Wither the Jasmine

China's Two-Phase Operation for Cyber Control-in-Depth

Scott J. Henderson*

China's Jasmine Revolution, an online movement that emerged from the embers of revolutions sweeping the Middle East, experienced an enthusiastic birth but ultimately suffered a premature and rather mundane death. A passive shrug of the shoulders, and the embryonic movement withered and died on the vine. Some would argue that the Jasmine Revolution never took the breath of life—that it was merely a manifestation of the Chinese government's overreaction to the possibility of social unrest and the Western media's exuberance to cover it. The timing was wrong: China is not the Middle East, economic conditions were not conducive to a revolution, and it was not a serious movement. These and a host of other reasons explain the Jasmine Revolution's untimely demise. Whether the result of one or a combination of these factors, the downfall of the nascent movement illuminates the mechanisms behind Beijing's ability to provide comprehensive cyber control-in-depth through a two-phased system comprised of seven components: external monitoring, internal monitoring, blocking, attacks, intimidation, campaigning, and self-censorship.

---

*The author is an analyst for the Foreign Military Studies Office, Fort Leavenworth, Kansas. Mr. Henderson retired from the Army after serving 20 years in the intelligence community as a Chinese linguist. He holds a BA in Chinese studies and graduated from the Defense Language Institute in Monterey, California. In 1997 he was on special assignment to the US Embassy in China, and in 1995 he attended the Beijing Institute of Economic Management Immersion Program. Mr. Henderson is a subject-matter expert on Chinese cyber crimes and information operations; an open-source analyst focusing on strategic and tactical objectives of the People's Republic of China; an instructor for the Open-Source Information Research and Analysis Course; and a trainer at the FBI Cyber Crimes Lab. He created TheDarkVisitor.com, a website cited in the *New York Times*, *Popular Science*, *Computer World*, the *Register*, *Information Week*, MSNBC, *Sydney Morning Herald*, and *Economic Times*. Mr. Henderson has written several articles on China, such as "The Dark Visitor" (inside the world of Chinese hackers), "In the Shadow: Chinese Special Forces Build a 21st Century Fighting Force," "Things That Disturb Dragons" (China's reaction to the United States' reentry into Southeast Asia), "Songs of Chu" (China's military regions), "China Shaping the Operational Environment" (Chinese military science), and "Mao e-Guerrilla" (Chinese insurgents on the Internet).

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Wither the Jasmine: China's Two-Phase Operation for Cyber Control-in-Depth	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI) ,155 N. Twining Street,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**13**	

The Jasmine Revolution represents Beijing's latest, but not its first, attempt to control and smother a burgeoning online uprising in the crib. Government officials have developed and perfected their skills at online manipulation for 17 years, cutting their teeth on the Falun Gong, Free Tibet, Hong Kong pro-democracy, and anti-Japanese protest movements. It isn't necessary to study the specific details or chronology of each of these events. Rather, one need only understand the objective and current evolution of China's online crisis-control mechanisms. According to Chinese military writings, one attains control through reducing the destructive and negative effects of a crisis to their lowest level in order to terminate them in the shortest time and with minimum cost. Doing so involves the implementation of methods that will prevent and contain crises before they occur.[1] As we will see, the process is far from flawless, and the formulation needs constant adjustments and tweaks.

Historical precedents are plentiful. For example, in April 2005 Japan's bid for a seat on the United Nations Security Council, along with revisions to historical textbooks that downplayed Japan's actions in World War II, spawned large anti-Japanese demonstrations which spread across China, attacking anything symbolic of Japan.[2] In late April, the Chinese Ministry of Public Security sought to bring the demonstrations to a halt. Utilizing Internet postings and text messages in combination with traditional print media, the ministry ordered protestors not to organize anti-Japanese demonstrations without police approval. Summing up the Communist Party's ability to control the populace, China's minister of state council information declared that "most citizens obey no-demonstration orders. For example, a Beijing newspaper's warning against illegal demonstrations deterred all but a few hundred protesters from gathering for a second weekend of demonstrations in the capital last April. You need to understand that Chinese citizens still respect the government. So if the government makes clear that this kind of demonstration is not OK, 90% of the people won't go."[3]

Taking the statement issued from the ministry at face value, along with an understanding of known Chinese methodologies employed in online campaigns, this article examines the most effective method of deterring the remaining 10 percent. It does so by selecting the Jasmine Revolution as a case study of procedures used by the Chinese government to curtail online dissidence, laying out events chronologically to give the reader a better indicator of reactions from that government.

