

蕭強

道高一尺，牆高一丈：東亞 網絡封鎖和反封鎖技術演進 介紹



加大柏克萊分校逆權力實驗室



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



第一封電子郵件 (1987) :

“Across the Great Wall we can reach every corner in the world”

<https://bit.ly/2NsTe2Q>



中大國九互聯網關

中国互联网布局

互联网络名称	互联单位	运营性质
■ 中国公用计算机互联网	中国电信集团公司	商业
■ 中国网通公用互联网 ■ 宽带中国CHINA169网	中国网络通信集团公司	商业
■ 中国教育和科研计算机网	教育部-清华大学	公益(教育)
■ 中国科技网	中国科学院-计算机网络信息中心	公益(科技)
■ 中国联通互联网	中国联合通信有限公司	商业
■ 中国移动互联网	中国移动通信集团公司	商业
■ 中国长城互联网	总参通信部	公益(军队)
■ 中国国际经济贸易互联网	中国国际电子商务中心	公益(经贸)
■ 中国卫星集团互联网	中国卫星通信集团公司	商业

<https://bit.ly/2NsTe2Q>

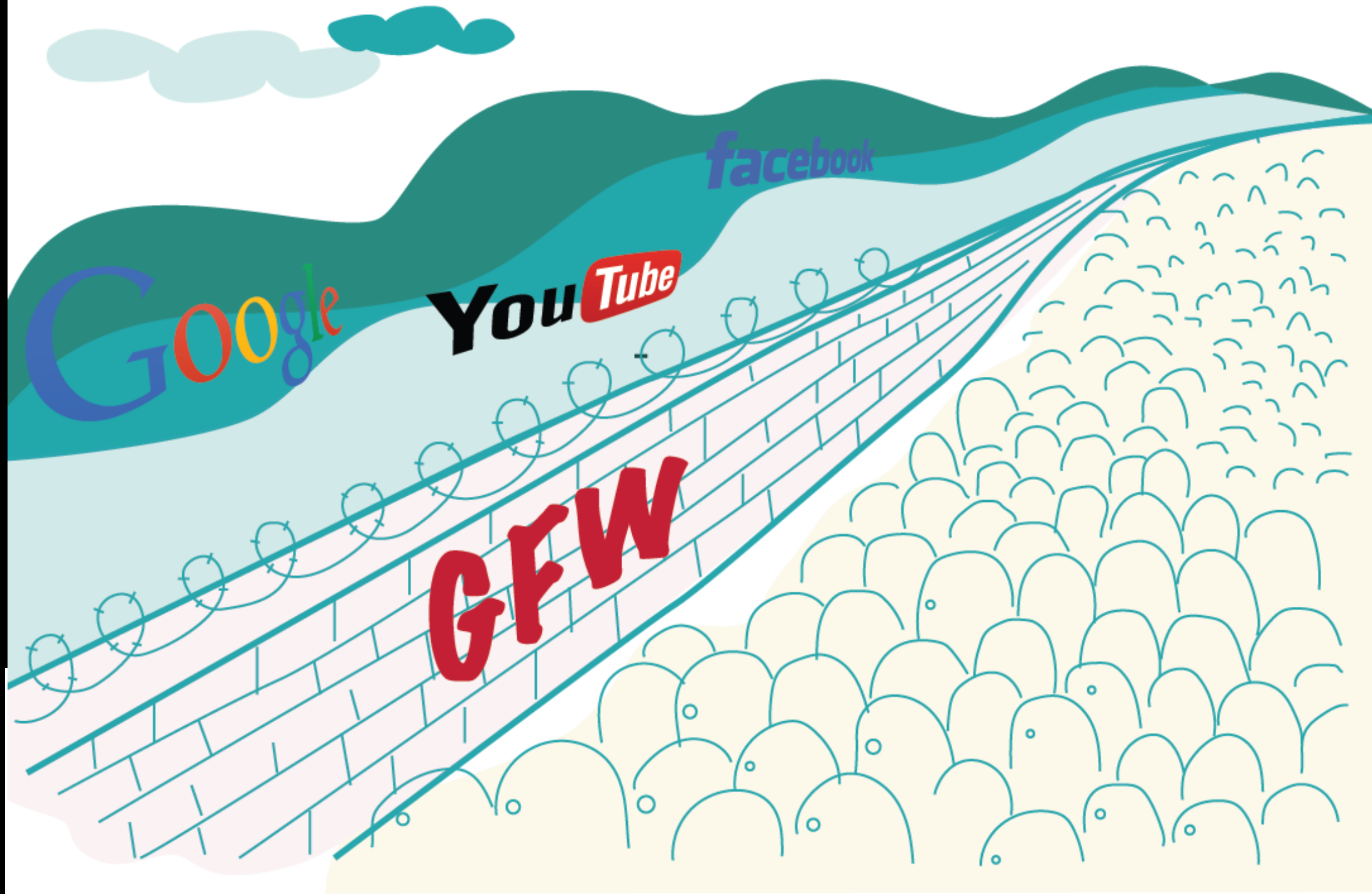


HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD





國家公共網絡監控系統俗稱中國網絡防火牆
(**The Great Fire Wall of China**，常用簡稱「**GFW**」
或「牆」)。



網絡封鎖的歷史背景（1999）

- 國家信息化工作領導小組
- 組長: 吳邦國





HIKING GFW

漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



GFW 成立的背景



<https://bit.ly/2uOp7LL>



<https://bit.ly/2LowL9P>



網絡審查組織

中国互联网的管理

信息产业部

国务院新闻办公室

国家信息化工作办公室

公安部

国家计算机网络与信息安全管理中心

文化部

国家知识产权局

.....

<https://bit.ly/2mrOU8F>



HIKING GFW

漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



國家計算機網絡與信息安全管理中心 CNCERT/CC (GFW)



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD





<https://bit.ly/2LoATGR>

中國國家防火牆之父：方濱興

国家计算机网络与信息安全管理中心总工程师（2000-2002）



“國家信息安全話語範式”

- 通過國家意志——法律來定義“信息安全”：包括了“內容安全”和“意識形態安全”
- 將“煽動...煽動...煽動...煽動...捏造...宣揚...侮辱...損害...其他...”等加入定義為所謂的網絡攻擊、網絡垃圾、網絡有害信息、網絡安全威脅
- 在實現層面完全技術性、中立性地看待“信息安全”，對意識形態與信息科學進行牢不可破的焊接



CNCERT/CC “合作夥伴”

- 违法和不良信息举报中心（網信辦）
- 國家計算機網絡入侵防範中心（中科院）
- 國家計算機病毒應急處理中心（公安部，科技部）
- 國家反計算機入侵及防病毒研究中心（公安部）
- 中國互聯網用戶反垃圾郵件中心（中國互聯網協會）



防火長城 GFW 的決策機制



<https://bit.ly/2mrOU8F>



<https://bit.ly/2NsTe2Q>



<https://bit.ly/2JBa5hP>



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



防火長城 GFW 的工作流程

- 封禁標準
- 封禁流程
- 封禁技術



GFW 重點封堵翻牆工具的條件（特點）：

- 大規模使用
- 特定時期的特定使用
- 有明顯翻牆意圖的使用
- 被外圍GFW人員舉報的使用



防火長城 GFW 技術實施原則

- “主要是強調綜合平衡安全成本與風險，如果風險不大就沒有必要花太大的安全成本來做。在這裡面需要強調一點就是確保重點的，如等級保護就是根據信息系統的重要性來定級，從而施加適當強度的保護。” ----- 方濱興
《五個層面解讀國家信息安全保障體系》



