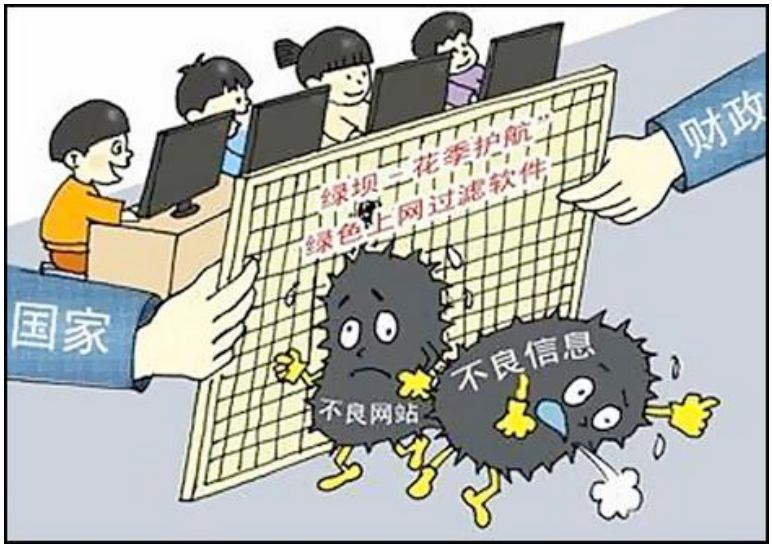
OpenNet Initiative Bulletin

# China's Green Dam

## The Implications of Government Control Encroaching on the Home PC



## Executive Summary

A recent directive by the Chinese government requires the installation of a specific filtering software product, Green Dam, with the publicly stated intent of protecting children from harmful Internet content. The proposed implementation of software as reviewed in this report would in fact have an influence that extends beyond helping parents protect their children from age inappropriate material; the filtering options include blocking of political and religious content normally associated with the Great Firewall of China, China's sophisticated national-level filtering system. If implemented as proposed, the effect would be to increase the reach of Internet censorship to the edges of the network, adding a new and powerful control mechanism to the existing filtering system. As a policy decision, mandating the installation of a specific software product is both unprecedented and poorly conceived. In this specific instance, the mistake is compounded by requiring the use of a substandard software product that interferes with the performance of personal computers in an unpredictable way, killing browsers and applications without warning while opening up users to numerous serious security vulnerabilities. The level of parental control over the software is poor such that this software does not well serve parents that wish to the limit exposure of their children to Internet content. The mandate requiring the installation of a specific product serves no useful purpose apart from extending the reach of government authorities. Given the resulting poor quality of the product, the large negative security and stability effects on the Chinese computing infrastructure and the intense backlash against the product mandate, the mandate may result in less government control.

Robert Faris, Hal Roberts and Stephanie Wang authored this report.

Hal Roberts and Oliver Day carried out the technical analysis with valuable contributions from Max Weinstein, Branden Palmen of the StopBadWare Project and Jonathan Doda and Jamie Liu of the Citizen Lab.

Rebekah Heacock, Lokman Tsui, and Christina Xu provided substantial contributions to the research.

Ronald Deibert, Urs Gasser, John Palfrey, Rafal Rohozinski and Jonathan Zittrain provided key guidance and advice.

### About the OpenNet Initiative

The OpenNet Initiative is a partnership between the Advanced Network Research Group at the University of Cambridge, the Citizen Lab at the Munk Centre for International Studies at the University of Toronto, the Berkman Center for Internet & Society at Harvard Law School, and the Oxford Internet Institute at the University of Oxford. ONI's mission is to identify and document Internet filtering and surveillance, and to promote and inform wider public dialogue about such practices. For more information about ONI, please visit http://opennet.net.

## Key Findings

### Green Dam exerts unprecedented control over users' computing experience

The version of the Green Dam software that we tested, when operating under its default settings, is far more intrusive than any other content control software we have reviewed. Not only does it block access to a wide range of web sites based on keywords and image processing, including porn, gaming, gay content, religious sites and political themes, it actively monitors individual computer behavior, such that a wide range of programs including word processing and email can be suddenly terminated if content algorithm detects inappropriate speech. The program installs components deep into the kernel of the computer operating system in order to enable this application layer monitoring. The operation of the software is highly unpredictable and disrupts computer activity far beyond the blocking of websites.

### The functionality of Green Dam goes far beyond that which is needed to protect children online and subjects users to security risks

The deeply intrusive nature of the software opens up several possibilities for use other than filtering material harmful to minors. With minor changes introduced through the auto-update feature, the architecture could be used for monitoring personal communications and Internet browsing behavior. Log files are currently recorded locally on the machine, including events and keywords that trigger filtering. The auto-update feature can used to change the scope and targeting of filtering without any notification to users.

### The effective level of parental control over the software is poor

Technically, the software may be turned off or uninstalled and the filtering settings adjusted. In practice, a large number of users accept pre-installed software and never change default settings. Moreover, a combination of poor implementation and opaque design makes it very difficult for even expert users to understand what the system is doing by default, let alone understand the impact and scope of auto-updates and configuration changes. These factors severely erode any arguments over parental choice. Moreover, the bundling of filtering to cover many different targets through poorly designed and implemented interfaces leaves parents with inadequate choices in customizing filtering setting to match their personal family preferences.

## Mandating the use of a specific software product is a questionable policy decision

Introducing a product standard by mandating the use of a particular software product made by a specific company for individual use at a national level is unprecedented. We are not aware of any comparable requirement by any country in any context. A product mandate provides a strong measure of central control at the cost of consumer choice, security, and product quality, with implications for personal computer performance. This is a remarkably poor choice for computer users in any country. The effects of this product mandate are magnified by the fact that the product and company in question are reported to have little or no experience in the development, testing, deployment, or support of a very widely used software product.

