EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

ASIA CENTRE
centreasia.eu

CHINA ANALYSIS

CHINA'S EXPANDING CYBERSPACE

ABOUT

The Chinese have long been obsessed with strategic culture, power balances and geopolitical shifts. Academic institutions, think tanks, journals and web-based debate are growing in number and quality and give China's foreign policy breadth and depth.

China Analysis, which is published in both French and English, introduces European audiences to these debates inside China's expert and think-tank world and helps the European policy community understand how China's leadership thinks about domestic and foreign policy issues. While freedom of expression and information remain restricted in China's media, these published sources and debates provide an important way of understanding emerging trends within China.

Each issue of China Analysis focuses on a specific theme and draws mainly on Chinese mainland sources. However, it also monitors content in Chinese-language publications from Hong Kong and Taiwan, which occasionally include news and analysis that is not published in the mainland and reflects the diversity of Chinese thinking.

The French version of China Analysis can be accessed online at www.centreasia.eu.

Introduction
by François Godement

If China's most famous dictionary was aptly called "the sea of words", then plunging into Chinese cyberspace is like embarking on a journey in space. The West tends to see China's online world through the narrow perspective of cyberspying and hacking, a game at which China's agencies excel – even if they do leave too many fingerprints behind.

However, China's cyberspies and hackers could not be so prolific if moving in the virtual world had not become the number one activity for China's people. This has contributed to an extraordinary unification of Chinese society, as well as to an unprecedented expression of its individualism. If foreign policy constitutes less than 10 percent of any Chinese leader's agenda, it follows that more than 90 percent of issues related to the internet are domestically rather than internationally oriented. But in the longer term, the extraordinary innovation that is emerging in the Chinese web and mobile space is bound to create business models that will spread well beyond China itself, influencing the development of the sector across the entire world.

The reason for these innovations is clear: a vibrant society and its market actors are leapfrogging technical development and getting around bureaucratic rigidity by circumventing it. This is happening in all spheres, and it is taking place in China more quickly than in developed economies. To cite just one minor example, where Uber and its few competitors have had to fight pitched legal battles

against taxi corporations, dozens of similar Chinese web-based companies have revolutionised the taxi industry in China in the space of one year.

The pent-up demand for change is huge. The spread of internet payment and online funds is the best example of the trend: in eight months, a fund created by Alibaba's founder has collected more than $65 billion from individual Chinese and Hong Kong savers. Elsewhere, our sources point out how internet "manhunts" – collective investigation and pillorying of suspects – have become a tool in the fight against corruption. Microblogging has created instant courts of opinion on any topic. This has set up a system of fairly unregulated polling in a country in which the party previously held a total monopoly on the public expression of opinion.

Technology is neither good nor bad, and so the revolutionary effects of these innovations cut both ways. Internet banking and online funds are encroaching on the traditional state bank system, which has up until now relied on its monopoly to maintain huge disparities between borrowing and lending rates as well as to supply cheap funds for limitless investment. This development represents an equaliser for individual households and now offers the only way to increase household revenue while acting as a check on the frenzy for real estate, hitherto the only available piggy bank for the Chinese. But it also carries tremendous risks of under-regulation, and these risks are probably not well understood by our sources. "Human flesh searches", the gory name for internet investigations, are an affront to individual freedom and a worrying echo of the Cultural Revolution, when any individual was fair game. Yet liberals see government efforts to quell "rumours" as another attempt to put a lid on China's scandals.

It should be added that almost universal software piracy, which is carried out by companies and government units as well as ordinary users, has resulted in the world's most active virus environment on the web. It is often said that an unprotected computer will be infected less than a minute after connecting to the web in China.

By contrast to the innovation taking place among Chinese internet users and firms, China's official positions on global internet governance appear stodgy, almost a carbon copy of the Chinese stand on any transnational governance issue. The government opposes American hegemony, but maintains the unlikely goal of creating "trust". It rejects European value-laden policies, especially on internet freedom. And it emphasises each country's sovereign rights. If these standards were to be applied internationally, the global web that we take for granted (forgetting the filtering ability of our own search engines) would fragment into national spheres.

China's extraordinary wave of business and social innovations on the web will have a global impact, just as its hardware and communications producers have already had. However, it is likely that the Chinese politics of the web will continue to provide a model that will only find favour with other authoritarian regimes. Here, as in other issues, the huge contradiction inherent in China's rise is alive and well.

1. The mobile revolution and China's internet giants

Camille Boullenois

Sources:

Chen Lin, "Big changes in the world of China's internet", *Caijing*, 19 April 2014.[1]

Song Wei and Chen Qingchun, "The BAT are worried", *Caijing*, 19 April 2014.[2]

Song Wei, "The fight for the autonomy of start-ups", *Caijing*, 19 April 2014.

The internet industry in China is dominated by three big names: Baidu (百度), Alibaba (阿里巴巴), and Tencent (腾讯). Baidu specialises in "search" (搜索, *sousuo*), Alibaba in "e-commerce" (电商, *dianshang*), and Tencent in "social networks" (社交, *shejiao*). Together, these companies are referred to as the BAT. For the past two years, the BAT have had to adjust to face the same mobile revolution that is shaking up the IT industry worldwide. Their positions within China's internet sector have been turned upside down by the need to come to terms with the rapid shifts in the industry. Some observers predict that new, mobile-era companies will emerge to overtake the old guard. Others say that the BAT have become increasingly aggressive in their efforts to adapt to the new competition.

A continually changing ecosystem

For two years now, the BAT have been seriously concerned about the risk of losing their internet monopoly because of the the mobile web revolution. "Mobile traffic" (移动流量, *yidong liuliang*) is inherently more scattered and harder to control than desktop traffic. Song Wei and Chen Qingchun say that the success of the BAT will be determined by their ability to build "open platforms" (开放平台, *kaifang pingtai*) that can integrate their various products.

Since 2011, the fear of being overtaken by more innovative companies has pushed the BAT to adopt extremely aggressive strategies to preserve their control of the market. Over the past three years, a greater number of mergers and acquisitions have taken place than in the entire previous decade, and the economic importance of the mergers has also been greater than in previous years. Within these three years, Alibaba has acquired or become a shareholder in 30 companies, Tencent in 40 companies, and Baidu in more than 30 companies. Each of the internet giants has been in fierce competition with the others for all these acquisitions, which has resulted in over-inflated purchase prices.

Each of the three major companies has its own strengths and weaknesses within this constantly changing "internet ecosystem" (互联网生态, *hulian wang shengtai*).

Baidu

Baidu was founded in 2000 and is now the largest search engine in China. It has developed its own applications in search, online mapping, and mobile assistance, as well acquiring e-commerce (Nuomi, 糯米), travel (Qunar, 去哪儿), and video (iQiyi, 爱奇艺) applications. Baidu currently owns 14 applications that together reach over 100 million users. In April 2014 the company launched the Baidu Wallet (百度钱包, *baidu qianbao*), giving it a presence in the mobile payments market. Baidu also plays an important role in the O2O sector (online-to-offline, which involves online maps in particular). This capability is a major asset in its competition with the other two giants. In 2013 Baidu still had a 72 percent market share in mobile search. However, it is now struggling not to lose its footing, following the development of a mobile search market that is "intrinsically fragmented" (移动互联网流量天生是分散的, *liudong hulian wang tiansheng shi fensan de*). Because of this, even though Baidu was the most important internet company when desktop computers were the main means of internet access, its share value has experienced a relative decline in recent years. The company is now worth just half of competitor Alibaba's estimated value.[3]

Baidu's answer to the challenge has been to develop LBS (location-based services). These services integrate search, online mapping, and social networking, and aim to redefine "search" for the mobile environment. Baidu has put significant investment into the project, which has helped it to attract large amounts of traffic to its LBS, and in particular, to its mapping and e-commerce applications, Baidu Maps and Nuomi.

