UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
April 2015

China's Great Cannon

Authors: Bill Marczak(Lead), Nicholas Weaver (Lead), Jakub Dalek, Roya Ensafi, David Fiflield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, Vern Paxson

Media coverage: New York Times, Deutsche Welle, Wall Street Journal, The Guardian, Washington Post (The Switch), Washington Post (editorial), Business Insider, Bloomberg, Forbes, CNNi (video included), NBC News, South China Morning Post, Epoch Times, Japan Times, Radio Free Asia, Threatpost, SC Magazine, The Daily Beast, The Register, Foreign Policy, The Hill, Krebs on Security, The Daily Dot, Wired, Fast Company (1), Fast Company (2), Engadget, Gizmodo, Slashdot, BuzzFeed News, PCMag, PCWorld, ZDNet, Popular Mechanics, TechCrunch, Quartz, China Digital Times, Infosecurity, The Verge, Ars Technica, Motherboard, Global Voices Online, CFR's Cyber Week in Review, The Conversation, US News & World Report, Committee to Protect Journalists, HelpNet Security, The Hill (Apr. 26), MSN, VOA News, Computer Business Review, National Post.

SECTION 1: INTRODUCTION, KEY FINDINGS

On March 16, GreatFire.org observed that servers they had rented to make blocked websites accessible in China were being targeted by a Distributed Denial of Service (DDoS) attack. On March 26, two GitHub pages run by GreatFire.org also came under the same type of attack. Both attacks appear targeted at services designed to circumvent Chinese censorship. A report released by GreatFire.org fingered malicious Javascript returned by Baidu servers as the source of the attack.[1] Baidu denied that their servers were compromised.[2] Several previous technical reports[3] have suggested that the Great Firewall of China orchestrated these attacks by injecting malicious Javascript into Baidu connections. This post describes our analysis of the attack, which we were able to observe until April 8, 2015.

We show that, while the attack infrastructure is co-located with the Great Firewall, **the attack was carried out by a separate offensive system, with different capabilities and design, that we term the "Great Cannon."** The Great Cannon is not simply an extension of the Great Firewall, but a distinct attack tool that hijacks traffic to (or presumably from) individual IP addresses, and can *arbitrarily replace unencrypted content as a man-in-the-middle*.

The operational deployment of the Great Cannon represents a significant escalation in state-level information control: the normalization of widespread use of an attack tool to enforce censorship by weaponizing users. Specifically, the Cannon manipulates the traffic of "bystander" systems outside China, silently programming

their browsers to create a massive DDoS attack. While employed for a highly visible attack in this case, the Great Cannon clearly has the capability for use in a manner similar to the NSA's QUANTUM system,[4] affording China the opportunity to deliver exploits targeting any foreign computer that communicates with any China-based website not fully utilizing HTTPS.

Report Structure

We organize our Report as follows:
Section 2 locates and characterizes the Great Cannon as a separate system;
Section 3 analyzes DDoS logs and characterizes the distribution of affected systems;
Section 4 presents our attribution of the Great Cannon to the Government of China;
Section 5 addresses the policy context and implications;
Section 6 addresses the possibility of using the Great Cannon for targeted exploitation of individual users.

SECTION 2: THE FIREWALL & THE CANNON: SEPARATE SYSTEMS, SIGNIFICANT SIMILARITIES

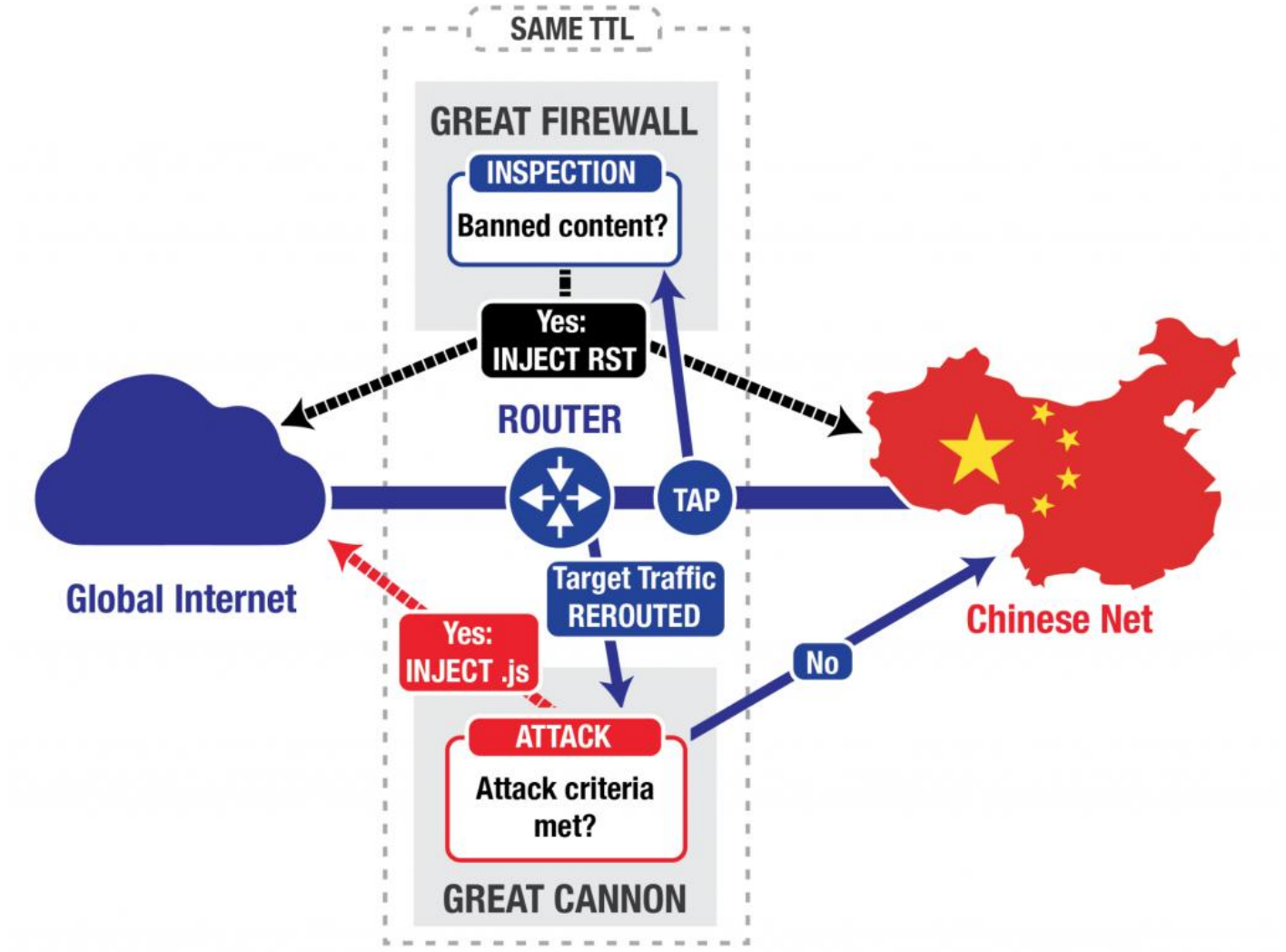

Figure 1. **Simplified logical topology of the Great Cannon and Great Firewall**

In general, a *firewall* serves as an *in-path* barrier between two networks: all traffic between the networks must flow *through* the firewall. In contrast, an *on-path* system like the Chinese "Great Firewall" (GFW) sits off to the side: it eavesdrops on traffic between China and the rest of the world (**TAP** in *Figure 1*), and terminates requests for banned content (for example, upon seeing a request for "http://www.google.com/?falun",[5] regardless of actual destination server) by injecting a series of forged TCP Reset (RST) packets that tell both the requester and the destination to stop communicating (**INJECT RST** in *Figure 1*).[6] *On-path* systems have architectural advantages for censorship, but are less flexible and stealthy than *in-path* systems as attack tools, because while they can inject additional packets, they cannot prevent *in-flight* packets (packets that have already been sent) from reaching their destination.[7] Thus, one generally can identify the presence of an *on-path* system by observing anomalies resulting from the presence of both injected and legitimate traffic.[8]
The GFW keeps track of connections and reassembles the packets ("TCP bytestream reassembly") to determine if it should block traffic. This reassembly process requires additional computational resources, as opposed to considering each packet in isolation, but allows better accuracy in blocking. While a web request often fits within a single packet, web replies may be split across several packets, and the GFW needs to reassemble these packets to understand whether a web reply contains banned content.