防火長城的技術演進



GFW 技術結構: 入侵防禦系統, 檢測-攻擊兩相模型

域名劫持

IP封锁

关键字过滤阻断

HTTPS证书过滤

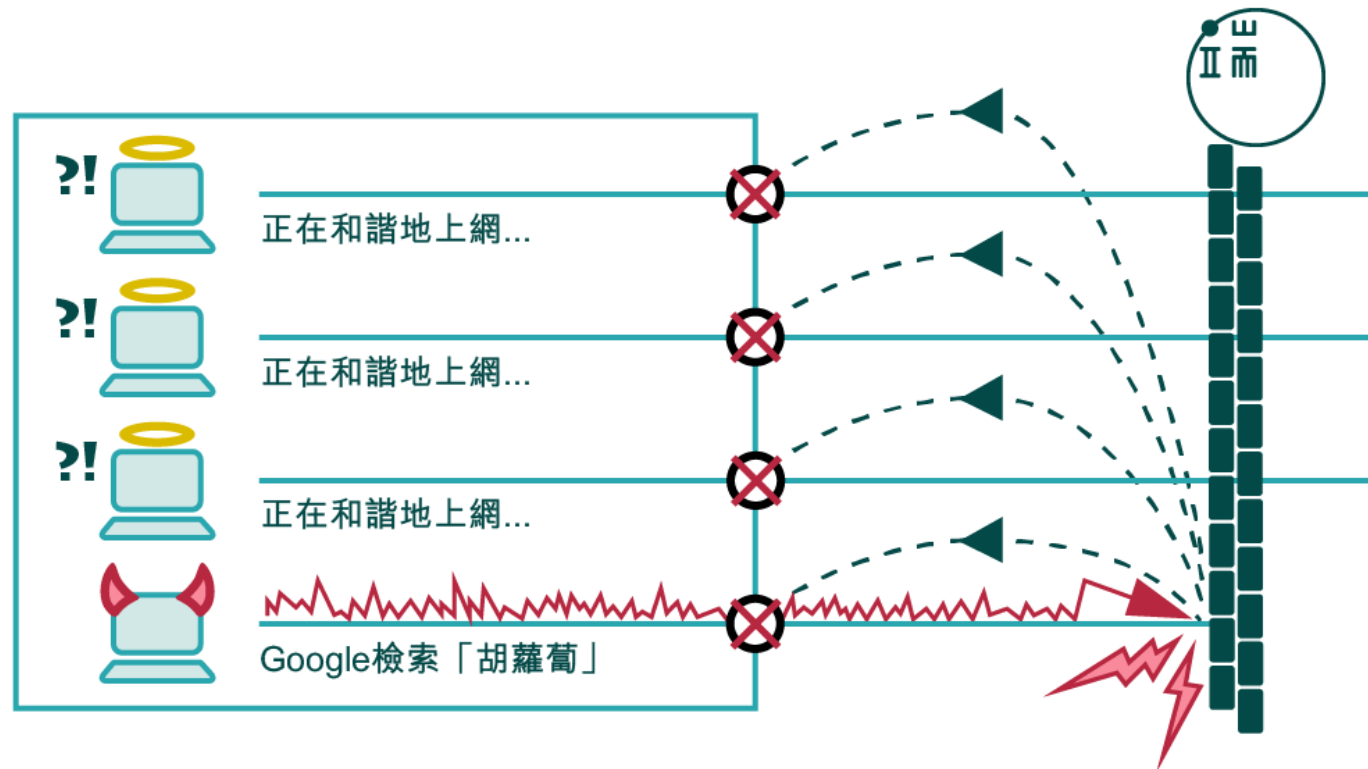


HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD





內網某個用戶登陸Google檢索「敏感信息」，這意味著一個端口「撞牆」，「牆」把接連着的四千多個端口都封掉，令無辜群眾也無法使用Google。



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



Censorship Technologies

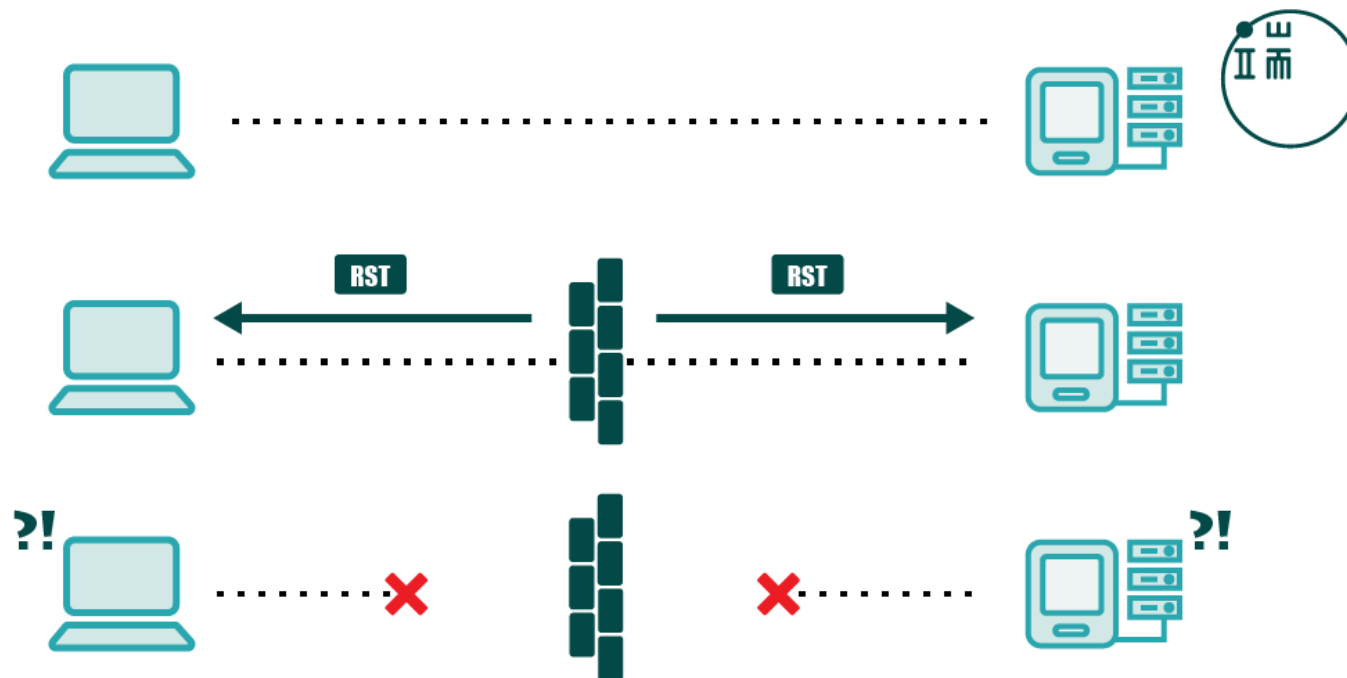
- IP Blocking
- DNS Poisoning
- Keywords Filtering (TCP Reset)
- URL Filtering (HTTP Proxy, IR)



更多的封鎖行為

- Application protocol parsing (“deep packet inspection”)
- Participation in a circumvention system as a client
- Scanning to discover proxies
- Throttling connections
- Temporary total shutdowns