The Jasmine Revolution: A Case Study

Phase One: Passive Defense (External Monitoring, Internal Monitoring, and Blocking)

From 17 December 2010 through 18 February 2011, Chinese monitors increased their active screening of events taking place in the Middle East, concerned that the latter would foment internal unrest at home. Outside observers are aware of several groups and methods associated with China's monitoring of domestic Internet communications (the State Council Information Office [SCIO], Cyber Police, and Great Firewall), but they know less about Beijing's external monitors.

External Monitoring. Two sources hint that the People's Liberation Army (PLA) plays a role in reporting external hot spots. First, in 2009, sources inside the PLA's University of Foreign Languages suggested that, due to critical deficiencies in mission training, the curriculum would need revamping, with emphasis placed on research involving open-source military intelligence.[4] Second, in May 2011 reports out of the Guangzhou Military Area Command explained that, in order to expand international strategic vision, departments under the headquarters of troop units were "specially-assigned personnel for the collection, organization and post production of the materials that come from major news media outlets, academic reports of some research institutes, lectures of military academies, and so on."[5] These types of PLA units likely would be responsible for the dissemination of information regarding potential hot spots worldwide.

Although we are not certain about the exact government agencies or organs that conduct external monitoring, the timeline from the Jasmine Revolution makes clear that these observations are taking place (fig. 1). On 17 December 2010, the self-immolation of a Tunisian graduate student set off violent protests inside Tunisia, marking the beginning of that country's Jasmine Revolution.[6] Officials inside the People's Republic of China (PRC), monitoring world events, quickly picked up the news and followed the situation as it unfolded. In less than a week, China began online blocking tactics to filter out references to the revolutions taking place in Tunisia and Egypt.[7]