For this reason, Song and Chen say, many observers now see Baidu as the most innovative of the BAT and, as a result, the best placed to stay on top of future trends. However, Song and Chen say that Baidu remains "conservative" (保守派, *baoshou pai*) in its acquisitions. The company spent a lot of money to acquire a controlling stake in the large mobile app store, 91 Wireless, but it has generally not tried to compete with the others in the race to acquire start-ups. This means that it is now at risk of being marginalised by the other two internet giants. Even so, Song and Chen say that the company's large cash reserves should allow it to catch up by acquiring several companies in 2014.

Alibaba

Alibaba is the biggest player in Chinese e-commerce. It is commercially aggressive and it has grown rapidly – 2.27 times faster than competitor Tencent. In 2013 its revenues exceeded those of both Baidu and Tencent.

[1] Chen Lin is a journalist for *Caijing*.

[2] Song Wei and Chen Qingchun are staff journalists for *Caijing*.

[3] In March 2014 Alibaba announced that it would list on the US stock exchange. With an estimated value of between $150 billion and $200 billion, the listing will be one of the most valuable in history.

Founded by Jack Ma in 1998, Alibaba has benefited from the unique offering of its main e-commerce site, Taobao. Unlike US company Amazon, which sells directly to consumers, Taobao leases space on its website to vendors and advertisers. It does not take responsibility for product quality, shipping, or after-sales support. Through its Taobao and Tmall sites, Alibaba currently controls 80 percent of China's online retail market, equivalent to 5 percent of the country's total retail sales. And its Alipay site gives it a key position in the online payment market.[4]

The mobile revolution has presented Alibaba with some serious challenges. The company has struggled to create an open portal capable of integrating its different products. In spite of significant investment, the company's Aliyun (阿里云) mobile operating system did not take off. And Song and Chen argue that the constant upheaval in Alibaba's offline sector, including changes in CEO in March 2013 and in March 2014, has prevented the establishment of clear guidelines for growth.

Song and Chen interview Long Wei, the co-founder of ratings and review site Dazhong Dianping (大众点评), who says that Alibaba must also find a way to innovate within its "'light commercial' model" ("轻商业"的模式, *qing shangye de moshi*). The important O2O sector requires much larger and better-supplied sales teams than Alibaba currently uses. However, Song and Chen interview a former Alibaba vice-president who says that the group is reluctant to make changes to a model that has so far enabled it to make huge profits.

To try to hedge against these uncertainties, Alibaba has acquired and invested in up-and-coming companies such as group deal site Meituan (美团), location-based instant messaging service Momo (陌陌), mobile browser UCWeb, microblogging site Xinlang Weibo (新浪微博), and online mapping app AMAP (高德).

Alibaba wants to create infrastructure that combines both online and offline elements. To this end, in March 2014 Alibaba announced its acquisition of a 9.9 percent stake in the bricks-and-mortar Yintai (银泰) retail chain. However, this type of partnership may cause problems, because the interests of the internet majors and of offline groups may differ. Song and Chen note that it may be difficult to safeguard the interests of Yintai's shops and website at the same time as protecting Alibaba's global interests.

Tencent

Tencent was founded in 1998. The company owns the two largest social networks in China, QQ and Weixin, and it is also the world's largest video game company. QQ has around 800 million users in China. The estimated value of Weixin is around $64 billion, three times the price that Facebook paid to acquire messaging application WhatsApp in February 2014. But most of Tencent's income comes from its innovative freemium online gaming business model: Tencent offers free-to-play games in which players make microtransactions to improve their gaming experience.

The freemium model is the basis of Tencent's current success, but slower growth in the mobile gaming market may soon reduce profits. Song and Chen interview the CEO of social shopping site Mogujie (蘑菇街), Chen Qi, who says that Tencent will have a hard time monetising its social networks, even though they are formidable communication tools. Going forward, monetisation is one of the key components of the company's strategy. Song and Chen quote a high-ranking group employee as saying that QQ's online gaming and entertainment services make it the company's most promising application for monetisation. More caution will be needed in adding online payments to Weixin, if its popularity is not to suffer.

Since 2011, the fear of being overtaken by more innovative companies has pushed the BAT to adopt extremely aggressive strategies to preserve their control of the market.

Tencent's acquisitions strategy has allowed it to compete with Baidu and Alibaba on their own ground. In September 2013, the company spent $448 million acquiring a stake in Sogou (搜狗), China's third-largest search engine. In March 2014 it agreed a partnership with Jingdong (京东), one of the largest e-commerce companies in China, which should help Tencent to compete with Alibaba's Taobao.

Potential challengers

Some second-tier companies that were created as a result of the mobile revolution are attempting to challenge the dominance of the BAT. These innovative companies are experiencing exceptional growth.

Smartphone manufacturer Xiaomi (小米) is one of the biggest potential threats to the BAT companies. Xiaomi has only recently launched e-commerce operations and begun to construct a mobile internet platform. But its dominance in the manufacture of internet terminals has given it a significant advantage in the technological battle that will help to decide the fate of the BAT.

Qihoo 360, which provides antivirus software, technical support, and internet routers, has developed a unique entry point for mobile internet. Its rapid growth and its new search engine also give it the tools to provide real competition to the BAT.

[4] See Agatha Kratz's article in this issue for further information on this subject.

Finally, some companies in the new market of "local services" (本地服务, *bendi fuwu*) are also growing fast and could produce a future internet giant. These companies include Dazhong Dianping and Meituan. Both companies have agreed to partnership terms with the BAT, but Long Wei tells Song and Chen that the two companies have retained enough independence to allow them to continue autonomous growth.

Start-ups, or how to grow in the shadow of the BAT

Below these emerging powerhouses, many smaller start-ups have original product offerings and strengths. However, the BAT's aggressive policies have often worked to prevent their development.

The "taxi wars" (打车大战, *dache dazhan*) are a good example of how the BAT has discouraged the growth of smaller companies. In 2012, around 30 companies created applications to connect customers with taxis in major Chinese cities. Alibaba invested in one, Didi Dache (嘀嘀打车), and Tencent in another, Kuaidi Dache (快的打车). The others obtained investments from independent venture capital funds. Didi Dache and Kuaidi Dache benefited from substantial subsidies and huge traffic from their BAT patrons, and after a short price war, the companies that were not backed by the BAT majors collapsed.

Song and Chen say that the two companies supported by the internet giants did not fare much better than their competitors. Kuaidi Dache and Didi Dache quickly became empty shells, dependent on the parent company and with no users of their own. One start-up founder interviewed by Song says that any company facing a buy-out proposal should ask whether the company is likely to become an essential part of the buy-out group, or whether it will simply be subsumed by it.

Even in this difficult environment, some companies have succeeded in growing in the shadow of the internet giants. Mogujie, an e-commerce site that redirects users to Taobao and Tmall, is one such example. Alibaba's buy-out attempts have all failed, and the partnership agreed between Mogujie and Tencent's Weixin in August 2013 allowed the start-up to retain some autonomy.

However, this kind of independent growth is becoming increasingly rare. An investor interviewed by Song Wei says that the internet giants are replacing market forces in determining the success or failure of start-ups. In this way, the BAT are seriously holding back innovation.

The next few years will be both difficult and pivotal for the BAT. The three giants will have to deal with competition within their own ranks as well as from up-and-coming internet companies. At the same time, they will have to adapt to a mobile market that is not a natural environment for the internet giants.

2. Chinese perspectives on cyber security and international relations

Camille Liffran

Sources:

Jiang Li, Zhang Xiaolan, and Yu Feibao, "Deadlock in international cooperation regarding cyber security and its solutions," *Xiandai guoji guanxi – Contemporary international relations,* No. 9, 2013.[5]

Tan Youzhi, "Worldwide governance of cyberspace: international trends and Chinese approach," *Shejie jingji yu zhengzhi – World economy and policy,* No. 12, 2013.[6]

Lang Ping, "Cyber security: new rivalries and new challenges," in "Report on security and world governance 2014", *Guoji xingshi huangpishu – Yellow book on the international situation*.[7]

Internet attacks have become more and more frequent over the past few years, making "cyber security" (网络安全, *wangluo anquan*) a major concern for the entire international community. Between 2012 and 2013, cyber attacks worldwide rose by nearly 42 percent.[8] The attacks have grown in scale and have had increasingly severe economic consequences. Moreover, new scandals about actual or alleged international cyber-espionage have emerged, including the February 2013 revelations from United States-based company Mandiant and the allegations made by Edward Snowden beginning in May 2013.[9] These scandals have caused serious diplomatic tensions and raised concerns about the potential for "cyber conflict" (网络战争, *wangluo zhan*). Now, with the US leading the

[5] Jiang Li is a professor at Century College, Beijing University of Posts and Telecommunications. Zhang Xiaolan is a professor at the University of International Relations in Beijing. Yu Feibao is a researcher at the China Institute of Contemporary International Relations.