好比A和B正在打電話，「牆」想要掐斷電話，它對A說：「B掛你電話了」，同時又對B說，「A掛你電話了」，不明真相的兩人就真把電話掛掉了。

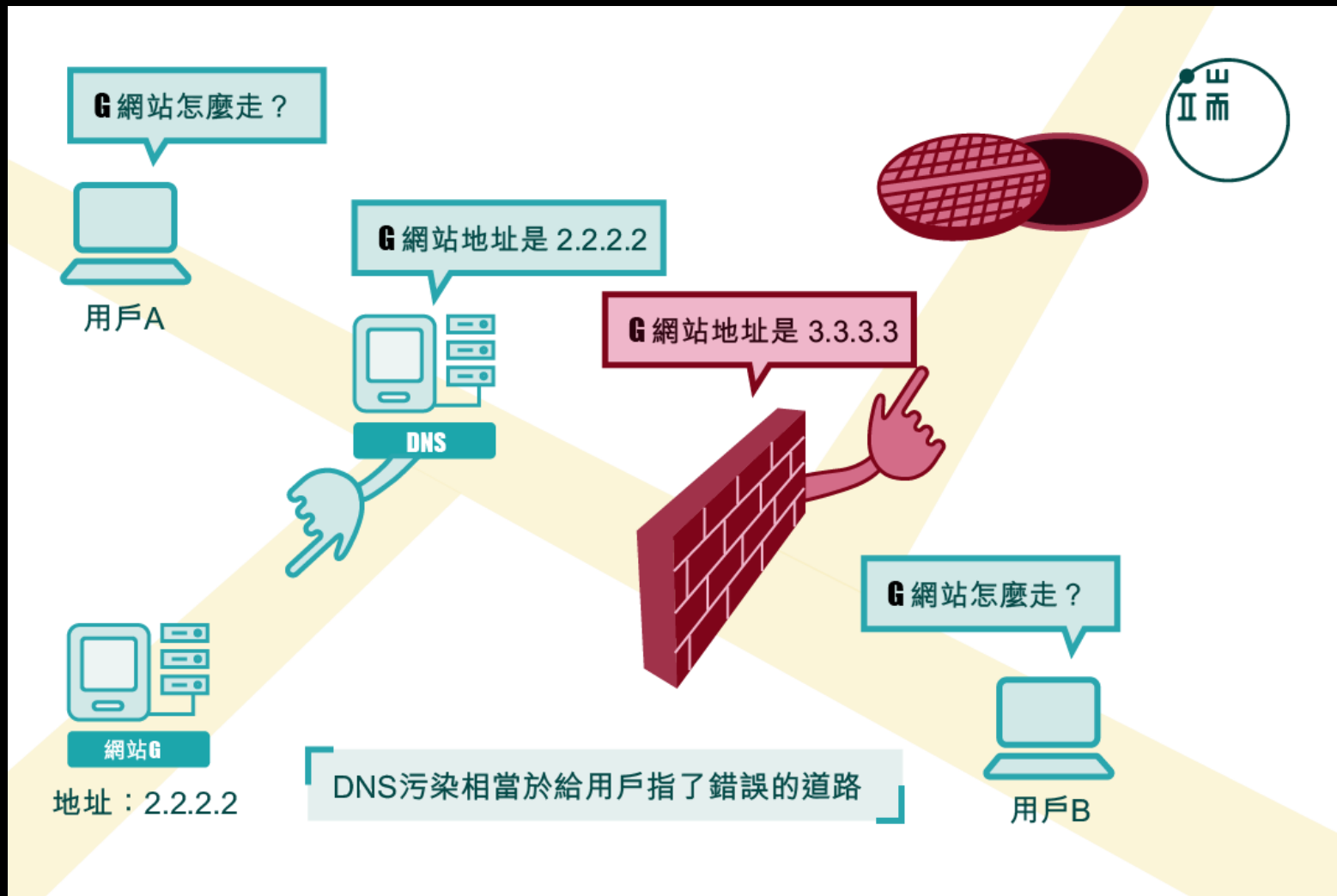


HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



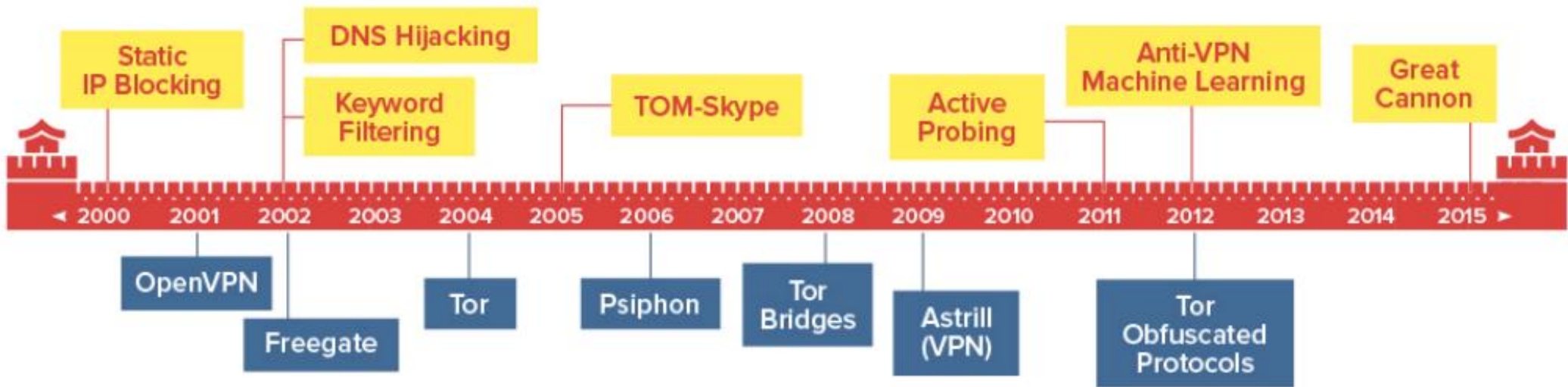


Measurement

- IP Blacklist
- DNS Blacklist
- Keyword, URL blacklist



GREAT FIREWALL OF CHINA



CIRCUMVENTION TOOLS



HIKING GFW

漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



HIKINGGFW.ORG





HIKING GFW

[HOME](#)[ABOUT](#)[BLOCKED DOMAINS](#)[BLOCKED KEYWORDS](#)[CIRCUMVENTION TOOLS](#)[GFW FAQ](#)[User](#)

BLOCKED DOMAINS

Sorted by Alexa

Asc

Desc

Sorted by Alphabet

Asc

Desc

Filtered by Topic

All | None

☒ - Unknown -

☒ Activism

☒ Blogger

☒ Education

☒ File sharing

☒ Gambling

☒ Games

☒ Images

☒ News

☒ Online forum

☒ Proxy

☒ Religions

☒ Search engines

☒ Service providers

☒ Shopping

← Previous 1 2 3 4 5 6 7 8 9 ... 46 47 Next →

Displaying blocked sites 1 - 30 of 1382 in total

1

 google.com

Enables users to search the world's information, including webpages, images, and videos. Offers unique features and search technology.

HTTP

DNS

IP

2

 youtube.com

User-submitted videos with rating, comments, and contests.

HTTP

DNS

IP

3

 facebook.com

A social utility that connects people, to keep up with friends, upload photos, share links and videos.