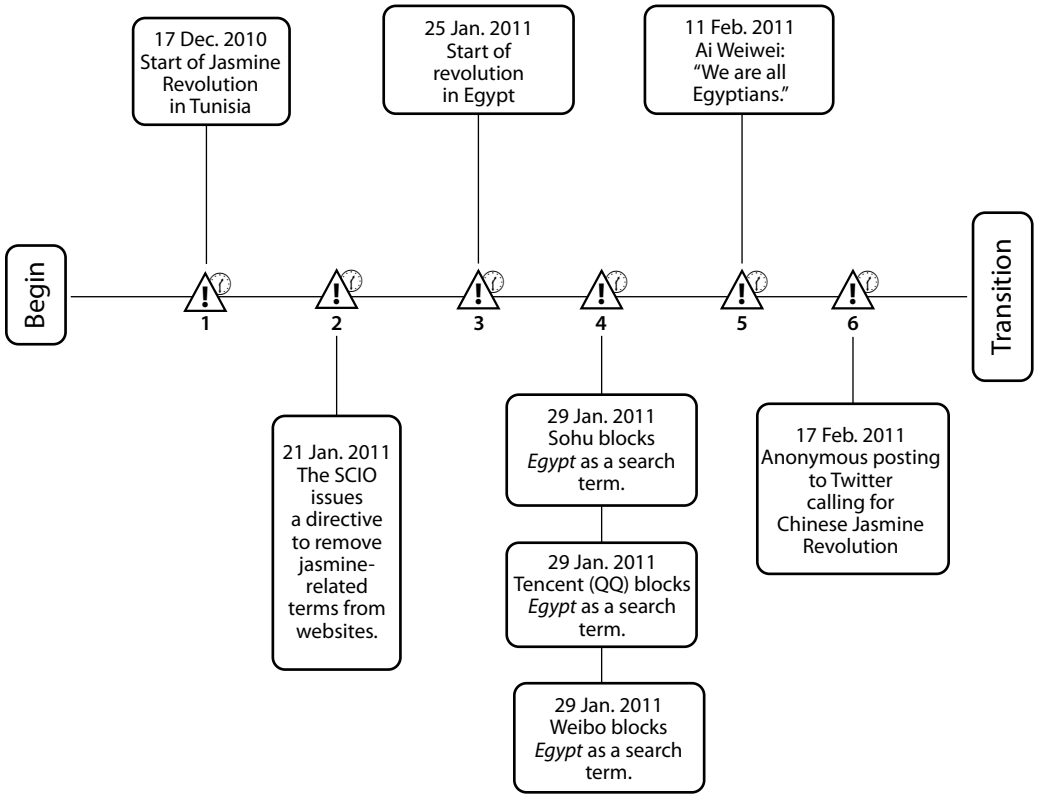

Figure 1. Monitoring and blocking timeline, 17 December 2010–17 February 2011

Blocking. On 21 January 2011, sensing a potential catalyst for domestic unrest, the Chinese SCIO issued a directive requesting all websites to "conduct strict searches of interactive spaces such as online forums, blogs, microblogs, instant message tools, and text message services. Immediately delete the phrase 'A nice bunch of jasmine' and related information."[8]

External Monitoring. As the Arab Spring continued to spread across the Middle East, actions inside the PRC showed signs of growing tension and unease with the rebellions. On 25 January 2011, the turmoil reached Egypt, causing Chinese officials to expand blocking operations.

Blocking. On 29 January 2011, three of China's most popular and highly trafficked social websites (Sohu, Tencent, and Weibo) blocked the Chinese word for *Egypt* as a search term.[9]

Internal Monitoring. On 11 February 2011, renowned Chinese artist and activist Ai Weiwei posted a message to Twitter: "Today we are all Egyptians. . . . It took merely 18 days for the collapse of this 30-year-old military regime—one which looked harmonious and stable. This thing . . . that has existed for 60 years may take several months."[10] On 3 April 2011, authorities arrested Ai Weiwei, ostensibly for committing financial crimes.

External Monitoring. On 17 February 2011, an anonymous message appeared on Twitter, calling for a Chinese revolution similar to the upheavals taking place in Egypt and Tunisia.[11] The simple posting stated that the Jasmine Revolution (named after the uprising in Tunisia) would begin on 20 February in the busy downtown areas of 13 Chinese cities. Two days later, Boxun.com, a US-based website, echoed the calls and provided specific locations for the first protests, including the McDonald's restaurant in the Wangfujing shopping district, perhaps one of the busiest commercial areas in Beijing.[12]

Phase Two: Active Defense (Attacks, Intimidation, Campaigning, and Self-Censorship)

The postings to Twitter and Boxun on 17 and 19 February, respectively, calling for real-world protests, mark the transition from the passive to active defense phase. The announcement of these physical demonstrations, visible to the general public, likely crossed a line of demarcation in the minds of Chinese officials. The active defense phase, which lasted from 19 February to at least 19 April 2011 (fig. 2), involved increased confrontation and consisted of four components: attacks, intimidation, campaigning, and self-censorship. It is important to understand that Chinese officials do not view these measures as offensive actions or operations but merely as reactions to events and efforts to restore stability. The transition to active defense does not curtail the passive measures of phase one, which continue throughout the active phase.

Attacks. On 19 February 2011, almost instantly after the call for Chinese demonstrations, patriotic or government hackers launched a distributed denial of service (DDOS) attack against Boxun.[13] Not a passive blocking operation carried out by the Great Firewall, the attack sought to limit the site's influence and shut it down (fig. 3).