[6] Tan Youzhi is a professor at the School of International Relations at the University of International Business and Economics in Beijing.

[7] Lang Ping is a researcher at the Institute of World Economics and Politics at the Chinese Academy of Social Sciences.

[8] Lang Ping cites these statistics from a report on cyber threats published in April 2013 by US company Symantec. See Symantec, "Internet Security Threat Report 2013", Volume 18, April 2013, available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

[9] In February 2013 Mandiant revealed that a large number of cyber attacks perpetrated against the US were the work of Chinese hackers who may have been working with the Chinese People's Liberation Army. The Chinese cyber pirates had stolen confidential information from at least 141 American companies and institutions. These revelations were the origin of a series of frictions between China and the US and caused a debate in the US on the threat of China as a cyber power. The Snowden affair regards revelations made by Edward Snowden, a former consultant for the National Security Agency (NSA), on the PRISM and XKeyscore programmes, two large-scale espionage programmes implemented by the NSA aimed at collecting electronic and telephonic communications. A number of foreign institutions, including European institutions, embassies, and the United Nations building, were found to be the target of taps. These revelations provoked international outcry and elicited strong condemnations from foreign governments.

way, several countries have begun to integrate cyber security into their foreign policy strategies, and in so doing, have set off a cyberspace "arms race" (军备竞赛, *junbei jingsai*).[10] But at the same time, various actors on the international stage stress the need to actively co-operate on virtual security and to implement "global cyberspace governance" (网络全球治理, *wangluo quanqiu zhili*). In recent years, many new co-operation agreements have been signed between governments and within international organisations such as the European Union and NATO.

The Chinese government also recognises the importance of the challenges of cyber security. China has emerged as a genuine "cyber power" (网络大国, *wangluo daguo*) – Tan Youzhi cites a report published in July 2013 by the China Internet Network Information Centre saying that China had more than 590 million internet users in 2013. The government has begun to more actively engage with international cyber security, especially since the 18th Party Congress in December 2012. As the issue has become more important, Chinese media and academic experts have begun to analyse cyber security. Most of the experts cited here echo the government's positions on the subject, while also trying to analyse the international situation without indulging in too much anti-Americanism. The authors explore the many obstacles to effective international co-operation on cyber security and advocate the implementation of equitable global cyberspace governance. They also examine potential future responses to cyber security challenges.

International co-operation is incomplete

Tan Youzhi says that there is "a universal request and common demand" (一种普遍诉求与共同期待, *yi zhong pubian suqiu yu gongtong qidai*) for global cyberspace governance. But the Chinese experts all agree that efforts to develop international co-operation on cyber security have so far been limited and superficial. Jiang Li, Zhang Xiaolan, and Yu Feibao say that at the moment, co-operation is just an "empty shell" (虚多实少, *xu duo shi shao)*. There is little agreement on international co-operation, and several key issues, such as cyber-espionage and military cyber security, have not been dealt with in bilateral discussions. Most international co-operation mechanisms and bodies, such as the ITU and ICANN, only co-ordinate on technical matters.[11] Jiang, Zhang, and Yu say that the co-operation that exists is not very effective. Different countries have ideological standpoints, even among members of the EU, and governments want to preserve their own "cyber sovereignty" (网络主权, *wangluo zhuquan*).

Effective co-operation is held back by the intense competition in cyberspace between different international actors. Reflecting the logic of international relations, the internet has become the battlefield in a harsh struggle for "cyber power" (网络权力, *wangluo quanli*), both in military and strategic terms and also in terms of soft power. Jiang Li, Zhang Xiaolan, and Yu Feibao talk about the possibility of a "cyber Cold War" (网络冷战, *wangluo lengzhan*). The authors describe a digital competition between "a superpower and two large camps" (超多强，两大阵营, *yi chaoduoqian, liang da zhenying*). The superpower is the US, which maintains a hegemonic position on the worldwide web, and, Tan Youzhi says, has taken cyber security to a "quasi-hysterical level" (几近癫狂的地步, *jijin diankuang de dibu*). The first large camp consists of the developed countries that are US allies. The second camp is made up of emerging countries, which are struggling to make their voices heard. The authors say that the current distribution of cyber power throughout the world corresponds to the distribution of political and economic power since the end of the Cold War. They see the imbalance of power between different countries as a fundamental obstacle to true global cyberspace governance.

Reflecting the logic of international relations, the internet has become the battlefield in a harsh struggle for "cyber power".

Tan Youzhi thinks that cyberspace remains an "unexplored territory, not governed by common standards" (一个没有形成全球共同规范的未知领域, *yi ge meiyou xingcheng quanqiu gongtong guifan de weizhi lingyu*). He says that this lack of governance reinforces the "digital gap" (数字鸿沟, *shuzi honggou*) that separates developed countries from the others. Lang Ping suggests that the shortcomings in co-operation on cyber security are mostly because the problem has not been around for a long time. He does not believe that an open cyber war is likely. He says that the tensions in the area relate mainly to economic security and that "conflicts remain within a controllable framework" (这些冲突都会停留在可控的范围内 , *zhe xie chongtu dou hui tingliu zai kekong de fanwei nei*). Even so, he says there is cause for concern: "if no progress is made, for example, in establishing internet standards, the digital world will most certainly face the risk of disintegration." (如果不能够在制定互联网标准等方面取得进展，互联网世界很可能会面临分崩离析的风险, *ruguo bu nenggou zai zhiding hulianwang biaozhun deng fengmian qude jinzhan, hulianwang shejie hen keneng hui mianlin fenbenglixi de fengxian*). Therefore, building co-operation and rethinking the model of internet governance is a matter of urgency.

[10] US President Barack Obama has defined cyber threats as "one of the greatest challenges for states' security and economic development in the twenty-first century". In May 2009 the US established a Cyber Security Office, and in May 2011 the White House published an "international strategy for cyberspace". See "Remarks by the President on Securing our Nation's Cyber Infrastructure", The White House, Office of the Press Secretary, May 29, 2009. Available at: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[11] The International Telecommunication Agency (ITU) is the specialised UN agency in charge of co-ordinating global regulations for information and communication technologies. ICANN (the Internet Corporation for Assigned Names and Numbers) is a US company in charge of the administration of digital internet resources, particularly domain names.

Creating a new governance model for cyberspace

The authors do not believe current governance models are effective. Jiang Li, Zhang Xiaolan, and Yu Feibao describe the US's preferred model as being based on the "theory of hegemonic stability" (霸权稳定论, *baquan wending lun*). This model consists of reforming the system in such a way as to maintain US leadership at all costs. However, this system would be "contrary to international justice and equality" (违国际公平正义, *wei guoji gong ping zhengyi*). Moreover, it would be unstable and could not last forever. Europe's preferred model would aim at reinforcing existing mechanisms, but it is also unworkable, because it is based on "Western values" (西方价值, *xifang jiazhi*) and is therefore impossible to apply across the entire world. The authors believe that the governance model proposed by emerging countries, based on a more balanced and fairer distribution of digital resources and governance rights, would be more respectful of the principles of the United Nations and of each country's independence and sovereignty. Nevertheless, the experts believe this model would be difficult to adopt, because it would lack legitimacy in the eyes of other international partners.