On any given physical link (e.g., a fiber optic cable), the GFW runs its reassembly and censorship logic in multiple parallel processes[9] (perhaps running on a cluster of many different computers). Each process handles a subset of the link's connections, with all packets on a connection going to the same process. This *load-balanced* architecture reflects a common design decision when a physical link carries more traffic than a single computer can track. Each GFW process also exhibits a highly distinctive *side-channel* -- it maintains a counter, and numbers the forged TCP Reset packets it injects (via the value of the IP TTL field).
The Great Cannon (GC) differs from the GFW: as we will show, the GC is an *in-path* system, capable of not only injecting traffic but also directly suppressing traffic, acting as a full "man-in-the-middle" for targeted flows. The GC does not actively examine all traffic on the link, but only intercepts traffic to (or presumably from) a set of targeted addresses. It is plausible that this reduction of the full traffic stream to just a (likely small) set of addresses significantly aids with enabling the system to keep up with the very high volume of traffic: the GC's full processing pipeline only has to operate on the much smaller stream of traffic to or from the targeted addresses. In addition, in contrast to the GFW, the GC only examines individual packets in determining whether to take action, which avoids the computational costs of TCP bytestream reassembly. The GC also maintains a *flow cache* of connections that it uses to ignore recent connections it has deemed no longer requiring examination.

The GC however also shares several features with the GFW. Like the GFW, the GC is also a multi-process cluster, with different source IP addresses handled by distinct processes. The packets injected by the GC also have the same peculiar TTL side-channel as those injected by the GFW, suggesting that both the GFW and the GC likely share some common code. Taken together, this suggests that although the GC and GFW are independent systems with different functionality, there are significant structural relationships between the two.
In the attack on GitHub and GreatFire.org, the GC intercepted traffic sent to Baidu infrastructure servers that host commonly used analytics, social, or advertising scripts. If the GC saw a request for certain Javascript files on one of these servers, it appeared to probabilistically take one of two actions: it either passed the request onto Baidu's servers unmolested (roughly 98.25% of the time), or it dropped the request *before* it reached Baidu and instead sent a malicious script back to the requesting user (roughly 1.75% of the time). In this case, the requesting user is an individual outside China browsing a website making use of a Baidu infrastructure server (e.g., a website with ads served by Baidu's ad network). The malicious script enlisted the requesting user as an unwitting participant in the DDoS attack against GreatFire.org and GitHub.

LOCALIZING THE CANNON

The GFW continues to operate as normal: on-path and statefully

We began our investigation by confirming the continued normal operation of the GFW's censorship features. We did so employing measurements between our test system outside of China and a Baidu server that we observed returning the malicious Javascript. We sent the Baidu server a request that the GFW would process as a query for "http://www.google.com/?falun", a URL long known[10] to trigger the GFW to inject forged TCP Resets to terminate the connection. This packet capture shows the results of our experiment, which confirmed that the normal, well-understood operation of the GFW continues. Note that the capture includes both the injected TCP Reset and, later, the legitimate response (an HTTP 403 reply) from the Baidu server. This occurs because the GFW operates as an *on-path* system, and, as discussed earlier, on-path systems cannot prevent *in-flight* packets from reaching their destination.

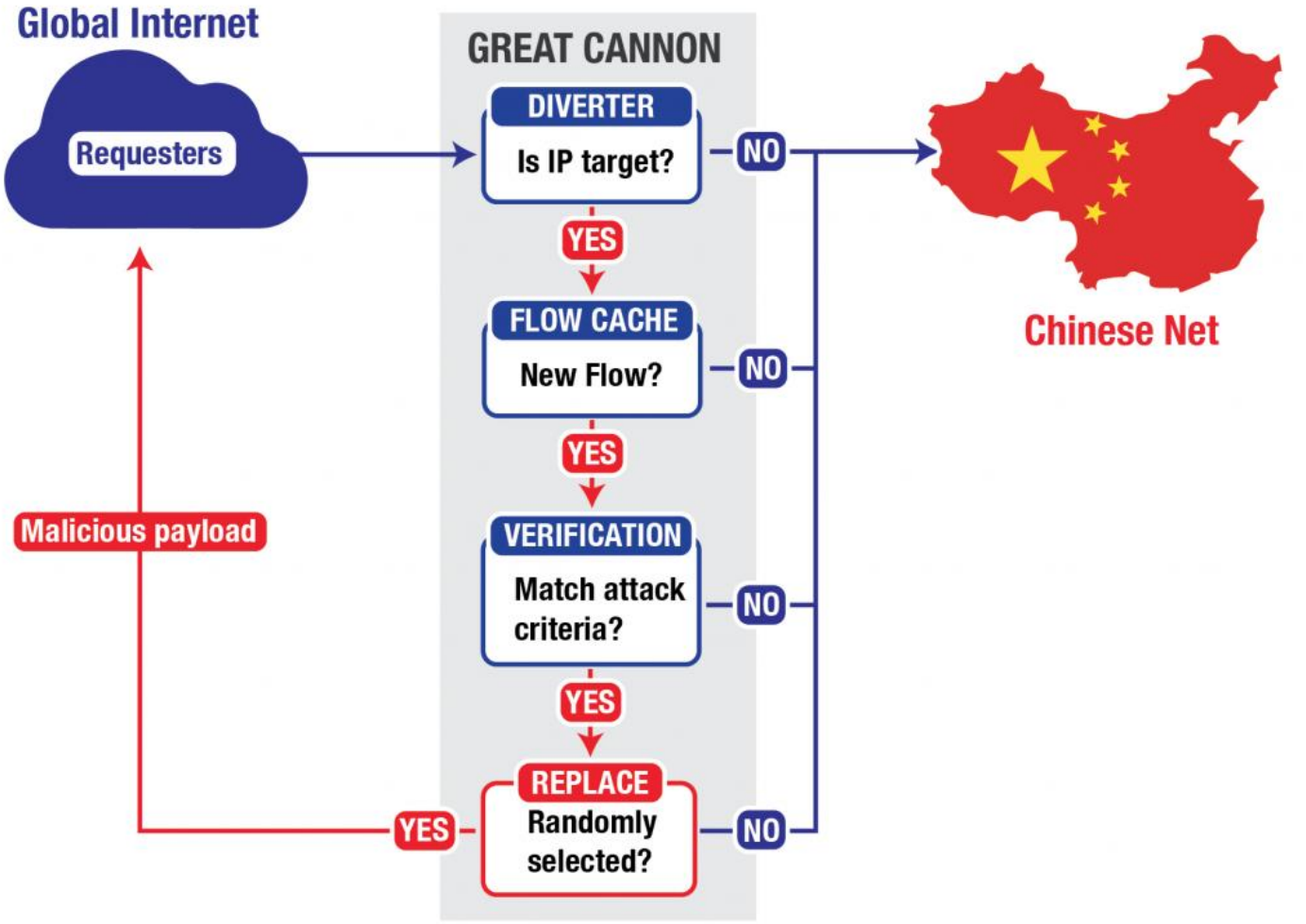

Figure 2. **How the Great Cannon was deployed in the GitHub and GreatFire.org attacks**

