A Smoking Cursor? New Window Opens on China’s Potential Cyberwarfare Development

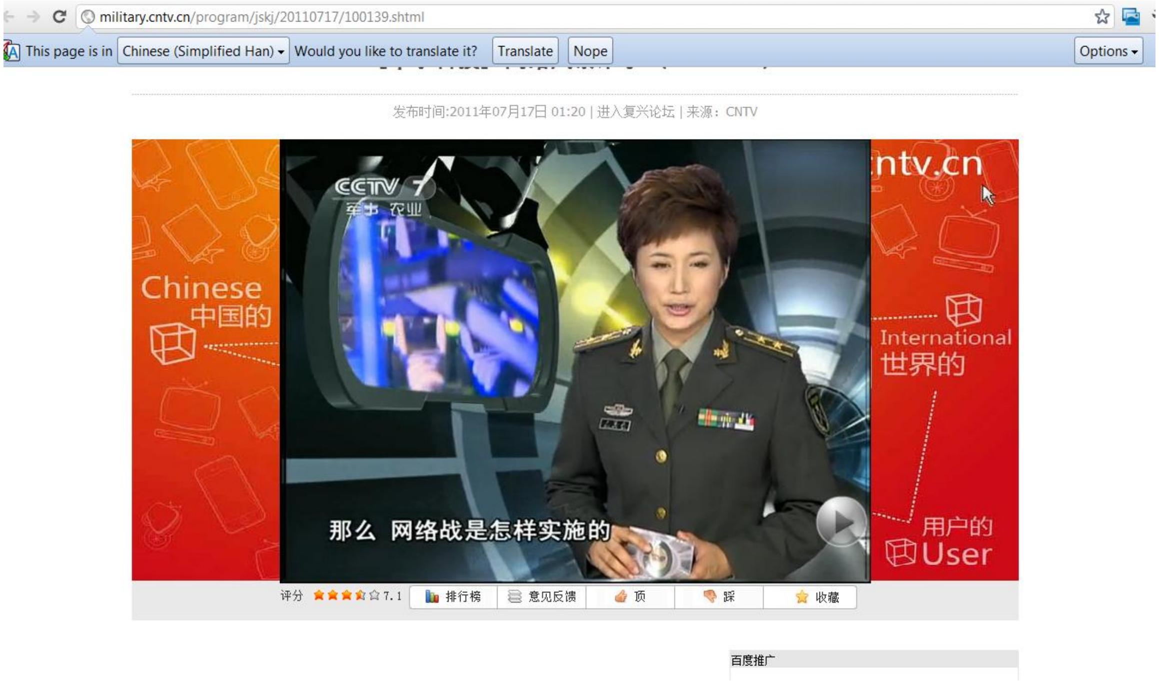
CCTV 7 program raises new questions about Beijing’s support for hacking

Andrew Erickson and Gabriel Collins

The positions expressed here are the authors’ personal views. They do not represent the U.S. Naval War College, Navy, Department of Defense, or Government, and do not necessarily reflect the policies or estimates of these or any other organizations.

***China SignPost*™ 洞察中国–“Clear, high-impact China analysis.”©**

Amid growing U.S. concerns of ongoing Chinese cyberattacks, attribution remains the most complex issue. At the open source level at least, it has been hard to find a “smoking cursor.” That is, until the broadcast of a recent cyberwarfare program on the military channel of China’s state television network. It appeared to show dated computer screenshots of a Chinese military institute conducting a rudimentary type of cyberattack against a United States-based dissident entity. However modest, ambiguous—and, from China’s perspective, defensive—this is possibly the first direct piece of visual evidence from an official Chinese government source to undermine Beijing’s official claims never to engage in overseas hacking of any kind for government purposes. Clearly, Washington and Beijing have much to discuss candidly here if they are to avoid dangerous strategic tension.



military.cntv.cn/program/jskj/20110717/100139.shtml

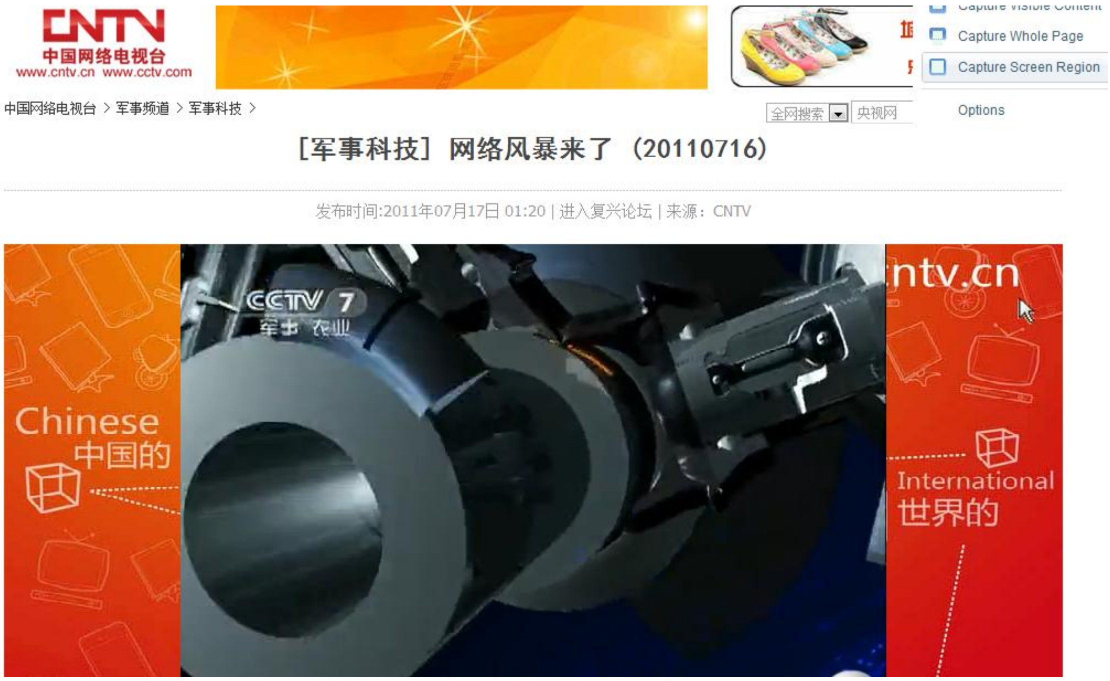
This page is in Chinese (Simplified Han) Would you like to translate it?

发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV

那么 网络战是怎样实施的

What Happened?

