部〔１９９６〕４９２号）
>
> 第二条 我国境内的计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。
>
> 任何单位和个人不得自行建立或者使用其它信道（含卫星信道）进行国际联网。
>
> 北大法宝 【法宝引证码】 CLI.4.14832 （现行有效）

1、什么是邮电部国家公用电信网提供的国际出入口信道?

有很多人一看到“自行建立或使用”、“国际出入口信道”就激动地跳了起来，认为其含义和“使用 vpn 访问境外网站”是同一种意思，但实际上这是一个非常大的误解。

首先，从立法渊源上看，“国际出入口信道”一词最早起源于 1996 年出台的《中华人民共和国计算机信息网络国际联网管理暂行规定》（下称暂行规定）和关于发布《计算机信息网络国际联网出入口信道管理办法》的通知（邮部〔１９９６〕４９２号）（下称管理办法）。但很遗憾，在两部规范性法律文件内，并没有对“国际出入口信道”作出释义。但从后者的第二条第二款我们可以从“（含卫星信道）”这一标注中洞察到“信道”可能的含义——即它很可能具有物理意义。

好在，1998 年国务院信息化领导小组又出台了一部相关的部门规章，对“国际出入口信道”的含义作出了明确的规定。

> 关于印发《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》的通知（国信［１９９８］００１号）
>
> 第三条 本办法下列用语的含义是：
>
> （三）国际出入口信道，是指国际联网所使用的物理信道。
>
> 北大法宝 【法宝引证码】 CLI.4.19760 （现行有效）

因此，国际出入口物理信道，只限于陆地光缆、海底光缆以及卫星通讯等实际存在的、供国内外进行数据、信息交换的物理介质。

根据《电信业务分类目录（2015 年版）》，国际联网所使用的物理信道包括但不限于以下几种：国际陆缆、国际海缆、陆地入境站、海缆登陆站、国际地面传输通道、国际卫星地球站、卫星空间段资源、国际传输通道的国内延伸段，以及国际通信网带宽、光通信波长、电缆、光纤、光缆等国际通信传输设施。

与此同时，我们在立法中可以发现不少细节，其足以就“国际出入口信道属于物理信道”这一论点找出进一步的佐证。

首先必须对 GFW 的渊源有一定的了解。

> 防火长城（英语：Great Firewall，常用简称：GFW，中文也称中国国家防火墙，中国大陆民众俗称墙、网络长城、功夫网等等），是对中华人民共和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**，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》，取与 Great Wall（长城）相谐的效果，简写为 Great Firewall，缩写 GFW。
>
> （维基百科）
>
> https://zh.wikipedia.org/wiki/%E9%98%B2%E7%81%AB%E9%95%BF%E5%9F%8E

可以发现，GFW 项目在 1998 年才刚刚起步，其命名甚至在 2002 年才出现，继而才出现“翻墙”这一概念。1996 年《中华人民共和国计算机信息网络国际联网管理暂行规定》出台之时，甚至没有 GFW 这一概念的存在，事实上也根本不存在互联网审查，**那么，1996 年、1998 年规范性法律文件中的概念何以提前预测并指向 1998 年以后才诞生的事物？一项禁止性规定又何以禁止不存在的东西？**

因此，毫不避讳地说，若国内各地基层公安机关真的广泛存在“依据上述规范性法律文件对公民的‘翻墙’行为予以处罚”的现象，那绝对是明显的适用法律错误。

更进一步，《暂行规定》为“擅自设立非法国际出入口信道”的行为设定了行政处罚事项，而该处罚的裁量基准是“15000 元人民币以下”。这个数字，从当今的经济水平来看，对于个人来说不算一个很大的数字（但实际

上这个上限对于个人来说已经很高了）。但是我们不要忘了，设立该处罚事项的规范性法律文件是在 1996 年出台的，我们必须关注 1996 年前后的职工平均工资水平，才能洞察“1 万 5”在行政裁量基准上的合理与否。

> 关于公布上海市 1998 年度职工月平均工资、国有企业职工年平均工资及增长率的通知
>
> ## 二、1998 年度全市国有企业职工年平均工资为 11546 元，比上年增长 0.8%（增幅按国家统计局新口径作了相应调整）。凡按 1998 年国有企业职工年平均工资计算的事项，均按此水平执行。
>
> 沪劳保综发（1999）18 号 上海市劳动和社会保障局 （链接：http://law.51labour.com/lawshow-36037.html）

你很难想象，在 1998 年，上海市作为全国经济重镇，职工的年平均工资才 1 万余元，但“翻一次墙”的行政处罚上限就可以达到一个上海普通职工工作一年半获得的工资——这不仅完全与行政法比例原则相违背，且即使是没有法学基础的人看到这样的景象都会感到震惊和难以置信。因此，我们从行政处罚的裁量基准可以反推得出，触犯上述规定的行政相对人，更可能是资本力量雄厚的企业——毕竟，一家有能力往台湾海峡私拉电线埋下海底光缆、或者为了“逛推特”专门制造并发射私人通信卫星的企业，才可能承受 1 万 5 的罚金。“建立国际出入口信道”，还真不是你普通人玩得起的！

但很有意思的是，《暂行规定》历经 20 多年，裁量基准竟然从未发生变化，依旧是上限一万五。但是 1996 年的一万五和 2020 年的一万五，可完全不是一个数量级的。但立法部门竟然从没有想着修订，也着实让人奇怪。

2、1996 年的“国际出入口信道”的概念在 20 年间是否发生变化

有人会进一步质疑，“国际出入口信道”这一概念，有没有可能随着时代的发展以及新规范性法律文件的出台，从而被赋予新的内涵和外延呢？我们不妨找一找最近几年的相关文件和新闻来分析一下。

> 为了推动中国与塔吉克斯坦、巴基斯坦间国际通信业务的共同发展，促进区域的共同繁荣，工业和信息化部批准中国电信设置塔什库尔干国际通信信道出入口，为中亚、南亚区域经济发展提供良好的通信平台和保障。
>
> 中塔直达光缆的建设，可以满足中塔间双边落地业务需求……（省略）…… 中巴直达光缆的建设将从根本上改变……（省略）……，满足中把双边落地及转接业务需求，对巴基斯坦国际出入口带宽能力

> 的丰富和提升具有重大战略意义。
> 工业和信息化部批准设置塔什库尔干国际通信信道出入口 发布时间：2011-06-27 来源：电信管理局
> （链接：http://www.miit.gov.cn/n1146290/n1146402/n7039597/c7065495/content.html）

首先，从 2011 年工业和信息化部的“批准设置塔什库尔干国际通信信道出入口”的新闻中，我们可以明显看出一个因果联系，即【国际出入口的设立→提升了国际出入口带宽能力】，而只有物理意义的光缆才可能事实上增强数据出入境的吞吐量，虚拟网络连接是做不到的，因此很容易进一步推导得出——“设置国际通信信道出入口”其本身就是“建设直达光缆”，因此，此时“信道”仍然是物理意义上的。
进一步，从近期的规范性法律文件来看，与“翻墙”关系最密切的莫过于工业和信息化部关于清理规范互联网网络接入服务市场的通知（工信部信管函 [2017]32 号） 以及工业和信息化部办公厅关于深入推进互联网网络接入服务市场清理规范工作的通知（工信厅信管函〔2018〕161 号）。

> 工业和信息化部办公厅关于深入推进互联网网络接入服务市场清理规范工作的通知
> 但随着清理规范工作深入开展，一些深层次矛盾逐步浮出水面，部分企业违规自建传输网络、非法经营传输业务及违规经营跨境数据通信等问题仍较为突出，……（省略）…… 有关事项通知如下：
> 四、各基础电信企业要加强网络资源和用户台账管理，采取技术、管理、法律等措施，防范网络资源被用于非法经营。要配合各通信管理局做好违规线索核查，及时关停被用于非法经营、违规使用的网络资源。
> 北大法宝 【法宝引证码】 CLI.4.314373

> 工业和信息化部关于清理规范互联网网络接入服务市场的通知（工信部信管函 [2017]32 号）
> 二、工作重点
> （二）严格资源管理，杜绝违规使用
> 4. 违规开展跨境业务问题。未经电信主管部门批准，不得自行建立或租用专线（含虚拟专用网络 VPN）等其他信道开展跨境经营活动。基础电信企业向用户出租的国际专线，应集中建立用户档案，向用户明确使用用途仅供其内部办公专用，不得用于连接境内外的数据中心或业务平台开展电信业务经营活动。
> 北大法宝 【法宝引证码】 CLI.4.289332