In view of this impasse, the Chinese researchers believe it is essential to move beyond antagonism and to prepare a new governance model based on "mutual respect and trust" (互相尊重, 包容互信, *huxiang zunzhong, baorong huxin*). Lang Ping and Tan Youzhi say that traditional governance concepts need to be re-evaluated, because, Tan Youzhi says, these concepts do not fit with the nature of the internet. And any effort to define new governance models should take account of the deep changes to the traditional balance of power in the world, as evidenced by the emergence of new powers such as China.

Chinese cyber security and Chinese soft power

Jiang, Zhang and Yu say that China has a key role to play in promoting "common and inclusive global internet governance" (全球网络的共享共治, *quanqiu wangluo de gongxiang gongzhi*). The writers say that China must implement a cyber-security strategy as a matter of urgency. Tan Youzhi says that China is a "late developing country" (后起之国, *houqi zhiguo*) in terms of cyber security. Digital security was not included in the foreign policy framework until March 2011, when China's 2010 defence white paper was published. This delay is partially responsible for China's bad reputation on cyber security. In the absence of new and strong measures to address the issue, China will continue to be "the one that is wrongly accused instead of others" (无辜的'被告'带人受过, *wugu de beigqo dairen shouguo*).

Jiang, Zhang, and Yu believe that China must prepare a "macroscopic strategy" (宏观战略, *hongguan zhanglüe*) for security. It should improve legislative and regulatory institutional structures and strengthen the country's capacity for technological innovation. Jiang Li, Zhang Xiaolan, and Yu Feibao believe that China must not focus on cyber-weaponry, but instead on developing China's digital soft power through industrial and scientific advances. China must also work to reinforce flexible, pragmatic international co-operation that does not involve a struggle for ideological influence. To do so, it should strengthen ties both with Russia, its strategic cyber security partner, and with the US. In spite of the serious tensions between China and the US, it is essential that Beijing build a relationship of mutual trust with Washington.

The author's points of view are close to the official government position on the subject. Since cyber security's place within international relations is still relatively new, it is too soon for more diverse opinions on the issue to appear in China. Moreover, while the writers comment on the need for a new international governance model for cyberspace, they fail to clearly define what this model would look like. The authors' message is mostly that China must keep pace with international trends in the field of cyber security.

3. Online finance: a challenge to traditional banking

Agatha Kratz

Sources:

Zong Liang and Xiong Qiyue, "How are commercial banks dealing with online banking?", *Caijing*, 14 April 2014.[12]

Song Wei, Liu Qilin, and Xie Lirong, "Two giants of online banking: rebuilding the internet and finance sectors", *Caijing*, 6 January 2014.[13]

Sheng Hong, "The significance of Alipay is not technological, it is institutional", Unirule Institute of Economics, 9 April 2014.[14]

Chen Long, "Looking at Yu'e Bao from a historical perspective", *Shanghai zhengquan bao – Shanghai Securities Newspaper*, 22 April 2014.[15]

Chen Long, "The future of Yu'e Bao", *Xin shiji – New Century*, 10 March 2014.

Fan Yifei, "Online finance: challenges and opportunities", *Xin shiji – New Century*, 11 February 2014.[16]

In the last decade, massive internet companies such as Alibaba, Tencent, and Baidu have taken over the Chinese market.[17] These companies are gradually beginning to move into "online finance" (互联网金融, *hulianwang jinrong*). They now offer a wide variety of products and services that have traditionally been provided by commercial banks. Will online finance radically change the Chinese financial sector? Or will its impact be limited, and will the new companies simply act as a complement to traditional banking?

Zong Liang and Xiong Qiyue say that the online finance sector consists of non-financial companies that offer financial services to their customers. Among these services, the most popular are "third-party payments" (第三方支付, *disanfang zhifu*). These services are particularly useful for internet users because they facilitate secure payments for online purchases and reduce the risks of e-commerce transactions. For this reason, e-commerce companies are most interested in developing them.

The largest provider of third-party payments is Alibaba's subsidiary, Alipay (支付宝), a Chinese counterpart to the American company, PayPal. In 2013, third-party payment activities amounted to 5,373 billion yuan (€629 billion) in transactions, an increase of almost 50 percent on the previous year. Mobile transactions accounted for 1,280 billion yuan (€150 billion) in 2013, an increase of more than 700 percent on the previous year, making up 23 percent of all third-party payments. Other services, such as P2P (peer-to-peer) lending platforms and "crowdfunding" (众筹, *zhongchou*), have also experienced significant growth. P2P lending platforms gave out 89.7 billion yuan in loans in 2013, and there are now 21 Chinese crowdfunding platforms.

Sheng Hong says that these internet services meet a real financial need that traditional commercial banks are not fulfilling. They provide financial intermediation, interest rate liberalisation, active management of savings, debt securitisation, and other useful services. The transfer of banking activity to the internet is a direct result of the monopolistic and over-regulated structure of the Chinese financial sector. Because they do not have to face competition, traditional banks have not invested in providing innovative services to individuals or companies. Unlike Alipay and P2P lender Alixiaodai (literally "Ali small loans", 阿里小贷), Chinese banks offer few online payment services or loans to small- and medium-sized enterprises. Alixiaodai, on the other hand, has already provided loans for 600,000 small- and medium-sized enterprises, at a total of 150 billion yuan (€17.6 billion), according to Zong and Xiong. These new companies and services could have a transformational effect on China's financial landscape.

Online finance: opportunity or threat?

Fan Yifei believes that online finance represents an opportunity for traditional finance institutions, because it increases the number of supply channels available for financial services. Banks can use the internet to offer services that are currently expensive to run, such as teller transactions, which would become far more affordable if provided through online platforms. The initial high set-up costs of these operations would be offset by the fact that the cost per customer would be almost zero once systems were in place. The savings obtained could allow banks to free up resources for other, more lucrative activities, while guaranteeing service quality even for their smallest customers.

The internet provides traditional banks with the opportunity to implement a more customer-focused strategy, as well as an unprecedented capacity to process data. Fan says that traditional banks would retain their advantage over their online competitors because of their customer numbers, reputation, human capital, and risk management. They also have advantages in providing specialised business services, financial advice, asset management (particularly in private banking), merger and acquisition financing, and other financial products.

[12] Zong Liang is deputy director of the International Finance Institute of the Bank of China. Xiong Qiyue is a PhD student at the International Finance Institute of the Bank of China.

[13] Song Wei, Liu Qilin, and Xie Lirong are journalists with *Caijing*.

[14] Sheng Hong is director of the Unirule Institute of Economics in Beijing.

[15] Chen Long is professor of finance at the Cheung Kong Graduate School of Business in Hong Kong.

[16] Fan Yifei is vice-president of China Investment Co. Limited and chairman of the board of the Bank of Shanghai.

[17] See the article by Camille Boullenois in this issue.

The other authors disagree. Zong and Xiong say that online finance represents a serious attack on the traditional sector. To fight back, commercial banks will have to reinvent themselves, to co-operate with each other, and, crucially, to innovate. One serious threat is the fact that online platforms offer services similar to those provided by the banks, but at a lower cost. And the products offered by online platforms are more attractive: they offer limited initial investment, the opportunity to divest at any point, and high returns on investment. This is why internet-based finance is cornering part of the traditional bank savings market and could go on to threaten the entire traditional financial sector.

Song Wei, Liu Qilin, and Xie Lirong call online finance the "Terminator" (终结者, *Zhongjiezhe*) of traditional finance. They think the war has already been lost: by the end of 2013, Alibaba had a turnover of 35 billion yuan (€4 billion), Alipay had 300 million active users, WeChat had 270 million active users (and 600 million registered users), and Mobile QQ had around 800 million users. Song, Liu, and Xie believe that the future of finance, along with the future of market competition, will be internet-based. Online companies will battle each other without mercy, and two of the giants will clash particularly violently: Ali Finance (阿里金融, *Ali jinrong*) and Tencent Finance (腾讯金融, *Tengxun jinrong*).

The case of Yu'e Bao

Chen Long's articles focus on money market fund Yu'e Bao (余额宝). Founded in June 2013 by Alipay together with fund management firm Tianhong Asset Management (天弘), Yu'e Bao has in less than a year become China's most important money market fund. In early March, it was managing more than 400 billion yuan (€47 billion) and had 80 million customers. On some days, says Chen, it deals with more than 20 billion yuan (€2.3 billion) in subscriptions.