## Background and Context

On May 19, 2009, the Ministry of Industry and Information Technology (MIIT) in China sent a notification to computer manufacturers of its intention to require all new PCs sold in China after July 1 to have filtering software pre-installed.[1] The notice, jointly issued by the MIIT, the Civilization Office of the Central Communist Party Committee, and the Ministry of Finance, according to the PRC Government Procurement Law, mandates the procurement of all rights and services related to a designated software to be made available for free public use. The software, called "Green Dam Youth Escort," is a product of the Jinhui Computer System Engineering Co., with input from Beijing Dazheng Human Language Technology Academy Co.[2]

The purported intent of the Green Dam software is to filter harmful online text and image content in order to prevent the effects of this information on youth and promote a healthy and harmonious Internet environment.[3]

The Wall Street Journal reported that, similar to anti-virus and operating system software, Green Dam would regularly update PCs with a database of banned sites and block access to those addresses.[4] According to the Wall Street Journal, the founder of Jinhui confirmed that the software can be turned off and uninstalled with a password; blocked sites can be accessed either with a password set by the administrator or by adding addresses to a 'white list' of allowed sites; and URLs can be added to the black list on the user's hard drive.[5]

Jinhui compiles and updates the blacklist of websites, which it says is primarily focused on pornographic sites.[6] While users would have the option to add other content to the blacklist, Jinhui said it had no reason to do so and that its cooperation with a research institute of the Ministry of Public Security on image-recognition technology was limited to pornography.[7] The

---

1 See Rebecca MacKinnon, "Original government document ordering "Green Dam" software installation," June 8, 2009, http://rconversation.blogs.com/rconversation/2009/06/original-government-document-ordering-green-dam-software-installation.html.

2 "Notice Regarding the Pre-Installation of "Green" Online Filtering Software on Computers (关于计算机预装绿色上网过滤染件的通知,*guanyu jisuanji yuzhuang luse shangwang guolu ranjian de tongzhi*)," Ministry of Industry and Information Technology Notice No. 226 [2009], May 19, 2009, http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml.

3 *Ibid.*

4 Loretta Chao, "China Squeezes PC Makers," The Wall Street Journal, June 8, 2009, http://online.wsj.com/article/SB124440211524192081.html.

5 Geoffrey A. Fowler and Ben Worthen, "New China Web-Filtering Rules Still Murky," The Wall Street Journal, June 9, 2009, http://online.wsj.com/article/SB124450534684996071.html.

6 Loretta Chao, "China Squeezes PC Makers," The Wall Street Journal, June 8, 2009, http://online.wsj.com/article/SB124440211524192081.html.

7 *Ibid.*

company also engaged in technical cooperation with the People's Liberation Army's Information Engineering University.[8]

Even if the software were limited to only pornographic sites, it reaches a scope well beyond personal home use of new PCs. According to a press release for the software, the MIIT is working with the Ministry of Education, Ministry of Finance, and the State Council Information Office to require primary and middle schools across the country to have Green Dam installed and functional by the end of May.[9]

However, comments on the now-closed official Green Dam BBS translated by blogger Roland Soong revealed dissatisfaction and frustration among teachers and school administrators over the software's functionality.[10] Users complained about the nuisance of upgrading without network capabilities, the blocking of non-pornographic websites, and the recording of Internet usage data, as well as the inclusion of spyware with the ability to obtain periodic screen captures.[11]

Self-reported usage statistics for Green Dam since end of March 2009:[12]

- made available for download at 95 domestic websites
- downloaded 3.27 million times
- installed at 518,000 computers at approximately 2279 schools
- in use by 6957 websites, at approximately 1.16 million computers[13]
- installed in more than 53 million PC units marketed for home use.[14]

According to MIIT sources, computers being sold in rural China at an average 13 percent discount have already had the software pre-installed.[15] Although companies including Lenovo, Inspur and Hedy have agreed to include the software,[16] Dell, China's third-largest

---

8 *Ibid.*
9 http://www.lssw365.net/lvhang/index.php/Content/index/pid/1/sort/3/id/512.
10 EastSouthWestNorth, "Daily Brief Comments, June 1-10, 2009, No. 017: User Reviews of Green Dam Software," June 9, 2009, http://www.zonaeuropa.com/200906a.brief.htm#017.
11 *Ibid.*
12 http://www.lssw365.net/lvhang/index.php/Content/index/pid/1/sort/3/id/512.
13 This is a literal translation; researchers at the OpenNet Initiative are unsure of the phrase's technical meaning or implications.
14 The 53 million number seems high.
15 "Anti-porn filter software stirs up disputes in China," Xinhua, June 11, 2009, http://news.xinhuanet.com/english/2009-06/11/content_11522822.htm.
16 http://www.lssw365.net/lvhang/index.php/Content/index/pid/1/sort/3/id/512.

vendor of PCs, was still determining whether it would install the software as of June 8.[17] The Notice requires computer manufacturers to report the number of computers shipped with the software for each month in 2009, and then annually for subsequent years.[18] No penalties for non-compliance were detailed in the Notice.

## Green Dam filtering software: a rapid assessment

Researchers at the OpenNet Initiative and StopBadware project collaborated on a rapid, initial assessment of the behavior of the Green Dam software. This initial testing focused on understanding the basic behavior of the system (what does it block, when, and how) rather than the underlying technical implementation, which we and others will explore in depth in future research. A core finding of our initial assessment is that the behavior is in itself complex enough to require significant effort to understand.