看到这两份文件的一些措辞，很多人又会将“专线（含虚拟专用网络 VPN）等其他信道”等同于 1996 年、1998 年文件提及的“国际出入口信道”，但两者是不同的概念。
首先应当明确的是，两者的规制主体范围是不同的，1996 年文件针对的是所有企业和个人，而 2017 年文件仅限于跨境业务经营的企业；96 年文件中“国际出入口信道”概念的外延仍然受到 1998 年《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》的限制，即其外延仅限于物理层面的信道，而 2017 年文件中的“专线”（含虚拟专用网络 VPN）同时包含物理层面的信道以及虚拟专用网络。因此，前者（因“信道”的物理性而）不限制个人使用虚拟 vpn，后者也（因规制主体不包括个人而）不限制个人使用虚拟 vpn。
另外，分析法条不能脱离于立法背景，之所以将 17 年、18 年两份文件并列展示，是因为两者立法在“规制 vpn”领域的意图是一致的——“部分企业违规自建传输网络、非法经营传输业务及违规经营跨境数据通信等问题仍较为突出”、“防范网络资源被用于非法经营”。其表明，相关文件的出台针对的是企业违规跨境经营以及无资质企业非法经营网络服务（包括云服务、CDN 服务），但与个人访问境外网站皆无直接关系。

值得一提的是，虽然上述文件是为了规制“企业违规使用 vpn 服务”的乱象，但其具体的措施却是将市场上一切没有相关资质的 vpn 服务全部一刀切，而相当多的 vpn 服务的主要受众是普通大众。因此，从名义上，政府规制的是企业违规跨境经营，但实际上对于个人用户访问境外网站产生了极为深远的消极影响，一个很直观的事实就是——自 2018 年以来，apple store 的所有 vpn 软件全部下架。因此，其公开的立法目的和最后的政策效果是有很大差距的。

3、当我们讨论“翻墙行为”究竟是否违法时，我们首先应该讨论什么

我认为近些年人们对于“翻墙”的研究和讨论有些本末倒置了。

行政法规作出一个禁止性规定，首先要有禁止的主体和对象。换言之，在我们讨论“翻墙违法性”之前，我们应当先讨论到底什么是“墙”，“墙”到底存不存在。

这道墙在我们每个人眼中看来，显然它是事实存在的。我在上一篇文章提及一个想法——“在一个个生活事实和亲身体验中，人的大脑永远不会欺骗自己”。但是，生活事实和亲身体验很可能影响我们对于一件事情在法律意义上的判断——因为人们倾向于相信，如果一件事情在生活中是被事实禁止的，那么他就一定规定在了法条上。

但实际上：

没有任何一个公开的规范性文件规定过：个人不允许访问境外网站。

没有一个哪怕是效力最低的红头文件敢声称：访问 youtube、Twitter 是违法的。

如果你觉得有，请带着法条来找我（但请不要携带上述我提及的规范性法律文件来找我）。

其实到这一段为止，关于个人翻墙的法律问题已经全部讲完了，但还没有形成完整的逻辑链。因为上文只解决了大前提的问题，若没有论证翻墙行为的本质这一小前提，那么就不能得出翻墙合法或违法的结论。因此在下面一节，我提前总结了技术方面的几个重要结论（虽然不是法律问题，不应放在这一章），它们的论证部分统一放在本文第四章，其论证过程是相当庞杂和啰嗦的，因此第四章仅供感兴趣的朋友们阅读。而对于大多数人来说，看完下一节的结论性总结（且无条件相信的话），对于个人翻墙问题的讨论实际上已经可以就此终结了。

4、翻墙行为是否属于私自架设物理信道?

在上文，我们明确了现行法对于个人上网的禁止性规定只限于“禁止违规搭建违法物理信道”，那么翻墙是否就是其字面意思——从一堵墙私拉一根网线翻过去呢？答案是否定的。

在看完第四章的互联网技术讨论部分，你会对以下几个重要事实有基本的认识。

（1）

任何人通过任何手段访问任何境外网站，不管是合法手段还是非法手段，不管是访问合法网站还是有违法信息的网站，其必定要通过中国电信、中国联通和中国移动三家电信运营商（经批准）架设的陆上或海底光缆。因此，翻墙不可能违反关于“物理信道”的规定，如果有，那就是适用法律错误。

（2）

全球互联网的本来面貌并非是每一个国家都在各自为政，各自建立一个庞大的“局域网”，相反，几乎所有国家的网络都是互联互通的。有了国家之间建设的陆上、海底光缆，民众访问境内网站和境外网站从技术上是没有任何区别的，在现行法意义上也是没有任何区别的。

（3）

你不能访问境外网站唯一的原因，是你正在遭受 DNS 劫持、域名污染、DDOS 攻击、TCP 旁路阻断、BGP 劫持（黑洞路由）等网络攻击或防御手段。（这些专业名词会在第四章详细介绍。）这些攻击防御手段只有技术人员才能感受到，普通人唯一的感受就是无法访问外网。当前没有任何公开的官方文件证实了上述攻击手段存在，现行法也没有为上述任何网络攻击手段提供合法性依据。

（4）

你通过任何手段进行翻墙，这一行为的本质是抵御或逃避上述网络攻击，并使用国家批准的合法互联网基础设施访问境外网站，不存在违法的问题，也没有实际的社会危害。

三、提供翻墙方法、售卖翻墙服务的违法性

这一段虽然和本文主题“个人翻墙”并没有直接关系，但本文的结论和现行司法实践对于“出售翻墙工具”的论证是矛盾的，所以必须指出来。

下图展示了可能涉及“翻墙”的罪名，我们主要关注第一类案由：“非法出售可访问境外互联网网站的'VPN'翻墙服务”，其对应的罪名是“提供侵入、非法控制计算机信息系统程序、工具罪”。

表 1：“翻墙”行为触犯罪名一览表

案号	法院	案由	触犯罪名
（2018）豫 12 刑终 271 号	河南省三门峡市中级人民法院	非法出售可访问境外互联网网站的“VPN”翻墙服务	提供侵入、非法控制计算机信息系统程序、工具罪
（2018）沪 0113 刑初 1606 号	上海市宝山区人民法院		
（2017）粤 1971 刑初 250 号	广东省东莞市第一人民法院		
（2017）粤 0307 刑初 1824 号	广东省深圳市龙岗区人民法院	通过翻墙软件收集国家领导人不实言论，在国内媒体上散布涉恶性政治谣言	寻衅滋事罪
（2018）豫 1623 刑初 224 号	河南省商水县人民法院	借助翻墙软件，在境外发布色情视频，并以此牟利	制作、复制、出版、贩卖、传播淫秽物品牟利
（2016）冀 08 刑终 343 号	河北省承德市中级人民法院	利用翻墙软件下载“法轮功”邪教组织内容材料，并制作成小册子、光盘等宣传品进行宣传	利用邪教组织破坏法律实施罪
（2018）鲁 0811 刑初 489 号	山东省济宁市任城区人民法院	利用翻墙软件，在境外网站多次捏造散布虚假信息，随意贬损诽谤国家领导人	诽谤罪

目前出售翻墙服务是违法犯罪行为，相关的案例在无讼的检索结果中不计其数。法院判决的论述部分基本上与下面的引用大同小异：

> 本院认为，被告人为牟取非法利益，违反国家规定，在互联网推广用于侵入计算机信息系统的程序、工具，情节特别严重，其行为已构成提供侵入、非法控制计算机信息系统的程序、工具罪。公诉机关指控的罪名成立。经查，本案的“XXX”软件，利用公用网络架设专用网络，并进行数据加密传输，使计算机信息系统自由访问中国境内无法访问的境外网站，因此，该软件属于“用于侵入计算机信息系统的程序、工具”。被告人在未经电信主管部门批准的情况下，提供的“XXX”软件使客户的计算机自由访

> 问境外网站，数据传输受到加密保护，突破我国技术安全防护措施，危害了国家信息网络安全，符合提供侵入、非法控制计算机信息系统的程序、工具罪的客体。
> （2018）鄂 1202 刑初 389 号

自从我学习了这个罪名以来，就对此抱有极大的质疑。翻墙工具怎么可以等同于“用于侵入计算机信息系统的程序、工具”？

一个最简单的反驳实例就是，GFW 最早的原理是将 google.com 指向无效 ip 地址（即第四章论述的 DNS 污染 / 域名劫持），而最早的翻墙原理是在本地建立一个 DNS 库，将 google.com 指向真实的 ip 地址，或者使用 8.8.8.8 这样尚未被污染的 DNS 服务器，这样当你在浏览器键入 google.com 这一域名的时候，其就会访问正确的服务器。而这一行为的唯一操作步骤，就是打开 windows 的一个名为 hosts 的系统文件，将谷歌域名对应的 ip 地址录入，或者修改本地网卡的 DNS 设置，翻墙的效果就达成了。这样一个简单的步骤，怎么可能侵入了外人的计算机信息系统?