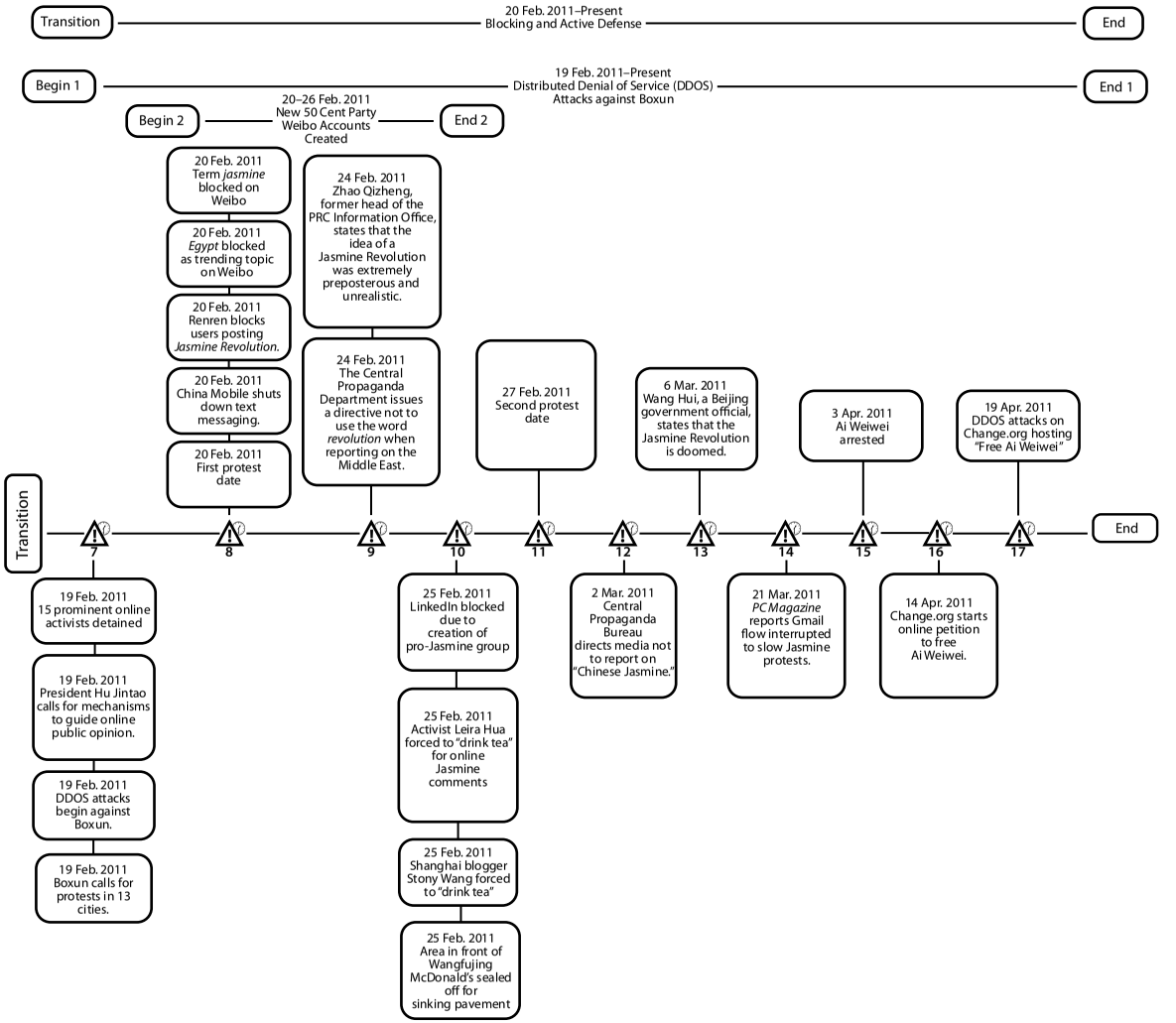

Figure 2. Blocking and active defense timeline, 19 February–present

Figure 3. Screen capture from Boxun.com announcing the attack and directing visitors to a temporary website.

Intimidation. On 19 February 2011, at least 15 prominent activists and lawyers were detained prior to the start of announced street protests.[14] Authorities invited some of them to "chat" or "drink tea" (online slang for forced interrogation), detaining and forcing additional activists to do the same over the next few months.[15] Stoney Wang, a blogger from Shanghai, offers his account of one of these interrogations:

> At first there were two relatively serious men with very rigid attitudes, who first asked me to confirm my Twitter ID, and then asked what trouble hotspots I'd been involved in lately, constantly twisting my words. I said that since they were unwilling to tell me what sensitive phrase they'd come across, I wasn't going to say either. There are a lot of these hotspots, and I'd been on Twitter for years, and posted tens of thousands of tweets: which of these was the issue now? Actually, I was laughing to myself that these three characters [茉莉花—Jasmine] had them so scared that they didn't dare say them in front of me.
>
> And then, twisting, twisting, twisting, winding me up tighter and tighter and tighter, until we reached stalemate . . . I followed what they were saying exactly: the country needs management, and the Internet also needs management in accordance with the law, so I personally had to be willing to accept a certain degree of scrutiny. Now that you've come and found me, I said, I'm certain that something I said must have been untrue; if you'll just point to it specifically, I'll take another look, and if I've made a mistake, I'll admit it, apologise, and delete it, and that'll be that, right?
>
> But throughout this winding, they just wouldn't say which was the offending phrase. In fact, their aim in coming here was quite clear: it was to intimidate me into keeping my mouth shut. From my point of view, though, this was a good opportunity for me to observe the police in the aftermath of 2/20.[16]