Other researches have been working on assessing the functionality and weaknesses of Green Dam. The most comprehensive open evaluation that we have seen was carried out a team of Chinese researchers.[19] This report posted on Wikileaks continues to be updated and covers many aspects of the software, from the core functionality to the image processing software and the programs that are monitored by Green Dam. Another review of Green Dam, quoted in greater length below, carried out by researchers at the University of Michigan highlighted security threats for users of Green Dam such that "any web site the user visits can exploit these problems to take control of the computer."[20]

Green Dam Youth Escort is a Windows client application that blocks content primarily on Internet Explorer (IE) but also on other browsers and even in some cases in user applications like notepad. To perform its blocking, Green Dam inserts hooks deeply into the operating system in both the networking and windowing system. We tested the 3.17

---

17 Owen Fletcher, "China Demands New PCs Have Web Site-blocking Program," IDG News Service, June 8, 2008, http://www.pcworld.com/businesscenter/article/166280/china_demands_new_pcs_have_web_siteblocking_program.html.

18 Section 5, Notice Regarding the Pre-Installation of "Green" Online Filtering Software on Computers (关于计算机预装绿色上网过滤染件的通知, *guanyu jisuanji yuzhuang luse shangwang guolu ranjian de tongzhi*) Ministry of Industry and Information Technology Notice No. 226 [2009], May 19, 2009, http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml.

19 Zhao Huiqin et al. A technical analysis of the Chinese 'Green Dam Youth-Escort' censorship software, https://wikileaks.org/wiki/A_technical_analysis_of_the_Chinese_%27Green_Dam_Youth-Escort%27_censorship_software.

20 Scott Wolchok, Randy Yao, and J. Alex Halderman, "Analysis of the Green Dam Censorware System," Computer Science and Engineering Division, The University of Michigan, Revision 2.4, June 11, 2009, http://www.cse.umich.edu/~jhalderm/pub/gd/.

version of the Green Dam software as downloaded from http://www.lssw365.net/ and installed on a clean version of Windows XP Pro running within VMWare. The Windows XP installation was brought up to date with all Windows updates and configured for Chinese language support.[21]

The Green Dam system is hard to understand (and therefore for users to evaluate and control) because it displays a variety of seemingly inconsistent behaviors depending on a combination of opaque design decisions, updates, and configuration settings. Different versions of the software, updated automatically in the background without user knowledge, significantly change what sites are filtered and how they are filtered. The categories presented in the configuration interface often do not correspond to actual sites blocked. Pages are blocked in a variety of different ways, including blocking the pages from loading, displaying a warning window on top of the page, killing the web browser tabs, killing the whole browser, and even killing other user applications. Sometimes the blocking happens while a page is loading, sometimes before a page loads while typing in a URL, sometimes after a page loads, and sometimes while typing content into another application. Furthermore, how and when content is blocked changes over time, even without updating or configuring the Green Dam application. And in general, simple parts of the application are poorly designed and implemented, increasing user confusion and leading to serious security vulnerabilities.

The following table explains the relationship between a) Green Dam's version and configuration and b) Green Dam's blocking behavior for sites representing various types of content:

| | sex.com | google sex | glaad.org | falundafa.org | freetibet.org | epochtimes.com | notepad falundafa. | notepad epochtimes |
|---|---|---|---|---|---|---|---|---|
| control | S | S | S | S | S | S | S | S |
| 3.17 no filtering | S | S | S | S | S | S | S | S |
| 3.17 category filtering | R | R | R | S | S | S | S | S |
| 3.17 language processing | S | S | S | KL | S | KC | KC | S |
| 3.173 no filtering | S | S | S | S | S | S | S | S |
| 3.173 category filtering | S | S | S | S | S | S | S | S |
| 3.173 language processing | S | S | S | KL | S | KC | KC | S |
| uninstalled | S | S | S | S | S | S | S | S |

The left hand axis of the above table represents the different configurations of the system, the top axis represents the sites loaded (or blocked), and the fields indicate the result of attempting to load each site under each configuration. The system generally exhibits one of five behaviors when loading a site: success (S), network reset (R), browser kill triggered by content (KC), or browser kill triggered by location entry (KL). The configuration of the system depends on three variables: the version of software, the category filtering settings, and the language processing settings. The latest download version of the system at the time we tested it was 3.17, but an update to 3.173 was available by clicking on a manual update

[21] Early testing of the Green Dam software without Windows Chinese language support led to significantly different results than testing with Chinese language support installed.

button in the configuration interface. The configuration interface also has an update period setting that determines how often the application is automatically updated to the latest release (3.173 at the time of this report). The configuration interface also has a screen that has a check box by each of the following filtering categories: pornography, pornography (severe), violent games, illegal drugs, and gay sites. For the purposes of the above table, we either checked all of these category settings or unchecked them all. And the configuration interface also has a screen with a single checkbox labeled "language processing."

