Congressional-Executive Commission on China
Hearing
Chinese Hacking: Impact on Human Rights and Commercial Rule of Law
June 25, 2013

Testimony of Louisa Greve
Vice President for Asia, Middle East and North Africa, and Global Programs
National Endowment for Democracy

The Congressional-Executive Commission on China is to be heartily commended for bringing much-needed attention to the extremely important issue of today's intensified, globalized harassment of human rights activists working to bring about the rule of law and human rights in China.

Since 1949, Chinese citizens who dare to speak freely have faced a blanket of harsh repression – there is no freedom of speech in China. Since the dawn of the global Internet, even Chinese who dare to speak freely in any other place on earth have faced a continually renewed campaign of cyberhacking that acts as a virtual blanket of repression of their freedom of speech on human rights in China. Freedom of speech and action is now impeded even outside China.

For Chinese, Tibetan, Uyghur and Southern Mongolian democracy advocates and human rights activists working from exile in democratic countries, cyberhacking has the direct effect of reaching across the boundaries of state sovereignty to directly and severely undermine activists' ability to exercise the fundamental political freedoms they should enjoy in democratic countries. Being under sustained cyber-attack means these groups are not, in practice, able to routinely avail themselves of ordinary access to free communications media and the public square because they cannot count on being able to use normal modern means of communication. Victimized by widespread and gross human rights violations at home, after leaving their homelands, they still contend with cyberhacking – concerted, strategic, and targeted disruptive tactics administered from afar via the Internet.

Numerous human-rights groups concerned with China experience routine and persistent denial-of-service attacks and implanting of malicious code on their websites. Organizations and news sites that have gone public about hackers' success in embedding malware, or closing their websites for days or weeks, include the Human Rights in China, Asia Catalyst, China Aid, the Independent Chinese PEN Center, Canyu, the Office of the Dalai Lama, Aboluowang, Boxun, China Human Rights Defenders, New Century, Livelihood Watch, the World Uyghur Congress, the Uyghur American Association and the Uyghur Human Rights Project.

Activists working on China have contended for at least the past 8-10 years with fake emails spoofing their addresses going out to numerous recipients, purporting to be emails from them, and spear-phishing methods targeting addresses in their own contact lists designed to install surveillance and extraction software on victims' computers, some as early as 2005. The "GhostNet" report by researchers at Information Warfare Monitor made headlines in March 2009 by documenting extensive cyberspying software installed on computers used by Tibetan activists (and dozens of embassies) all over the world, from India to Europe to the U.S., through which hackers could turn on webcams and microphones at will.

Hackers' efforts to shut down the ability of groups to function normally, however, involves much more than DoS attacks and spoofing, spear-phishing and malware, and remote surveillance via keystroke monitors and webcams. Activists report evidence in the past year or two of new, even more Orwellian features of some of the targeted hacking: round-the-clock, real-time, non-machine (human) interference; all-device tracking; and software innovation to attack previously untouched systems, including, most

recently, android systems for mobile phones and tablets. The World Uyghur Congress (WUC) has prepared detailed documentation of its experience in this regard.

Real-time and pre-emptive interference with communication: Spear-phishing attacks are routinely sent among and from Uyghur, Chinese and Tibetan activist circles. In the past, these messages, with attachments containing malware, could often be spotted because the content of the email was strange and poorly written, to the point of misspelling information in the purported senders' address block. Increasingly, hackers obtain genuine messages and re-send them – often within hours, which is a significant factor in increasing their plausibility – for example when they purport to give information about an upcoming conference or event. On May 9 this year, the World Uyghur Congress prepared a written statement on behalf of an ECOSOC-accredited NGO about the Maralbeshi incident in Xinjiang (East Turkestan). On the same day that the writer sent the draft statement for review, the text of the original email asking for comments, and a malware-infected attachment, were sent from a spoofed email address to hundreds of people, not only to addresses in the original sender's contact list, but also to people with whom the sender had never had previous contact. The malware in the attachment was designed to enable the hacker to retrieve the recipients' usernames, passwords, and credit card details. The Uyghur American Association reports at least one incident in which a staff member received a reply to a message to a colleague within an hour, giving a plausible response on an issue that they had been working together on, that turned out to be the work of a hacker. Many of the hackers' fake emails received by Uyghur activists are written in fluent Uyghur (Latin script).

All-device harassment:
--The office and private telephone land-line numbers of several World Uyghur Congress staff in Munich were taken out of commission for a full week around July 5, 2011 due to continuous calls that blocked any use of the phones.
--At the same time, the WUC staff and general email accounts were subject to a massive spam attack. Between July 2 and July 7, a total of 15,000 spam emails were sent to the general account.
--The website was also disabled during this time.

Innovation for attacks via new platforms:
On March 26, 2013, Kapersky Labs[1] documented the first-ever use of a spear-phishing email used specifically to attack android users. The content of the spear-phishing email was extracted from a message sent by the WUC to speakers and participants in its just-concluded conference in Geneva. The email was purportedly sent by a high-profile Tibetan activist who had been at the conference. The malware was designed such that when the victim reads the email, the malware reports the infection to a command-and-control server and then begins to harvest information stored on the device. The copied data includes data about the phone itself (phone number, OS version, phone model, SDK version); contacts stored both on the phone and the SIM card; call logs; SMS messages; and geo-location.