Campaigning. Beijing used the standard practice of having high-ranking officials make public statements to dissuade protesters. Leaders such as Hu Jintao, Wen Jiabao, Zhao Qizheng, and others called for greater

control of online opinion, dismissed the Jasmine Revolution as preposterous and unrealistic, and pronounced it doomed.[17]

The most interesting evolution in the campaign strategy came in the form of the 50 Cent Party, which derived its name from the amount of Renminbi (Chinese currency) that online commentators receive to post messages supporting the PRC government. Party commentators distract online conversations about unpopular government policies or failures.[18] From 20 to 26 February, the 50 Cent Party created fake Weibo (the Chinese version of Twitter) accounts, sometimes using the names of popular activists to make positive statements about the government. The website *China Digital Times* translated a sampling of these messages left on Weibo, aimed at virtual deception:

> @kesen4 Li Jianlong: Recently there were some police officers who told me not to participate in the "Jasmine" thing. I replied that only idiots would participate. . . .
>
> @meimeib1101: People who are saying these things [encouraging a jasmine revolution] are totally evil. Their evil intentions are abundantly clear. Isn't it the case that they themselves are attempting to be the rulers of China and then use their power to enslave us?! Don't even think about it!!!. . . .
>
> @yiwannianaini yiwannianaini: Every time there's a political revolution, it's at the expense of the common people's happiness. Everyone's got to open their eyes. . . .
>
> @wangwei7509 wangwei: Those of you always going on about how bad the Communist Party is, why don't you try governing 1.5 billion people for a bit? Winning the approval of the vast majority of people as they have is an amazing achievement! Not everyone gets along in America, either: why do you think there's so much crime there?[19]

Self-Censorship. Documenting specific incidents of self-censorship with regard to the Jasmine Revolution is difficult; nevertheless, it is known that people who operate websites inside China commonly engage in this practice. During a normal day, website operators remain cautious about posting sensitive topics, going on heightened alert when directives from the SCIO and Propaganda Bureau begin circulating. Danwei.org conducted interviews with several Chinese bloggers, summing up the most powerful argument for self-censorship: "To run a website hosted in China legally, you need an Internet Content Provision License—an ICP license. And if you have one of those, you don't want to lose it because then you won't be able to run a website. So most websites will actually censor themselves. They

are often guessing about what will annoy the government, and they will take down content that they think may get them into trouble."[20]

Monitoring and Blocking. On 20 February 2011, the presence of large concentrations of police officers in the Wangfujing shopping district demonstrated that the authorities had kept abreast of the online calls for protests and were prepared to halt organized gatherings. Furthermore, on the same day, Weibo blocked the term *jasmine* and kept *Egypt* off the trending list; Renren (China's Facebook) blocked users posting the term *Jasmine Revolution*; and China Mobile shut down text messaging.[21] On 24 February, China's Central Propaganda Department issued the following directive:

> Media reports on the current changing situation in the Middle East must use standard copy sources. Reports cannot have the word "revolution" (*geming*). Regarding the reasons for the emergence of these mass protests, nothing can be reported regarding demands for democracy or increases in commodity prices. Reports also cannot draw connections between the political systems of Middle Eastern nations and the system in our country. In all media, when the names of the leaders of Egypt, Tunisia, Libya, and other countries are given, the names of Chinese leaders cannot appear next to them.[22]