HTTP

DNS

IP



翻墙

[HOME](#)[ABOUT](#)[BLOCKED DOMAINS](#)[BLOCKED KEYWORDS](#)[CIRCUMVENTION TOOLS](#)[GFW FAQ](#)[User](#)

BLOCKED KEYWORDS

越过防火长城，我们可以到达世界的每一个角落

ACROSS THE GREAT FIREWALL, WE CAN REACH EVERY CORNER OF THE WORLD

search over 1,000 keywords

Q

☒ Google

☒ Wikipedia

Reset

← Previous 1 2 3 4 5 6 7 8 9 ... 102 103 Next →

Displaying blocked keywords 1 - 30 of 3086 in total

敏感词	Translation
严家其	Yan Jiaqi
世界通訊	WorldCom
一寸山河一寸血	World War Two in Asia (Taiwanese documentary)
世維會	World Uyghur Congress
User_支持法輪功	User_Support Falun Gong
User_平反六四	User_Redress June, 4 Incident
User_江澤民理論體系	User_Jiang Zeming Theory System
User_香港民主黨	User_Hong Kong Democratic Party
User_反藏獨	User_Anti Tibet Independence

The map below shows where 1616 blocked domains are hosted in the world based on the geolocation information extracted from their IP addresses. These blocked domains are among world's top one million domain names, ranked by Alexa.com.

Three different methods have been detected to be used by Chinese government to censor the domains. They include 1) DNS pollution, 2) HTTP request reset, 3) IP blacklist. HTTP request reset is the most common way to censor a domain. The GREEN dots on the map shows domains blocked by HTTP request reset. When the censorship bureau gets serious, combinations of methods are applied to make sure Chinese citizens can never access a domain in normal ways. The ORANGE dots on the maps shows domains blocked by combinations of HTTP reset, plus DNS pollution. The RED dots shows domains blocked by combinations of HTTP reset, DNS pollution and IP blacklist.

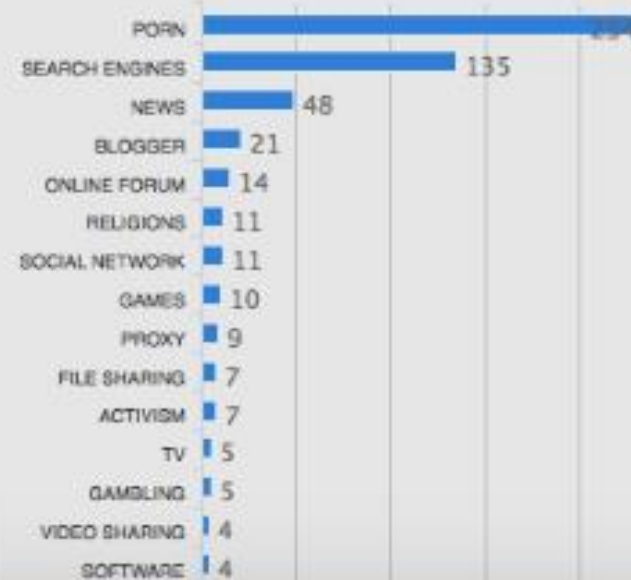
How to interact with the map:

The map is **ZOOMABLE!!!** Hovering the mouse over a dot to view its details.



of Blocked Domains by Category

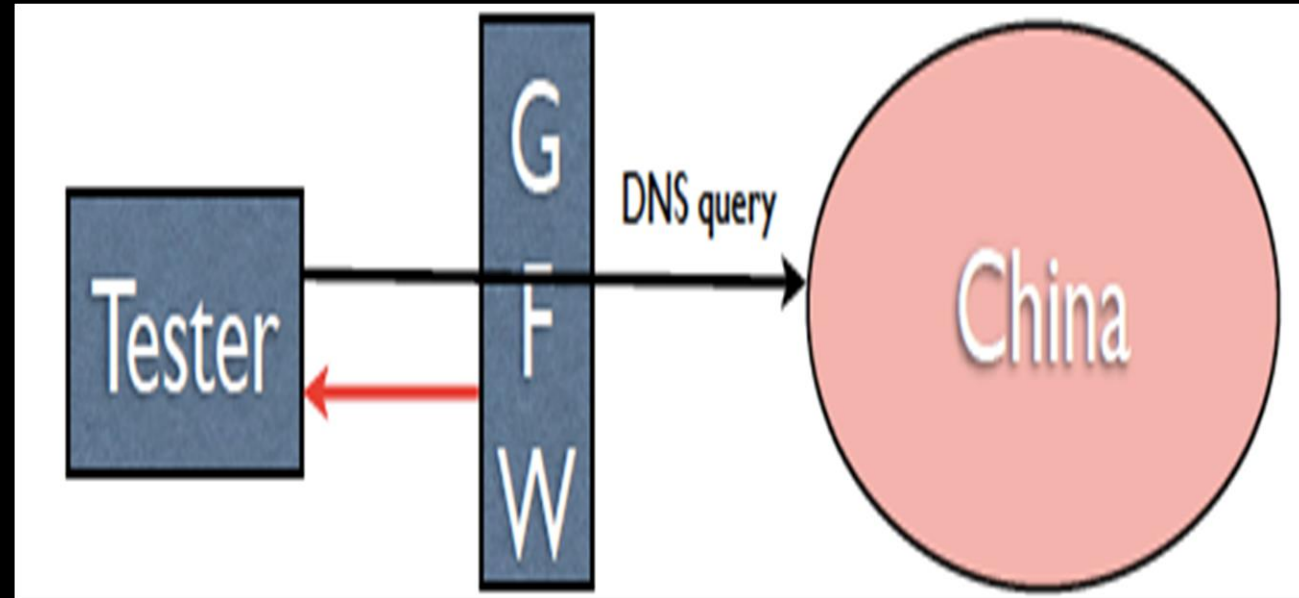
among all blocked domains



Free expression and media freedom	Gaming
Political transformation and opposition parties	Alcohol and drugs
Political reform, legal reform, and governance	Minority faiths
Militants, extremists, and separatists	Religious conversion, commentary, and criticism
Human rights	Anonymizers and circumvention
Foreign relations and military	Hacking
Minority rights and ethnic content	Blogging domains and blogging services
Women's rights	Web hosting sites and portals
Environmental issues	Voice over Internet Protocol (VOIP)
Economic development	Free e-mail
Sensitive or controversial history, arts, and literature	Search engines
Hate speech	Translation
Sex education and family planning	Multimedia sharing
Public health	P2P
Gay/lesbian content	Groups and social networking
Pornography	Commercial sites
Provocative attire	
Dating	
Gambling	

