Remarks presented before the Congressional-Executive Commission on China
by Greg Walton[1]

长城, 小世界

Great Wall, Small World[2]
CECC Open Forum, Monday, March 10, 2003

Washington D.C. Good afternoon. Thank you to the CECC Staff for organizing this forum. I have followed the proceedings of the Commission since its inception, and note with interest the real progress being made with regards to understanding human rights, the rule of law, and the internet in China.[3]

My name is Greg Walton. I am an independent research consultant focused on the impact of the internet on human rights and democratic development – particularly in Asia. [I will reference the URL of my eJournal for supporting documentation and further written testimony I wish to submit for the record.][4]

I have no affiliation to any organization. However, I have working relationships with a number of international human rights NGOs, and other groups and individuals, engaged in advancing human rights in China – particularly in the digital sphere - through internet activism or "hacktivism". By "hacktivism"[5] I mean specifically the adoption and extension of universal human rights principles and mechanisms to the needs of an information-based society[6] – "including where this runs counter to the preferences of authoritarian regimes".[7]

Information Society increasingly employs advanced information and communication technologies in daily life. These technologies are - more often than not - derived from hi-tech military research programs. Sophisticated networks which were originally designed to track the movements of troops on the battlefield, for example , are increasingly part of the modern surveillance arsenal. Such systems have been described as the "central nervous system of the repressive regime that connects the brain to the boot."[8]

My own preliminary research suggests that the application of such so-called "neutral", dual-use technology is a double-edged sword. It can easily be abused in the hands of totalitarian governments, --in fact, in the absence of democratic accountability, nationwide database-driven surveillance systems – for example - *will* be used against the interests of the general public in a systematically destructive way[9]: it's a path that gradually but inevitably suffocates civil society.

Now, more than ever, it is critical for technologists to act responsibly: one suggewithin a trust model inspired by the Hippocratic Oath -- "Above all, do no harm" [10]

The fundamental question that should be asked is, "does this technology expand the democratic experience, or does it cause irreparable damage"? It is a given that any technology can be abused by the enemy's of democracy. But, going by the averages, does the technology do more good than harm?

This afternoon, I would like to present a snapshot of my inbox last week and examine how the development of two parallel internet routing technologies underscores the importance of these questions in everyday China.

Developed in the labs of a cutting-edge hi-tech corporation, the first set of routers are governed by code that restricts – closing down the free flow of information, and deployed right across national networks hard wired for centralized control.

The other network of routers, a shared resource developed around an open source protocol, opens up secure, decentralised channels of communication – connecting people in a secure, private, trust-based environment.

A respected industry consultant in Beijing characterized the current end-user impact of the "closed" routers as being as if all China's online population were "breathing through the same tiny air hole"[11]

In obvious contrast, the open network of routers seeks to expand the global democratic sphere through "peer-to-peer technology that makes it possible to carry out almost any internet activity securely and—more importantly, for all sorts of reasons—anonymously."

There is little time for extended analysis so I hope to allow the facts speak for themselves.

So in our first story[12] AP reports that China's internet users are "suffering sharp slowdowns in access, which industry experts blame in part on heightened efforts by the communist government to police online content. " The BBC reports that "these problems have worsened as Security operations in China have been stepped up as the annual National People's Congress continues in Beijing"[13]

The Commission's staff will be aware that these problems emerged in October after "packet-sniffer" software was integrated into key routers on China's internet backbone – this was following the redirecting of Google's domain name.[14]

It was also noted at the time that Chinese authorities were systematically hi-jacking the domain names of thousands of websites – including some belonging to the U.S. government, human rights organizations, and other civil society organizations. [15] Banned topics include human rights and the outlawed Falun Gong spiritual group.[16] The result is a huge - quite intentional - bottleneck, and a much slower service, especially at "sensitive" times. This was at the same time that ICANN – the body that governs the global Domain Name System (DNS) - was meeting in Shanghai.[17]

I would like to draw the commissions attention to forthcoming research by Dynamic Internet Technology Inc.[18] I would like to highlight their growing understanding of how this system is working today, and why it leads to sharp slowdowns during "sensitive" periods.

The main body of the DIT Inc research – part of a series of in-depth briefings that I believe will be released over the coming months, provides explanation of the routing mechanism, exhaustively explores the keyword list that triggers the domain name hijacking system.

The second story – that is the other set of internet routers I'd like to touch on today comes from an eWEEK Labs review in which the magazine evaluated a beta version of the developers edition of the Six/Four System[Hacktivismo], which became available last week[19] under the Hacktivismo Enhanced-Source Software License Agreement[20] [HESSLA].