China Central Television 7 (CCTV-7) is China's official channel for military and agricultural issues. As part of its wide-ranging coverage, every Saturday at 1440-1500 Greenwich Mean Time (GMT), CCTV-7 runs a 20-minute program on military S&T developments in China and abroad called "Military Science and Technology." It's always worth watching, given the range of timely topics covered and the detailed analyses offered by Chinese specialists. The 16 July 2011 edition was particularly so.

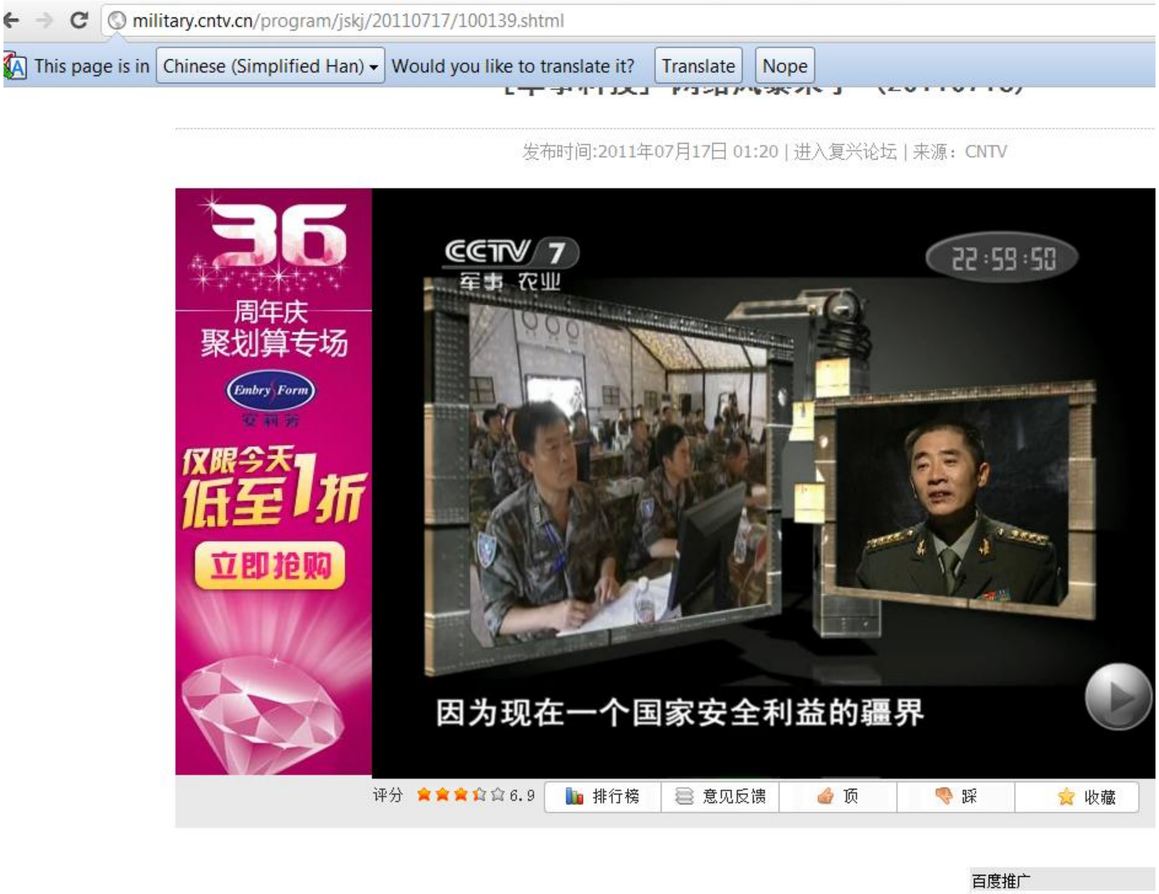


中国网络电视台 > 军事频道 > 军事科技 >

[军事科技] 网络风暴来了 (20110716)

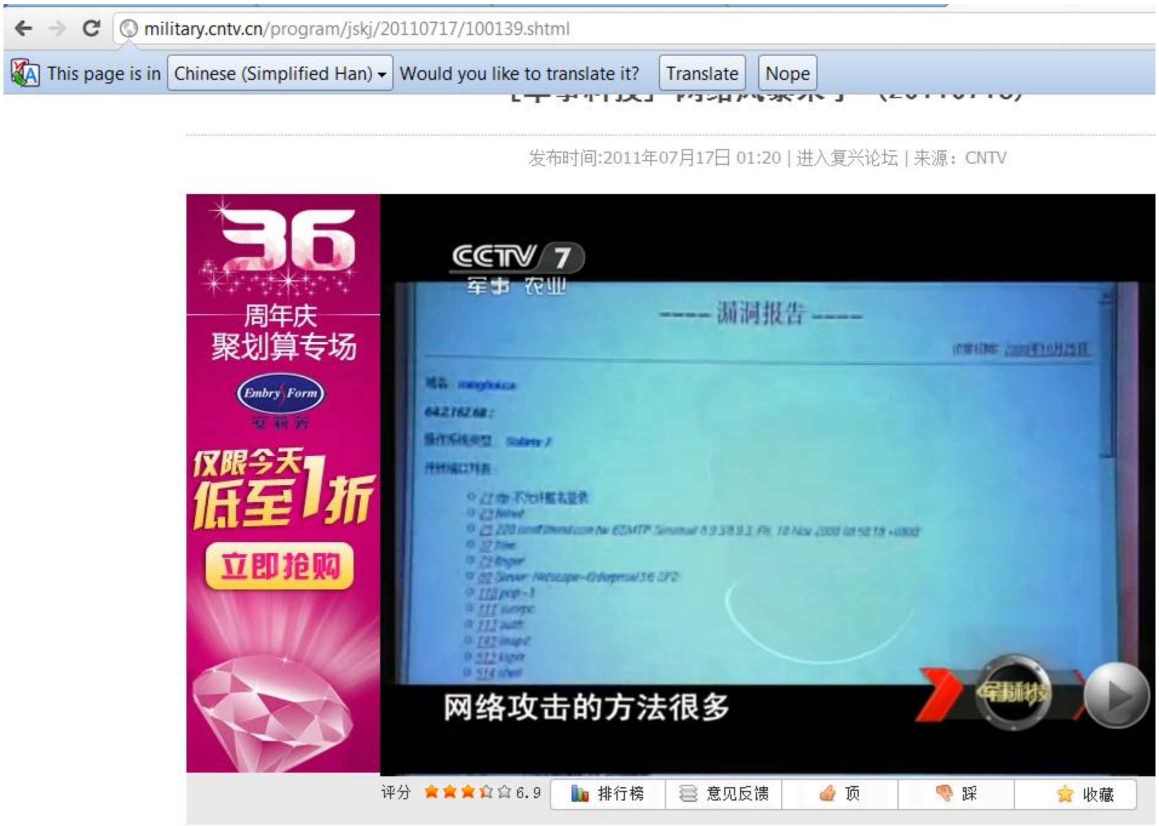
发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV