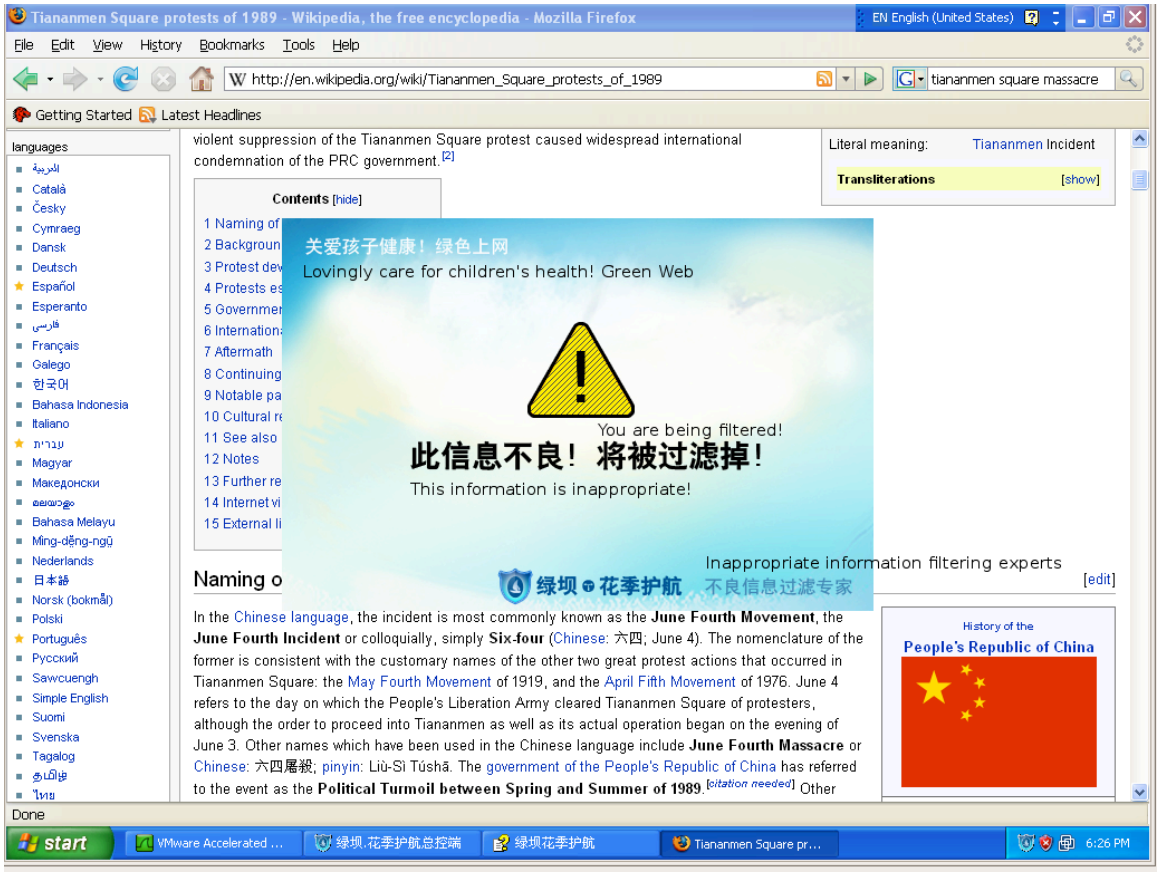
In both the 3.17 and 3.173 versions, turning off category filtering and language processing disables all functionality of the system. We found no evidence of any content blocking, in web browsers or other user applications, while these settings were turned off. Both versions offer an uninstall option that has the same effect of disabling all blocking behavior by the system and also stopping any of the supporting processes from running. By default, both versions of the software are configured with all category filtering and language processing turned on.

In the 3.17 version, category blocking turns on the filtering of pornography and gay sites through connection resets triggered by keywords. We tested several popular English language shooter computer gaming sites and could find no filtered sites, even with those categories turned on. We found several examples of illicit drug-related sites that are blocked with the associated category turned on. We also found no examples of sites blocked by the pornography (severe) category, though it is possible that that category is used for blocking child pornography sites, which we did not test. Turning on the pornography (severe) category and turning off the pornography category causes the application not to block any of the pornography sites we tested, including several popular hardcore pornography sites. We know that the system uses keyword blocking for these sites because it does not use either IP blocking (requests to the same IP with different content are not blocked) or DNS blocking (network traces show DNS requests are not blocked). We know from monitoring network traffic using a packet sniffer that the system is using TCP resets to kill the connections.[22]

In the 3.17 version, language processing turns on blocking for political and religious content by killing browser tabs and applications and even other user applications like notepad. In some cases, including falundafa.org in our tests above, the kill action is triggered by entering a particular URL into the location bar or window of the browser. When such a URL is entered into the location bar at the top of IE, Green Dam displays the following warning over the browser for less than a second before killing the whole browser application

[22] A TCP reset is a special message sent within a network connection that tells the client to drop the entire connection immediately, thereby aborting the current request.

(including not just the particular window but every window and every tab currently open in the browsing session):[23]




When such a URL is a entered into the location window (the window displayed when a user chooses File -> Open in IE), Green Dam sometimes kills just the active tab and sometimes kills every single tab open in every single IE window. IE tries to reload all tabs killed this way with the previous content for each tab (unlike with the browser kill action, which makes the browser go away altogether until restarted by the user). The language processing also triggers application kills for a small range of user applications, including Notepad and Wordpad.[24] When language processing is on and a user enters one of the URLs that triggers location bar kill actions by default ('falundafa.org' but not 'epochtimes.com'), Green Dam will kill any of these applications either immediately or a few seconds after the user types in the offending keyword.

---

23 The English translations of the blockpage have been added by the authors. There is no English text in the actual blockpage.

24 For a list of applications that are monitored by Green Dam, see Zhao Huiqin et al. "A technical analysis of the Chinese 'Green Dam Youth-Escort' censorship software," https://wikileaks.org/wiki/A_technical_analysis_of_the_Chinese_%27Green_Dam_Youth-Escort%27_censorship_software.

For other URLs, including epochtimes.com in our tests above, the language processing is triggered by the content on the page itself. In these cases, the user can see some or all of the page load briefly before seeing the warning screen flash on the screen followed by the whole browser dying as described above. In all of these cases, whether the URL or the content causes the language processing feature to kill the browser tab or window, the language processing feature will thereafter always kill the browser when the user enters that URL into the location bar or window. So the first time the user loads epochtimes.com, Green Dam will kill the browser window after displaying the content briefly. If the user tries to enter epochtimes.com into the location bar again, the system will kill the browser immediately without loading the page.