The Six/Four System is eWeek reviewers found that "Hacktivismo hasn't quite achieved its goals. The peer-to-peer network, which relies on many node clients with some trusted peers that handle routing, is understandably very small right now. Also, the Six/Four System's capabilities are very raw."

This is a fair analysis: It should be noted that this version of Six/Four is a developer release. My understanding is that, once an intuitive application interface has been developed and localized– and once a significant user base has been installed in the liberal democracies – I anticipate the tool will be widely distributed in China. My prediction/hope is that Peer2Peer computing - Six/Four and systems like it[21] - will render state sponsored censorship ultimately impossible.

I understand that a number of the CECC Commissioners and Staff are tech-savvy and will submit further details of the Six/Four system for the record.[22] The Commission will note among the feature set, what the U.S. government classifies as munitions-grade encryption.[23]

So which of these technologies expands the democratic process – which constricts? Which of these technologies does more good than harm? To human rights – to civil society – to business?

The HESSLA licence agreement says that anyone using the code released under it must respect digital human rights: that is to say, software distributed under Hacktivismo "enhanced source" licence will be legally prohibited from censoring or spying on users. The Hacktivismo legal team was very careful to define that anyone using code released under it must respect privacy, free expression, due process and other human rights. [24]

In contrast DIT's research is examining in some considerable detail how Chinese authorities redirect or "hijack" proscribed domain names. I think – that for the first time – and this is what is really remarkable about this research – DIT are evolving a robust and reproducible methodology, accurate across provinces and ISPs. I believe part of the motivation in publishing the in depth briefs is in the hope that other researchers can further their own studies in the implementation of China's internet censorship and surveillance system.

In brief, as DIT researchers explore Chinese networks they are finding that the domain name hijacking is implemented systematically on a nationwide basis and regardless of ISP. They found there is a key word list – and yes -- it does change from time to time – the more "sensitive" that day is in the Communist calendar– the longer the word list – the slower the connection. The system seems adaptive – maybe it is even "learning".

What intrigues me, is that a handful of routers sited very close to the international gateways are "sniffing" millions of dns requests each second. Based upon CNNIC bandwidth surveys these devices are processing a certain amount of traffic. They must be fairly sophisticated[25]. One can't but help wonder about the provenance of this technology. If it was designed by a western corporation it seems ironic that not only does this one sale effect millions of individuals rights – it also impacts international business productivity.[26] Perhaps "people don't realize we're exporting censorship."[27]

Understanding the impact of surveillance networks on China means recognising a society often in the grips of a shadowy security apparatus - a truly Kafkaesque legal system without any apparent logic or Rule of Law; an economy without transparency – whole sectors rife with corruption. The context of China is a state without democratic accountability. Exporting dual-use technology to China is about placing technology in that political context: a profoundly anti-democratic context.

I would ask that the Commission further investigate the reality of internet censorship and digital surveillance in China and then apply appropriate pressure to all levels of the Chinese government.

This is particularly the case with regards the growing number of Internet prisoners that Amnesty International[28] has recently noted constitute a new class of prisoner of conscience – for a new form of crime.[29]

The Chinese authorities must release all those currently detained or jailed for using the internet to peacefully express their views or share information:

"Everyone detained purely for peacefully publishing their views or other information on the internet or for accessing certain websites are prisoners of conscience, They should be released immediately and unconditionally".[30]

I hope the Commission particularly to regularly re-examine the role of U.S. corporations engaged in exporting equipment that enables censorship and surveillance infrastructure in China.

Finally I would urge the Commission to take every opportunity to remind governments and corporations that international legal instruments are clear:

International law requires that: online free expression shall not be restricted by direct or indirect means, such as censorship, restrictive governmental or private control over computer hardware or software, telecommunications infrastructure, or other essential components of the electronic networks. The right to privacy, anonymity and security includes the protection from arbitrary massive surveillance of either content or association online as well as the right the choose privacy technology such as cryptography to protect communication.

My belief in global internet freedom is based upon an understanding of communication as the universal driving force of human civilization, and as the foundation of individuality, as well as community:

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and ***regardless of frontiers****.*[31]

---

[1] CECC Open Forum, Monday, March 10, 2003, at 2:00 PM in Room 2200 of the Rayburn House Office Building. http://www.cecc.gov/…….