而“架设专用网络，进行数据加密”是一个非常常用的网络应用，很简单的例子，在家里访问学校的图书馆以及学术资源，要打开 vpn 软件，这就是建立了一个加密通道，其和翻墙软件的原理是一模一样的，只存在结果上的不同。而这种技术突破“我国技术安全防护措施”的唯一原因，是由于这个所谓的“防护措施”会对你的网络请求进行分析，而加密流量很难被分析。况且，现行的规范性法律文件从没有提及这些法院判决中提到的“我国技术安全防护措施”。

另一个很有意思的问题是法院判决中通常会提到的“使计算机信息系统自由访问中国境内无法访问的境外网站”。但看了本文第四章，你就会认识到，这个世界上的互联网的本来面貌，就是让每个人可以自由地访问不同国家的服务器，并且这种自由在 2002 年以前是普遍存在的，在 2010 年以前也是大部分人都能享受到的。除非真的有一部行政法规出台，告诉我个人不能访问境外网站，这样我才能理解法院竟然能给出这样的表述。

另外，你可以洞察到，在法官论证部分，通常会有常人难以发现的跳跃性和滑坡论证。例如，“利用公用网络架设专用网络，并进行数据加密传输，使计算机信息系统自由访问中国境内无法访问的境外网站，因此，该软件属于“用于侵入计算机信息系统的程序、工具”。”这句话看似行云流水，但你细究下来，就会产生非常多的疑问——为什么一个工具可以自由访问原本无法访问的境外网站，就是侵入计算机信息系统的工具？为什么有些网站不能访问，其依据是什么？侵入的是哪一个计算机信息系统？该系统的 ip 地址是什么？地理位置具体在哪里？有什么相关规定吗？这种暧昧和含糊其辞其实不难理解，因为 GFW 这个词真的从未出现在某个文件上，但难以想象，“翻墙”这个词居然可以在相关的判决文书中随处可见。

但是，我是绝对支持对一些市面上大部分出售翻墙工具的人进行惩罚的，因为他们之中很多人都只是偷窃了开源项目技术人员的劳动成果，亦或是提供与其宣称不符的劣质（违法）产品，从而收取暴利，收割智商税。从构成要件上看，我认为其更加符合非法经营罪的构成要件，而非提供侵入、非法控制计算机信息系统程序、工具罪，因为后者在论证上存在着严重的逻辑漏洞。

另外，不仅仅是出售翻墙工具，还有很多技术人员因为编写开源翻墙项目而获此罪名。因此，这一领域的法律问题应该结合计算机技术问题被更深入、更广泛的探讨，这也是我写这一篇文章的初始动机。因为很多人确实需要通过境外网站查询学术资料、海淘等，这些行为都不存在违法性。而当他们使用翻墙工具访问境外网站大多不受惩罚的同时，惩罚却被转嫁到了提供翻墙方法的人之上。

而与此同时，现在社会上出现一种声音，他们也同意国家根本不禁止个人翻墙，但他们更进一步表达了他们的自信和乐观，他们认为国家不仅不禁止翻墙，还鼓励有独立思考能力的人翻墙输出文化（依据是李子柒）；同时认为：对于真正有独立思考能力的人来说，翻墙实在是太容易了，甚至他们会用嘲讽的语气阴阳怪气道：“没有独立思考能力的人活该待在墙内”。这种风气我认为非常不好，毫不避讳地说，这是吃人血馒头的

行为。因为他们不知道，真正致力于“为他们寻找访问境外网站方法”的人，大多承受着极大的法律风险，而与此同时，GFW 的技术手段越来越强悍，翻墙的成本越来越高，普通人甚至很容易在这一领域被骗——对于这些问题，他们向来是采取无视态度的。如果让这种声音成为这个社会的主流，那么我对这一领域在未来进展的预测将是极其悲观的。

更进一步，我们应当思考，当程序员为“人们正常访问合法境外网站”而努力的时候，法律工作者的努力又在哪里？为什么现在大部分法律工作者都在就着错误的计算机基本常识来进行法律方面的论证呢？我不禁陷入了深思……

四、从计算机技术角度解读：什么是墙，什么是翻墙

在了解 GFW 和翻墙的原理之前，你必须对互联网运行的基本原理有一个宏观的了解——**至少，你需要知道当你在浏览器键入 baidu.com，页面呈现在你眼前时，究竟发生了什么。**你只有知道发生了什么，才可能看懂 GFW 是怎么样阻止你访问网页，而翻墙又是如何让你穿越重重阻碍成功访问境外服务器的页面的。

1、互联网访问的基本原理——OSI 参考模型

我们之中一定有很多人还依稀记得高中、大学计算机课曾提及“互联网分成好几个层次”。最浅显易懂的当然是物理层，因为日常生活中，光纤、网线、电话线之类的东西是随处可见、看得见摸得着的。

那么，关于 GFW 和翻墙的一切话题，都在上述模型中的哪一层呢？你以为他们在第一层（物理层），实际上他们分布在第三层（网络层）、第四层（传输层）和第七层（应用层）。

为了让大家更好地理解这个“老千层饼”，我分别以访问 baidu.com 主页和境外服务器 ip 来简单阐述一下其过程中涉及的原理（对应 OSI 参考模型）。

（1）国内网站访问原理

a. 在浏览器输入 baidu.com

浏览器并不会直接聪明地找到百度的服务器。

正如我们在使用传统电话时，不可能直呼一个朋友的名字，电话就自动打过去了——

我们一定需要知道朋友的电话号码。此时 baidu.com 就相当于你的一个朋友的名字，

而它的电话号码就是我们熟知的 ip 地址（第三层：网络层）。但我们不可能像记住朋友手机号那样记住 baidu.com 对应的 ip 地址 39.156.69.79，而是需要一个电话号码簿替我们记住。

这个电话号码簿有很多种，例如浏览器缓存（短时）、本地 DNS 缓存、hosts 文件、网卡配置信息里的 DNS 服务器以及 DNS 根域名服务器，优先级从前到后。在上述所有“电话号码簿”中，都记载了“baidu.com=39.156.69.79”这样一个信息，当我们命令浏览器访问 baidu.com 时，（若浏览器缓存、本地 DNS 缓存、hosts 文件都没有记载这位朋友的号码），那么浏览器就会使用 UDP 协议（第四层：传输层）向 DNS 服务器请求 baidu.com 背后的 ip 地址，DNS 服务器域名系统解析（第七层：应用层）后返回正确的 ip 地址。

b1. 浏览器拿到 ip 地址后向正确的服务器发送 http 请求

http 协议（第七层：应用层）是建立在 tcp 协议（第四层：传输层）基础之上的的，tcp 在建立连接前有三次握手。

> 通过 dns 解析之后，拿到了 ip，就可以通过 ip 向服务器发送 http 请求了，因为 http 是工作在第七层应用层，tcp 是工作在第四层传输层，所以发生 http 请求之前，还会进行 tcp 的三次握手。
> tcp 的三次握手是：客户端首先向服务器发送一个带有 SYN 标识和一个 seq 的随机数，服务端收到后，需要给客户端回应一个 ack，ack 的值就是刚才的 seq 随机数的值 + 1，在回应包里，还包含一个 SYN 的标识和一个 seq 随机数。客户端收到服务端发过来的回应包之后，再给服务端发送一个 ack，ack 的值就是刚才服务端发过来的 seq 的值 + 1。上面三步完成之后，三次握手就完成了，下面就可以开始传数据了。
> 《用户访问网站原理及流程》 链接：https://blog.csdn.net/heart_mine/article/details/79539224