The deliberate, directed characteristics of this campaign deserve emphasis.

Many overseas groups experience interference that is extremely sophisticated and conducted in real time. Hackers are creating fake emails, often of a spear-phishing nature or with malicious code attached, using content that had been sent between colleagues, within an hour or two after initially being sent. Often, the hacker uses the same errors in syntax, spelling, and grammar that the purported sender makes when using a second or third language on a day-to-day basis.

The attacks over the past few years reveal a significant upgrading of resources devoted to the attacks, in terms of increasing technical skills, language proficiency, and technical means. Activists report, for

[1] http://www.securelist.com/en/downloads/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf, June 5, 2013

example, that the English-language proficiency and Uyghur-language proficiency of the hackers is much better than it was only a year ago. Hackers are using the most up-to-date code available – often same-day code -- to evade commercially available defenses. The extent of new and innovative software used in the hacking is an indicator of massive resources being devoted to the effort.

And we should note that the political targeting is explicit: attacks surge before sensitive political anniversaries in China – June 4 every year, and since 2009, on and around July 5, the date of the deadly street violence in Urumqi that escalated from a peaceful protest to deadly ethnic rioting and lethal riot-suppression.

Hacking is a potent tactic for hampering and impeding the work of human rights advocates because of its numerous practical effects:

It silences activist groups' ability to communicate with the wider public or, in the case of independent media, disseminate news, when sites are shut down for extended periods.

It degrades their ability to conduct professional human-rights documentation by compromising groups' ability to keep information confidential. This can be devastating, and extends to assistance to refugees, as for example cases when Uyghurs are in deportation proceedings in Europe; alternative, manual means of communicating and documenting abuses take enormous time or make documentation impossible when researchers and witnesses are dispersed across different continents.

It distracts and diverts the energies of activists, by forcing them to deal with recovery from cyber-attacks and to double-check the authenticity of all the communications they receive.

It raises the monetary cost of the work by requiring multiple data backup systems, expensive specialized technical assistance, and often extensive and time-consuming searches for alternative server space .

It sows distrust and wastes time, as activists routinely cannot trust incoming communications.

It undermines cooperation in the wider world, as international organizations, experts, and media experience the frustration of fake and malicious emails purportedly from the targeted NGOs.

Hacking also increases fear, even among those who live in free countries. The real-time, all-device surveillance and tracking achieves a potent deterrent effect by making people afraid to be in contact with each other, whether outside of China (for fear of compromising strategies or confidential information, such as the identities of witnesses or victims) or inside China (for fear of instigating harassment or arrest of contacts).

The repressive effects of cyberhacking – bringing about conditions that silence critical voices, undermine the credibility of independent actors, undermine trust among dissidents, increase isolation, raise costs, and induce fear – is a remarkable extraterritorial extension of the tactics of repression practiced by authoritarian states. It deserves the outraged condemnation of all responsible institutions and defenders of universal human rights.

DETAILS OF SAMPLE DENIAL-OF-SERVICE CASES

June 14, 2013 - The Independent Chinese PEN Center (ICPC) and Canyu, the human rights documentation site maintained by China Free Press, publisher of the widely read citizen-journalism site Boxun, came under malicious attacks for 24 hours on June 14.

September 2012 – One of a series of regular DoS attacks on the website of the Uyghur American Association, designed to embed malicious code to infect website visitors' computers, succeeded. This series of attacks was identified as originating from IP addresses in China.

The websites of both the Uyghur American Association and the Uyghur Human Rights Project are blocked inside China. Yet these sites report that they experience regular flooding-style DDoS attacks (overwhelming numbers of data requests) that originate in part from IP addresses in China, which suggests that the attacking Chinese IP servers have unrestricted access to the Internet beyond the Chinese firewall.

February 2011 - Aboluowang, a news site run by Falun Gong volunteers, was attacked for two weeks, forcing even readers outside China to use proxies to visit the site.

Nov-Dec 2010 and Jan-April 2011 - The Independent Chinese PEN Center website was taken down for extended periods during the period when Liu Xiaobo's Nobel Peace Prize was in the news and the first few months of the Arab Spring.

October 2010 – Canyu and Chinese Human Rights Defenders, sites dedicated to documentation of human rights abuse, had their data deleted.

January 2010 – ICPC, Canyu, Chinese Human Rights Defenders, New Century, Livelihood Watch issued a joint statement condemning the series of DDoS attacks on their sites and numerous others in the period after the sentencing of Liu Xiaobo and the Google pullout. The scale and sophistication of the attack prompted a commercial server-space vendor based in the US to cancel its contract with a NED-supported US-based NGO that was providing hosting services for several of these sites. The NGO was forced to turn to inadequate temporary solutions using Twitter and disseminating information from blogspot pages for a number of weeks. For more details:

五中文网站关于网站受到恶意攻击的联合声明
http://peacehall.com/news/gb/china/2010/01/201001241220.shtml
关于《参与》网站近期被持续攻击的声明
http://peacehall.com/news/gb/china/2010/10/201010160141.shtml
"维权网"关于网站受到攻击的声明
http://peacehall.com/news/gb/china/2010/01/201001241233.shtml
博讯、参与等网站关于网站受到恶意攻击的联合声明
http://boxun.com/news/gb/intl/2012/04/201204282215.shtml#.UbNJFS2DE5s