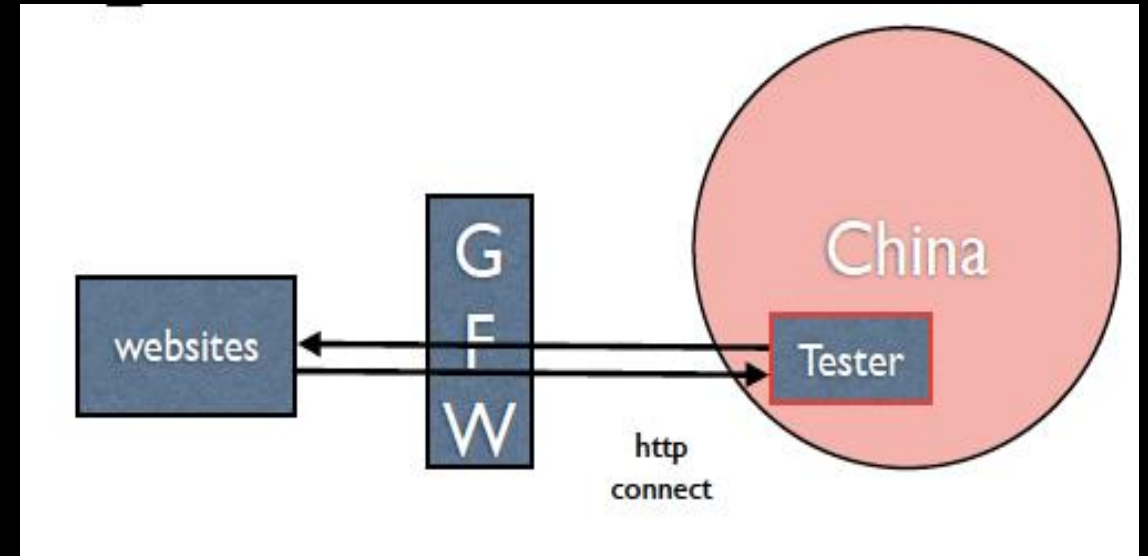
dns_bl: Domain Name polluted

- Input : a list of Domain Names
- Alexa.com Top 1M????
- COM, NET, ORG, INFO
- Test methods
- Clustering:
- pictwitter.com, twitter.computer.com => twitter.com



ip_bl: IP addressed blocked?

- Input: domain names or IP addresses
- Output: IP reachable or not
- Get the real IP address in China
- `dig +tcp -f blacklist_domain`
- HTTP connect
- `wget`, `curl`,
- Socket



rst_bl: Keywords by TCP Reset

- Input: Keyword(Chinese, English)
- Output:



Test Tools & Website

- domain_test
- ip_test
- keyword_test
- article_test
- A Web form accept users' input
- Monitoring Services, also for ourselves



防火長城 GFW 具體的封鎖方式

- GFW 只是一個執行指令的機器，沒有標準判斷功能。至於採取什麼方式要看程度，一般情況是：關鍵詞>DNS>IP



GFW 實體 「哨所」



http://www.dnp.cn/images/up_images/20170630124647692.jpg



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



GFW 基本封禁技術 (1) IP 封鎖

- GFW採用的是一種比傳統的訪問控制列表 (Access Control List, ACL) 高效得多的控制訪問方式——路由擴散技術



訪問控制列表（ACL）



路由協議與路由重新分發（redistribution）

- “歪用” 路由協議



動態路由協議簡介



靜態路由



路由重分發



GFW 路由擴散技術的工作原理

- 靜態路由
- 黑洞服務器
- 虛假回應



GFW 封禁IP的特点：

- 把以前配置在ACL裡的每條IP地址轉換成一條故意配置錯誤的靜態路由信息
- 這條靜態路由信息會把相應的IP報文引導到黑洞服務器上，通過動態路由協議的路由重分發功能，這些錯誤的路由信息可以發佈到整個網絡
- 對於路由器來講現在只是在根據這條路由條目做一個常規報文轉發動作，無需再進行ACL匹配
- 既提高了效率，又達到了控制報文之目的

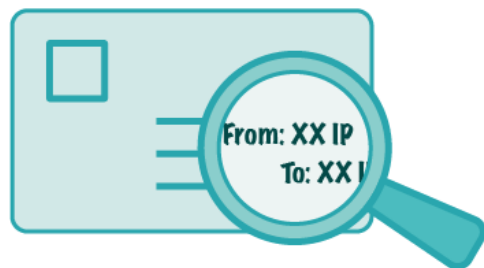


GFW 基本封禁技術（2）：入侵檢測

- 傳輸層的TCP和UDP解析都是入侵檢測業界的標準配置。UDP通常用來做DNS查詢劫持，一個附加效果就是國內的域名緩存充滿了
- TCP主要用作阻斷，把攻擊者的連接關閉掉/阻止攻擊者進行連接
- 應用層方式更多，因為解析一個協議不困難。所謂的SSL證書攔截不過是稍微做了一下SSL/TLS協議的解析，
- 入侵檢測的靈活之處在於它的部署和撤銷都很便捷無副作用無延遲，匹配精確無誤傷，是GFW最為強大靈活的功能



深度數據包檢測



淺度



深度



「淺度」的數據包檢測，像是看信封上的發件人和收件人，即決定是否放行。
「深度」的數據包檢測，可以理解成對信件內容的探查。



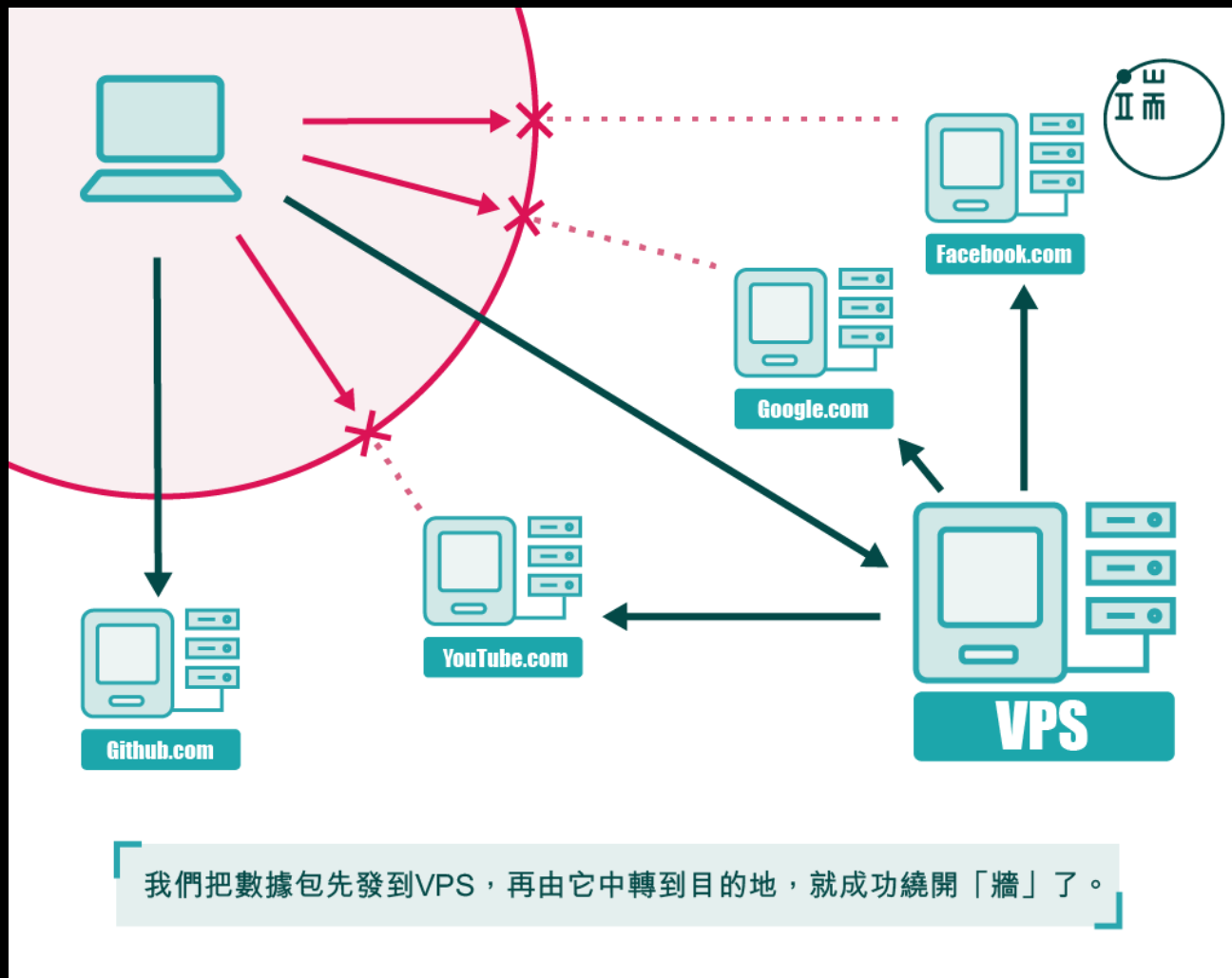
HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