Entitled "The Internet Storm is Coming" (网络风暴来了), as pictured above in a CCTV-7 website screenshot, it begins with a broad discussion of cyberattacks. It highlights a statement by then-U.S. Secretary of Defense Robert M. Gates at the Shangri-La Dialogue in Singapore on 4 June 2011. This important international conference was also attended by Gates' Chinese counterpart General Liang Guanglie. Emphasizing that the U.S. was extremely concerned about the cyberattacks that it was continually suffering from, Gates suggested that some attacks could rise to the level of an act of war and prompt the U.S. to respond with force.[1]


military.cntv.cn/program/jskj/20110717/100139.shtml
This page is in Chinese (Simplified Han) Would you like to translate it? Translate Nope
发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV
36
周年庆
聚划算专场
Embry Form
安莉芳
仅限今天
低至1折
立即抢购
CCTV 7
军事 农业
22:59:50
因为现在一个国家安全利益的疆界
评分 6.9
排行榜
意见反馈
顶
踩
收藏
百度推广

PRC Military expert Du Wenlong (pictured above) then highlights President Obama’s May 2009 remarks in which he emphasized the importance of securing the nation’s digital infrastructure and declared it a strategic national asset. Du explains that Washington would regard some types of cyberattacks as acts of war because modern military operations rely heavily on digital networks and cyberspace: “networks have become the basis for military action and for winning a war.”[2] Du appears to be well acquainted with his subject matter, and provides cogent explanations of complex cyber issues. The program proceeds to explain how cyberwarfare may be waged, in both the defensive and offensive dimensions.

Here is where the program deviates from its typical theoretical coverage of broad military trends, many focused on foreign militaries for six seconds to offer an unusually-specific Chinese example. An initial screen (below) is labeled “Vulnerability Report” in large letters; a narrator intones that “there are many Internet attack methods.”

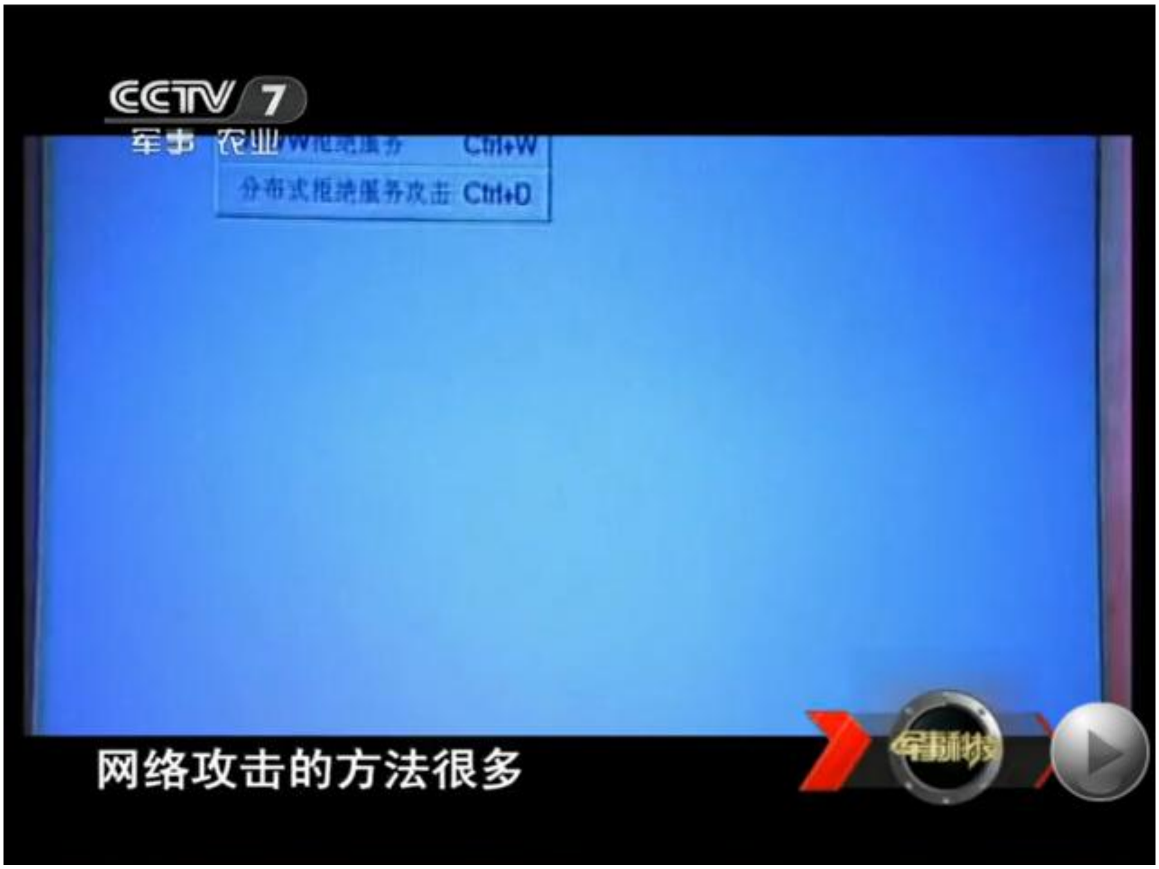


military.cntv.cn/program/jskj/20110717/100139.shtml

This page is in Chinese (Simplified Han) Would you like to translate it?