All URLs that are killed within the location bar are also killed whenever they appear in the auto-complete list of the location box. This is an extremely buggy and intrusive method of killing sites because it extends the kill action to single letters that auto-complete to kill blocked sites. For example, if a user enters epochtimes.com into the location, the user will see the page briefly, see the warning box briefly, and then have the whole browser killed. But after the user restarts the browser, epochtimes.com will be in the browser history and therefore in the auto-complete list. So depending on the other URLs in the auto-complete list, the user may only have to type 'e' into the location box to trigger the appearance of epochtimes.com in the auto-complete list and therefore cause Green Dam to kill the whole browser. The end effect of this is that Green Dam can effectively ban, through the extremely intrusive kill action, all URLs beginning with a given letter ('e' for 'epochtimes.com', 'f' for 'falundafa.org', etc). There are several other methods for causing kill-blocked sites to enter the browser history and therefore trigger these extremely intrusive auto-complete kills; for instance, the user can enter www.falundafa.org instead of falundafa.org into the location bar to get the same behavior as with epochtimes.com. This behavior can be reset by deleting the browser history, and therefore removing the offending sites from the auto-complete list. But it is highly unlikely that most users will make the connection between entering a specific single letter into the location bar and a particular site visited, perhaps long ago and perhaps not even by the same user.

We updated the test system with the latest version of Green Dam by clicking on a manual update button on the update configuration screen. That same screen also has a setting for how often the Green Day software will automatically update itself. This auto-updating feature raises the possibility that the functionality of the software will change significantly in the future without user participation or even knowledge. The biggest change in the 3.173 version of the software is that all filtering categories other than pornography (severe) have been removed from the configuration screen and, according to our testing, from the filtering altogether. None of the first page Google results for 'sex' or 'gay' were blocked by the 3.173 version of the software, even with the single, pornography (severe) category turned on. The language processing feature remains largely the same in the 3.173, with the only detected change being that www.falundafa.org was added to the default list of location bar kill URLs

(though typing www.falundafa.org into the location window still brings the falundafa.org site up and then causes the auto-complete kill problem for 'f').

The result of these changes in the 3.173 version is that this version of the software is only useful as a tool for blocking political and religious content, not pornography. This is likely a mistake.

In addition to these filtering features, Green Dam has a logging system that stores a record of every site visited, every site blocked, and why each blocked site was blocked. We have seen no evidence that this file is being sent back to a central server or anywhere outside of the client computer. Still, the log file does not obey the browser privacy controls, leaving a trail of a user's browsing history even after the user has tried to delete the trail for the browser. This is of course a desired feature for many parents who want to monitor their children's Internet usage, but the log is on by default for all users on the computer and can only be disabled by uninstalling the Green Dam software altogether.

In general, the software has a number of other problems that result from poor design and implementation. The language, especially describing the language processing function, does not make at all clear the kinds of content the option blocks or the extremely intrusive kill methods used to block the content. The update mechanism itself, leaving alone questions of centralized control of the software, is unreliable – it failed to update for about half of the three days in which we tested the software, under an order of magnitude less load than it would see were the software installed on every computer in China. The system has whitelist and blacklist functionality in its configuration interface, but we were unable to get either to work (whitelisted sites remained blocked, and blacklisted sites remained unblocked). The system claims to do sophisticated image processing to detect pornography images, but after browsing many pornography sites, the only picture we saw blocked was a photograph of a face in a news article.

Interestingly, the Green Dam software is identified as malware by anti-virus software from the largest free anti-virus company in China (www.360.cn).[25] The StopBadware Project at the Berkman Center confirmed that the application violates its Badware guidelines for software, as it does not disclose the filtering of political speech or the unexpected behavior of completely killing processes that contain such speech.

Most critically, researchers at the University of Michigan have already found serious security problems with the software:

> We examined the Green Dam software and found that it contains serious security vulnerabilities due to programming errors. Once Green Dam is installed, any web site the user visits can exploit these problems to take control of the computer. This could

[25] See http://www.fec.com.cn/hzhb/u_whlyty/content.php3?id=2633.

allow malicious sites to steal private data, send spam, or enlist the computer in a botnet. In addition, we found vulnerabilities in the way Green Dam processes blacklist updates that could allow the software makers or others to install malicious code during the update process.

We found these problems with less than 12 hours of testing, and we believe they may be only the tip of the iceberg. Green Dam makes frequent use of unsafe and outdated programming practices that likely introduce numerous other vulnerabilities. Correcting these problems will require extensive changes to the software and careful retesting. In the meantime, we recommend that users protect themselves by uninstalling Green Dam immediately.[26]

The ramifications of these vulnerabilities are difficult to overstate. The mandate by the MIIT ensures an enormous pool of victims for any attacker smart enough to either lure Chinese web surfers to a web site or infiltrate the server storing the update files. The prevalence of "drive by downloads" makes for an easy mechanism to populate thousands of websites with code that could turn every Chinese computer running Green Dam into a member of a botnet.

If an attacker were able to compromise the web server hosting the update code, then every computer that phoned home could also be infected. Major software vendors like Apple or Microsoft use cryptographically signed code to ensure that only approved software is sent to clients requesting an update. Green Dam does not use any visible safeguards to ensure the safety of their users during the critical update process.

## Internet content regulation in China

China maintains one of the most extensive and technologically sophisticated filtering systems in the world. The 'great firewall of China' uses a variety of overlapping techniques for blocking content containing a wide range of material considered politically or socially sensitive by the Chinese government. While China employs filtering techniques used by many other countries, including DNS (domain name system) tampering and IP (internet protocol) blocking,[27] it is unique in the world for its system of breaking Internet connections when triggered by a list of banned keywords. Known as a TCP reset, this filtering strategy

---

[26] Scott Wolchok, Randy Yao, and J. Alex Halderman, "Analysis of the Green Dam Censorware System," http://www.cse.umich.edu/~jhalderm/pub/gd/.

[27] For more details on these filtering techniques, see Steven J. Murdoch and Ross Anderson, "Tools and Technology of Internet Filtering," *Access Denied*, (Cambridge: MIT Press, 2008). See also the OpenNet Initiative, "About Filtering," http://opennet.net/about-filtering.

operates by forging legitimate reset signals in order to implement a keyword filtering scheme at a large scale.[28]

TCP reset filtering is based on inspecting the content of IP packets for keywords that would trigger blocking, either in the header or the content of the message. When a router in the Great Firewall identifies a bad keyword, it sends reset packets to both the source and destination IP addresses in the packet, breaking the connection. Users anywhere in the globe can experience this by searching for 'falun' or other sensitive words at Baidu.com or other search engines hosted in China.