常見翻牆工具的原理

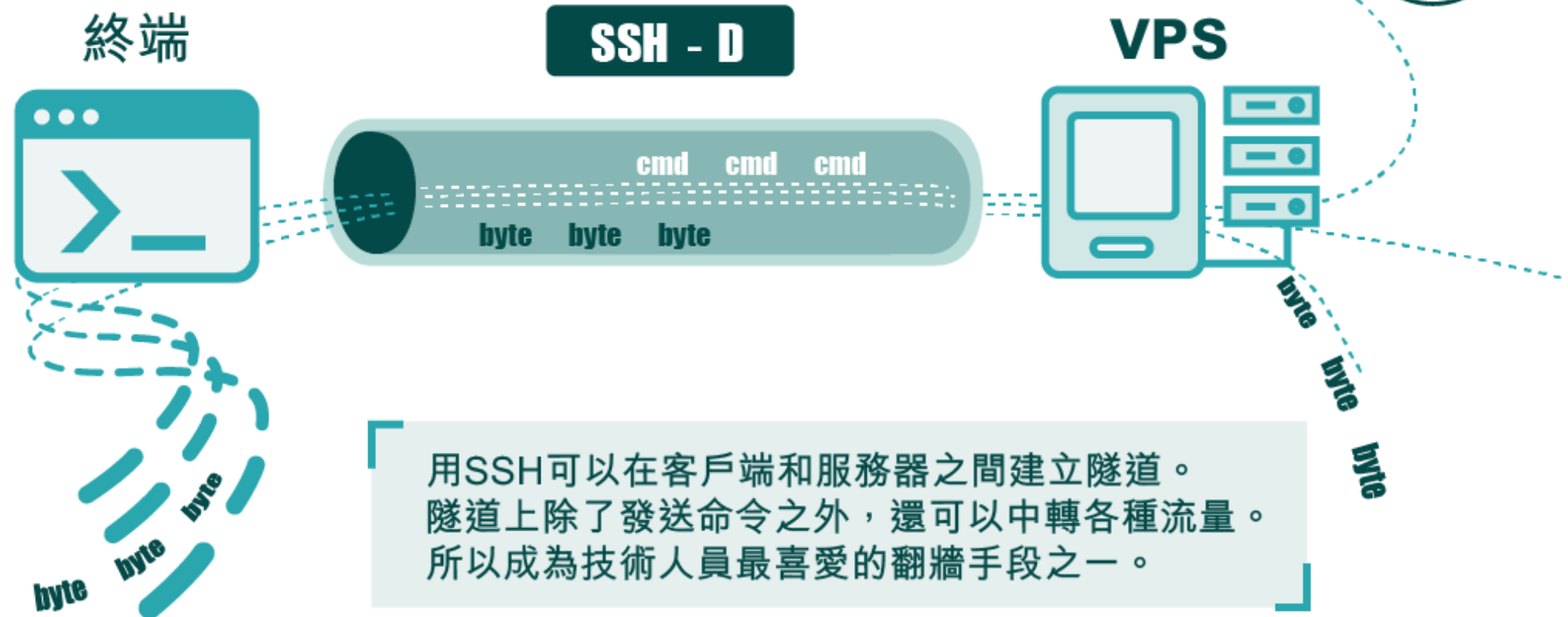


HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD





HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



“翻牆”：Censorship Circumvention

- Destination (domain, ip) blocking - bypass: proxy outside
- Communication inspection - bypass: encrypted tunnel
- Most bypass solutions combine two methods
- Encrypted traffic, route to one or more proxies



防火長城對翻牆技術的反制措施：

- Detect and block proxy servers used for circumvention via analyzing Internet traffic
- Technologies to recognize encrypted protocols