[2] *The Great Firewall of China*, XIAO QIANG and SOPHIE BEACH http://www.cpj.org/news/2002/China_Firewall25aug02.html;

The Small World problem. S. Milgram Psychology Today, 2:60-67, 1967

Citations: http://citeseer.nj.nec.com/context/302442/0

[3] Noting particularly the innovative roundtables: China's Cyber-Wall: Can technology break through? (11/04/02)http://www.cecc.gov/pages/roundtables/110402/index.php?PHPSESSID=544c601e2b3f199980e642804f9e84d1; the quality of the contributions to Wired China: Whose Hand is on the Switch? April 15, 2002 http://www.cecc.gov/pages/roundtables/041502/index.php

[4] http://go.openflows.org/cecc

[5]Hacktivism and Human Rights: Using Technology to Raise the Bar:
http://www.cultdeadcow.com/panel2001/hacktivism_panel.htm

[6] Article Zero::Access Universal, on the occasion of the World Summit on Information Society in Geneva. forthcoming, December 2003

[7] WHAT IF THERE IS A REVOLUTION IN DIPLOMATIC AFFAIRS?

David Ronfeldt and John Arquilla: http://www.usip.org/vdi/vdr/ronarqISA99.html

[8] http://www.amnesty.ie/news/2001/irelandarms.shtml The use of the term *arms trade* has the effect of making many people think that it is only tanks and guns and weapons of mass destruction that are the problem. . . By focusing solely on weapons and torture equipment, we can ignore the fact that in some cases it is state of the art technology and communications equipment that allows repressive governments to moniter and arrest human rights defenders and pro-democracy campaigners. Electro-shock equipment and leg irons may be the visible implements of torture but it is the use of global positioning devices and call interception equipment that enables a government to track the movements of its opponents.

[9] http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html [English]
http://internetfreedom.org/gb/articles/1069.html [Chinese]

[10] http://www.almaden.ibm.com/software/dm/Hippocratic_Databases/hippocratic.pdf - scientists at IBM Almaden are working on a system where "contracts" are created between databases and administrators/primary users to ensure the privacy and integrity of data. This contract system is based on 10 principals, including stipulations that the information will be kept accurate and up-to-date, the data is used solely for what it was specifically collected for, and the data is only retained for as long as it is needed.

[11] Michael Iannini, general manager of Nicholas International Consulting Services Inc. in Beijing. "Through this hole the government has set up many filters," he said. http://www.securityfocus.com/news/2907: , China's Web surveillance slows access even as government promotes Internet use [The Associated Press Mar 5 2003]

[12] ibid.

[13] http://news.bbc.co.uk/2/hi/asia-pacific/2828433.stm

[14] http://www4.gartner.com/DisplayDocument?doc_cd=110031: The Chinese government commonly blocks access to sites it deems to have inappropriate content, but it has never before redirected users trying to access certain domains to other Web sites. Doing so turned a political decision into a trade problem.

[15] http://www.dit-inc.us/

[16] http://www.wired.com/news/politics/0,1283,56699,00.html

[17] http://www.icannwatch.org/article.pl?sid=02/10/07/151227&mode=thread ICANN’s China Question.

[18] http://dit-inc.us, forthcoming, http://www.dit-inc.us/hj-09-02.html for background.

[19] http://www.eweek.com/article2/0,3959,919681,00.asp

[20] Full text of the Hacktivismo Enhanced-Source Software License Agreement is available at:
http://www.hacktivismo.com/hessla.html

[21] Freenet-china.org for example.

[22] http://www.hacktivismo.com/news/modules.php?name=Content&pa=showpage&pid=19

[23] http://cryptome.org/DOC_BIS.pdf

[24] http://cryptome.org/hack-cow.htm

[25] – perhaps a best-of-class Intrusion Detection System of some sort: [applied across an entire country]

[26] http://news.bbc.co.uk/2/hi/business/2264508.stm**: The cost of China's web censors**

[27] http://hacktivismo.com/news/modules.php?name=News&file=article&sid=229: Lee Tien, senior staff attorney for the Electronic Frontier Foundation, the online civil liberties group in San Francisco

[28] China: Internet users at risk of arbitrary detention, torture and even execution http://www2.amnesty.se/aidoc/press.nsf/thisweekpr/80256AB9000584F680256C78004EEF43?opendocument

[29] see George Orwell, 1984.

[30] http://www.dfn.org/focus/china/netattack.htm: Attacks on the Internet in China: Chinese individuals currently detained for online political or religious activity. Digital Freedom Network provides a list of individuals currently detained for online activity. DFN has also compiled a list of Chinese legal actions and site shutdowns since January 2000 that restrict online expression. These lists are updated regularly. DFN also has a useful page containing the latest news related to Net restrictions in China (http://dfn.org/focus/china/chinanetreport.htm).

[31] The Universal Declaration of Human Rights, Article 19