为什么建立连接要这么复杂呢？一切为了安全和可靠。DNS 服务所运用的 UDP 协议和 http 请求的 tcp 协议最大的区别在于，UDP 就像一个在国际货物运输过程中前赴后继、不顾一切的承运人，它努力以最快的速度把“货物”交付到你手上，但态度极差，从来不主动跟你联系，也不会接你的电话，货物是否损毁或者送错了人都不在它的义务范围内；而 TCP 就像一个严谨、可靠、负责、慢条斯理的承运人，它在为你进行货物运输时会不断和你建立联系，在送货前不停打电话跟你反复确认，而且要打三次，生怕送错了人，送完货物也会不紧不慢地和你再三确认，要跟你打四通电话。

网上一个更形象的例子是——

> TCP 三次握手好比在一个夜高风黑的夜晚，你一个人在小区里散步，不远处看见一位漂亮妹子迎面而来，但因为路灯有点暗等原因不能 100% 确认，所以要通过招手的方式来确定对方是否认识自己。
> 你首先向妹子招手 (syn)，妹子看到你向自己招手后，向你点了点头挤出了一个微笑 (ack)。你看到妹子微笑后确认了妹子成功辨认出了自己。
> 但妹子有点不好意思，向四周看了一看，有没有可能你是在看别人呢？她也要确认一下。妹子也向你招了招手 (syn)，你看到妹子向自己招手后知道对方是在寻求自己的确认，于是也点了点头挤出了微笑 (ack)，妹子看到你的微笑后确认了你就是在向自己打招呼。于是两人加快步伐，走到一起，彼此之间相互拥抱。
> CSDN 链接：https://blog.csdn.net/weixin_42221136/article/details/90765716

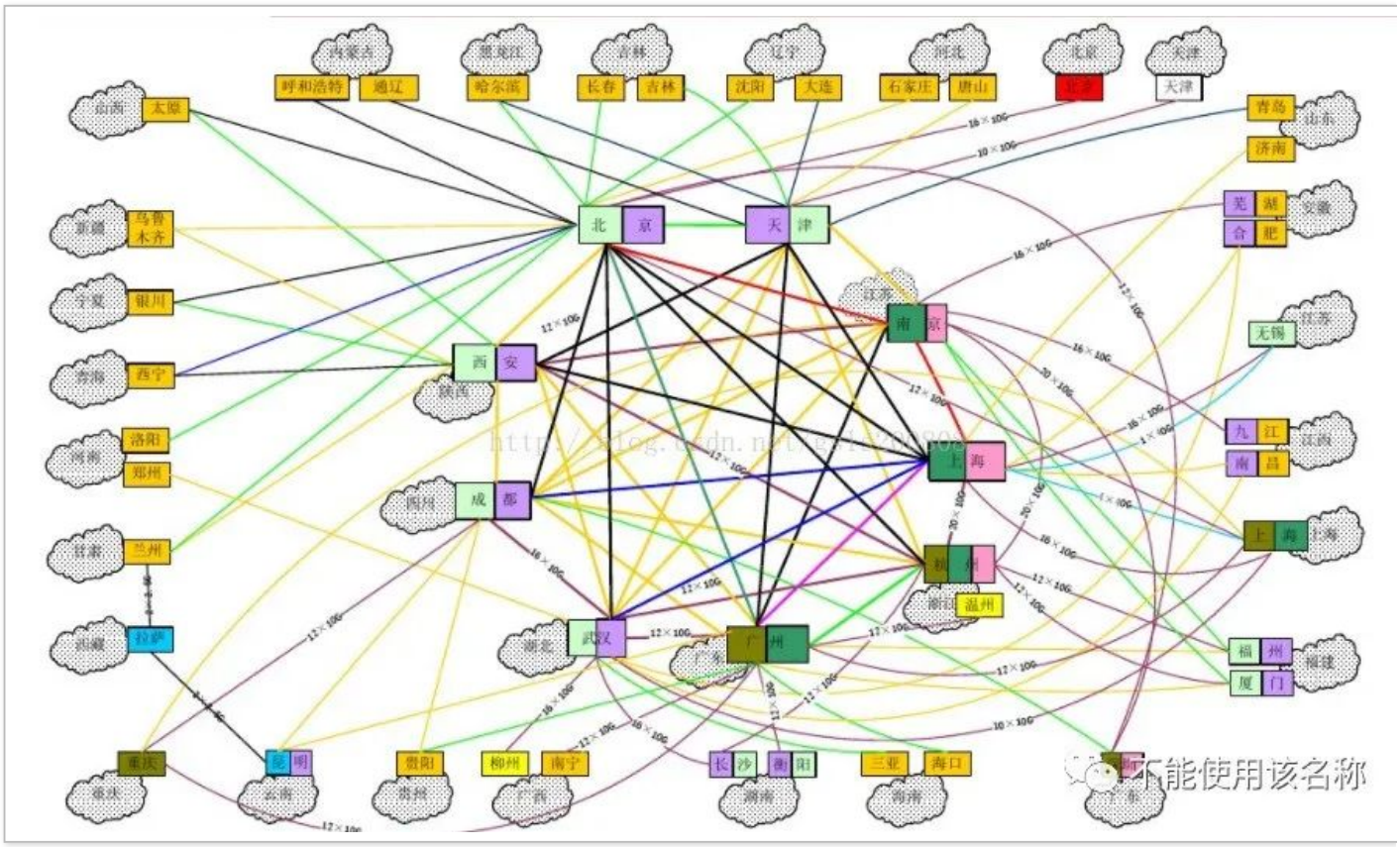
b2. 数据包是如何从你在上海的计算机发至架设在北京的百度服务器呢?

tcp 三次握手已经很生动形象了，但毕竟从上海发送一个数据包至百度架设在北京的服务器的难度，与“在小区里和美女当面互相打招呼”的难度压根不在一个数量级，数据包是如何通过祖国大地下架设的“杂乱无章”、连通全国的光纤中找到去往北京的最快的路，而不至于兜圈或者迷路呢?

A14-2 互联网国内数据传送业务

互联网国内数据传送业务是指经营者通过组建互联网骨干网和城域网，并可利用有相应经营权运营者的互联网国际出入口提供的互联网数据传送业务。无国内通信设施服务业务经营权的运营者不得建设国内传输设施，应租用有相应经营权运营者的国内传输设施。

这要得益于国内几家国有电信运营商建立的庞大的骨干网和城域网。我们作为外行，可以把这种网络理解成一个个互相连通的节点。



例如，中国电信 163 骨干网分为北京、上海、广州 3 大片区，这三个片区有大型的骨干路由作为邻近省级区域的数据交汇中心，例如上海片区涵盖了上海、江苏、安徽、山东、浙江、福建、江西这几个省，而每个省的内部又有庞大的、互相连接的城域网，而在某个城市的城域网内部，又有数以万计的学校、企业、家庭等局域网的接入，从而形成了从局域网→城域网→广域网三个层级。

此外，不只是中国电信，其他运营商也有各自的骨干网，例如中国联通有 CHINA169 骨干网和 CNCNET 骨干网，中国移动有 CMNET 全国骨干网…… 不同国家级互联网业务提供商（Internet Service Provider， ISP）

建立的不同骨干网之间也有数据交换的中心，这使得信息和数据包可以自由地从全国的任何地方流向任何地方。（相关链接：《互联网骨干网全面解析》https://zhuanlan.zhihu.com/p/32090927）

连通性的问题解决了，还要解决数据包在庞大的“网上公路”迷路的可能性。在上述提到的各个级别的网路中，分布着无数路由节点，每一张骨干网都有自己负责的路由群组和节点，整个群组统称为 as 自治系统（Autonomous system），每一个骨干网管理的 as 自治系统都经过名为互联网号码分配局的国际机构分配唯一识别代码，例如，中国电信 163 骨干网的 as 自治系统编号为 AS4134。每一张骨干网都有内部路由协议，每一个节点都在依据某种规定互相交换他们所连通的 ip 地址信息，作为数据包在“旅行”过程中的指路人。而全国性的骨干网之间也依靠外部路由协议互相交换它们所掌握的“服务器地图“，典型的有 BGP 协议。