Technical filtering associated with the so-called Great Firewall of China is only one of several tools for controlling Internet content that are applied in China. For example, to manage the explosion of the Chinese blogosphere,[29] blog service providers must not only install filters that prevent the posting of potentially thousands of keyword combinations, but also flag certain posts for review. Comment sections, forums, and other interactive features that pose a higher risk of containing sensitive content can be shut off, while posts can be deleted or concealed by the provider so that only the author can see them.[30] Bloggers who are considered to have written too many troublesome posts can have their accounts cancelled at will.

At the same time, because these compulsory control mechanisms are actually implemented through informal processes, provider-based content control is neither narrow nor entirely predictable. A study of Chinese blog service providers demonstrated that there is substantial variation in censorship methods, the amount of content censored, and providers' transparency about deleting or de-publishing content.[31] Similar findings were reached in a Citizen Lab study of four popular search engines in China, which found significant variations in the level of transparency about filtering, actual content censored, and methods used, suggesting that there is not a comprehensive system for determining censored content.[32] While Google and Microsoft, which are hosted outside China, actually de-listed certain search results, the two search engines hosted inside China, Yahoo! and Baidu, ran their Web

---

28 Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson, "Ignoring the Great Firewall of China," University of Cambridge, www.cl.cam.ac.uk/~rnc1/ignoring.pdf.

29 One estimate puts the number of bloggers in China as high as 162 million at the end of 2008. China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China," issued March 23, 2009, p. 38, http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf.

30 *See* Stephanie Wang and Robert Faris, "Welcome to the Machine," Index On Censorship, (Volume 37, Issue 2 May 2008), pages 106 – 113.

31 Rebecca MacKinnon, "China's Censorship 2.0: How companies censor bloggers" First Monday [Online], Volume 14 Number 2 (25 January 2009), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

32 Nart Villeneuve, Search Monitor Project: Toward a Measure of Transparency, 2008, http://www.citizenlab.org/papers/searchmonitor.pdf.

crawlers behind the China's filtering system, and therefore did not index Web sites already blocked by the Chinese government.

Although Google censored considerably less that the other search engines, it also has a practice of prioritizing authorized local content, which researcher Nart Villeneuve found amplified the significance of the censored Web sites as they were the only ones to offer differing viewpoints.[33] Indeed, the complexity of these informal control mechanisms was further revealed in April 2009, when an employee of China's leading search engine, Baidu.com, leaked a folder containing the substance and flow of internal censorship.[34] These included lists of topics, keywords, and URLs to be blocked, lists of banned forums, employee guidelines for monitoring work, censorship guidelines for the popular Baidu post bars, and guidelines of how to search for information that needed to be banned.[35]

The Chinese government's legal control over Internet expression and content is also multilayered and achieved by distributing criminal and financial liability, licensing and registration requirements, and self-monitoring instructions to non-state actors at every stage of access, from the ISP to the content provider and the end user. Some of these blunt and frequently applied methods include job dismissals; the closure of Web sites, often by their Web hosting service, for a broad array of infractions;[36] and the detention of journalists, writers, and activists. All Internet services that fail sufficiently to monitor their Web sites and report violations face fines and other serious consequences, including shutdown, criminal liability, and license revocation.[37] The government has used this approach to bring social media outlets such as video sharing sites in line with the larger governing framework for Internet content regulation. Green Dam, designed for use at the household and institutional level, adds another layer of control and complexity to an elaborate and well-developed content regulatory system in China.

---

33 Nart Villeneuve, Search Monitor Project: Toward a Measure of Transparency, 2008, p. 19, http://www.citizenlab.org/papers/searchmonitor.pdf.

34 "Baidu's Internal Monitoring and Censorship Document Leaked (1) (Updated)," China Digital Times, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/.

35 See, e.g., http://chinagfw.org/2009/04/blog-post_5218.html.

36 China Human Rights Defenders, Tug of War over China's Cyberspace: A Sequel to Journey to the Heart of Censorship (Part II), March 19, 2009, http://crd-net.org/Article/Class9/Class11/200903/20090319000543_14370.html.

37 Article 20, Measures for Managing Internet Information Services (*Hulianwang xinxi fuwu guanli banfa),* issued by the State Council on September 25, 2000, effective October 1, 2000.

## International points of comparison

China is not alone in seeking technological filtering solutions aimed at protecting its children from material on the Internet that is perceived to be harmful to minors and, in doing so, reaching down to the institutional and household level for the application of regulatory mechanisms. The United States and Australia are two apt points of comparison. Legislation in the United States links federal funding for schools and libraries to the installation of filtering software that blocks access to content harmful to minors.[38] Although controversial, this regulatory approach has survived legal challenges in the US courts. This approach places considerable discretion in the hands of local librarians and school administrators, who can disable the filters for adults and may choose to alter the blocking configurations offered in the software. Unlike the current Chinese model to promote the use of Green Dam, there are several competing filtering products that can be used to fulfill this mandate.

At the household level in the US, filtering is entirely voluntary, again with a number of software products vying for this household filtering market.[39] Filtering software at the household level has played an indirect role in national-level filtering policy. The US courts, in rulings that broad-scale mandatory filtering in US is unconstitutional, have referenced the effectiveness of household-based filtering mechanisms as comparable to more centralized solutions in terms of level of protection for children but with a lower burden on constitutionally protected free speech.