By 25 February 2011, the area in front of the Wangfujing McDonald's was sealed off with signs saying that the area was under construction due to sinking pavement.[23] On the same day, China blocked LinkedIn, a professional networking website, after the establishment on the site of a pro–Jasmine Revolution group advocating that Tunisia's Jasmine Revolution spread to China.[24] On 2 March 2011, China's Central Propaganda Bureau issued a directive to media outlets not to report on "Chinese Jasmine."[25] On 21 March 2011, Google issued a statement that a government blockage designed to look like a problem with Gmail had disrupted its e-mail distribution in China. Reportedly, this blockage was tied to the Jasmine Revolution.[26]

Attacks. On 14 April 2011, responding to Ai Weiwei's arrest, the US-based website Change.org started an online petition calling for his release. Attracting high-profile sponsors from the art world such as the Guggenheim, the Metropolitan Museum of Art, and the Tate Museum, the petition went viral and drew more than 124,000 signatures. On 19 April 2011, the website began experiencing DDOS attacks.[27]

Summary and Conclusion

Viewing China's cyberspace as perhaps the natural successor to a real-world gathering place for dissent, one could see it as the potential venue for a virtual Tiananmen. From Beijing's perspective, the digital landscape is inhabited with millions of young nationalists and activists who discuss explosive topics that could lead to revolutionary zeal. Large social-networking websites such as Tencent, Sohu, Weibo, and Renren are the public squares; cell phones and online forums serve as platforms that could launch these virtual citizens into flesh-and-blood mobs taking to the streets. For these reasons, over the last 17 years, PRC officials have incrementally increased and perfected the government's ability to implement cyber control across the full spectrum of Chinese cyberspace. These control mechanisms range from human to machine, cyber police to software. They appear to be sequenced in a two-phase operation made up of seven primary components.

Although this case study of the Jasmine Revolution covered a specific time period, phase one (passive defense) operations likely occur daily. External monitors would need to maintain a constant vigil for outside events that could cause internal unrest and quickly disseminate information to national-level decision makers with the authority to set countermeasures in motion. The SCIO would then issue guidance and directives to subordinate units, informing them of the words and phrases to restrict and the topics to declare off limits. Internal monitors would have to become twice as vigilant, observing the effects of external influences and keeping watch on internal dynamics. Filtering software could block and record the volume of censored words running across the web, but it probably would not add much context, intensity, or direction. Human analysts would have to evaluate the subjective nature of these types of postings.

It is difficult to ascertain the metric used by Chinese officials to move beyond passive defense; clearly, however, some sort of catalyst signals the need to escalate defensive measures into the active stage. In the case of the Jasmine Revolution, the call for demonstrations in 13 major cities throughout China represented the final act that brought about a stepped-up response. However, the postings alone probably did not tip the scale. Internal monitoring must have shown enough widespread reaction to the Jasmine Revolution to warrant action. The exact formula of online activity and increased calls for civic initiative that determines the tipping point remains unknown—but likely

exists. When a situation crosses the line, authorities add the four components of active defense (attacks, intimidation, campaigning, and self-censorship) to the passive measures of monitoring and blocking.

The decision to launch DDOS attacks against offending websites, perhaps to restrict their ability to reach a wider audience, appears contingent upon their location outside China. As with passive measures, the websites could have been blocked or search results skewed and filtered. Instead, government officials needed to isolate and punish the parties involved, perhaps judging them the most egregious key nodes in the publicity battle for world opinion. Further, time sensitivity seems to have played a part in the risk-management factors for launching the attacks. Although DDOS attacks can last for days or weeks, normally they prove ineffective beyond a certain length of time because website administrators can block attacks on Internet provider addresses or set up an alternate site. Paralyzing or delaying the harmful information would also be a high-priority objective of Chinese authorities.

Inviting prominent bloggers and activists to "drink tea" brings about the destruction of individual anonymity and the mental safety that protection affords. This type of pressure reveals the state's ability to track and monitor the activist even in cyberspace and highlights the fact that postings contrary to official positions have real-world consequences. Harassment and thinly veiled threats used in this manner can dampen and deter future involvement in actions against the state. As with other methods, intimidation is not designed to be completely effective; rather, it is used to prevent and contain.