Localizing the GFW

We then localized where (with respect to our measurement system) in the network topology the GFW operates, as follows. For a given measurement packet, we can control how far into the network it transits from our measurement system to its destination by controlling the packet's *TTL value*. The TTL value determines

after how many intermediate hops a packet will be discarded by the Internet's internal routers. We sent the "Falun" queries from our test system to the Baidu server with TTL values increasing from 1 on up. We observed that the GFW's TCP Reset injection only occurred when we sent packets with TTL values >= 18, suggesting that the GFW acts on traffic flowing between the 17th and 18th hop along the path from our test system to the Baidu server (which was itself 24 hops away from our test system). This packet capture shows our localization results.[11]

The GC operates as a separate, in-path system

As noted previously, our traces of GFW operation showed both the injected TCP Reset, as well as the legitimate server reply. In contrast, no legitimate server reply accompanied the injected malicious reply from the GC. We ran further testing, where we *retransmitted* our request to Baidu over the same connection, and with the same sequence numbers, after we received a malicious response. We observed Baidu responding as normal to the retransmitted request. **Thus, we conclude[12] that the GC *dropped* our request before it reached Baidu, a capability not present in the GFW.**[13]
We also checked whether the GFW and GC might share the same injector device,[14] but found no evidence that they do. In particular, from a given TCP source port, we sent one request designed to trigger GC injection, followed by a request designed to trigger GFW injection. We repeated the experiment from a number of source ports. While packets injected by both the GFW and GC exhibited a similar (peculiar) TTL side-channel indicative of shared code between the two systems, we found no apparent correlation between the GFW and GC TTL values themselves.

The GC appears to be co-located with the GFW

We used the same TTL technique to localize the GC on the path between our test system and the Baidu server. We found that for our path, the GC acted on traffic between hop 17 and hop 18, the **same link we observed as responsible for the GFW**. We also observed that unlike the GFW, we could trigger the GC using "naked" requests (i.e., requests sent in isolation, with no previous TCP SYN as required for standard communication). Acting on "naked" requests implies that the GC's content analysis is more primitive (and easily manipulated), but does offer significant performance advantages, as the GC no longer needs to maintain complex state concerning connection status and TCP bytestream reassembly.
We also checked two separate servers in China whose traffic the GC targets to observe whether the GC existed along with the Great Firewall on multiple network paths. From our measurement system outside of China, we examined the path to both 115.239.210.141 and 123.125.65.120. For 115.239.210.141, the GFW and the GC both exist between hop 12 and 13, on the link between 144.232.12.211 and 202.97.33.37, as the traffic enters China Telecom. For 123.125.65.120, the GFW and GC both exist between hop 17 and 18, on the link between 219.158.101.61 and 219.158.101.49, belonging to China Unicom. A previous report by Robert Graham used the same TTL technique to conclude that on one link, the GC was located *"inside China Unicom infrastructure."*[15]

The GC is currently aimed only at specific destination IP addresses

When we probed an IP address adjacent to the Baidu server (123.125.65.121), the GC ignored the requests completely, although the GFW acted on censorable requests to this host.

Unlike the GFW, the GC only acts on the first data packet of a connection

For a given source IP address and port, the GC only examines the first data packet sent when deciding whether to inject a reply. To avoid examining subsequent packets requires remembering which connections it has

examined in a *flow cache*. Unlike the GFW, **the GC does not reassemble packets, a significant implementation difference.** In addition, the GC will process invalid HTTP requests, while the GFW will not, also indicating differing implementations.

We confirmed these behaviors by sending a number of probes to the Baidu server, requesting resources that trigger the GC's injection. Each probe had a different source port. We sent 500 probes, each with the request split across three packets (so 1,500 packets total). The GC ignored each probe. We then sent 500 probes where the first packet's data is an invalid HTTP request, and the second packet's data is a complete, valid request for a targeted resource. The GC ignored each probe. We then sent a final 500 single-packet probes, each containing a complete, valid request for a targeted resource, to confirm normal GC operation. As expected, the GC injected malicious content in some cases, seemingly based on its probabilistic decision-making process.

How big is the GC flow cache?

We attempted to completely fill the GC flow cache by sending packets to the Baidu server with different source IP addresses and ports, while probing to see whether the entries that we previously added had now expired. Our attempt suggests that at least in some cases, the GC flow cache between our test system and the Baidu server supports up to around 16,000 entries for a single sending IP address.

Unlike the GFW, the GC appears to act probabilistically

Censorship systems generally operate in a deterministic fashion: they aim to block all content that matches the target criteria. The GC, on the other hand -- at least for this particular attack -- appears to act probabilistically, and ignores most of the traffic it could act on. In one test, it completely ignored all traffic from one of four measurement IP addresses, and on the three other measurement IP addresses it only responded to 526 requests out of an initial 30,000 from the three (1.75%).

The cache capacity test also provides evidence that the GC's probabilistic choice occurs on the decision to *act* on a particular flow, and not as some sort of pre-filter for reducing analysis load. When we succeeded in completely filling the flow cache, subsequently injected packets occurred for *different* source ports than in the initial test. If the GC only intercepted a subset of flows to the target IP address, we would expect subsequent injections to appear for the same flows, since most schemes to probabilistically select flows for interception (such as hashing the connection 4-tuple) would select the same set of flows the second time around.

Does the GC have a load-balanced architecture?

We determined that the GC uses a separate flow cache for different source IP addresses, and that packets injected from different source IP addresses have distinct TTL side-channels. This finding suggests a load-balanced architecture similar to the GFW, where packets are routed to GC nodes based on source IP address. We then sent traffic alternating from four measurement IP addresses in an attempt to fill a 16,000 entry cache. This attempt did not manage to fill the cache, suggesting that the GC not only processed the different source IP addresses with different injection elements, but did so using different flow caches. As stated before, one of the four source IP addresses never received any injected replies.

SECTION 3: ANALYSIS OF THE DDOS LOGS FROM THE ATTACK AGAINST GREATFIRE

The staff of GreatFire.org provided the authors with server logs covering the period of March 18 to 28.[16] (A report previously published by Great Fire uses a different sample.[17]) This period appears to capture the end of the DDoS attack on GreatFire.org's services, as shown by the size of server log files over this period:
To keep our analysis tractable, we examined a sample of the data from March 18th 11:00 GMT to March 19th 7:00 GMT, as seen from two of the three most commonly seen backend servers. For each hour, we selected 30MB of compressed logs for each server.[18] The total sample includes 16,611,840 web requests, with 13,183 unique source IP addresses. We used the MaxMind GeoIP2 Lite database[19] from March 3rd, 2015 to assign a country of origin to each source IP address. For any IP address that did not result in a definite geolocation using this tool (31 addresses), we looked up the address manually using the *iplocation.net* service.
The figure below summarizes the top countries of origin, with China added for comparison.