> 边界网关协议（英语：Border Gateway Protocol，缩写：BGP），一个去中心化自治路由协议。它通过维护 IP 路由表或‘前缀’表来实现自治系统（AS）之间的可达性，属于矢量路由协议，其使用基于路径、网络策略或规则集来决定路由。
> 维基百科
> https://zh.wikipedia.org/wiki/%E8%BE%B9%E7%95%8C%E7%BD%91%E5%85%B3%E5%8D%8F%E8%AE%AE

BGP 协议使得各大骨干网的路由节点可以以 tcp 数据包的形式互相转发其掌握的路由信息，从而形成一个庞大的、完整的决策网，对数据包提供全面的“导航服务”，它能计算出数据包从一个客户端通往另一个外省客户端必经的最优路线和路由节点。条条大路通罗马，当一个路由节点故障时，因为各个节点都互相沟通，从而可以带领数据包选择其他路线通网可达的节点，避免“兜圈子”、“迷路”等情况。
使用 traceroute（链接：https://tools.ipip.net/traceroute.php），可以利用 ICMP 协议定位您的计算机和目标计算机之间的所有路由器节点。下图展示了我从自己的计算机访问百度设在北京的服务器 39.156.69.79 所经过的骨干网和路由节点，可以看见其经过了 AS4812（中国电信 163 骨干网）的 124.74.232.53、124.74.166.125 等路由节点，而其途径的 AS9808 为中国移动骨干网的 AS 自治系统。

目标 IP：39.156.69.79

跳数	IP	主机名	地区（仅供参考）	AS号（仅供参考）	时间（毫秒）
1	*	*	*	*	*
2	10.100.111.254	10.100.111.254	局域网		1.1 / 0.8 / 1.8
3	*	*	*	*	*
4	124.74.232.53	124.74.232.53	中国上海 chinatelecom.com.cn 电信	AS4812 / AS4134	2.5 / 1.7 / 2.5
5	124.74.166.125	124.74.166.125	中国上海 chinatelecom.com.cn 电信	AS4812 / AS4134	2.4 / 8.2 / 3.4
6	202.101.63.58	202.101.63.58	中国上海 chinatelecom.com.cn 电信	AS4812 / AS4134	27.9 / 30.2 / 27.8
7	202.97.34.33	202.97.34.33	中国北京 chinatelecom.com.cn 电信	AS4134	44.8 / 45.1 / 44.8
8	202.97.88.234 * *	202.97.88.234 * *	中国北京 chinatelecom.com.cn 电信 * *	AS4134 * *	45.7 * *
9	221.183.66.1	221.183.66.1	中国北京 chinamobile.com 移动	AS9808	47.6 / 48.3 / 47.4
10	221.183.25.113	221.183.25.113	中国北京 chinamobile.com 移动	AS9808	47.1 / 47.1 / 47.1
11	* 221.183.19.50 *	* 221.183.19.50 *	* 中国北京 chinamobile.com 移动 *	* AS[illegible] *	* [illegible] *

c. 传输数据，发送 http 请求报文，加载页面（省略）

→http 协议是明文协议

→https 协议更加安全，其在 tcp 握手的基础之上增加了以下步骤：

验证服务器数字证书、在 SSL 安全加密隧道协商加密算法的密钥等。

d. 关闭连接前的 tcp 四次握手（省略）

（2）境外网站访问原理

在了解了国内数据包交换原理之后，全球的数据交换就很好理解了——你可以简单地把它理解为国家级骨干网之间的连接和交换。而从国内访问境外服务器有一个特殊之处就在于，我国的国际出入口运营资质是被中国电信、中国联通、中国移动三家国家级 ISP 垄断的。

> 跨国企业使用跨境服务合规方式。跨国企业因协同办公、数据交互等自用需求，可以采用以下方式实现跨境联网：跨国企业从境内发起直接租用 3 家基础电信企业的国际专线（包括虚拟专网），与企业办公自用网络和设备连接；跨国企业从境外直接发起或委托境外运营商，向 3 家基础电信企业租用国际专线（包括虚拟专网），与企业办公自用网络和设备连接。跨国企业租用国际专线自建自用办公网络时，可委托有资质的第三方（含持国内 IP-VPN、固定网国内数据传送等业务许可的企业）提供系统集成、代维代管等外包服务，但第三方企业不得从事国际专线（包括虚拟专网）的线路资源租售等电信业务经营活动。
>
> 2018 年 1 月 10 日在北京召开了《跨境数据通信业务政策宣贯会暨产业联盟筹备大会》，国内数十家 IP-VPN 等相关业务经营企业参加了此次大会。

而国内数据跨境的物理传输介质一般为陆上光缆和海底光缆。通过上海直达美国的 CN2 骨干网海底光缆，亦或是从广州到香港的 163 骨干网线路的连接，国内和国外的数据完全可以自由地进行交换，而服务器的连接、数据包的交换、路由的选择，其本质上和访问国内服务器并没有什么区别，其协议的使用也是全球通用的。所以，一个真正的国际互联网并不存在所谓的“墙”，它依旧是通过海底光缆等物理介质，作为 OSI 模型中的第一层，为其他几个层次的互联网运行提供服务。**不管你是否翻墙，不管你访问的是合法的境外网站还是受到管制和审查的网站，一旦你成功 ping 同，实现了数据的交换，那么数据包就一定要通过我国设立的互联网国际出入口，从一条条光缆直达国外的服务器。**
因此，我很遗憾地看到，即使是律所发表的相关文章《天衡解析 | “翻墙”上网的正确姿势》，也犯了非常严重的计算机常识性错误，导致该篇文章论证的前提就是不正确的。这篇文章指出：

> 由于企业的“翻墙”行为既未使用合法的“国际出入口信道”，也未接入合法的“接入网络”，甚至未使用境内的“互联网络”，已经违反了《中华人民共和国计算机信息网络国际联网管理暂行规定》的规定，公安机关有权责令企业停止国际联网行为，同时给予警告，并处以 15000 元以下的罚款。（链接：http://www.tenetlaw.com/index.php?m=content&c=index&a=show&catid=8&id=989）

然而， 当我们对互联网运行的机制和原理有了初步的了解后就能轻松发现这句标红的话的严重错误——我在上文所介绍的一切专业术语的实际运作，不管是 DNS 解析、TCP 握手，还是 AS 自治系统、BGP、路由跳转、ICMP 协议…… 一切的基础都是物理层。

如果你没有接入各大运营商设立在城市里的合法的城域网；

如果数据包没有经过各大国家级 ISP 的合法骨干网和路由节点 AS 自治系统；

如果境外数据访问没有经过国内三大运营商经国家批准设立的合法国际出入口并通过合法的陆上、海底光缆设施直达境外服务器……

你的一切数据交换和网站访问都是不可能凭空实现的。

换句话说，即使一家企业使用某个国外代理服务器作为中转节点以逃避 GFW 的审查，这一翻墙行为的一切基础都是建立在使用合法的国家互联网基础设施之上的。因为你不可能自己去发射一颗卫星专门用来刷推特，也不可能自己制造海底电缆，自发地潜水到海底接入别的国家的网络。

因此，对于普通个人和企业来说（这里的“普通”是指没有能力发射卫星、埋海底光缆），根本不存在所谓“非法的国际出入口信道”、非法的“接入网络”、“在不使用境内互联网络的前提下访问域外服务器”。

一个最直接的证据，也是每个人都能亲身试验的方法，就是使用前文介绍的 traceroute 命令，访问某个境外服务器的 ip 地址，遍历数据包途经的骨干网和路由节点，你就会知道，你到底是不是在使用国家级电信运营商布建的、国家批准的网络基础设施了。我随机使用一个尚未被限制的境外服务器 ip 测试一下，结果如下：

局域网		1.2 / 1 / 2.5
* 中国上海 chinatelecom.com.cn 电信 中国上海 chinatelecom.com.cn 电信	* AS4812 AS4812	* 3.7 2.1
中国上海 chinatelecom.com.cn 电信 中国上海 chinatelecom.com.cn 电信 *	AS4812 AS4812 *	4.1 2.5 *
中国上海 chinatelecom.com.cn 电信	AS4812	3.4 / 48.9 / 75.8
中国上海 chinatelecom.com.cn 电信	AS4812	13.1 / 55.9 / 4.1
中国上海 chinatelecom.com.cn 电信	AS4134	38.3 / 28.5 / 3.6
中国上海 chinatelecom.com.cn 电信	AS4134	47.5 / 46.1 / 40.9
中国上海 chinatelecom.com.cn 电信		18.8 / 27.9 / 19.9
国加利福尼亚州洛杉矶 chinatelecom.com.cn 电信		206.9 / 188 / 200.9
* 国加利福尼亚州洛杉矶 chinatelecom.com.cn 电信 *	* AS4134 *	* 241.2 *
* 美国加利福尼亚州洛杉矶 quadranet.com 美国加利福尼亚州洛杉矶 quadranet.com	* AS8100 AS8100	* 208.9 208.9