Yu'e Bao's exponential growth is in line with the extremely fast development of money market funds in China over the past few years. These funds have seen almost 500 percent growth between 2011 and 2013. But Yu'e Bao's success is even greater than that of its peers. Chen says that the fund's success is both cyclical and structural. It has benefited from high rates on interbank markets, especially, as in June 2013, during periods of liquidity shortage. This has allowed Yu'e Bao to offer its customers attractive rates, higher than those offered by traditional banks. But the fund's biggest advantage is its association with Alipay, whose customers were the first subscribers to Yu'e Bao. The collaboration between Alipay and Yu'e Bao is the most revolutionary aspect of the fund's business model: the cost of acquisition of the majority of Yu'e Bao's customers was almost zero, because the fund was able to leverage the pre-existing portfolios of Alipay customers.

Some people believe that Yu'e Bao is not truly innovative, because it simply combines individual deposits in order to invest them in pre-existing products. Yu'e Bao now invests up to 93 percent of its funds in interbank deposit contracts, 5.3 percent in short-term government debt and AAA rated bonds, and keeps the remainder in cash. This spread is not very different to the investments offered by other money market funds. However, others believe that the real innovation represented by the fund is the fact that it removes barriers to asset management. Chen says Yu'e Bao is innovative in several different ways: it offers "product innovation" (产品创新, *chanping chuangxin*), "channel innovation" (渠道创新, *qudao chuangxin*), "process innovation" (流程创新, *liucheng chuangxin*), and "organisational innovation" (组织创新, *zuzhi chuangxin*).

Chen Long says that to understand Yu'e Bao's success, it is necessary to look back to the birth of money market funds in the United States in the 1970s. In a time of economic depression, financial authorities restricted the banks' ability to invest household and business savings, which limited their access to profitable investment opportunities. Money market funds were thus developed within a context of fiscal restraint. These funds could provide attractive returns for investors because of the significant difference between market rates and the fixed rates offered by banks. From $300,000 in 1971, funds under management grew to $390 million in 1974 and $930 million in 1978. Even so, this still represented less than 1 percent of US savings. But the trend quickly picked up pace: in 1979, $44.3 billion was invested, representing 6 percent of US savings. By 1989, the funds amounted to $432.8 billion (30 percent of US savings) and by 1999, these funds held $1,480 billion (63 percent of savings). Peak investment was reached in 2001, when $2,140 billion, 77 percent of US savings, was invested in money market funds. Since then, the proportion of savings invested in funds has declined, especially after the 2008 economic crisis. In January 2014, just 28 percent of US savings were invested in this kind of fund. However, money market funds in the US still offer real competition to investment banking.

Song Wei, Liu Qilin, and Xie Lirong call online finance the "Terminator" of traditional finance. They think the war has already been lost.

By contrast, money market funds in China held 900 billion yuan (€106 billion) in 2014, representing less than 1 percent of bank deposits. But Chen believes that the Chinese situation echoes the US situation in the 1970s. Both the US and China saw an explosion of money market funds after intermediaries entered the market offering innovative financial products. Moreover, in the US, these funds were first established within the context of rate controls and a gap between market rates and bank rates. China has this disparity today, which presents a real investment opportunity that is driving the development of money market funds. If the US example is anything to go by, the market for Chinese money market funds has yet to

peak. Chen thinks it could eventually be worth between 30,000 billion yuan (€3,534.3 billion) and 50,000 billion yuan (€5,890.6 billion). The internet will accelerate the phenomenon by increasing the accessibility of these funds.

Chen says that Yu'e Bao and its like could fundamentally alter the structure of the Chinese financial sector. In the US, money market funds continued to attract savings, even as restrictions on banking rates were gradually lifted. Clients and services were subsequently redistributed across the finance sector. For short-term financing, the highest-rated companies turned to money market funds rather than banks. The banks kept control of higher-risk lending to individuals and small- to medium-sized enterprises. If the same process occurs in China, the traditional financial sector could be radically changed.

Risks and regulation of internet finance

Chen Long says that Yu'e Bao is a major innovation, especially because it seems to offer good guarantees of security. As with all money market funds, its assets under management are invested in low-risk assets. But Yu'e Bao seems even more secure: around 93 percent of its funds are invested in bank deposit contracts. Because of this, Yu'e Bao would only really be exposed in the case of a large-scale banking failure. And Yu'e Bao is at little risk of any liquidity crisis – an online "bank run". Its investments are mainly short term, and under Alipay terms of use, its subscriber savings are captive for at least seven days. However, as the financial market is gradually reformed, Yu'e Bao will have to diversify its investments towards relatively more lucrative products within the money market framework. These products would present more risk. Chen says that stricter regulation of money market funds, which are currently less regulated than in the US, should be implemented.[18] He warns that regulation should not be achieved through the establishment of minimum reserves (as in the banking model).[19] Instead, China should follow the US model and impose conditions on the types, diversity, and duration of investments. Chen Long believes the P2P and crowdfunding markets are most in need of regulation, because by nature they carry more risk. Zong and Xiong agree, pointing to the numerous P2P failures of 2012, including Tianli Dai (天利贷), Wangying Tianxia, (网赢天下), and Dongfang Chuangtou (东方创投).

Sheng Hong says that, while the online financial sector has risks because of the structure both of the banking and of the internet sectors, the development of online finance is a good thing for the Chinese economy and financial sector. It will facilitate more rapid liberalisation and the "deepening" (深化, *shenhua*) of the financial system. Any effort to regulate the sector should be limited and should take into consideration the fact that the online business sector could be a driver for huge growth in the Chinese economy.

[18] Since the publication of Chen Long's articles, the China Banking Regulatory Commission (CBRC) has publicly announced that it wants the online financial sector to be much more strictly regulated, to limit complex financial risks linked to the sector, as well as the use of these platforms for illegal activities. See "Central Bank and Banking Regulators declare together: Not only must the online finance sector be regulated, it must be tightly regulated", originally published in *Shanghai Securities Newspaper*, 12 May 2014, available at http://m.hexun.com/content.php?ref=1100&id=164680688

[19] Since the publication of Chen Long's articles, Sheng Songcheng, director of the statistics department of the People's Bank of China, has said that deposits in money market funds will soon be subject to reserve ratio requirements, a rate currently fixed at 20 percent for China's large financial institutions. See "China's Popular Internet Funds To Be Hit By RRR: Press", *MNI*, 6 May 2014, available at https://mninews.marketnews.com/content/chinas-popular-internet-funds-be-hit-rrr-press.

4. Information management and internet regulation in China

Florence Rountree

Sources:

Wang Yukai, "The origins and impact of the Central Leading Small Group for Internet Security and Informatisation", *Renmin Wang – People's Daily*, 3 March 2014.[20]

Liu Jun, "The structure of authority behind internet 'rectification'. Twenty years of change in internet management", *Nanfang Zhoumo – Southern Weekend*, 20 March 2014.[21]

Xi Jinping, "Transforming China from a cyber power to a cyber superpower", *Xinhua*, 27 February 2014.

Han Yuanjun, "The State Internet Information Office invites the heads of microblogging at well-known media organisations for informal discussion", *Xinhua*, 4 December 2014.[22]

Lei Lei, "The 'Weibo court': online cases, netizen rulings", *Nanfang Zhoumo – Southern Weekend*, 5 December 2013.[23]

In recent months, the Chinese government has stepped up its campaigns against what they define as "online rumours" (网络谣言, *wangluo yaoyan*) and "internet pornography" (网络淫秽色情, *wangluo yinhui seqing*) in Chinese cyberspace.[24] The latest such campaign is called "Cleaning the Web 2014" (净网2014, *jingwang 2014*). This campaign has caused controversy by targeting the web portal Sina.com, which – among other services – hosts China's hugely popular microblogging Facebook/Twitter hybrid, Weibo (微博).