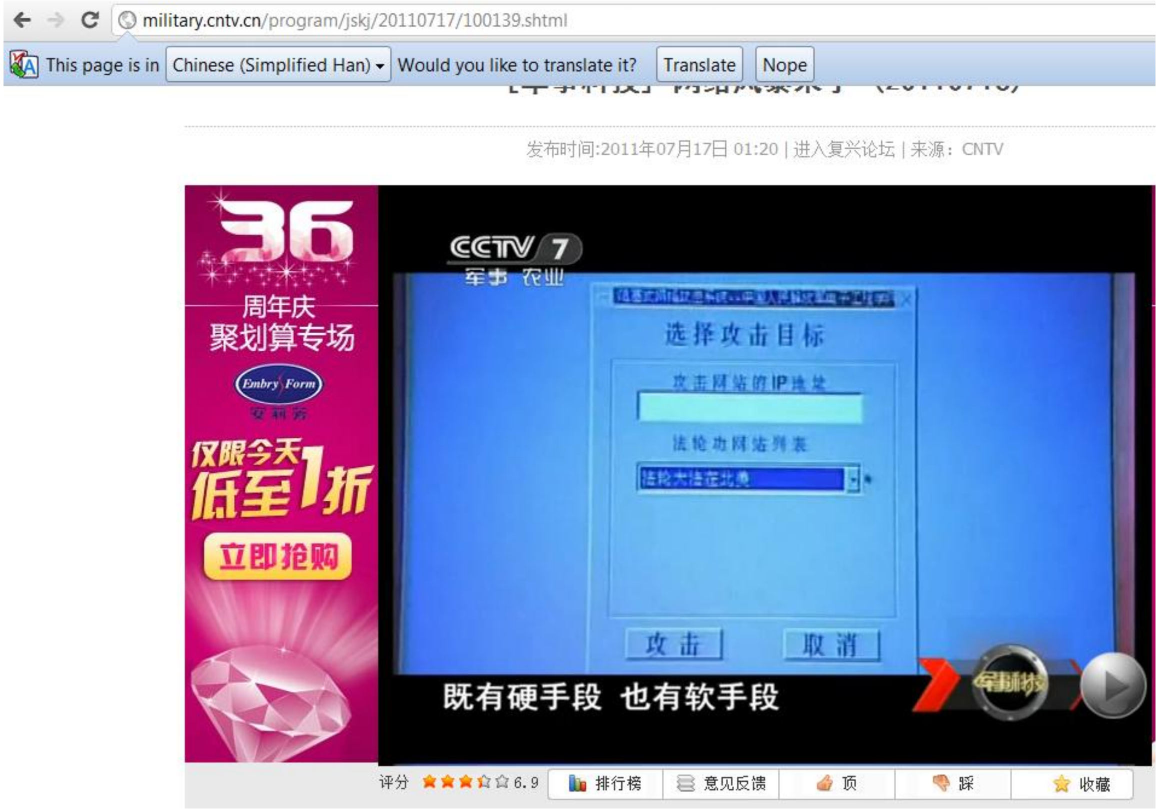
发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV

As the narrator is discussing means of implementing hard and soft cyber/network attacks (at 11:04 in the program time code), footage displays what appears to be a human-operated cursor using a software application with Chinese character labeling launching a “distributed denial-of-service” (DDOS) attack (as pictured below).



网络攻击的方法很多

This particular DDOS is against a website formerly affiliated with the dissident religious group Falun Gong. Under large characters reading "Select Attack Target," the screenshot below shows "Falun Gong in North America" being chosen. Here it must be emphasized that DDOS attacks are generally extremely rudimentary. As will be explained later, if the footage in question is real, it is likely a decade old.

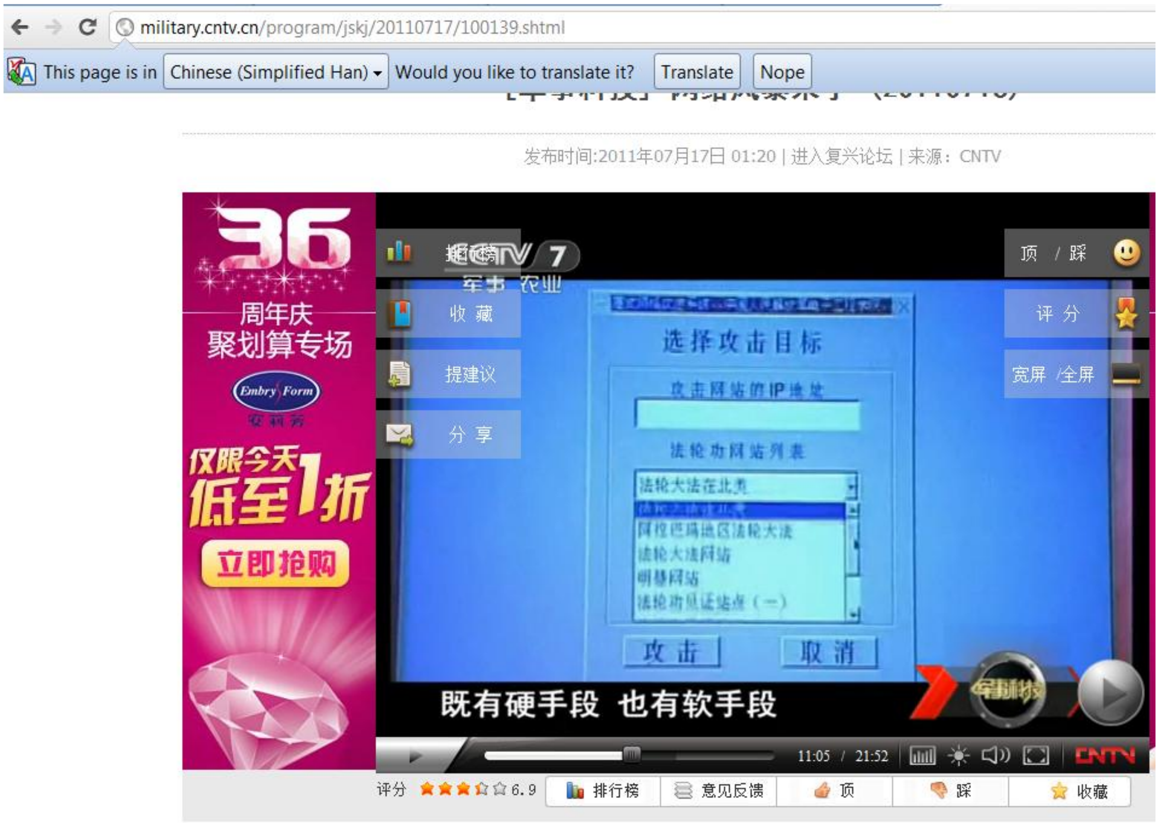


military.cntv.cn/program/jskj/20110717/100139.shtml

This page is in Chinese (Simplified Han) ▾ Would you like to translate it? Translate Nope

发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV

Drawing on a “Falun Gong website list" encoded in the software, the cursor selects the “Minghui Website” from a pulldown menu of Falun Gong websites (as pictured below). Minghui.org is the main website of Falun Gong’s spiritual practice, and hence a logical target. The other options visible are “Falun Dafa websites in North America, Falun Dafa in Alabama Area; Falun Dafa Websites, Minghui Website; and Falun Gong Witness Site (1).” The cursor then depresses a large button on the bottom left corner of the software menu labeled “Attack.” The one on the bottom right corner, labeled “Cancel,” is not selected.



military.cntv.cn/program/jskj/20110717/100139.shtml

This page is in Chinese (Simplified Han) Would you like to translate it?