Australia invested considerable resources in developing software that could be implemented by households across the nation to filter content harmful to minors. The adoption rates for this software for its proponents have been woefully low (only 137,000 copies of the filter were downloaded or requested on CD; Australia has over 6 million Internet subscribers. These figures do not indicate how many of the downloads have been installed and continue in use.).[40] Soon after its release, a teenager described online a way to disable the

---

38 United States Cong. Senate, 106th Congress, 2nd Session, "HR 4577: An act making appropriations for the Departments of Labor, Health and Human Services, and Education, and related agencies for the fiscal year ending September 30, 2001, and for other purposes," June 15, 2000, http://w2.eff.org/Censorship/Internet_censorship_bills/2000/hr4577_censorware_20000615_excerpts.html. See also Gwendolyn Mariana, "Net-porn law applies deadline pressure," ZDNet Asia, October 29, 2001, http://www.zdnetasia.com/news/hardware/0,39042972,38028681,00.htm.

39 In 2007, 53% of families in the United States with teenagers used filters (Pew, Internet & American Life Project, "Teens, Privacy & Online Social Networks," April 18, 2007, http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.pdf.

40 Fran Foo, "Net censorship to cost users," Australian IT, August 5, 2008, http://www.australianit.news.com.au/story/0,,24128728-15306,00.html.

software.[41] The failure of this voluntary household-based filtering strategy undoubtedly informed the much debated plans in Australia for developing a mandatory filtering policy, which was intended to be implemented by ISPs.[42] The original plan was to introduce an opt-out system, whereby the default choice for users would be a filtered connection unless they explicitly requested an open unfiltered connection. Although a trial is currently underway, recent signals suggest that the government will be backing away from the opt-out design, instead reverting to a less restrictive opt-in regime.[43]

Technology companies also play an important role in controlling online content. Internet applications also act to shield consumers from offensive or sensitive materials. Search engines such as Google and Yahoo include safe search options. Blogging hosts and social media, including YouTube among others, include terms of service restrictions that limit the type of content that users can post on these sites, relying heavily on user feedback reports to identify infringing content.

Many other countries around the world are adopting various strategies for addressing concerns over child safety online that combine to different degrees legal restrictions, voluntary programs in conjunction with technology companies and options for controls at the household level.

## Green Dam: a shift in filtering strategy and capability for China?

Compared to China's existing filtering apparatus, the addition of this system marks a substantially different approach to filtering, moving the implementation of filtering to institutions and end-users on the periphery. One of the principle problems with large-scale filtering strategies that rely on intervention through a small number of points of control is the cost of implementation, both in technological infrastructure and a reduction in connectivity speeds. Intensive monitoring of content can not take place through a centralized system without either tremendous investments in processing facilities or at the cost of dramatically reduced Internet speed. Distributing the control mechanisms through client-side software offloads the burden of sorting through content to the individual machines on the network. In essence, such a system amounts to a huge distributed super computer dedicated to controlling online content. This allows a much more intrusive and comprehensive filtering

---

41 Jo Best, "Teen cracks AU$84 million porn filter in 30 minutes," ZDNet Australia, August 27, 2007, http://www.zdnet.com.au/news/security/soa/Teen-cracks-AU-84-million-porn-filter-in-30-minutes/0,130061744,339281500,00.htm.

42 "Australia to implement mandatory internet censorship," Herald Sun, October 29, 2008, http://www.news.com.au/heraldsun/story/0,21985,24568137-2862,00.html.

43 Brett Winterford Ben Grubb, "Conroy to opt for tiered Internet filtering," IT News, June 2, 2009, http://www.itnews.com.au/News/104642,conroy-to-opt-for-tiered-internet-filtering.aspx.

system than the more centralized ISP-level filtering schemes, including dynamic content analysis and image processing. However, leveraging the technological potential of client-side control requires either government control over personal computers or the voluntary participation of computer administrators and users.

## Blurring the lines between parental and government controls

The Australian and US experiences with content control highlight the philosophical and architectural differences between filtering strategies that place control in the hands of government versus households. Household control of filtering mechanisms implies that participation is entirely voluntary, that there is adequate control over the scope and targeting of filtering, that content control options are easily understandable and transparent, and that controls can be easily implemented with software that is configurable by users. At the opposite end of the spectrum, government controls are mandatory and leave no discretionary control in the hands of users. Online content control strategies may fall somewhere between these two extremes of pure household and government control.

In the case of Green Dam, the setting of defaults will have a substantial influence on user decisions. If the software comes loaded on all new computers, that software will remain there for a large number of users. Even though the software we reviewed allows users to uninstall it, many users will leave it there unaltered on the computers merely because that is the default. The process of removing the software does appear to be fairly straightforward but requires users to put in the effort to do so.

Whether the intention of the mandate is to require the software to come pre-installed on all computers sold in China is still unclear.[44] One reading of the notification implies that pre-installation would be required on all new PCs sold in China after July 1, 2009. A different interpretation would allow manufacturers to send the installation software on a CD with the new computer, effectively allowing consumers the option to install the software or not. This will have a large influence on the adoption and continued use of the software in China.

Green Dam is designed to allow limited customization such that users can increase or decrease the level of filtering by choosing different categories of blocking, by adding sites to the blacklist, or by unblocking sites by adding them to a white list. Again, the default settings are critically important. The default options in the software we reviewed included the highest level of filtering, including not only pornography but also political content and the most intrusive methods of blocking, which kills applications on the computer. These default

---

[44] "关于计算机预装绿色上网过滤软件的通知 (Notification Regarding Requirements for Pre-installing Green Filtering Software on Computers)," translated by Human Rights in China, June 8, 2009, http://www.hrichina.org/public/contents/press?revision_id=169834&item_id=169820.

options would then likely remain the choice of many users, because defaults tend to be sticky and the design of the software makes the relationship between configuration settings and application behavior unclear.