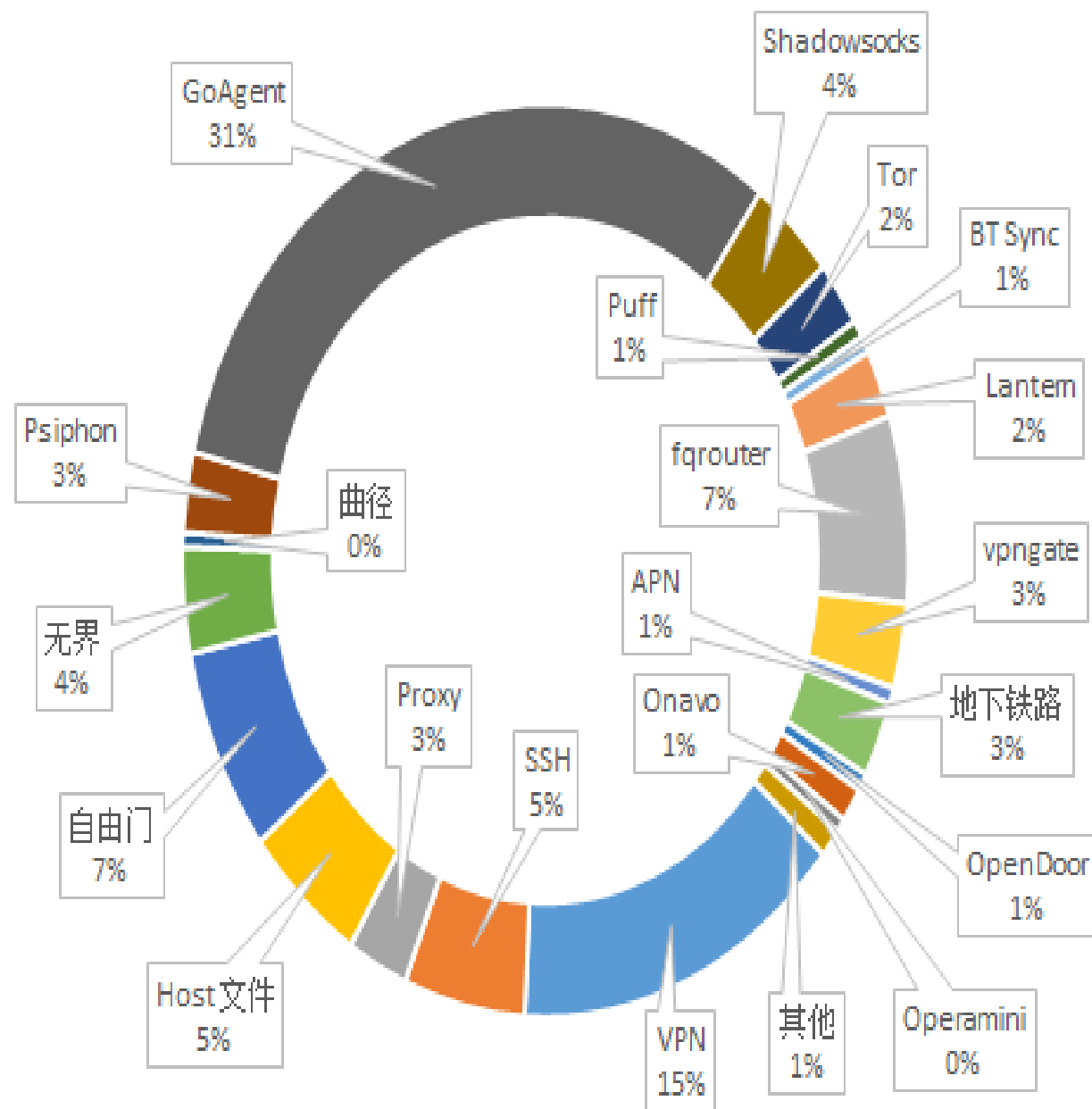


翻牆工具



HIKING GFW
漫步防火长城

翻牆工具热门程度排名



目前常見的幾 種翻牆工具

- TOR
- Lantern
- Psiphon
- Firefly



以 TOR 為例 (1)

- Tor started as an anonymous communication tool in 2002 and was used for circumvention by many Chinese Internet users.
- Tor used a centralized directory server which maintains a list of proxy nodes.
- GFW blocked all the IP address of the directory server by 2009



以TOR為例 (2)

- 2010: TOR's "hidden "bridge" nodes that are not listed in the directory server
- 2011: GFW learned the way to block hidden private bridge nodes In 2011.
- 2012: Tor launched **obfsproxy**, a tool that can transform the Tor traffic into innocent looking traffic so that the GFW cannot differentiate the use of Tor from other Internet activities
- 2013: GFW finds a way to defeat **obfsproxy**

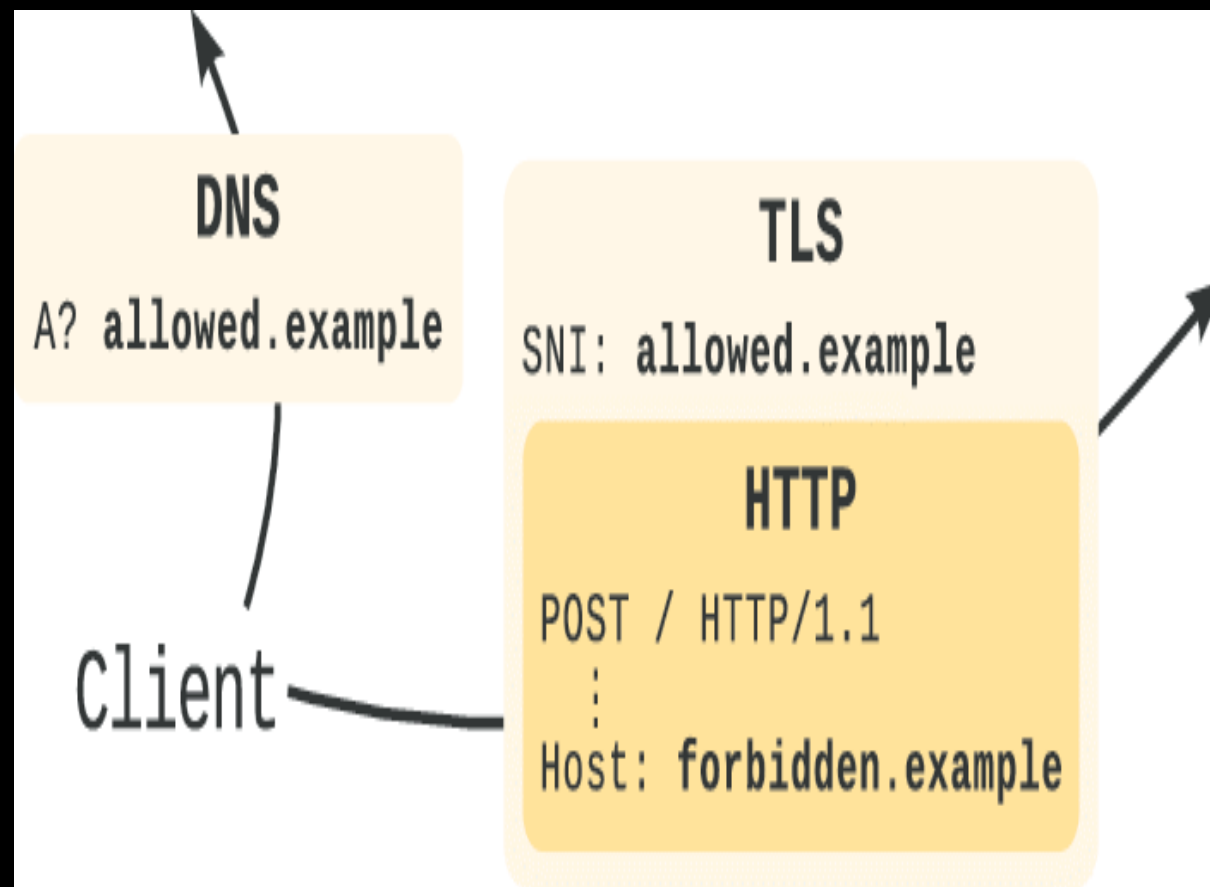


新思路：“連帶自由 Collateral Freedom”