发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV

选择攻击目标

攻击网站的IP地址

法轮功网站列表

法轮大法在北美

阿拉巴玛地区法轮大法

法轮大法网站

明慧网站

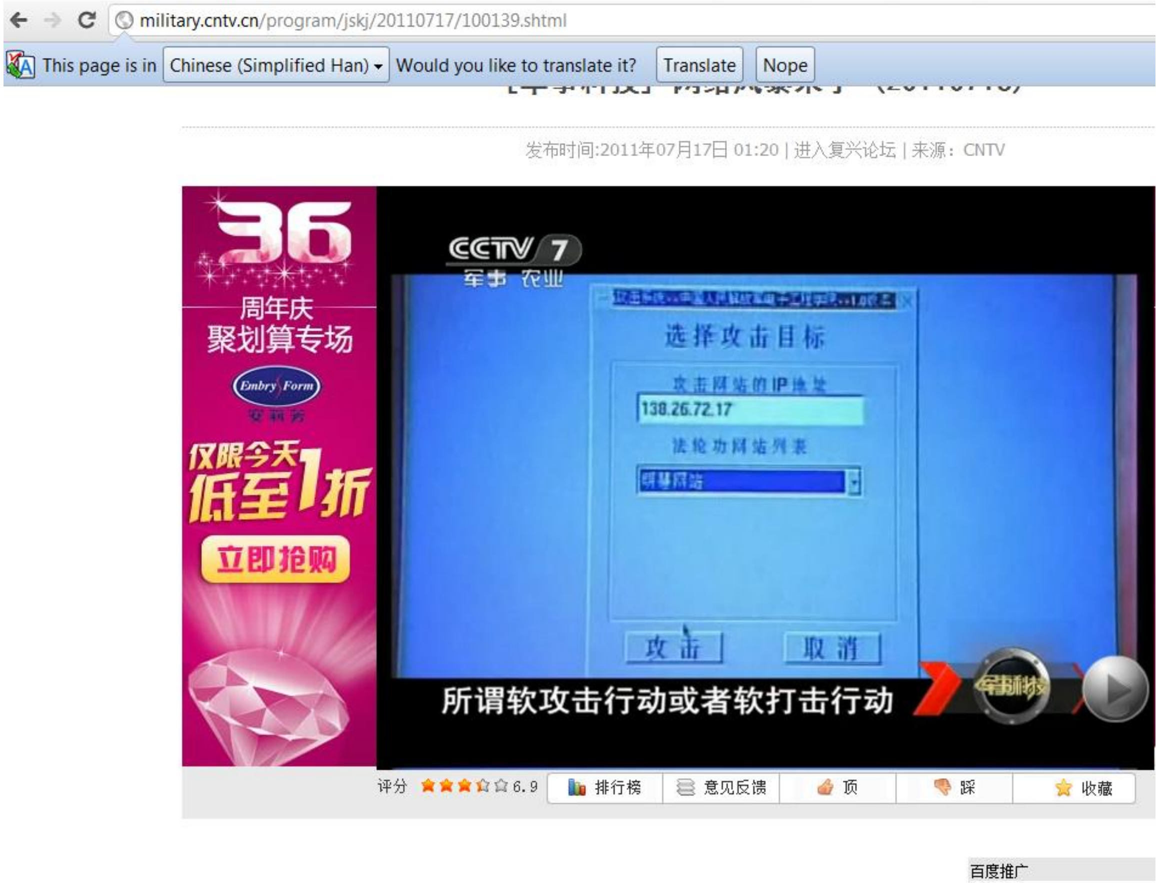
法轮功员证站点（一）

攻击 取消

既有硬手段 也有软手段

11:05 / 21:52

Hovering over a software window labeled “IP Address of a Website Chosen to Attack,” the cursor selects the IP address 138.26.72.17. This was once linked to the University of Alabama in Birmingham (UAB). According to the Falun Gong-supporter-founded *Epoch Times*, a UAB network administrator recalled that there had been a Falun Gong practitioner at the university some years ago who held informal Falun Gong meetings on campus. They could not confirm whether that individual used” the IP address in question, “and said it had not been used since 2001.” [3] PC World adds that “The site was created ‘by a former student and was decommissioned in 2001 as it violated our acceptable use policy,’ according to Kevin Storr, a UAB spokesman.”[4]



military.cntv.cn/program/jskj/20110717/100139.shtml

This page is in Chinese (Simplified Han) Would you like to translate it? Translate Nope

发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV

选择攻击目标

攻击网站的IP地址

138.26.72.17

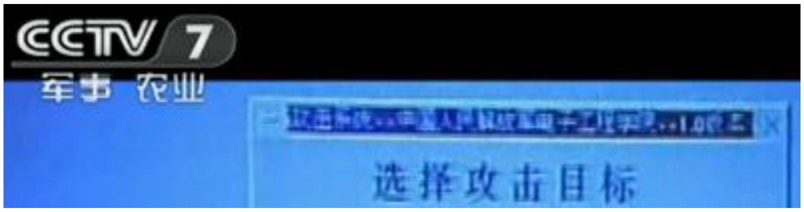
法轮功网站列表

明慧网站

攻击 取消

所谓软攻击行动或者软打击行动

During this sequence, some interesting characters remain at the top of the screen, as pictured in light blue highlighted against a dark blue background block in the cropped image below: “Attack system..[periods in original] PLA Electronic Engineering Institute.”



The program then returns to general cyberattack themes.