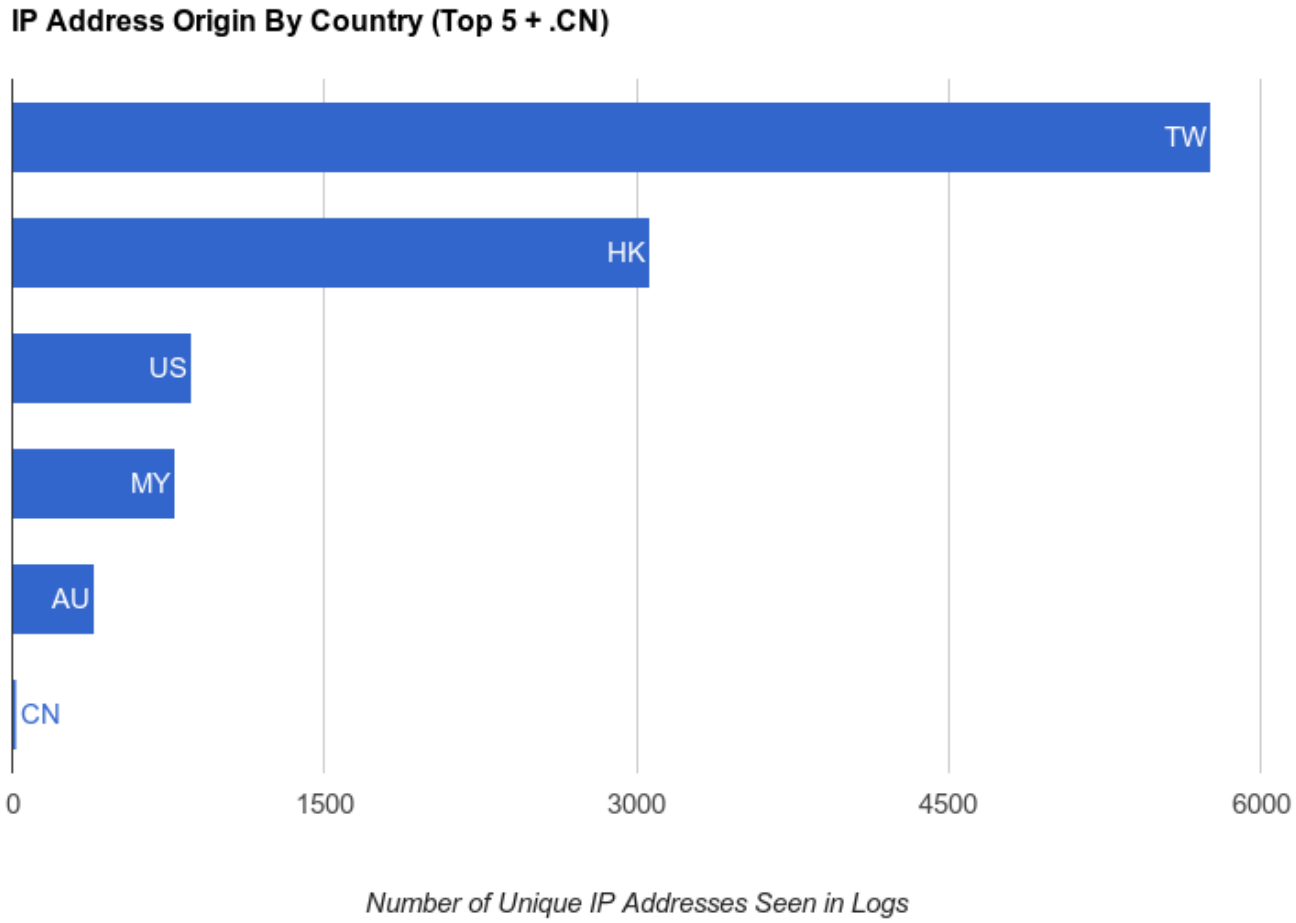

Figure 3. **Number of Unique IP addresses seen in DDoS log sample showing the top 5 countries/regions, with Chinese traffic included for comparison.**

Note that 8,827 (66.9%) of the IP addresses originate from Taiwan and Hong Kong, two regions where Chinese is the official language. China, however, accounted for only 18 requests. This is consistent with malicious code injected into China-hosted websites at the border of the Chinese Internet.

To determine which websites have their responses altered by the injection of malicious code, we extracted the domain names of the 25 most frequently seen referrers in our dataset,[20] finding that these domains account for 55% of the total requests in the sample.

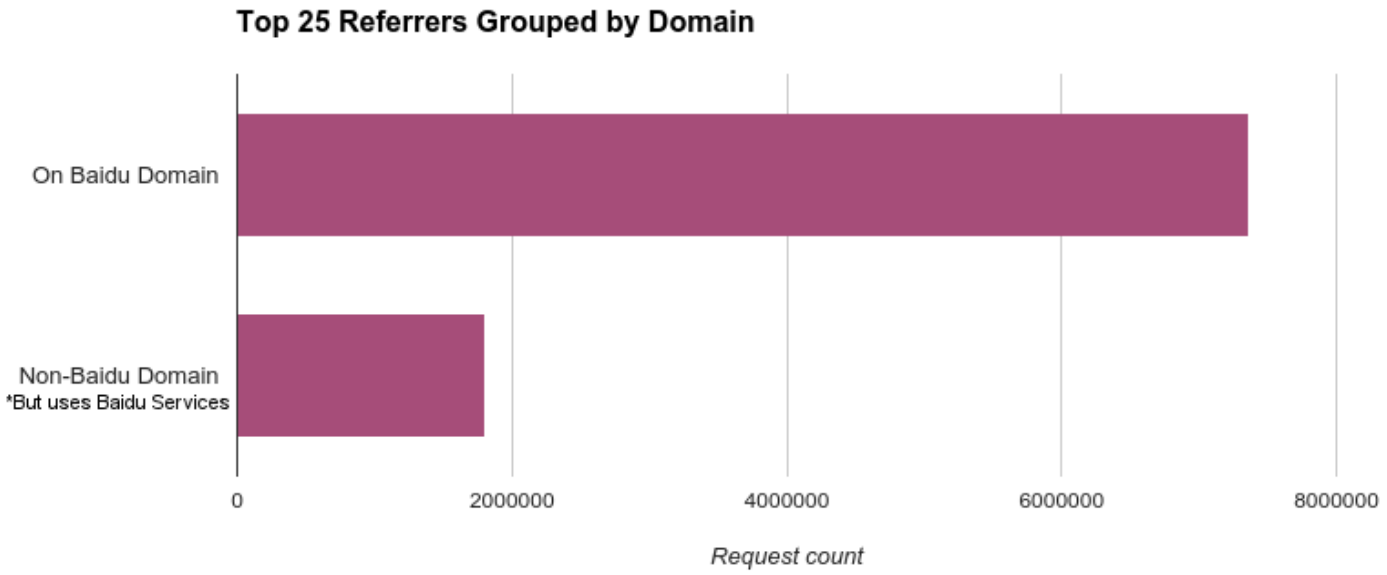

Figure 4. **Top 25 referrers found in the DDoS logs, grouped by domain. The top bar reflects domains directly in the baidu.com DNS space. Manual verification confirms that all top 25 referrers use Baidu services such as advertising or analytics.**

The most commonly seen domain is *pos.baidu.com* (37.7% of total requests in the sample), a part of Baidu's ad network. Many non-Baidu sites display ads served through Baidu's ad network, indicating that visitors to non-Baidu sites displaying ads also became targeted.[21]

We examined the top 25 domains, and linked each one to Baidu: in each case, the site is either a Baidu property or uses Baidu analytics, advertisements, or static resources.[22] This finding indicates that Baidu was a major injection target for this attack. According to Alexa statistics, Baidu itself is the fourth-most visited site globally, the highest ranking China-based site on the global list,[23] and has received an estimated 4.99 million unique visitors from the US alone in the past 30 days.[24]

We speculate that Baidu was chosen as an injection target because it is a simple way to target many users.

SECTION 4: ATTRIBUTING THE GREAT CANNON TO THE CHINESE GOVERNMENT

We believe there is compelling evidence that the Chinese government operates the GC. In recent public statements, China has deflected questions regarding whether they are behind the attack, instead emphasizing that China is often itself a victim of cyber attacks.[25]

Where is the GC Located?

We tested two international Internet links into China belonging to two different Chinese ISPs, and found that in both cases the GC was co-located with the GFW. This co-location across different ISPs strongly suggests a

governmental actor.

Who built the Great Cannon?

That the GFW and GC have the same type of TTL side-channel suggests that they share some source code. We are unaware of any public software library for crafting packets that introduces this type of TTL side-channel.

What is the Great Cannon's Function?

Our observations indicate that the GC's design does not reflect technology well-suited for performing traffic censorship. Its operation only examines the first data packet of a given connection, which provides a weak censorship mechanism compared to the GFW. More generally, the GC's design does not, in practice, enable it to censor any traffic not already censorable by the GFW. Thus, the evidence indicates that the GC's role is to inject traffic under specific targeted circumstances, not to censor traffic.

Who is the Great Cannon attacking?