可见，当你成功访问境外服务器，当然也意味着成功实现了翻墙，但你的数据经过的是 AS4812（中国电信上海路由群组）、AS4134（中国电信 163 骨干网路由群组），最后通过海底光缆直连美国加利福尼亚州洛杉矶的 AS8100 路由群组。你使用的一切光缆、路由节点、海底光缆，全都是经过工信部审批通过的国家级互联网基础设施。翻墙就是使用了非法的信道——这种逻辑是很可笑的。

因此，国际出入口就在那里等着你，海底光缆也在向你招手，凭什么不能访问境外网站呢？在看了下文 GFW 原理和翻墙原理的介绍，你就会知道，**你不能访问境外网站的唯一原因是你正在遭受一个不受法律规制的系统的不间断网络攻击，而你使用任何途径翻墙的基本原理永远都是——你使用了某种技术抵御或避免了上述网络攻击。**

2、GFW 的原理

首先，我们反复强调，GFW 这个概念在当前一切公开的规范性法律文件中都是不存在的。因此，对“翻墙”进行处罚、甚至将“翻墙”这个词写在一个法律文书中简直是无中生有、自取其辱，是非常荒谬的行为。

其次，在学习了以下原理之后，你将清楚地认识到：现行法律规定的所谓“信道”都是在物理层的，而 GFW 和翻墙的较量基本上都发生在传输层、网络层、会话层、应用层（参见 OSI 模型）等等，这些层级是法外之地。

在看下文之前，可以同时回顾——你究竟是如何能够访问一个网站的页面的。GFW 目前已知的原理有以下几种：

（1）基于 UDP 协议的域名解析服务劫持 / DNS 缓存污染

大家一定还记得那个电话号码簿的故事。GFW 最早、最初始的原理，就是将这个电话号码簿掉包，或者将号码簿里的电话号码替换成错误的号码，这个原理诞生于 2002 年，在 2012 年以前达到高峰。GFW 对所有经过骨干出口路由的基于 UDP 的 DNS 域名查询请求进行 Intrusion Detection Systems（入侵检测系统）检测，一旦发现处于黑名单关键词中相匹配的域名查询请求，防火长城作为中间设备会向查询者返回虚假结果。

简而言之，DNS 域名污染就好比你想在电话号码簿上查询朋友的电话号码，但是不曾想，电话号码簿被人掉包了，你拿到的是假的电话号码簿，原本正确的手机号码被替换成了错误的号码，导致你无法打通电话。而该系统触发的规则使用了类似正则表达式的结构，例如规定“对于一切 *.google.com 的域名解析到某个不存在的 ip 地址”。

直接使用 windows 的 ping 命令就可以亲眼看到 DNS 污染的运作效果。谷歌官网的服务器明明架设在美国科罗拉多丹佛，但从下图可以看见，在国内从 DNS 服务器请求到的 ip 地址却是 93.46.8.90 这个来自意大利的无效 IP 地址。

此项技术不仅是 2012 年前后人们无法再访问 Google 的直接原因，其在运转过程中更是殃及了全球 DNS 域名解析服务的正常运作。

> 这种 DNS 污染的方式曾经向中国大陆以外的用户造成影响。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。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。
> 维基百科 链接：
> https://zh.wikipedia.org/wiki/%E9%98%B2%E7%81%AB%E9%95%BF%E5%9F%8E#TCP%E8%BF%9E%E6%8E%A5%E9%87%8D%E7%BD%AE

DNS 污染殃及全球用户的基本原理很简单，就是诸多国外用户的 DNS 请求被他们的 ISP 电信运营商随机分发给了全球的根域名缓存服务器（也就是那个优先级最低的电话簿），而碰巧，他们请求被分发给了来自中国的根域名服务器，而因为 GFW 的存在，其提供的是错误的、虚假的 DNS 解析服务，其造成的后果可想而知。

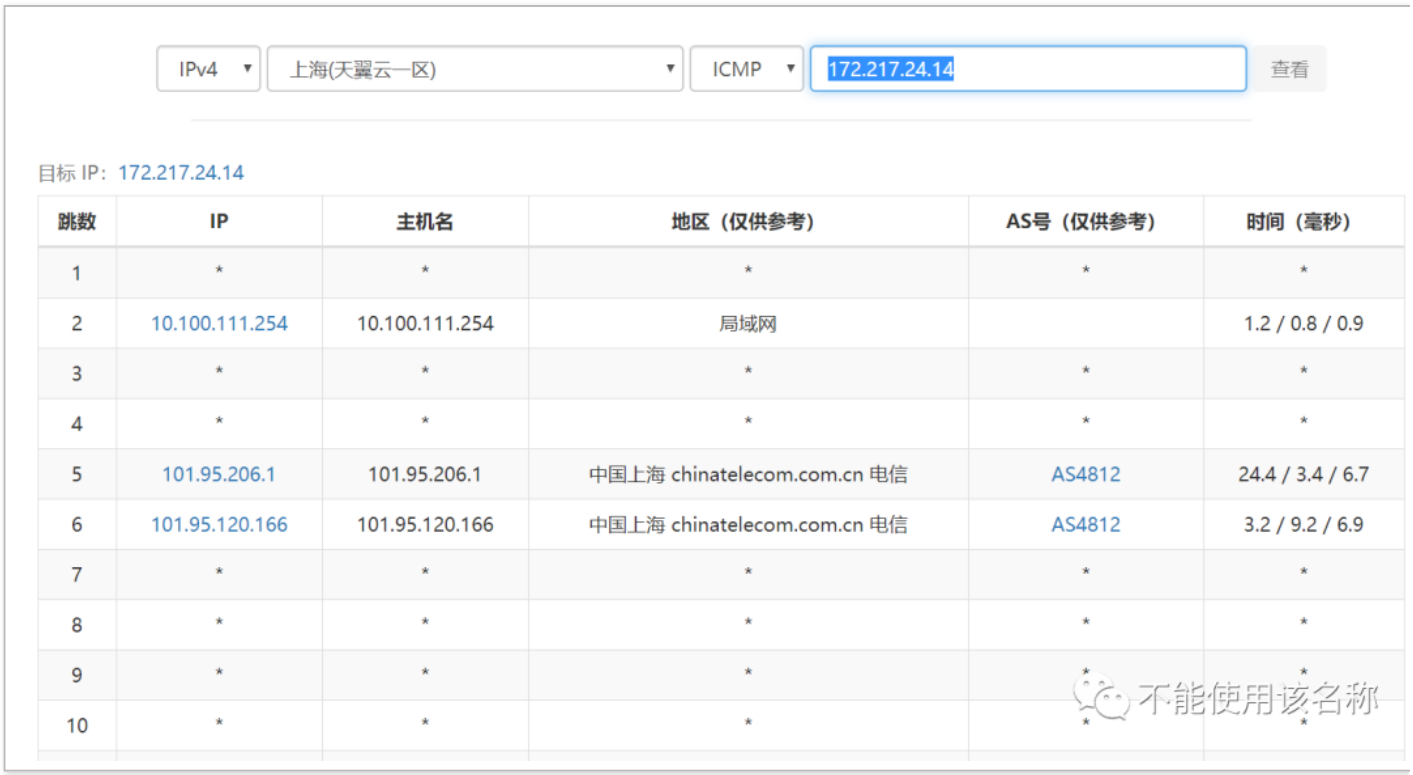
因此在这里我忍不住插一句题外话。我曾亲耳听见一个计算机专业毕业的人谈及中国的互联网安全现状。他说，因为全球大部分根域名服务器都设立在美国，所以美国掌握互联网的底层，中国必须建立 GFW 来保障互联网安全。现在，你应该可以体会到这种言论的恶毒之处。因为现在你终于了解到，电话簿可以随时复制，根域名服务器根本就不是什么互联网的底层，而是最高层（应用层）中一个很简单的技术，你的浏览器永远最先访问本地 DNS 缓存，往往一般都无须根域名服务器就能解析 IP 地址；而中国的根域名服务器会对境外服务器域名解析错误的 ip 地址，因此现实情况是中国的 DNS 污染在影响全球的互联网运行，而非美国影响了中国的互联网安全，这是完全的颠倒是非。