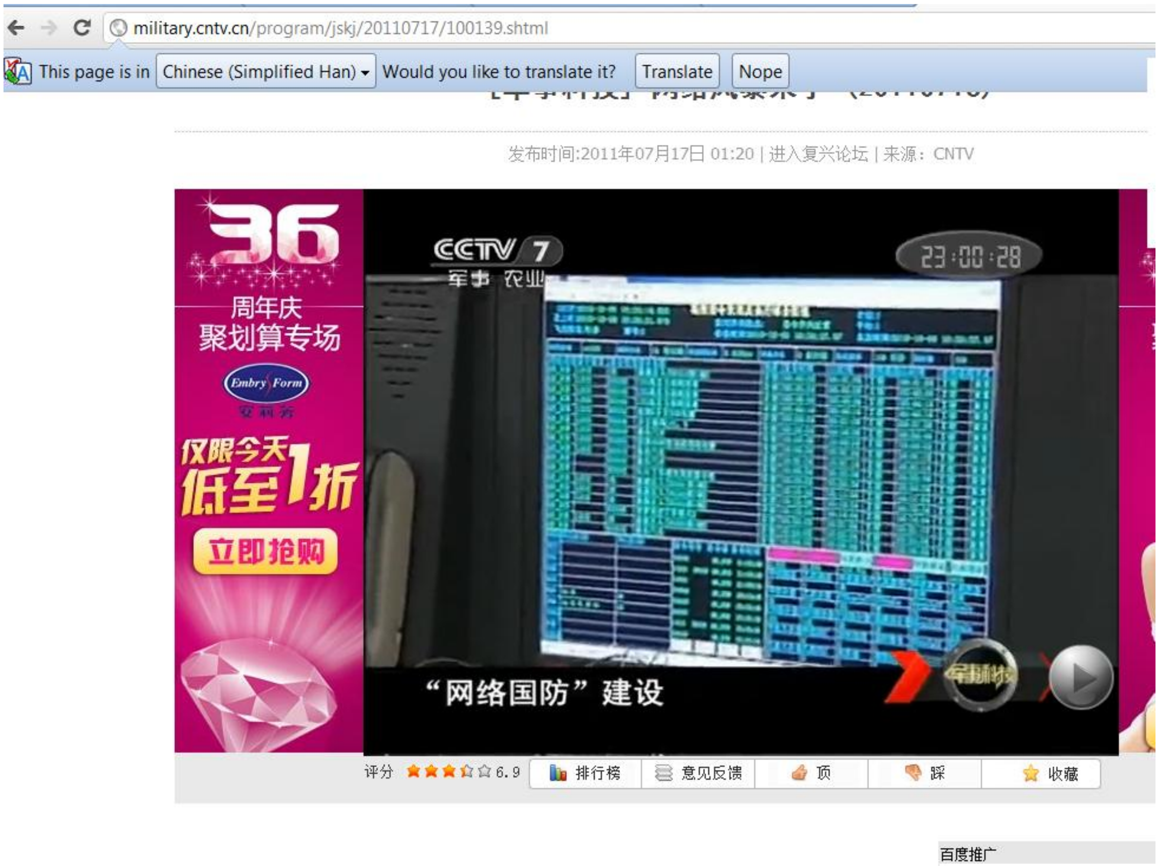
As this research note went to press, the program footage remained readily visible and viewable on the CCTV website at <http://military.cntv.cn/program/jskj/20110717/100139.shtml>.

Why it Matters

It is significant that an official Chinese state television channel showed even a symbolic representation of a cyberattack, particularly one on entities clearly located in a foreign sovereign nation. First, as one of its central emphases, China insists forcefully on realizing an extremely expansive definition of national sovereignty—it is difficult to see how such activities could possibly be in accordance with this overall approach. One of the greatest sources of friction in U.S.-China relations are fundamental differences regarding the scope of sovereignty, with China almost invariably the more indignant and assertive party. Second, official spokespeople for most other nations thought to have substantial offensive cyber and intelligence capabilities studiously refrain from addressing those capabilities directly, and hence from potentially making statements that did not appear to be credible about such issues. But Chinese officials instead issue blanket denials in this regard.

In September 2007, for example, Chinese Foreign Ministry spokeswoman Jiang Yu declared: "Some people make groundless accusations against China… China has all along been opposed to and forbids criminal activities undermining computer networks, including hacking. China is ready to strengthen cooperation with other countries, including the U.S., in countering Internet crimes."[5] In 2010, Jiang again denied that China has been responsible for cyberattacks: "Some reports have, from time to time, been heard of insinuating or criticising the Chinese government... I have no idea what evidence they have or what motives lie behind. Hacking is an international issue and should be dealt with by joint efforts from around the world."[6]

Unfortunately, despite this recent incident and a larger "Inbox" of mounting evidence to the contrary, Chinese official responses are likely to follow the well-trod path of deliberate denial of responsibility—thereby further straining Beijing's credibility in foreign audiences.



military.cntv.cn/program/jskj/20110717/100139.shtml

This page is in Chinese (Simplified Han) Would you like to translate it?

发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV

“网络国防”建设

Alternative Explanations

As with many incidents involving apparent, alleged, or uncertain Chinese military capabilities, this one raises more questions than answers:

- What was the motive for displaying the software footage?
- Where did the footage come from, and how was it created?
- At what level were decisions to insert and retain coverage made?
- Who was the intended audience?

Since it seems unlikely, given its professed cyber security concerns and substantial technological capabilities, that Beijing allows itself to be defenseless against what it alleges to be the extensive predations of others in the offense-dominant domain of cyberspace, the alternative would appear to be that China is not being forthcoming in public about its development of offensive cyber capabilities. But why should this be, since virtually no Western experts or government officials believe such statements to be true? The most plausible answer would appear to be that China's government sees value in appearing to be defensive, and morally virtuous, before a domestic audience—its most important audience, and the most important audience for virtually any government. It is also possible that calling too much Chinese public attention to the nation's cyber capabilities could remind Chinese netizens further of the extensive Internet censorship that currently constrains their lives online, and which many find increasingly frustrating. Then there is the issue of the extent to which China's government may work with semi-, loosely-, and irregularly-affiliated, or firewalled-off, "Patriotic Hackers" to do its bidding. Perhaps it is seen as best to preserve at least some form of "plausible deniability" to deflect inquiries concerning these controversial issues, the better to unite citizens against perceived "foreign threats."

None of this, of course, explains the CCTV-7 footage's provenance and appearance *per se*. On the one hand, a large "Attack" button may seem cartoonish. On the other hand, this is no doubt a popular concept among Chinese cyberwarriors and their foreign counterparts alike, who have been schooled originally in video and computer games like World of Warcraft and may have some say in how things are constructed—there is no reason why such a configuration would be inherently disfunctional.

Perhaps the least unlikely explanation is that program producers sought specific footage to document specific cyberattack techniques. For reasons of Chinese pride, and perhaps PLA assertiveness, they wanted to show that China could do something itself in the face of perceived threats. Falun Gong, particularly despised by Beijing, offered a politically-correct and "morally justified" target even for ideologically dubious techniques. Footage from previous interviews and interaction with the PLA Electronic Engineering Institute may have happened to be available in convenient form, and met visual requirements. In any case, it would seem that nobody in the decision-making chain objected at the time.