The DDoS attack launched by the GC using "bystander" machines directly aligns with known political concerns of the Chinese government. The Cyberspace Administration of China has previously referred to GreatFire as a "foreign anti-Chinese organization" (境外反华组).[26] The particular GreatFire service targeted in this attack provides proxies to bypass the GFW using encrypted connections to Amazon's CloudFront cloud service.

GreatFire also hosts two GitHub repositories, https://gitub.com/greatfire and https://github.com/cn-nytimes, that provide technology for users who wish to circumvent Chinese government censorship. The attack on GitHub specifically targeted these repositories, possibly in an attempt to compel GitHub to remove these resources. GitHub encrypts all traffic using TLS, preventing a censor from only blocking access to specific GitHub pages. In the past, China attempted to block Github, but the block was lifted within two days, following significant negative reaction from local programmers.[27]

SECTION 5: POLICY CONTEXT AND IMPLICATIONS

This section describes some policy implications of deploying the Great Cannon, addresses the impact of targeting Baidu traffic specifically, and discusses the Chinese authorities that may be involved in operation of the GC.

Implications of the GC for Chinese Policy

Deploying the Great Cannon is a major shift in tactics, and has a highly visible impact. It is likely that this attack, with its potential for political backlash,[28] would require the approval of high-level authorities within the Chinese government. These authorities may include the State Internet Information Office (SIIO),[29] which is responsible for Internet censorship. It is also possible that the top body for cybersecurity coordination in China, the Cybersecurity and Informatization Leading Group (CILG),[30] would have been involved. The CILG is chaired by Xi Jinping and includes as members senior leaders from across the government; its administrative office is housed within the SIIO.[31]

The government's reasoning for deploying the GC here is unclear, but it may wish to confront the threat presented to the Communist Party of China's (CPC) ideological control by the "collateral freedom" strategy advanced by GreatFire.org[32] and others. The attack was exceptionally costly to GreatFire, according to their public statements,[33] as well as disruptive to the companies that hosted GreatFire content. Such a disruption could be both an attempt to block the operations of an undesirable resource, and a signal sent to other organizations of the potential price tag for this kind of activity. Deployment of the GC may also reflect a desire to counter what the Chinese government perceives as US hegemony in cyberspace.
This approach would be consistent with the CPC's paramount focus on protecting "domestic stability" (and its own authority) against entities it has identified as "foreign hostile forces," including not only governments but also Western media outlets (such as the *New York Times*) and NGOs or other civil society actors (such as GreatFire.org).[34] According to such a world view, the collateral freedom strategy is a provocative, hostile act that threatens China's security.

Implications of Using Traffic to Baidu Services

The incorporation of Baidu in this attack suggests that the Chinese authorities are willing to pursue domestic stability and security aims at the expense of other goals, including fostering economic growth in the tech sector. Selecting Baidu's international traffic may appear counterproductive given the importance of Baidu to the Chinese economy: the company enjoys stature as one of China's "big three" Internet firms, alongside Alibaba and Tencent,[35] and currently ranks as the top site in China.[36] While its shares came under pressure after the February release of its Q4 and fiscal year 2014 reports,[37] its total revenue in 2014 was USD $7.906 billion, with online marketing revenues for that period valued at USD $7.816 billion.[38]
"Service interruptions could reduce our revenues and profits and damage our brand if our systems are perceived to be unreliable."[39]

Baidu has denied involvement in the attack and asserted its internal security was not compromised.[40] Yet the targeting of international visitors trying to reach sites that are Baidu properties, or that use Baidu analytics, advertisements, or static resources, could undermine the company's reputation and its appeal to overseas users and advertisers.

Baidu writes in its SEC filings that it was the target of legal action in the United States in 2011[41] for complying with Chinese censorship. Baidu explicitly notes that cooperation and coordination with Chinese censorship authorities could be costly in terms of brand image, profit, and stockholder confidence.
"our compliance with PRC regulations governing internet access and distribution of news and other information over the internet may subject us to negative publicity or even legal actions outside of China."[42]
Moreover, exploiting Baidu's international reach as a means for conducting digital attacks belies the government's recent commitment to enhance the global presence of Internet companies. At the meeting of the National People's Congress on March 5, 2015, Premier Li Keqiang (who is also Vice-Chair of the CILG) announced:

We will develop the "Internet Plus" action plan to integrate the mobile Internet, cloud computing, big data, and the Internet of Things with modern manufacturing, to encourage the healthy development of e-commerce, industrial networks, and Internet banking, and to *guide Internet-based companies to increase their presence in the international market*.[43]

This goal – which closely echoes that contained in a draft declaration presented (but not passed) at the November 2014 Wuzhen World Internet Conference[44] – may not come to fruition if Chinese domestic companies appear unreliable, their business objectives secondary to other objectives of the Chinese

Government.
Chinese authorities may, however, be betting that their use of Baidu traffic to mount this DDoS attack will ultimately be perceived as an isolated occurrence, a sort of "force majeure," with limited impact on Baidu's long-term economic prospects – particularly given Baidu's apparent status as unwitting victim and its strong market position.

Additionally, Baidu's CEO Robin Li is a member of the Chinese People's Political Consultative Conference[45] and well-positioned for lucrative government contracts going forward -- such as his artificial intelligence project "China Brain," for which he has sought military support.[46] He may have little personal incentive (let alone opportunity, given the existing legal and regulatory framework applicable to Internet companies in China[47]) to challenge this action by the government.

Thinking About Authorities Who May Be Responsible for Implementing The Great Cannon

Even for the GFW, it is difficult to pinpoint the precise authorities behind its deployment, or its operators and origins. This makes understanding the origins of the GC equally challenging. However, some clues are available. For example, the shared source code and co-location between the GFW and GC suggest that the GC could have been developed within the same institutional framework as the GFW. We might therefore draw further insight into the GC by assessing what we know about the GFW.

Some reports characterize the GFW as an element of China's "Golden Shield" project,[48] under the authority of the Ministry of Public Security. However, unverified insider information 'leaked' online suggests that the GFW was developed within a separate entity: the "National Computer Network and Information Security Management Center" (国家计算机网络与信息安全管理中心) (hereafter, "the Center").[49] Little is publicly known about the Center. It appears to bear close relationship[50] to the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) run by the Ministry of Industry and Information Technology (MIIT) -- indeed, the listed address for CNCERT/CC is the same as that of the Center as indicated on its patent applications -- and the former National Network and Information Security Coordination Team,[51] a subcommittee of the State Informatization Leading Group subsumed by the CILG in 2014.[52] Notably, "MIIT also regulates China's six Internet service providers (ISPs), which in turn are expected to monitor and filter content on their networks according to censorship guidelines established by the State Council Information Office and the SIIO."[53] Those ISPs include China Telecom and China Unicom, on the links of which we co-located the GFW and GC (see above).

It is unknown whether the GFW and/or the GC are in fact maintained (or may have been developed in whole or in part) by the National Computer Network and Information Security Management Center. However, patent applications filed by this entity, taken together, appear to indicate a mandate for large scale network surveillance, filtering, and defense. The Center has filed nearly 100 patent applications,[54] for designs such as "Method for detecting unexpected hot topics in Chinese microblogs;" "Method and system for recognizing Tibetan dialects;" "Website classifying method;" "Method and system for intelligent monitoring and analyzing under cloud computing;" "Method and device for managing global indexes of mass structured log data;" "Method, device and system for traffic monitoring and switching;" "Image searching/matching method and system for the same;" and "Internet basic information management system" (this last "comprises a national-level management sub-system, a provincial management sub-system and an enterprise management sub-system" that "can perform effective supervision on the Internet basic information throughout the country"). Moreover, according to state media, during the time of the GFW's development the so-called "father of the Great Firewall," Fang Binxing, was employed at CNCERT/CC,[55] an entity that appears closely tied to the Center.[56] Fang is likewise listed as an inventor on a 2008 patent application by the Center, indicating some collaboration with the Center prior to that point.