The influence of those that design and maintain this software is not limited to the defaults that are included in the software download package. The automatic update function can be used to remotely alter the filtering profile that guides the software, adding more topics, web sites and keywords that trigger blocking. The automatic update functionality could conceivably be used to reduce filtering as well. In theory, users also are able to adjust the way in which they configure the software to compensate for any changes in the scale and scope of the updated filtering instructions. In practice, this is highly impractical, even if users are given a detailed reporting of changes in the blocking lists and algorithms, which is also highly unlikely; the lists of keywords that guide the filtering process are contained in an encoded file. Although Green Dam technically offers parents considerable control over whether and how it is implemented, the practical level of control is small.[45] The most significant choices are whether the software is installed in the first place and the default settings that accompany the installation.

## Privacy, Surveillance and Security

The potential for using this software to track browsing habits and communications of users is high. We have not been able to confirm that personal information is being gathered centrally. It is not hard to image that a similar system could be implemented that behaves as the Tom-Skype platform, where logs were recorded on a server when certain keywords were used.[46] The possibility of personal information leaking could also be quite high as well.[47] The powerful central coordination mechanism is also accompanied by a higher vulnerability to security breaches and malicious activity. Several vulnerabilities have already been documented.

---

45 This behavioral constraint over practical user control is not limited to Green Dam. This is true for all software in which the tradeoffs between convenience and complexity reduce the practical involvement of users in fine-tuning software settings to match their own preferences. The vast number of potentially sensitive web pages makes it practically infeasible for users to choose what they wish to have blocked, except by the categories that are offered by software producers.

46 Nart Villeneuve, "Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform," Information Warfare Monitor and ONI Asia, October 1, 2008, http://www.nartv.org/mirror/breachingtrust.pdf.

47 In exploring the company website, we found unprotected files that contained user information.

## The potential perils of a software monopoly

The potential power of a single provider of filtering software and software updates is tremendous, particularly for software that can be updated automatically. Moreover, the influence of the government with Green Dam is apt to be very high given that the company has been granted a monopoly position by the government, a privileged position that could just as easily be taken away. In a different context, producers of filtering software that are competing for business are more likely to offer choices that are attractive to users and to be responsive to the needs of consumers. A government mandated monopoly has little incentive to provide user-friendly top quality software.

Furthermore, some Chinese citizens are questioning the 40 million RMB spent by the government to secure a year-long contract with Jinhui, saying that if users uninstall the software, the expense is a waste of taxpayers' money.[48] One Beijing-based lawyer is challenging the policy's legality based on an October 2008 Chinese legislative notice that requests government agencies to "hold hearings for items subject to examination and approval which concern the major public interests or the vital interests of the people" (the MIIT announced the Green Dam policy without holding a hearing).[49] Internet users are also questioning the policy based on the government's possible violation of China's anti-monopoly law or its law against unfair competition.[50]

For controlling Internet content, the benefits to the government of a centralized single provider solution are clear. This precludes the most effective elements in promoting innovation and quality assurance—user feedback, competition and market mechanisms—making this a highly questionable choice for promoting the development of effective, high-quality filtering software in China. If the ultimate goal is protecting children, then this is a dubious policy decision. Indeed, we think that, given the myriad problems we and others have unearthed with the tool, China will have to pull back from requiring installation of this tool in its current state.

---

48 "Anti-porn filter software stirs up disputes in China," Xinhua, June 11, 2009, http://news.xinhuanet.com/english/2009-06/11/content_11522822.htm.

49 Human Rights in China, "Chinese lawyer challenges filtering software order and requests public hearing," June 11, 2009, http://www.hrichina.org/public/contents/press?revision_id=169854&item_id=169851. The full text of the legislative notice is available at http://www.canyu.com/ (Chinese).

50 Rebecca MacKinnon, "'All new computers are required to wear condoms....,'" RConversation, June 11, 2009, http://rconversation.blogs.com/rconversation/2009/06/all-new-computers-are-required-to-wear-condoms.html. For the full text of these laws, see http://www.china.org.cn/government/laws/2009-02/10/content_17254169.htm (English) and http://www.gdgs.gov.cn/cyfg/FBZDJZf.htm (Chinese).

## Conclusions

A rapid review of the filtering software required for new computers in China corroborates the conclusions of other researchers: Green Dam is deeply flawed, poses critical security concerns for users and has a detrimental impact on normal computer activities. The confusing interfaces and unpredictable functionality erode any pretense of parental control over the Internet browsing habits of their children and significantly reduce the control of all Green Dam users over their computers.

We find the Green Dam product mandate to be dangerous both as a model of centralized client control and in the implementation of the model through this specific product mandate. Even if this software were a better implemented product, we find the overall policy model to be poorly conceived. Requiring equipment manufacturers to install a specific software product is at odds with the development, improvement and maintenance of quality software. Furthermore, the filtering behavior that we observed strays into the blocking of political and religious topics, suggesting that those maintaining the blocklists are interested in more than protecting children from material specifically damaging to children. If this in fact turns out to be a means to extend the influence of the Great Firewall of China, it represents a new approach to large-scale censorship that leverages far more computing power than any centralized filtering system. This would be consistent with a trend seen by ONI researchers in other countries of moving the implementation of filtering out towards the edges of networks, for example, employing filters in cybercafés and educational institutions. The implication of moving filtering to individual computers is that it allows computationally-intensive dynamic analysis of Internet content, or in the case of Green Dam, any content created on a personal computer, facilitating a much more intrusive mechanism for filtering and surveillance than could be achieved otherwise.

There is broad support around the world for policies that help parents to limit the exposure of their children to harmful materials online. This support varies widely, however, in relation to the share of responsibility and choice between governments, technology companies and parents. Many favor leaving control solely in the hands of parents, while others support government policies that mandate large-scale filtering. This legitimate debate has been superseded in China by a government mandate for new computers to be shipped with filtering software that is overly broad and excessively intrusive. Requiring the installation of a specific product provides no apparent benefits for protecting children, suggesting that it might be intended to extend the regulatory reach of government authorities into personal computers.