Perhaps most importantly, the CCTV-7 software contents appear to correlate so closely with a set of attacks that China is alleged to have engaged in a decade ago that their construction would appear to be tedious for the production schedule of a major weekly television program.

Larger Picture

Regardless of the realities concerning these particular software images, there does appear to be a larger pattern of related Chinese government activity. A 2002 RAND study by noted China security/cyber experts Michael Chase and James Mulvenon offers both context and a plausible explanation for the CCTV-7 footage. It may date to activities occurring in 1999 and 2000 that they analyze in depth, marshaling a range of sophisticated inductive and deductive approaches to support their arguments:

> There is some evidence to suggest that the Chinese government or elements within it have engaged in hacking of dissident and antiregime computer systems outside of China. … evidence exists to support the conclusion that the Chinese government or elements within it were responsible for one or more of the China-origin network attacks against computer systems

> maintained by practitioners of Falungong in the United States, Australia, Canada, and the United Kingdom. After the exposure of the role of certain Chinese security agencies in the attacks, the later, more sophisticated intrusions were believed to have been carried out by cut-outs, making it more difficult to ascertain the extent of government involvement. This was especially true of the attacks that occurred in winter and spring 2000.[7]

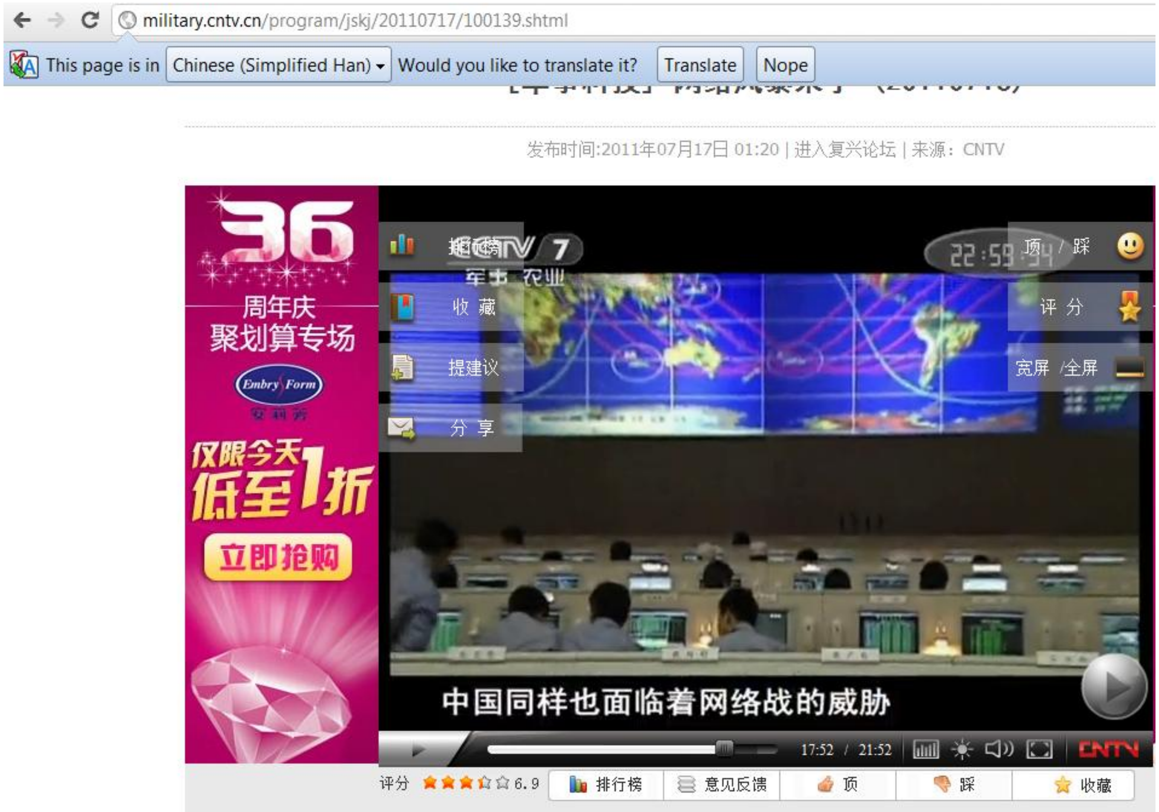
A 27 July 1999 attack on the www.falunusa.net website, for instance, was traced to the IP address 202.106.133.101, registered according to the Asia-Pacific Network Information Center (APNIC) database to 14 East Chang'an Street/ Dong Chang An Jie 14 in Beijing—precisely the location of China's Ministry of Public Security (MPS). While Chase and Mulvenon are careful to acknowledge that in theory a third party could have exploited this IP address to launch its own attack, they offer four reasons why this was not likely the case in practice:

> First, the network had been established shortly before the information operations began and was divorced from other explicitly identified MPS networks in other parts of Chinese cyberspace, such as the domain spaces belonging to the MPS web page (www.mps.gov.cn). Second, the name of the organization in the database—Information Service Center—suggests an intent to deceive outsiders about its actual affiliation. Third, at least one Western media source claimed to have called the telephone numbers listed… and was told by the person answering the phone that the numbers belonged to the Ministry of Public Security. A later call by the same news organization to the telephone operator at the ministry confirmed that the numbers belonged to the MPS Computer Monitoring and Supervision Bureau. The fourth and most telling piece of evidence resulted directly from the impending exposure in the Western media of the network's governmental affiliation. Probably as a result of the increasing media attention, especially an imminent article by Michael Laris in the *Washington Post*, the information in the APNIC database was altered on 29 July 1999…. Most important, the owners of the network space changed the damning street address of the owner of the network from #14 East Chang'an Street to #6 Zhengyi Road (…Zheng Yi Lu 6).
>
> If the ministry's network had itself been the victim of an attack and was thus wrongly accused as the perpetrator of the attacks on the Falungong site in the United States, why go to the trouble of changing the database information to an address other than MPS headquarters? And was it a coincidence that the network information was changed on the eve of an exposé in a major Western newspaper of the MPS's alleged role in the attack? Most damning, the new street address (No. 6 Zhengyi Rd) is the address of the Ministry of Public Security's No. 3 Research Institute, which is responsible for computer security. The evidence cited earlier, along with this last attempt to further disguise the true owner of the network, strongly suggests that the perpetrator was caught with its "hand in the cookie jar."[8]