While we cannot determine the exact role played by the Center, the patent documentation and the Center itself require further research and analysis to determine whether they are relevant to operation of the GC, or present other human rights-related concerns.

SECTION 6: CONCLUDING REMARKS: THE CAPABILITY FOR TARGETED EXPLOITATION BY CHINA

We conclude with some remarks about the precedent set by China in the use of the GC and outline further implications for targeted exploitation.

The attack launched by the Great Cannon appears relatively obvious and coarse: a denial-of-service attack on services objectionable to the Chinese government. Yet the attack itself indicates a far more significant capability: an ability to "exploit by IP address". This possibility, not yet observed but a feature of its architecture, represents a potent cyberattack capability.

A technically simple change in the Great Cannon's configuration, switching to operating on traffic *from* a specific IP address rather than *to* a specific address, would allow its operator to deliver malware to targeted individuals who communicates with any Chinese server not employing cryptographic protections.

The GC operator first needs to discover the target's IP address and identify a suitable exploit. The operator then tasks the GC to intercept traffic *from* the target's IP address, and replace certain responses with malicious content. If the target ever made a single request to a server inside China not employing encryption (e.g., Baidu's ad network), the GC could deliver a malicious payload to the target. A target might not necessarily realize that their computer was communicating with a Chinese server, as a non-Chinese website located outside China could (for example) serve ads ultimately sourced from Chinese servers.

Since the GC operates as a full man-in-the-middle, it would also be straightforward to have it intercept unencrypted email to or from a target IP address and undetectably replace any legitimate attachments with malicious payloads, manipulating email sent from China to outside destinations. Even email transmission protected by standard encryption (STARTTLS) can be undermined because the GC is in a position to launch a "downgrade" attack, steering the transmission to only use legacy, unencrypted communication.
Our findings in China add another documented case to at least two other known instances of governments tampering with unencrypted Internet traffic to control information or launch attacks -- the other two being the use of QUANTUM by the US NSA and UK's GCHQ. In addition, product literature from two companies, FinFisher and Hacking Team, indicate that they sell similar "attack from the Internet" tools to governments around the world.[57] These latest findings emphasize the urgency of replacing legacy web protocols, like HTTP, with their cryptographically strong versions, like HTTPS.

We remain puzzled as to why the GC's operator chose to first employ its capabilities in such a publicly visible fashion. Conducting such a widespread attack clearly demonstrates the weaponization of the Chinese Internet to co-opt arbitrary computers across the web and outside of China to achieve China's policy ends. The repurposing of the devices of unwitting users in foreign jurisdictions for covert attacks in the interests of one country's national priorities is a dangerous precedent -- contrary to international norms and in violation of widespread domestic laws prohibiting the unauthorized use of computing and networked systems.

ACKNOWLEDGEMENTS

Special thanks to: Adam Senft (Citizen Lab) and Paul Pearce (UC Berkeley, ICSI).
We wish to acknowledge GreatFire for making their logs available to us for analysis.
We also express our deep gratitude to several individuals, anonymous or pseudonymous at their request, including "Jack B," who aided us in understanding elements of the attack in the early days, and others who helped us formulate and develop this report.

FOOTNOTES

[1] Using Baidu 百度 to steer millions of computers to launch denial of service attacks," Anonymous author, March 25, 2015 (https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1)
[2] http://www.theverge.com/2015/3/27/8299555/github-china-ddos-censorship-great-firewall
[3] *Appendix C: Related Technical Reports*
[4] http://www.wired.com/2014/03/quantum/
[5] As discussed further below, this specific URL consistently triggers GFW responses, even though if actually sent to www.google.com it simply returns the Google home page.
[6] See https://www.cs.unm.edu/~crandall/concept_doppler_ccs07.pdf for a description of the GFW's general operation using injected Reset packets.
[7] Although, the GFW does send injected RSTs to both the requester and destination, these RSTs may arrive too late to suppress transmission of some subsequent packets.
[8] See http://www.icsi.berkeley.edu/pubs/networking/ndss09-resets.pdf for a description of how to detect injected RST packets. The same techniques apply to detecting injected data packets.
[9] For information on both the parallel nature and the TTL sidechannel present in the GFW, see https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf
[10] https://www.cs.unm.edu/~crandall/concept_doppler_ccs07.pdf
[11] The packet capture also confirms the *stateful* nature of the GFW's content analysis: it does not inject a TCP Reset unless it first observes a TCP SYN and an ACK for the SYN/ACK for the connection.
[12] If the GC did not drop requests sent to Baidu, then Baidu would have received our first request (which the GC responded to), and would have ignored our subsequent, duplicate request, as dictated by the TCP protocol. We verified that when the GC did not inject a response, Baidu did indeed ignore the duplicate request.
[13] Technically complex situations exist in which an on-path system like the GFW could conceivably prevent the appearance of a response from Baidu by disrupting session initiation. We conducted extensive measurements assessing this possibility. We omit those results from this report because the "retransmission" measurement discussed above definitively rules out that possibility, rendering the measurements moot.
[14] Analogous systems to the GC, like QUANTUM, make the architectural decision of having the injector as a distinct device from the rest of the system.
[15] http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html
[16] 1.1TB, compressed. Note that the logs include both malicious and non-malicious traffic
[17] https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1
[18] Files were randomly selected amongst a list of files that were near 30MB. This size was selected because it was largest file size that was present in all timestamp hours we focused on.
[19] http://dev.maxmind.com/geoip/legacy/geolite/
[20] Note that the malicious requests are being generated by Javascript. When a script makes a web request, the web browser sets the "*Referer*" header on the request to the URL of the page that loaded the script.
[21] It is typical for web advertisements to be displayed in *iframes*. This causes the "Referer" header to report the advertisement service, not the hosting page.
[22] See Appendix A.

[23] Alexa, "The top 500 sites on the web," http://www.alexa.com/topsites (accessed April 8, 2015).
[24] Alexa, "Site overview: baidu.com," http://www.alexa.com/siteinfo/baidu.com (accessed April 8, 2015).
[25] Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference," March 30, 2015, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1250354.shtml.
[26] http://www.cac.gov.cn/2015-01/22/c_1114097853.htm
[27] http://www.computerworld.com/article/2493478/internet/github-unblocked-in-china-after-former-google-head-slams-its-censorship.html
[28] Particularly after the Snowden disclosures, and the public / state outcry associated with the NSA's QUANTUM system and other programs, the Chinese government would presumably be aware of the significant international political ramifications of a decision to use the GC to target overseas entities, and escalate the matter accordingly.
[29] Note: also referred to as the Cyberspace Administration of China. "China sets up State Internet information office," Xinhua, May 4, 2011, at http://www.chinadaily.com.cn/china/2011-05/04/content_12440782.htm.
[30] See Jon R. Lindsay, "Introduction--China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay et al. [New York: Oxford University Press, 2015], 13-14; Adam Segal, "China's New Small Leading Group on Cybersecurity and Internet Management," Council on Foreign Relations: Asia Unbound, February 27, 2014, http://blogs.cfr.org/asia/2014/02/27/chinas-new-small-leading-group-on-cybersecurity-and-internet-management/.
[31] For discussion and a diagram of institutions involved in China's national cybersecurity system, see Jon R. Lindsay, "Introduction--China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay et al. [New York: Oxford University Press, 2015], 6-15.
[32] Charlie, "Collateral Freedom and the not-so-Great Firewall," GreatFire.org, March 12, 2015, https://en.greatfire.org/blog/2015/mar/collateral-freedom-and-not-so-great-firewall.
[33] Charlie, "We Are Under Attack," GreatFire.org, March 19, 2015, https://en.greatfire.org/blog/2015/mar/we-are-under-attack.
[34] For further discussion see Sarah McKune, "'Foreign Hostile Forces': The Human Rights Dimension of China's Cyber Campaigns," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay et al. [New York: Oxford University Press, 2015], 260-293. See also Wang Chen, "Concerning the Development and Administration of Our Country's Internet," translation by Human Rights in China, *China Rights Forum: "China's Internet": Staking Digital Ground*, no. 2 (2010), http://www.hrichina.org/en/content/3241, at para. III.6 ("We will perfect our system to monitor harmful information on the Internet, and strengthen the blocking of harmful information from outside China, to effectively prevent it from being disseminated in China through the Internet, and to withstand infiltration of the Internet by overseas hostile forces."); Central Committee of the Communist Party of China's General Office, "Communiqué on the Current State of the Ideological Sphere," April 22, 2013, English translation by ChinaFile available at https://www.chinafile.com/document-9-chinafile-translation; Chris Buckley, "China's New Leadership Takes Hard Line in Secret Memo," *New York Times*, August 20, 2013, http://cn.nytimes.com/china/20130820/c20document/dual/.
[35] Shuli Ren, "China Internet: Alibaba, Tencent, Baidu To Continue Buying Spree, R&D," *Barron's Asia*, January 7, 2015, http://blogs.barrons.com/asiastocks/2015/01/07/china-internet-alibaba-tencent-baidu-to-continue-buying-spree-rd/.
[36] Alexa, "Top Sites in China," http://www.alexa.com/topsites/countries/CN (accessed April 8, 2015).
[37] Doug Young, "Investors Burn Out On Baidu Mobile Story," *Forbes Asia*, February 12, 2015, http://www.forbes.com/sites/dougyoung/2015/02/12/investors-burn-out-on-baidu-mobile-story/.
[38] "Baidu Announces Fourth Quarter and Fiscal Year 2014 Results," PR Newswire, February 11, 2015, http://www.prnewswire.com/news-releases/baidu-announces-fourth-quarter-and-fiscal-year-2014-results-