（2）IP 地址或传输层端口人工封锁——BGP 路由劫持 /“路由黑洞”

我们依稀记得 BGP 好像是各个 ISP 主干网之间路由节点共享信息的协议，BGP 劫持就是伪造位于主干道的路由节点的路由表，将其根本没有或者不可能连通的 ip 地址导入路由表，诱骗邻近节点相信该节点拥有这一 ip 地址的访问通道。GFW 通过人工方式维护一个针对特定 IP 地址封锁的列表，从而实现特定 ip 地址的路由欺骗，这样一个节点我们将其称之为“路由黑洞”。因为基于 BGP 协议，各个节点之间是无条件信任的，所以这个“谎言”一传十、十传百，只要一个主干道路由节点被诱骗，其连接的所有节点都会被骗，成为 GFW 运作的"帮凶"。而 BGP 劫持的“可传染性”特征曾经导致全球互联网访问故障。

> 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。
> A Chinese ISP Momentarily Hijacks the Internet. PC World. 2010-04-09 [2011-05-19]. （原始内容存档于 2011-06-22）.

我们依旧可以通过 traceroute 观察到这一技术的运行效果，我们尝试 traceroute 一下 google.com 的真实 ip 地址，得到如下结果：



可以看见，当数据包跳转给中国电信上海 AS4812 群组的 101.95.120.166 路由节点之后，就再也跟踪不到数据包的踪迹了。这是因为在这一节点，存在着一个无效的路由黑洞，其声称自己拥有 172.217.24.12 这一 ip 地址的访问可达性，但话音刚落，它就把数据包丢弃在角落了……

与此同时，骨干路由器还有一种 ACL Based Forwarding (ABF) 的匹配规则，可以在全国骨干路由器同步步数 ip 端口封锁规则，由于理解不太深入，这里不做专门介绍。

另外，在路由黑洞成为封锁 ip 的主要途径以前，GFW 在早期使用的是访问控制列表（ACL）技术来封锁特定的 IP 地址，但这种方法有性能不佳的问题。这里不做专门介绍。

（3）TCP RST 重置（包括对基于 TCP 协议的 DNS 域名解析的重置）

我们依稀记得 TCP 建立连接前的三次握手，也一定还记得那天在小区里与美女浪漫的邂逅。将 TCP RST 重置套用到这个浪漫的故事里，可以直接表现为：当你对着妹子招手时，旁边突然冲出来一陌生男子骗你说，“对不起，这是我的女朋友，请不要打扰她”；而随后，他又挡在你面前伪装成你的样子，冲向那位女子说，“刚刚招手的就是我，你别误会，我根本就不是在跟你打招呼，我只是在打蚊子，拜拜”——这个生动的故事为我们展现了，一个无耻的第三人就这样强行闯入了一个纯洁男子和妙龄女子的浪漫邂逅。

RST 阻断也称为 TCP 旁路阻断，其运行的原理如下：

> 通常需要进行阻断的情况是审计控制系统旁路监听内网。旁路监听的方式一般是将主交换机的数据镜像到控制系统，控制系统可以采用 libpcap 捕获数据包。在这种情况下要阻断 tcp 连接的建立只要在监听到第一次握手的时候，控制系统伪造服务器发起第二次握手回应，就能阻断客户端与服务器连接的建立。因为我们的系统在内网，发出的报文肯定比服务器快，这样客户端接收到我们伪造的报文以后会回应第三次握手，当服务器真正的报文到达的时候客户端将不再处理，此时客户端再向服务器请求数据，因为 seq 号和 ack 号出错，服务器不会受理客户端的请求。
>
>

> TCP 协议规定，只要看到 RST 包，连接立马被中断。从浏览器里来看就是连接已经被重置。大部分的 RST 是条件触发的，比如 URL 中包含某些关键字。目前享受这种待遇的网站就多得去了，著名的有 facebook。还有一些网站，会被无条件 RST。也就是针对特定的 IP 和端口，无论包的内容就会触发 RST。比较著名的例子是 https 的 wikipedia。GFW 在 TCP 层的应对是利用了 IPv4 协议的弱点，也就是只要你在网络上，就假装成任何人发包。所以 GFW 可以很轻易地让你相信 RST 确实是 Google 发的，而让 Google 相信 RST 是你发的。
> 《G.F.W 的原理》 http://www.oneyearago.me/2019/06/14/learn_gwf/

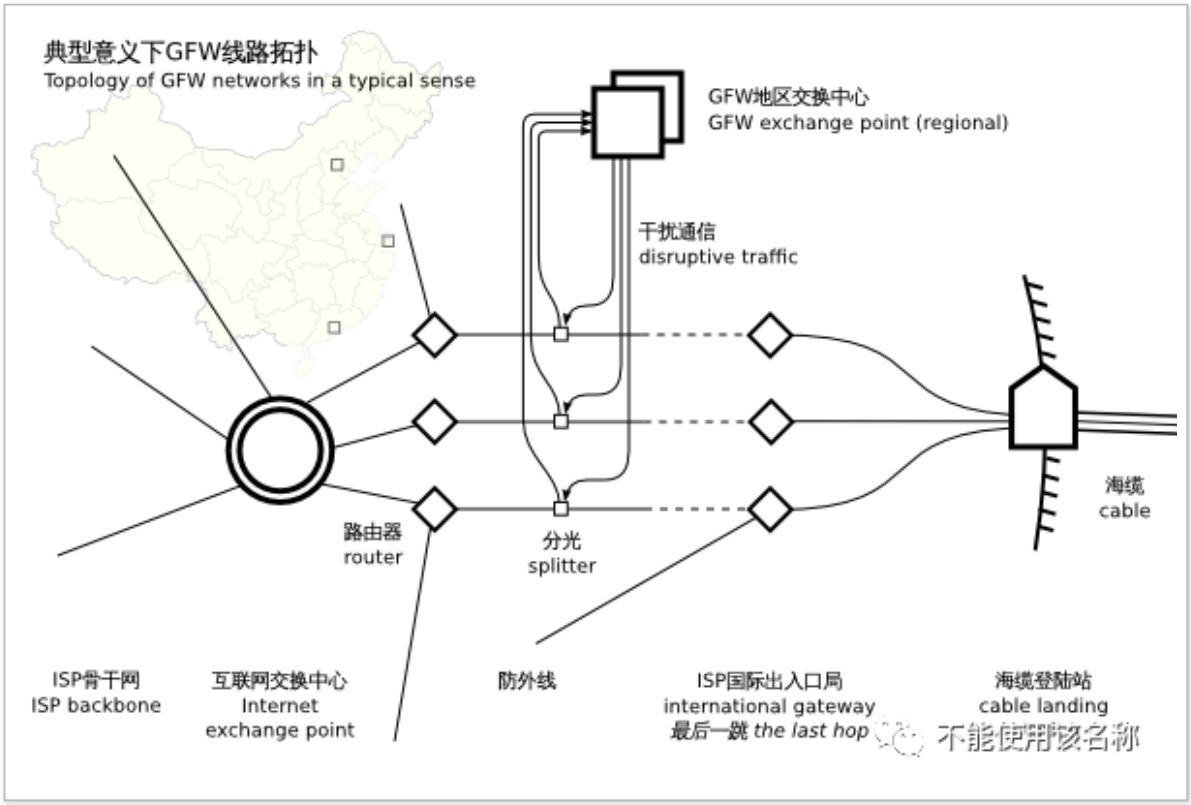
与此同时，DNS 解析服务并非全部都使用 UDP 协议，也有部分使用 TCP 协议的 DNS 解析请求，其被封禁也是依靠 TCP 的 RST 重置，
通过这一技术的反推，有业内人士定位了 GFW 存在的大致位置。其原理如下：