- 不是那種翻牆技術不能被對手屏蔽，而是如果對方封鎖這種技術，其（政治，社會或者經濟）的代價是什麼？



“域名前置 Domain Fronting” 技術



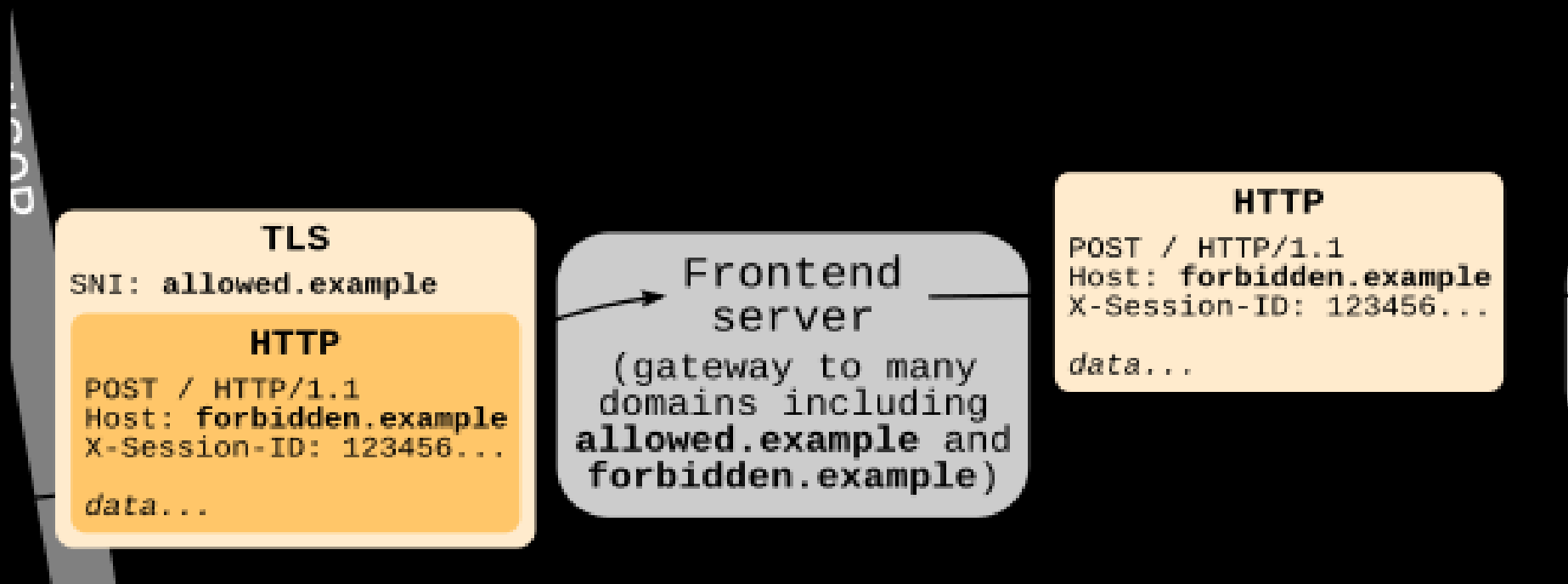
HIKING GFW

漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD





“域名前置 Domain Fronting” 技術

TOR Implementation



翻牆服務

Recommended Circumvention Tools



>> more circumvention tools...



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD

ShadowSocks



防火長城演進的未來趨勢



中共中央網絡安全和信息化領導小組



組長：習近平（2014-2-27）

<https://bit.ly/2LoATGR>



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



中共中央網絡安全和信息化委員會 2018-4

主任：習近平，副主任：李克強，王滬寧，辦公室主任：徐麟



<https://bit.ly/2LoATGR>



HIKING GFW

漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



「牆」的 進化 (2014 – 2018)



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD





HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



中國政府對VPN的控制

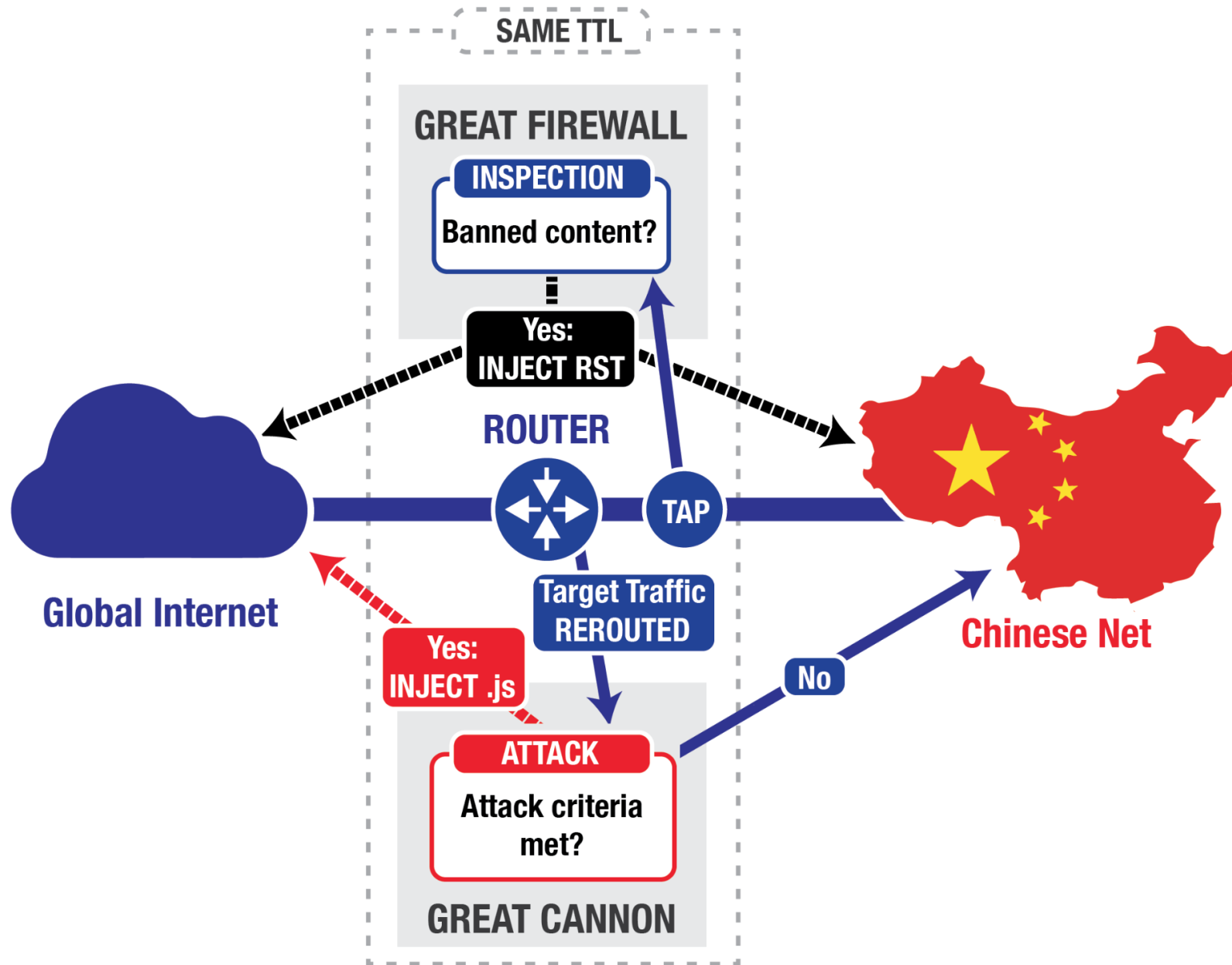
- “網絡主權”
- 關閉國內大部分VPN服務
- 干擾外國VPN
- 官辦VPN



「大砲」 China's Great Cannon

2015.3





2015年部分网络封锁事件

- 8月20日
- 8月21日
- 8月22日
- 8月25日
- 8月25日
- 8月25日
- 8月26日



翻牆工具技術演進的未來趨勢

- 動態平衡
- 理想穩態
- “連帶自由”的瓶頸
- 下一代的翻牆方法



2012 – 2018

防火長
城的威
力



HIKING GFW
漫步防火长城



越过防火长城，我们可以到达世界的每一个角落
ACROSS THE GREAT WALL, WE CAN REACH EVERY CORNER IN THE WORLD



主要參考文獻：

- Shen, F. (2014). **Great Firewall of China**. In Harvey, K. (Ed.). (2014). Encyclopedia of Social Media and Politics. SAGE, Volume 2, 599-602.
- David Fifield*, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson **Blocking-resistant communication through domain fronting** In <https://www.bamsoftware.com/>
- GFW Blog 功夫网与翻墙 <http://www.chinagfw.org/>
- 阅后即焚: GFW http://www.chinagfw.org/2009/08/gfw_30.html
- 刘刚, 云晓春, 方滨兴, 胡铭曾. "一种基于路由扩散的大规模网络控管方法". 通信学报, 24(10): 159-164. 2003.
- 李蕾, 乔佩利, 陈训逊. "一种IP访问控制技术的实现". 信息技术, (6). 2001.
- 道高一尺，牆高一丈：互聯網封鎖是如何升級的 <https://theinitium.com/article/20150904-mainland-greatfirewall/>