300034622.html.
[39] Baidu, Inc. SEC Form 20-F, FY 2011, http://www.sec.gov/Archives/edgar/data/1329099/000119312512139789/d243699d20f.htm.
[40] Sebastian Anthony, "GitHub battles 'largest DDoS' in site's history, targeted at anti-censorship tools," ArsTechnica, March 30, 2015, http://arstechnica.com/security/2015/03/github-battles-largest-ddos-in-sites-history-targeted-at-anti-censorship-tools/.
[41] Baidu, Inc. SEC Form 20-F, FY 2011 http://www.sec.gov/Archives/edgar/data/1329099/000119312512139789/d243699d20f.htm
[42] Baidu, Inc. SEC Form 20-F, FY 2011 http://www.sec.gov/Archives/edgar/data/1329099/000119312512139789/d243699d20f.htm
[43] State Council of the People's Republic of China, *Report on the Work of the Government (2015)*, delivered by Li Keqiang, Premier of the State Council, to the National People's Congress, March 5, 2015, http://english.gov.cn/archive/publications/2015/03/05/content_281475066179954.htm (emphasis added); see also Simon Sharwood, "China reveals 'Internet Plus' plan to modernise and go cloudy," The Register, March 9, 2015, http://www.theregister.co.uk/2015/03/09/china_reveals_internet_plus_plan_to_modernise_and_go_cloudy/; "When China's tech 'big four' meet 'Internet Plus,'" Xinhua, March 11, 2015, at http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20150311000020&cid=1102.
[44] The sixth point of the declaration was to "vigorously develop the Internet economy. We should improve cyberspace trade rules, step up cross-border e-commerce cooperation, facilitate customs clearance and logistics, expand information consumption, and quicken steps to form a global Internet market." Organizing Committee of the World Internet Conference, *Wuzhen Declaration*, November 21, 2014, available at http://www.scribd.com/doc/247566581/World-Internet-Conference-Draft-Declaration; see also Catherine Shu, "China Tried To Get World Internet Conference Attendees To Ratify This Ridiculous Draft Declaration," TechCrunch, November 20, 2014, http://techcrunch.com/2014/11/20/worldinternetconference-declaration/; Franz-Stefan Gady, "The Wuzhen Summit and Chinese Internet Sovereignty," Huffington Post, December 9, 2014, http://www.huffingtonpost.com/franzstefan-gady/the-wuzhen-summit-and-chi_b_6287040.html.
[45] "Baidu Founder Li and Politburo's Yu Join Top China Advisory Body," Bloomberg, February 4, 2013, http://www.bloomberg.com/news/articles/2013-02-02/baidu-chief-li-politburo-s-yu-join-china-s-top-advisory-body.
[46] Hsu Chang-ping, "Baidu welcomes China's military to join China Brain project on AI systems," WantChinaTimes, March 7, 2015, http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20150307000015&cid=1101.
[47] For further discussion of this framework see Crandall et al., "China Chats: Tracking Surveillance and Censorship in TOM-Skype and Sina UC," in *First Monday* 18, no. 7 (2013), http://firstmonday.org/ojs/index.php/fm/article/view/4628/3727.
[48] See Canada: Immigration and Refugee Board of Canada, *China: The Public Security Bureau (PSB) Golden Shield Project, including implementation and effectiveness; Policenet, including areas of operation; level and effectiveness of information sharing by the authorities (2010-February 2014)*, March 7, 2014, CHN104762.E, available at http://www.refworld.org/docid/543ba3824.html.
[49] See GFW的前世今生，一部GFW之父方滨兴的发家史 ["GFW Past and Present, Family History of the Father of the GFW Fang Binxing"], August 10, 2010, https://fangbinxing.appspot.com/2010/08/10/fangbingxing.html; see also Daniel Anderson, "Splinternet Behind the Great Firewall of China," *ACM Queue*, November 30, 2012, http://queue.acm.org/detail.cfm?id=2405036; Australian Centre on China in the World, "Fang Binxing and the Great Firewall," The China Story, https://www.thechinastory.org/yearbooks/yearbook-2013/chapter-6-chinas-internet-a-civilising-process/fang-binxing-and-the-great-firewall/.
[50] See GFW的前世今生，一部GFW之父方滨兴的发家史 ["GFW Past and Present, Family History of the Father of the GFW Fang Binxing"], August 10, 2010,

https://fangbinxing.appspot.com/2010/08/10/fangbingxing.html ("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。"). An official diagram mapping the relationship between CNCERT/CC, MIIT, and the National Network and Information Security Coordination Team is available in Zhou Yonglin, "Introduction on Chinese Network Emergency Response System & CNCERT/CC's Activities," CNCERT/CC, March 2004, p. 10, at http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016388.pdf.

[51] This entity is also known in English as the State Network and Information Security Coordination Group. Its responsibilities included: "researching and enacting strategy and policy of national information security safeguard[;] organizing and coordinating related departments of government to protect critical information infrastructure[;] mobilizing and directing computer emergency response[;] improving information sharing and notification." Li Jingjing, "Trends and Tactics in Cyber-Terrorism," Information Security Supervision Bureau, Ministry of Public Security, p. 13, at http://www.asean.org/archive/arf/13ARF/2nd-Cyber-Terrorism/Doc-7.PDF.

[52] Jon R. Lindsay, "Introduction--China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay et al. [New York: Oxford University Press, 2015], 8.

[53] Jon R. Lindsay, "Introduction--China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay et al. [New York: Oxford University Press, 2015], 11.

[54] It is important to note that patent applications do not necessarily reflect current capacities or actual deployment of a technology. They do, however, provide insight into the designs, focus, and goals of the filing entities.

[55] "Great Firewall father speaks out," *Global Times*, February 18, 2011, at http://english.sina.com/china/p/2011/0217/360411.html. This article presents the following timeline of Fang's career: "1984-1999 Teaches at Harbin Institute of Technology[;] 1999 Starts work at National Computer Network Emergency Response Technical Team/ Coordination Center of China as deputy chief engineer[;] 2000-2007 Appointed chief engineer and director of the center[;] 2001 Awarded special allowance by the State Council . . . ."