> IP 协议的特性叫 TTL。TTL 是 Time to Live 的简写。IP 包在每经过一次路由的时候，路由器都会把 IP 包的 TTL 减去 1。如果 TTL 到零了，路由器就不会再把 IP 包发给下一级路由。由于 GFW 会在监听到不和谐的 IP 包之后发回 RST 包来重置 TCP 连接。那么通过设置不同的 TTL 就可以知道从你的电脑，到 GFW 之间经过了几个路由器。比如说 TTL 设置成 9 不触发 RST，但是 10 就触发 RST，那么到 GFW 就是经过了 10 个路由器。

> 另外一个 IP 协议的特性是当 TTL 耗尽的时候，路由器应该发回一个 TTL EXCEEDED 的 ICMP 包，并把自己的 IP 地址设置成 SRC（来源）。结合这两点，就可以探测出 IP 包是到了 IP 地址为什么的路由器之后才被 GFW 检测到，结合 IP 地址地理位置的数据库就可以知道其地理位置。
> 《G.F.W 的原理》 http://www.oneyearago.me/2019/06/14/learn_gwf/

（4）协议检测→根据流量协议拆包→关键词匹配→封锁

我们在上面一段曾了解到，GFW 的 TCP 旁路阻断的前提是“将主交换机的数据镜像到控制系统”。这其实也是目前业内猜测的 GFW 系统存在的主要方式——GFW 存在于骨干路由器节点，其作为一个设备附着在主干路由器身边，通过“分光”的方式把数据包复制到另外一根光纤上。



基于此，GFW 作为一个独立设备就可以作为旁观者分析经过其附着的主干路由器的所有数据包。

HTTP 协议有非常明显的特征，可以轻易被 GFW 系统检测和识别，GFW 进而依据 HTTP 协议规则对数据包进行拆解，由于其表现为明文，所以可以直接进行关键词匹配。例如，从 HTTP 的 GET 请求中取得请求的 URL。然后 GFW 拿到这个请求的 URL 去与关键字做匹配，比如查找 Twitter 是否在请求的 URL 中。而关键字匹配使用的依旧是一些高效的正则表达式算。

（5）深度包检测（机器学习识别翻墙流量→直接阻断）

写到这里已经有点写累了 hhh，不知道有多少人看到了这里。当前流行的一切翻墙协议例如 shadowsocks、v2ray 的 VMess 协议等不具有非常显著的特征，而后者可以伪装成其他类型的流量，例如伪装成微信视频等。但无论如何，对于混淆流量和非传统加密协议，GFW 正在使用大家耳熟能详的“人工智能”技术，将这些各种各样难以判断和识别的翻墙流量与正规的政企跨境流量相区分开来。

（6）DDoS 攻击

不再展开论述，可参考近年来 Github 网站遭受的攻击。

3、翻墙的原理

这一部分我不再展开论述，因为是有法律风险的。有一定网络基础知识的人，在看完上述 GFW 原理之后，应当能够头脑风暴一下，想出很多合理的逃避审查的思路，也能理解为什么我在上文提及“翻墙不等于侵入计算机系统”了。主要的翻墙原理有以下几种。

（1）早期对 DNS 污染的应对——给 hosts 文件添加一个离线库就行了
（2）各种奇形怪状的加密协议，包括流量伪装，避免被直接拆包作关键词审查
（3）无视 GFW 发送的 RST 重置数据包（无视那个第三人，继续暧昧的相遇）
（4）连接境外未被封禁的代理服务器作为中转站，逃过 GFW 的 ip 封锁
……

五、结语

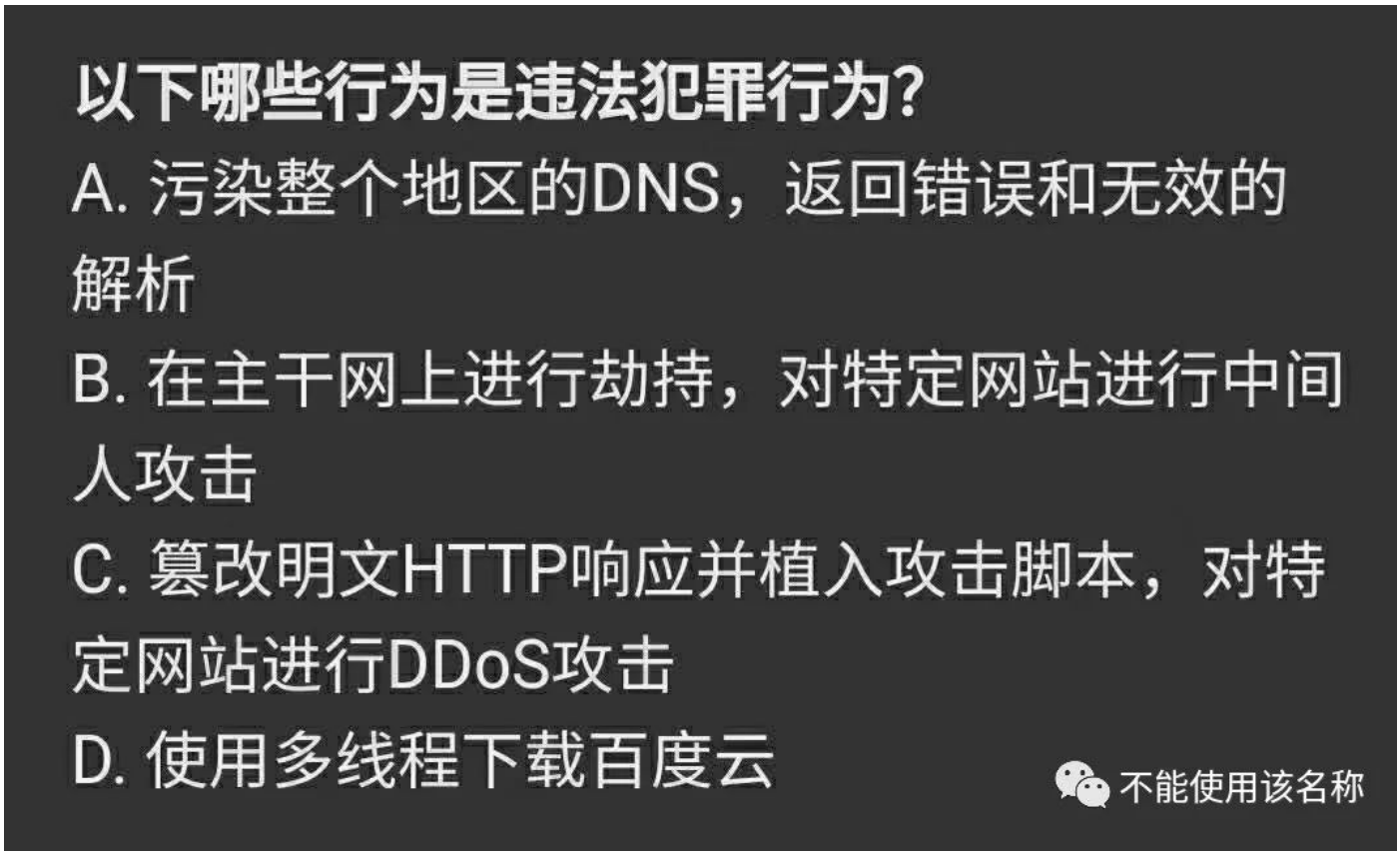
在文章结尾，我依旧要强调，本文不涉及有关“翻墙”的任何技术指导或方法的具体介绍，同时必须强调——千万不要翻墙访问、发布、传播违法有害信息。

我们很多人都记得 2012 年以前的那个时代，想要用谷歌搜索资料，只需要修改 DNS 服务器为 8.8.8.8 即可，再不济，改个 hosts 文件就行了。现在，越来越多的方法被封锁了，在这个节骨眼上，居然还有很多人盲目乐观，甚至以他人不懂翻墙而沾沾自喜，这样的现象伴随着民族主义思潮愈演愈烈。

但是我相信，认真学习自己的专业知识，同时广泛地接受和学习其他领域的专业知识，就能轻松避免被网上大肆输出情绪的人鼓动和欺瞒，保持冷静地思考——你真的可以对现状有一个清晰的认识和判断，并在不久的将来参与到各行各业的运行过程中，为社会做出贡献。

而这篇文章，就权当我在学习之余的放松心情、自娱自乐罢。

那么现在，你能否就程序员群体提出的以下选择题给出正确解答了呢?



全文完