Campaigning involves the blending of traditional and new-age media exploitation to send signals for halting certain types of behavior the state deems inappropriate or harmful. High-level government officials make comments through the traditional media that will bleed over into online social networks and forums to influence, guide, and direct the populace. Establishment of the 50 Cent Party creates the illusion that the government enjoys popularity where it may not exist. The weight or number of commentators supporting the government position can also make the current cause appear to lack widespread appeal. Engaging other people online enables members of the 50 Cent Party to take the conversation off-thread, distract from the original argument, and thus thwart reaching a consensus for action.

Self-censorship has been a Chinese cultural trait dating back hundreds of years, and the government has developed a vehicle to enhance this practice in the form of the Internet Content Provision License. Failure to properly censor one's own content or those of people commenting on one's website could result in suspending the license and, ultimately, shutting down the website. Threats such as denial of access will result, either consciously or subconsciously, in a moderating or watering down of ideas, removing a certain percentage of passion from the debate. The ultimate goal, once again, is to ensure that the underlying fuel does not spark and become a full-blown fire.

Though not a part of the efforts to defuse the Jasmine Revolution, preemptive reactions and defensive measures could become potential evolutions in this process. If the state decides to arrest a prominent dissident like Ai Weiwei in the future, why not attack a site such as Change.org before its petition gains popularity or shut down Boxun's ability to organize protests before it posts dates, times, and locations? It would be unrealistic to think that the Chinese government does not track and keep records of these types of websites. Could that effort also extend to physical intimidation outside China's sovereignty? The ability to organize pro–Chinese government operatives similar to the 50 Cent Party outside the nation could dissuade some organization from participating in anti-Chinese activities. Preemptive efforts need not necessarily be destructive or coercive in nature; they could take the form of influence or positioning, manifested by gaining financial interest in a potential adversary's online medium or control of an Internet service provider. As with domestic control, we are likely to see incremental changes as Beijing learns to manipulate its international message.

Notes

1. Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005), 202–3.
2. Scott Henderson, *The Dark Visitor* (Fort Leavenworth, KS: Foreign Military Studies Office, January 2007), 150–52.
3. Ibid., 151.
4. Wu Jianbin and Meng Qiang, "The People's Liberation Army Foreign Language Institute Pushes Educational Transformation" (in Chinese), *PLA Daily*, 30 December 2009, http://www.allzg.com/n64355c40.aspx.
5. Li Huamin and Pu Zhao, "Troop Unit Expands International Strategic Vision," *PLA Daily*, 8 June 2011, http://eng.mod.gov.cn/DefenseNews/2011-06/08/content_4245818.htm.
6. "Tunisia Suicide Protester Mohammed Bouazizi Dies," BBC, 5 January 2011, http://www.bbc.co.uk/news/world-africa-12120228.
7. This article uses the term *blocking* rather than *censorship* to denote the Chinese government's perspective that such references constitute an attack against its authority and sovereignty. Further, the Great Firewall filtering system carries out government directives for blocking certain words and phrases.

8. "Latest Directives from the Ministry of Truth, February 17–24, 2011 (UPDATED)," *China Digital Times*, 23 February 2011, http://chinadigitaltimes.net/2011/02/latest-directives-from-the-ministry-of-truth-february-17-21-2011/.

9. Michael Kan, "China Microblogs Block Chinese Word for 'Egypt,'" *PCWorld*, 29 January 2011, http://www.pcworld.com/businesscenter/article/218185/china_microblogs_block_chinese_word_for_egypt.html.

10. Dale Swartz, "Jasmine in the Middle Kingdom: Autopsy of China's (Failed) Revolution," *American Enterprise Institute for Public Policy Research*, no. 1 (April 2011): 2, http://www.aei.org/files/2011/04/15/AO-2011-04-No-1-g.pdf. ("This thing" refers to the Chinese Communist Party.)

11. Interestingly, some individuals speculated that the original message was a joke sent out over @mimitree0 (a Twitter robot), which allows anyone to post anonymous messages. The Western press and Chinese police took the calls seriously, inadvertently setting off the Jasmine Revolution. Richard Zhang, "Jasmine Revolution in China?," Chinatweeps.com, 22 February 2011, http://chinatweeps.com/archives/jasmine-china.html.

12. Michael Martina and Royston Chan, "Chinese Police Use Protest Clampdown as a Show of Force," *China Post*, 28 February 2011, http://www.chinapost.com.tw/china/national-news/2011/02/28/292723/Chinese-police.htm.