[56] See supra n. 50 and accompanying text.

[57] https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/

[58] http://www.secdev.org/projects/scapy/

[59] Although the GC will respond to a "naked" data packet, this tool first sends a SYN packet and an ACK packet to prevent NATs or conventional firewalls between the user and Baidu from dropping the probe packets. This test also first probes for the GC before probing for the GFW. Once the GFW decides to block two hosts from communicating, for the next minute it injects RSTs in response to any data packet it sees between those two hosts, which would confound the GC measurements somewhat.

[60] "Baidu's traffic hijacked to DDoS GitHub.com [Updated]," Anthr@X, Insight Labs, March 27, 2015 (GitHub.com(http://insight-labs.org/?p=1682); "China's Man-on-the-Side Attack on GitHub," NETRESC AB, March 31, 2015 (http://www.netresec.com/?month=2015-03&page=blog&post=china%27s-man-on-the-side-attack-on-github); "Pin-pointing China's attack against GitHub," Robert Graham, April 1, 2015 (http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html#.VSBOpHXd9hE)

[61] http://insight-labs.org/?p=1682

[62] http://www.netresec.com/?month=2015-03&page=blog&post=china%27s-man-on-the-side-attack-on-github

[63] http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html

APPENDIX A: LINK BETWEEN GREATFIRE.ORG REFERRERS AND BAIDU

This table lists the top 25 referrers seen in our sample of the GreatFire.org server logs, and links each one to Baidu.

Domain	Request Count	Link to Baidu Properties
pos.baidu.com	6,273,809.00	direct Baidu property
tieba.baidu.com	384,173.00	direct Baidu property
zhidao.baidu.com	321,619.00	direct Baidu property
www.dm5.com	207,398.00	does a GET to Baidu image
www.piaotian.net	187,894.00	uses jquery library from Baidu libs
cpro.baidu.com	155,007.00	direct Baidu property
wenku.baidu.com	143,271.00	direct Baidu property
comic.sfacg.com	114,382.00	uses Baidu ads
bbs.miercn.com	111,478.00	uses Baidu analytics
www.7k7k.com	94,994.00	uses Baidustatic.com resources
mangapark.com	94,986.00	uses Baidu analytics
ad.docer.wps.cn	93,881.00	uses Baidustatic.com resources
manhua.dmzj.com	93,622.00	uses Baidustatic.com resources
www.iciba.com	91,626.00	uses Baidu analytics
m.movietube.pw	87,396.00	uses Baidu analytics
pan.baidu.com	84,974.00	direct Baidu property
www.douyutv.com	84,945.00	uses Baidu analytics
www.lwxs520.com	75,964.00	does a GET to Baidu image
www.17k.com	75,514.00	uses Baidu analytics
www.jjwxc.net	71,385.00	uses Baidustatic.com resources
images.sohu.com	67,170.00	uses Baidu analytics
tw.zhsxs.com	65,896.00	uses Baidu analytics
m.yy.com	62,990.00	uses Baidu ads
www.4399.com	60,630.00	uses Baidu ads
www.zhibo8.cc	57,374.00	uses Baidu ads

APPENDIX B: A TOOL FOR TRACEROUTING THE GC AND GFW

We wrote cannon_traceroute.py, a tool that aims to trace the first hop between the user and Baidu at which the GFW and GC are active. As the GC no longer appears to be targeting Baidu traffic, this tool will not detect the GC, but will still detect the GFW. Our tool uses the scapy[58] library to first craft raw packets designed to trigger the GC at each hop,[59] and to then craft fake flows to trigger the GFW at each hop. An example output for a test:

```
> sudo ./cannon_traceroute.py 123.125.65.120
WARNING: No route found for IPv6 destination :: (no default route?)
Sniffer started
.................................................

Great Firewall and Great Cannon traceroute from 192.150.187.17 to 123.125.65.120
Traceroute for the Great Firewall
```

Hop 1: ICMPs: 192.150.187.1
Hop 2: ICMPs: 192.150.187.251
Hop 3: ICMPs: 169.229.0.140
Hop 4: ICMPs: 128.32.0.80
Hop 5: ICMPs: 128.32.0.64
Hop 6: ICMPs: 137.164.50.16
Hop 7: ICMPs: 137.164.22.7
Hop 8: ICMPs: 4.53.16.185
Hop 9: *
Hop 10: ICMPs: 144.232.19.33
Hop 11: ICMPs: 144.232.0.167
Hop 12: ICMPs: 144.232.12.211 144.232.12.213 144.232.9.177
Hop 13: ICMPs: 144.232.25.78 144.232.7.164
Hop 14: ICMPs: 144.232.19.24 144.232.6.104 144.232.6.41 144.232.9.192
Hop 15: ICMPs: 144.228.17.98
Hop 16: ICMPs: 219.158.102.125
Hop 17: ICMPs: 219.158.101.61
Hop 18: Firewall ICMPs: 219.158.101.49
Hop 19: Firewall ICMPs: 124.65.194.54
Hop 20: Firewall ICMPs: 202.106.34.6
Hop 21: Firewall ICMPs: 123.125.128.14

Traceroute for the Great Cannon
Hop 1: ICMPs: 192.150.187.1
Hop 2: ICMPs: 192.150.187.251
Hop 3: ICMPs: 169.229.0.140
Hop 4: ICMPs: 128.32.0.80
Hop 5: ICMPs: 128.32.0.64
Hop 6: ICMPs: 137.164.50.16
Hop 7: ICMPs: 137.164.22.7
Hop 8: ICMPs: 4.53.16.185
Hop 9: ICMPs: 4.69.152.144 4.69.152.16 4.69.152.208 4.69.152.80
Hop 10: ICMPs: 144.232.19.33
Hop 11: ICMPs: 144.232.0.167
Hop 12: ICMPs: 144.232.12.211 144.232.12.213 144.232.9.177
Hop 13: ICMPs: 144.232.25.78 144.232.7.164
Hop 14: ICMPs: 144.232.19.24 144.232.6.104 144.232.6.106 144.232.6.41 144.232.6.43 144.232.9.192
Hop 15: ICMPs: 144.228.17.98
Hop 16: ICMPs: 219.158.102.125
Hop 17: ICMPs: 219.158.101.61
Hop 18: Cannon ICMPs: 219.158.101.49
Hop 19: Cannon ICMPs: 124.65.194.54
Hop 20: Cannon ICMPs: 202.106.34.6
Hop 21: Cannon ICMPs: 123.125.128.14
In this example, the first hop at which the GC and GFW are active is hop 18, between 219.158.101.69 and 219.158.101.49 (a link apparently belonging to China Unicom).

APPENDIX C: SELECTED RELATED TECHNICAL REPORTS

The DDoS attack on GreatFire has been described in a range of technical reports.[60] This section provides a quick chronology and summary of several recent technical posts and discussions. On March 25, the first official report with technical details, written by an anonymous author, was released by Greatfire.org. This analysis was based on logs collected from one of the attacked sites (d19r410x06nzy6.cloudfront.net) that formed part of GreatFire's infrastructure. The report observed strange timestamps in some of the packets in the logs, which it linked to malicious Javascript code sent when some clients loaded resources from Baidu's servers, including dup.baidustatic.com and ecomcbjs.jomodns.com.

As the attack gained visibility, other researchers contributed analysis. On March 27, Anthr@X did the first analysis[61] on the malicious Javascript returned by Baidu, and pointed out that the packets containing the malicious code had different TTLs than the normal, non-malicious Baidu responses. Then, on March 31, NETRESEC[62] provided more details on the malicious packets' TTLs, determining that they varied between 30 and 229. On April 1, Robert Graham published a careful and detailed analysis[63] indicating that the GFW was injecting these packets. His findings match ours regarding localization of the injector; his report did not delve into the fine-grained workings of the injection that reveal the presence of a separate system from the GFW.