Such campaigns against rumours and pornographic content are part of what the Chinese government calls "information management" (信息管理, *xinxi guanli*) – the control of access to information. Although this has been ongoing for decades, it has since the early 1990s focused on the control of the stream of online content that is increasingly available across Chinese society. In particular, content which is seen by the Chinese government as potentially undesirable or harmful has become the target of official "internet rectification" (网络整治, *wangluo zhengzhi*) campaigns – that is, the deletion of articles, shutting down of websites, and in extreme cases, the arrest of some prominent netizens.[25] "Cleaning the Web 2014" is an example of this kind of work.

The Chinese government is now pursuing internet regulation, as a core component of information management, with more resources and more vigour than ever before. To do so, it has set up new institutions and adopted new methods.

Building an information management system

In 1982, even before the first connection was made from mainland China to the internet, the State Council set up China's first government body tasked with managing "informatisation" (信息化, *xinxihua*), the digital counterpart to industrialisation. Wang Yukai explains that this was the first step taken towards formalising and centralising government control over the development of "computers and large-scale integrated circuits" (计算机与大规模集成电路, *jisuanji yu daguimo jicheng dianlu*). Ever since then, the Chinese government has become more thorough and more forceful in its regulation of information.

In spite of China's efforts to regulate informatisation, institutional fragmentation has been an enduring feature of China's information management. Wang Yukai and Liu Jun say that too many government departments are directly involved in information management and that central and local authorities do not co-ordinate their work well.[26] Therefore, just as it has done in energy, transportation, and construction, the Chinese Communist Party (CCP) has been trying to use institutional reform to consolidate its control in information management.

Wang Yukai says that the 2008 "Two Sessions" brought about significant changes to the national information management system.[27] All State Council work on information management was placed under the remit of the newly established Ministry of Industry and Information Technology (MIIT, 工业和信息化部, *gongye he xinxihua bu*). This was intended to centralise regulation of the

[20] Wang Yukai is a member of the Advisory Committee for State Information and deputy director of the E-government Expert Committee at the National School of Administration.

[21] Liu Jun is a journalist for *Nanfang Zhoumo*, an influential and comparatively outspoken newspaper based in Guangdong.

[22] Han Yuanjun is a journalist for *Xinhua*.

[23] Lei Lei is a journalist and reporter for *Nanfang Zhoumo*, who voiced support via his Weibo account @雷磊ak for rights activists Guo Feixiong and Liu Yuandong after the Guangdong street demonstrations against censorship in January 2013.

[24] "'Cleaning the Web' is not a brief gust of wind, but a long-term mechanism", *State Council Information Office*, 6 April 2014, available at http://www.scio.gov.cn/zhzc/8/5/Document/1372056/1372056.htm.

[25] The word "整" in this context could be interpreted as a nod to the Yan'an Rectification Movement (延安整风运动, *Yán'ān Zhěngfēng Yùndòng*), which took place between 1942 and 1944. More than 10,000 people were killed in the "rectification" process as the Party made efforts to attack intellectuals and replace the culture of the May Fourth Movement with that of Communist culture.

[26] Liu Jun describes the pre-2011 system (before the establishment of the State Internet Information Office) as a case of "too many governing bodies" (九龙治网, *jiulong zhi wang*, lit. "network governance by nine dragons"). Wang Yukai describes the fragmentation of central and local authorities with the phrase "a thousand lines above, ten thousand needles below" (上面千条线、下面万根针, *shangmian qian tiao xian, xiamian wan gen zhen*).

[27] The "Two Sessions", or *lianghui* (两会), refers to the annual meeting of the NPC (National People's Congress) and the CPPCC (People's Political Consultative Conference), China's top legislative and advisory bodies.

development of information technology.

The next major step in strengthening the information management system came in May 2011, with the establishment of the State Internet Information Office (SIIO, 国家互联网信息办公室, *guojia hulianwang xinxi bangongshi*). Liu Jun says that over the past two years, the SIIO has become very visible in its dual role of initiator and co-ordinator for "internet rectification ". He says that the SIIO has brought real strength to the task of internet rectification, partly thanks to the authority the body has as an agency working alongside the three core internet management bodies: the State Council Information Office (SCIO), the MIIT, and the Ministry of Public Security (MPS). The SIIO has close links with the SCIO – the two bodies were set up under the principle of "two brands, one institution" (两快牌子，一套机构, *liangkuai paizi, yitao jigou*).[28] These ties provide the SIIO with credibility and influence at the Party level, helping it to co-ordinate its actions across the major departments involved.

The Central Leading Small Group for Internet Security and Informatisation

These reforms paved the way for the establishment of the new "Central Leading Small Group for Internet Security and Informatisation" (中央网络安全与信息化领导小组, *zhongyang wangluo anquan yu xinxihua lingdao xiaozu*), which was founded on 27 February 2014. Xi Jinping was announced as its chair, making him the first CCP General Secretary to chair a leading small group on information management. This shows that the group will have unprecedented authority and evidences the importance the CCP places on promoting information management and internet security.

Xi Jinping has talked about the motivations for the group's creation and its intended role, and his speech at the group's first meeting was published by *Xinhua* on 27 February 2014. In his speech, Xi said "China has already become a cyber power, but continues to lag behind when it comes to innovation." Xi went on to say that "without information development there is no modernisation, and without internet security there is no national security." Wang Yukai says that this shows the new group will co-operate closely with the National Security Commission and the Leading Small Group on Reform, both of which were established a few months earlier, at the 18th Party Congress Third Plenary Session in November 2013.

Wang Yukai says that the new group for the first time prioritises internet security as well as information management – not as "two disparate elements" (两张皮, *liang zhi pi*), but as aspects of a single entity. Wang says that the absence of this kind of co-ordinated approach has been a problem in the past. Former leading small groups considered cyber security to be a separate issue to the broader one of overall information management. But things have changed: in his speech, Xi described internet security and information management as "two wings of one bird, two wheels on one car" (网络安全和信息化是一体之两翼、驱动之双轮, *wangluo anquan he xinxihua shi yiti zhi liangyi, qudong zhi shuanglun*).

Regulation in the era of social media

Liu Jun defines three stages within China's internet rectification campaigns over the past 20 years. The first took place between 1994 and 2005, the Web 1.0 era, in which information flowed only one way and the Chinese government's focus was on preventing intrusion by hostile foreign forces and hackers. The second lasted from 2005 to 2011, the Web 2.0 era, in which bloggers began to become more important and the government's focus turned to stamping out pornographic content. The third stage began in 2011 and is still going on. This is the era of social media, in which, Liu says, "everyone is a reporter" (每个人都可以是新闻发布者, *mei ge ren dou keyi shi xinwen fabuzhe*) and the news flows two ways. The government's aim now is to prevent the spread of malicious rumours, cultivate core socialist values, and stimulate a "positive" (正, *zheng*, also understood to mean "correct") online energy.

This [since 2011] is the era of social media, in which, Liu says, "everyone is a reporter" and the news flows two ways.

One such rectification campaign against social media occurred in March 2012, around the same time as the 2012 "Two Sessions". Wang Yukai says that the time of the "Two Sessions" is always a period of great political sensitivity when internet rectification efforts are heightened. Liu Jun says that a special initiative was set up to combat "clickbait" headlines (标题党, *biaoti dang*).[29] Liu describes how the Beijing Public Security Bureau hurriedly detained six people over a Weibo rumour that falsely claimed military vehicles had entered Tiananmen Square. In the months afterwards, local public security bureaus and local internet information offices shut down 42 websites and "cleaned up" (清理, *qinglu*) 210,000 articles.

The National Office against Pornographic and Illegal Publications launched a new crackdown on internet pornography on 13 April 2014, named "Cleaning the Web 2014".[30] This campaign is to last until November, and will be carried out in collaboration with the SIIO, the MIIT, and

[28] A common phenomenon in Chinese government institutions, referenced by Liu Jun with the sentence: "The SIIO adds the SIIO brand to the SCIO" (国信办在国新办加挂国信办牌子, *guoxinban zai guoxinban jiagua guoxinban paizi*).