13. Boxun, "Boxun's Main Website Is under Serious DDoS," 18 February 2011, http://www.boxun.us/news/publish/usa_news/Boxun_s_main_website_is_under_serious_DDoS.shtml.

14. Sophie Beach, "Activists Detained as China Web Users Call for 'Jasmine Revolution' (Updated)," *China Digital Times*, 19 February 2011, http://chinadigitaltimes.net/2011/02/china-web-users-call-for-jasmine-revolution/.

15. "Drink Tea," *China Digital Times*, accessed 5 January 2012, http://chinadigitaltimes.net/space/Drink_tea.

16. Samuel Wade, "@StonyWang: Forced to Drink Jasmine Tea," *China Digital Times*, 25 March 2011, http://chinadigitaltimes.net/2011/03/stonywang-forced-to-drink-jasmine-tea/.

17. Official statements taken from the following collection of websites: *NewsDaily*, http://www.news-daily.com/stories/tre74h7n1-us-baidu-censorship-lawsuit/; *Financial Times*, http://www.ft.com/intl/cms/s/0/e7a66d8a-422d-11e0-8b34-00144feabdc0.html#axzz1PSklsVVY; *Taipei Times*, http://www.taipeitimes.com/News/front/archives/2011/02/25/2003496736; and Reuters Africa, http://af.reuters.com/article/worldNews/idAFTRE7250UF20110306.

18. Michael Bristow, "China's Internet 'Spin Doctors,'" BBC News, 16 December 2008, http://news.bbc.co.uk/2/hi/7783640.stm.

19. Xiao Qiang, "Remarkable Quotes from the Fifty Cent Party: Anti-Jasmine Revolution Tweets," *China Digital Times*, 28 February 2011, http://chinadigitaltimes.net/2011/02/fifty-cent-tweets-a-collection-of-anti-jasmine-revolution-messages/.

20. Commentary by Jeremy Goldkorn, in *Dancing with Shackles On* (video), Danwei.org, 1 March 2011, http://www.danwei.org/featured_video/dancing_with_shackles.php.

21. On Weibo, as with Twitter, when a topic becomes popular, it will appear on the trending list, which can also raise the status of more people talking or posting about the subject. See Anita Chang, "Jittery Chinese Authorities Try to Stamp Out 'Jasmine Revolution,'" MSNBC, 20 February 2011, http://www.msnbc.msn.com/id/41690185/ns/world_news-asia_pacific/t/jittery-chinese-authorities-try-stamp-out-jasmine-revolution/; and Michael Kan, "China Blocks Microblogs for 'Jasmine Revolution,'" *CIO*, 21 February 2011, http://www.cio.com.au/article/377359/china_blocks_microblogs_jasmine_revolution_/.

22. *China Digital Times* translator, "Latest Directives from the Ministry of Truth, February 17–24, 2011 (UPDATED)," *China Digital Times*, 23 February 2011, http://chinadigitaltimes.net/2011/02/latest-directives-from-the-ministry-of-truth-february-17-21-2011/.

23. Kenneth Tan, "Beijing's Wangfujing Morphs into a Construction Site," *Shanghaiist*, 25 February 2011, http://shanghaiist.com/2011/02/25/beijing-wangfujing-construction.php.

24. Young-Sam Cho and Thomas Giles, "LinkedIn Site Inaccessible in China after 'Jasmine' Pro-Democracy Posting," *Bloomberg*, 25 February 2011, http://www.bloomberg.com/news/2011-02-24/linkedin-unavailable-in-parts-of-china-web-monitors-show-1-.html.

25. *China Digital Times* translator, "Latest Directives from the Ministry of Truth, March 2–7, 2011," *China Digital Times*, 8 March 2011, http://chinadigitaltimes.net/2011/03/latest-directives-from-the-ministry-of-truth-march-2-7-2011/.

26. Chloe Albanesius, "Report: China Blocks Gmail to Stop Protests," *PCMAG*, 21 March 2011, http://www.pcmag.com/article2/0,2817,2382310,00.asp.

27. Andrew S. Ross, "Change.org Attacked after Backing China Dissident," *San Francisco Chronicle*, 28 April 2011, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/04/28/BU651J81MT.DTL.