Chase and Mulvenon acknowledge that an MPS "rogue element" might conceivably have perpetrated these attacks without senior party leadership or MPS leadership sanction. In analyzing the considerably-more-sophisticated follow-on attacks of 2000, however, they offer evidence to suggest a state-level interest in their coordination:

> The first of the renewed attacks against Falungong servers occurred on March 11, 2000, coinciding with the meetings of the National People’s Congress in Beijing. The hack, which used a denial-of-service technique… brought down the main server in Canada (www.minghui.ca), as well as three mirror sites (www.falundafa.ca, www.falundafa.org, and www.minghui.org). …
>
> Attacks on Falungong servers reached a crescendo in mid-April 2000, when five sites—three in the United States (www.falunUSA.net, www.falundafa.org, www.truewisdom.net).... The timing of the attacks coincided with two sensitive political events: (1) the impending vote in the United Nations Human Rights Commission on a UN resolution condemning Chinese human-rights abuses, including persecution of Falungong; and (2) the one-year anniversary of the April 25, 1999, gathering of Falungong practitioners outside the central leadership compound in Beijing.[9]

In viewing this summer’s CCTV-7 footage, then, we are quite possibly afforded a peek into relatively unsophisticated techniques from a decade ago. It certainly looks like a “smoking cursor,” albeit a relatively modest one. China undoubtedly has far superior capabilities at its disposal today.



military.cntv.cn/program/jskj/20110717/100139.shtml

This page is in Chinese (Simplified Han) Would you like to translate it? Translate Nope

发布时间:2011年07月17日 01:20 | 进入复兴论坛 | 来源：CNTV

中国同样也面临着网络战的威胁

Conclusion

Regardless of the Chinese government's public positions for domestic consumption regarding cyberattacks launched from Chinese soil, it will have to deal increasingly with an important foreign audience. The U.S. International Strategy for Cyberspace, issued in May 2011, reflects the increasing seriousness with which the U.S. government views cybersecurity. The report declares that "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests."[10] To be sure, identifying an attack source that could be retaliated against is exceedingly difficult. However, taking a more aggressive stance against cyberattacks, even to the point of having cyberattacks serve as a potential trigger for alliance mutual defense obligations such as Article 5 of NATO, raises a number of interesting doctrinal possibilities. One is that physical infrastructure utilized in a cyberattack on U.S. Government assets could be held at risk, while another is that—similar to the U.S. position on terrorism—the source country of a cyberattack could be held responsible for the actions of parties operating from its soil, whether or not they can be credibly linked to the country's government.

As one of his last major official contributions to U.S.-China relations, former Secretary of Defense Robert Gates placed a very important message in China's inbox:

> I think we could avoid some serious international tensions in the future if we could establish some rules of the road as early as possible that let people know what kinds of acts are acceptable, what kinds of acts are not, and what kinds of acts may in fact be an act of war… I think all countries should see the cyber threat as a potential problem for them. …One of the things that I have been trying to get going over the last four, four-and-a-half years, is to examine this world of cyber in the context of defense responsibilities, and what in fact does constitute an offensive act by a government. …I think that one of the things that would be beneficial would be for there to be a more open dialogue among countries about cyber (threats) and establishing some rules of the road [to achieve] clearer understanding of the left and right lanes, if you will, so that somebody doesn't inadvertently or intentionally begin something that escalates and gets out of control.[11]

At the very least, it is in both Washington and Beijing's interest to have such substantive cyber talks before attacks enter into new domains in ways that neither nation wants to see. It is vital for the security of both Pacific cyber powers that Beijing reply in kind without attempting to block or delete the message.

About Us

China Signpost™ 洞察中国–"Clear, high-impact China analysis."©

China SignPost™ aims to provide high-quality China analysis and policy recommendations in a concise, accessible form for people whose lives are being affected profoundly by China's political, economic, and security development. We believe that by presenting practical, apolitical China insights we can help citizens around the world form holistic views that are based on facts, rather than political rhetoric driven by vested interests. We aim to foster better understanding of key internal developments in China, its use of natural resources, its trade policies, and its military and security issues.

China SignPost™ 洞察中国 founders Dr. Andrew Erickson and Mr. Gabe Collins have more than a decade of combined government, academic, and private sector experience in Mandarin Chinese language-based research and analysis of China. Dr. Erickson is an Associate Professor at the U.S. Naval War College's China Maritime Studies Institute (CMSI) and an Associate in Research at Harvard's John King Fairbank Center for Chinese Studies. Mr. Collins is a commodity and security specialist focused on China and Russia.

The authors have published widely on maritime, energy, and security issues relevant to China. An archive of their work is available at www.chinasignpost.com.

[1] For additional details, see "04 June 2011 - - Agence France Presse - US calls for talks on cyber threats," International Institute for Strategic Studies, http://www.iiss.org/whats-new/iiss-in-the-press/june-2011/us-calls-for-talks-on-cyber-threats/?locale=en.

[2] For the original text of President Obama's address, see The White House, Office of the Press Secretary, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," 29 May 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

[3] Matthew Robertson and Helena Zhu, "Slip-Up in Chinese Military TV Show Reveals More Than Intended: Piece Shows Cyber Warfare against US Entities," *Epoch Times*, 23 August 2011, http://www.theepochtimes.com/n2/china-news/slip-up-in-chinese-military-tv-show-reveals-more-than-intended-60619.html.

[4] Robert McMillan and Michael Kan, "China Hacking Video Shows Glimpse of Falun Gong Attack Tool," *PC World*, 23 August 2011, http://www.pcworld.com/businesscenter/article/238655/china_hacking_video_shows_glimpse_of_falun_gong_attack_tool.html.

[5] "China Denies Hacking Pentagon Computers," *USA Today*, 4 September 2007, http://www.usatoday.com/tech/news/computersecurity/hacking/2007-09-04-china-us_N.htm

[6] "PRC FM Spokesman Denies Canadian Hacker Claims," *AFP*, 6 April 2010.

[7] "Chapter 2: Government Counterstrategies," in Michael S. Chase and James C. Mulvenon, *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies* (Santa Monica, CA: RAND, 2002), MR-1543, 71, http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1543/MR1543.ch2.pdf.

[8] Ibid., 72-75.

[9] Ibid., 79-81.

[10] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[11] For additional details, see "04 June 2011 - - Agence France Presse - US calls for talks on cyber threats," International Institute for Strategic Studies, http://www.iiss.org/whats-new/iiss-in-the-press/june-2011/us-calls-for-talks-on-cyber-threats/?locale=en.