[29] This kind of attention-grabbing headline, a cheap way to attract more user clicks by way of controversial or shocking statements, is also looked down on in Western cyberspace.

[30] The National Office against Pornographic and Illegal Publications official website for this campaign is available at http://www.shdf.gov.cn/shdf/channels/4482.html

the MPS.[31] The most high-profile victim of the campaign so far has been Sina, whose Weibo social media platform has long been a target for government internet regulations and crackdowns.[32] However, its Weibo platform has not been affected by the latest crackdown. Instead, the publication licences of Sina's article and video operations have been revoked, on the grounds that they have promoted lewd content. Sina has been forced to temporarily close down its literature site and has prevented users from viewing certain US television shows on its video site for "policy reasons".[33]

Involving businesses and the media in online security

The ferocity of the attack on Sina is surprising, since Sina Weibo and other internet companies tend to co-operate with the Chinese system of internet regulation. Liu Jun expects that internet companies will in the future become even more involved in internet protection. Liu says that at a joint seminar on 13 March 2014 between the MIIT, the MPS, and representatives of several major online firms, delegates agreed that government and businesses must join together for internet security and must share resources and data. Han Yuanjun reports from a similar forum held by the SIIO on 4 December 2013, to which 21 mainstream media corporations were invited. Han says that participants in the December forum agreed that media corporations should form the backbone in promoting the healthy development of Chinese microblogging.

Han says participants in the forum also agreed on the need to strengthen user-to-user interaction. One good example of this is the "Weibo court" (微博法庭, *Weibo fating*), a user-managed judicial system that was constructed around a year and a half ago. Lei Lei says that this structure protects the freedoms and actions of Weibo users, while minimising the need for direct involvement by authorities. It creates an appropriate "first line of defence" against rumour spreading and other illegal activities.

The system works in a similar way to Weibo's popular opinion polls, which allow users to vote "yes" or "no" on a range of innocuous questions about health, beauty, relationships, celebrities, and so on. However, in the "Weibo court", the opinion poll becomes a trial. Lei Lei describes the process: a post that contravenes Weibo laws is reported, an impartial Weibo user is appointed judge, and other users vote "guilty" or "not guilty". Since 28 May 2012, Weibo has decided on more than 330,000 cases, each lasting for an average of three minutes. In the case of a guilty verdict, punishments can range from deductions in user "credit" (a points-based system for measuring user behaviour), to temporary gags on user accounts, to account deletion.[34] However, double standards tend to emerge in cases involving officials' accounts, and judges are sometimes biased, because they face "credit" points deductions if they rule in favour of a minority opinion.

Ongoing challenges

As the information revolution surges forward, information management has become a more wide-ranging and more difficult task. Wang Yukai lists several challenges that China faces in its efforts to improve its "information management": weak co-ordination and oversight; overlapping responsibilities between different bodies and departments; poor investment management; weak leadership; and poor central-local management. The implication is that, in order to improve "information management", China will need to carry out much broader institutional reform. One indicator of current failings is China's position in the UN Department of Economic and Social Affairs "E-Government Development Index" (EDGI). Since 2005, China's rank has dropped from 57th to 65th in 2008, and then again to 78th in 2012. This trend looks set to continue, unless forceful campaigning is accompanied by real institutional reform. According to Wang, it is more important for China to strengthen its overall "informatisation" level than it is to guide and manage online public opinion.

[31] "China launches special initiative to combat online pornographic content", *Xinhua*, 13 April 2014, available at http://news.xinhuanet.com/legal/2014-04/13/c_1110219650.htm.

[32] Bill Bishop, "Gilding the cyber cage", *China Economic Quarterly*, December 2013, p.22.

[33] "The new initiative 'Cleaning the Web 2014' takes down 'The Big Bang Theory' and other American television series", *Youxia Wang*, 27 April 2014, available at http://www.ali213.net/news/html/2014-4/103086.html.

[34] "Censorship 3.0? Sina Weibo's New 'User Credit' Points System", *Wall Street Journal*, 29 May 2012, available at http://blogs.wsj.com/chinarealtime/2012/05/29/censorship-3-0-sina-weibos-new-user-credit-points-system/.

5. Human flesh searches: violating privacy or fighting corruption?

François Quirier

Sources:

"Who will protect our privacy at a time of human flesh searches?", *Renmin wang – People's Daily*, 20 February 2014.

Lu Jiayu, "Discussion on criminal penalties for human flesh searches", *Aisixiang*, 15 November 2013.[35]

Liu Han, "Privacy, freedom of expression, and the culture of Chinese internet users – the dilemma of regulating human flesh searches", *Aisixiang*, 10 July 2012.[36]

Li Chunjie, "The protection of citizens' privacy against human flesh searches", *Aisixiang*, 20 June 2012.[37]

Zhang Zuoguo, "Reasonable restrictions to provide freedom of expression on networks with regard to human flesh searches", *Aisixiang*, 6 June 2012.[38]

In August 2013, with the support of the country's largest internet companies, the Chinese government launched an "anti-rumour campaign" (打击谣言, *daqi yaoyan*).[39] It aimed to reduce the proliferation of "rumours", and thus to regulate the denunciations of corrupt officials that were multiplying on the internet, which sometimes produced destabilising results for the authorities. The anti-rumour campaign was deployed in parallel with the anti-corruption fight launched by Xi Jinping. It worked by exerting government control over internet users who made complaints against power-holders, most often local officials. The campaign led to the arrest of several "Big Vs", influential users of the microblogging site, Weibo.[40]

The anti-rumour campaign has now run its course, and the debates about the programme that were widespread in autumn 2013 have somewhat faded out. In their place, debate has resumed about "human flesh searches" (人肉搜索, *renrou sousuo*), which was last a subject of controversy in 2012. The debate is relatively less politicised than the one about the "anti-rumour campaign". It deals with all sorts of online accusations, including individual and private disclosures that have little to do with the public sphere, but instead jeopardise citizens' right to privacy.

"Human flesh searches" (人肉搜索, *renrou sousuo*) are the Chinese version of internet "manhunts". The practice consists of collectively searching the internet to identify an individual who has been seen breaking the law on the internet. For example, the article in *Renmin wang* in February 2014 was published after a local Chongqing newspaper ran a video showing images of a ten-year-old girl mistreating a new-born baby. Angered by the images, Internet users quickly found the girl's personal information and published it on social network forums. The information made public included photos of the young girl, her address, and even names of her family members.

The different sources discussed in this article examine the development of these "manhunts" in China and look at the characteristics of human flesh searches. Concern about these searches is not a recent development – three of the sources discussed here date back to 2012. But no appropriate response has yet been found. All the authors agree that human flesh searches are, as Li Chunjie says, a "double-edged sword" (一把双刃剑, *yi ba shuangrenjian*). They act as a first step towards the politicisation of the population and can help in the fight against corruption. However, they also lead to acts of hate and the disclosure of personal data, which is a violation of Chinese law that endangers the privacy of Chinese citizens.

Human flesh searches: a Chinese phenomenon

Searching for an individual's personal data on the internet happens in other places than China. It is an inevitable side effect of the new potential for finding information presented by the expansion of the internet and of social networks, and it takes place all over the world.[41] But internet "manhunts" in China differ in that they are not only related to issues of morality, but also to the fight against corruption. On several occasions, Chinese citizen oversight has revealed the suspicious wealth of local officials and politicians, who were subsequently removed from their positions and severely punished.[42]

Human flesh searches are thus a tool that the people can use to monitor their political leaders. Liu Jiayu describes them as "an effective means to promote exchange between men, a practice that promotes social progress" (无形中促进了人与人的交流，推动了社会的进步， *wuxing*

[35] Lu Jiayu is a professor at the Guangxi University for Nationalities.

[36] Liu Han is assistant professor at Tsinghua University School of Law.

[37] Li Chunjie is a professor at the Henan University Law School.

[38] Zhang Zuoguo is a professor at the Northwest University of Politcs and Law.

[39] See Clémence Mirgalet, "Le lancement de la campagne de lutte contre les rumeurs sur Internet", *China Analysis*, No. 45, Asia Centre, October 2013.

[40] "Big Vs" are very influential bloggers on Weibo whose articles are generally read by millions of Internet users. Their identity is verified by Weibo (the "V" comes from "verified"), and their accounts are approved by Chinese authorities. The "Big Vs" had appeared to be relatively protected from prosecution, but this series of arrests showed otherwise. Among the "Big Vs" arrested were the popular bloggers Zhou Lubao and Qin Huohuo, and even a company chairman, Fu Xuesheng.

[41] Among other examples, in France, in early February 2014, a young man posted a video online of himself mistreating a cat. The video was widely shared on the internet, creating strong indignation and leading to a collective search that led to the identification and prosecution of the young man in less than a week.

[42] For example, Yang Dacai, director of the Shaanxi province work safety administration, was accused of corruption because of the numerous luxury watches he was seen wearing in public on photos on the internet. Yang Dacai was sentenced in September 2013 to 14 years in prison.

zhong cujinle ren yu ren de jiaoliu, tuidongle shehui de jinbu). However, the authors also say that internet manhunts can lead to serious abuses. Violations of privacy, harassment, and quests for revenge can prove difficult to control. "Manhunts" are not only carried out against public servants and high-ranking officials, but can be pursued against any individual. And the searches often go hand in hand with a collective condemnation that undermines the principle of presumption of innocence. The legal system may in these cases end up judging both the crimes of the individual targeted by internet collective action and the excesses and breaches of privacy of the internet users who carried out the search.

The Chinese government has already taken a stand on the issue. The *Renmin wang* article cites Liu Zhengrong, secretary of the State Council Information Office (SCIO), who on 17 December 2013 declared that human flesh searches were dangerous and that the practice should be combatted with all the tools available under the law.[43] Liu's statement has two sides. On the one hand, it could provide better protection for the victims of collective internet searches. But on the other, it could also make it more difficult for Chinese internet users to continue the fight against corruption and to maintain their oversight of politicians. In the name of the protection of privacy and internet security, the government could increase its monitoring of freedom of expression.

Human flesh searches are thus a tool that the people can use to monitor their political leaders.

The balance between freedom and security

Liu Han says that there are two ways to look at human flesh searches, each based on opposing legal values and cultures. The first says that internet manhunts are wrong, based on respect for the "culture of confidentiality stemming from individuality" (个体主义的隐私权文化, *geti zhuyi de yinsiquan wenhua*). The second, which Liu calls the "culture of Chinese internet users" (中国网民文化, *Zhongguo wangmin wenhua)*, says that monitoring by internet users relates directly to the values of social morality and family ethics, which legitimise public criticism and are more important than individuality and the right to privacy. The political dilemma surrounding human flesh searches comes from the contradiction between these two viewpoints.

It is important to distinguish between meaningful, politically justified collective actions and those that violate an individual's privacy and integrity. Li Chunjie notes that the Chinese constitution gives citizens the right to criticise the government and its institutions. And in general, the authors support human flesh searches as long as they are conducted out of civic duty and with respect for the balance of powers. Zhang Zuoguo says that "human flesh searches enable citizens to fully exercise their constitutional right to freedom of speech" (利用"人肉搜索"这一工具，公民既充分行使了宪法赋予的言论自由, *liyong "renrou sousuo" zhe yi gongju, gongmin ji chongfen xingshile xianfa fuyu de yanlun ziyou*). The authors do not want the law to prohibit internet manhunts, which are not now illegal in and of themselves. Instead, they would like the law to be used to limit the collateral damage caused by these searches and so to better protect the privacy of Chinese citizens.

The law should better regulate the disclosure of personal information on the internet, but new legislation and greater penalties may not be enough to prevent the excesses of human flesh searches. The very nature of the internet makes it difficult to prosecute those guilty of disclosing personal data. Li Chunjie says that prevention and education on internet use will be necessary to "develop collective awareness of the importance of self-protection and confidentiality" (增强自我保护意识和维护隐私权的自觉性, *zengqiang ziwo baohu yishi he weihu yinsi quan de zijue xing*). If Chinese internet users are more aware that their actions on the web can be recorded and reused by a third party, they will be less vulnerable to violations of their privacy.

In conclusion, and to sum up the authors' points of view, it is extremely difficult to fight against collective actions taken against individuals on the internet. Any attempt to do so could quickly turn into an excuse for new limitations on freedom of expression, and lead to the destruction of a practice that the Chinese have developed into a valuable tool to fight corruption. The best solution would be to punish the negative criminal side effects of human flesh searches at the same time as implementing education and preventative measures that could encourage safer, more secure internet use, while still protecting access to internet users' personal data.

Editing: Justine Doody
Translation: Word Works

[43] For more information on the SCIO and on the regulation of the internet sector in China, see Florence Rountree's article in this issue.

About the authors:

After a master degree at Sciences Po, Camille Boullenois studied Chinese in Beijing and Chinese studies at Inalco. She will begin a PhD at Oxford University in September 2014, and study the consequences of urbanisation on Chinese society, she can be reached at nina.boullenois@hotmail.fr.

François Godement is an associate researcher at Asia Centre, a senior policy fellow and head of the China & Asia programme at the European Council on Foreign Relations, he can be reached at francois.godement@ecfr.eu.

Agatha Kratz is the chief editor of China Analysis, she can be reached at a.kratz@centreasia.eu.

Camille Liffran is a graduate of INALCO in China Studies and holds a Master in contemporary history from Université Sorbonne-Paris IV. She specialises on China's domestic policy, and especially on China's public administration and institutions. She can be reached at camille.liffran@hotmail.fr.

François Quirier graduated from Sciences Po Grenoble and the INALCO, and specifically works on China's policies related to the Internet, he can be reached at quirierf@gmail.com.

Florence Rountree is a consultant for the Asia & China Programme at the European Council on Foreign Relations. She specialises in Chinese domestic and foreign policy, and East Asian security issues, she can be reached at florence.rountree@ecfr.eu.

ABOUT ASIA CENTRE

Asia Centre, founded in August 2005, conducts research and organizes debate on international relations and strategic issues, as well as on the political and economic transformations in the Asia-Pacific; promotes cooperation and second track dialogue with partners in Asia, Europe and the world; publishes timely information and analysis from the region, executive briefs and reports from our research team.

Asia Centre programs cover the prevention of conflicts and regional integration, the challenges of democracy and governance, globalisation and national strategies, energy, proliferation and sustainable development. They also draw contributions and viewpoints from research associates and a network of research institutions.

www.centreasia.eu

ABOUT ECFR

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy.

ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members - politicians, decision makers, thinkers and business people from the EU's member states and candidate countries - which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Martti Ahtisaari, Joschka Fischer and Mabel van Oranje.
- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome and Sofia. In the future ECFR plans to open offices in Warsaw and Brussels. Our offices are platforms for research, debate, advocacy and communications.
- A distinctive research and policy development process. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to advance its objectives through innovative projects with a pan-European focus. ECFR's activities include primary research, publication of policy reports, private meetings and public debates, 'friends of ECFR' gatherings in EU capitals and outreach to strategic media outlets.

ECFR is backed by the Soros Foundations Network, the Spanish foundation FRIDE (La Fundación para las Relaciones Internacionales y el Diálogo Exterior), the Bulgarian Communitas Foundation, the Italian UniCredit group and the Stiftung Mercator. ECFR works in partnership with other organisations but does not make grants to individuals or institutions.

www.ecfr.eu

This issue of China analysis was produced with the support of Stiftung Mercator.

www.stiftung-mercator.de

This paper represents not the collective views of ECFR or Asia Centre, but only the view of its authors.

Copyright of this publication is held by the European Council on Foreign Relations and Asia Centre. You may not copy, reproduce, republish or circulate in any way the content from this publication except for your own personal and non-commercial use. Any other use requires prior written permission.

© ECFR / Asia Centre 2014
Contact: london@ecfr.eu, contact@centreasia.eu

ASIA CENTRE
centreasia.eu

EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu