

SPECIAL ISSUE

GOVERNING THE WEB

ABOUT

The Chinese have long been obsessed with strategic culture, power balances and geopolitical shifts. Academic institutions, think tanks, journals and web-based debates 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

This issue marks the second time in a year that *China Analysis* has focused on China's IT, spanning social media, e-commerce, the overarching issue of control, and cyber security.¹

The trends that we identified last year have been confirmed and reinforced by very effective government action. The pro-technology bias of the Chinese government – which does not have to contend with as many strong interest groups in civil society as a democracy would need to – is producing impressive results. E-commerce, mobile e-payment, and the main social media have a larger consumer base – and a larger share of overall domestic commerce – than in any other country. China has indeed leapfrogged to frontrunner status. A case in point is the sudden rise of a company such as Uber in China, where it now claims more clients than in the United States. Rogier Creemers, a noted analyst of Chinese society and its relation with web-based development, identifies a further positive bias in favour of the “internet of things”. Chinese industry may also be attempting to progress beyond its previous status as a leading producer of inexpensive, but not technologically advanced goods. Thanks to its embrace of IT processes, it may become a cutting-edge tech producer.

¹ See *China Analysis: China's Expanding Cyberspace*, European Council on Foreign Relations and Asia Centre, June 2014. Available online: http://www.ecfr.eu/publications/summary/chinas_expanding_cyberspace311.

There is, however, a flip side to this achievement. The Chinese government's attempt to regain control of the entire internet chain has been well documented. It takes the form of requiring servers to be China-based, and of prioritizing Chinese software and Chinese IT firms. A recent episode regarding bank technology rules led to a public outcry by foreign firms and some of their Chinese competitors alike, given the gap that still exists in management and communication software.² And one would indeed expect conservative voices (in this special issue, they are PLA-based) to lament the political risks associated with any opening of the internet to actors outside China. China has, in the space of one year, considerably strengthened its stranglehold on web surfing in China, as any visitor will quickly discover. In fact, the resulting slowdown in download speeds may also have serious consequences for productivity. Over the last year, some of China's methods of social control have been copied by other authoritarian regimes: for example, Russia has enacted a law that metes out punishment to bloggers and other social media actors not so much according to what they write, but according to the size of their audience.³

This issue, however, points to an even more worrying development. The spread of e-commerce and online payment means that new methods of checking consumer credit and sellers' track records are necessary. They have become part of our online lives, along with the cookies that allow marketing firms and banks to track our consumer and financial behaviour. But in China, this is opening the way to a programme of control on all aspects of social and individual life, including political and professional oversight.

The limits to such proposals remain unclear, but the introduction of compulsory real-name registration for hardware (such as phones), internet, and social media accounts implies that this programme of control could have almost universal application. This renders obsolete the old-style collection of data by the Party-state through questionnaires, personal files and informants. Like the anti-corruption campaign, it has ominous implications for Party members themselves. After all, who is beyond a computer's reach?

J. Edgar Hoover dreamed it, and now China's techno-bureaucrats are creating it: a society where an individual's every step, whether it is online chat, purchase or any electronically recorded action, can be stored for later use.

Just as worrying is the new national security law adopted by the Standing Committee of the National People's Congress at the start of July, which increases cyber security powers and links domestic and overseas collection of data and intelligence, effectively giving unlimited power to the party-state.⁴

Needless to say, China's government enjoys a perfect international environment to create this brave new world. The global fear of terrorism, the abuses of the NSA revealed by Edward Snowden, and copycat legislation by other democratic governments such as France (where judicial authorities have essentially been placed outside of the loop for much interception of communications) have opened a window of opportunity. Liberal critics of China will be asked to justify their own countries' records. What's unique about China, however, is the combination of some of the world's most advanced IT and a government that acknowledges no separation of powers.

2 For more information, see: Paul Mozur and Jane Perlez, "China Halts New Policy on Tech for Banks," *New York Times*, 16 April 2015. Available online: <http://www.nytimes.com/2015/04/17/business/international/china-suspends-rules-on-tech-companies-serving-banks.html>.

3 For more information, see: Tanya Lokot, "Blogger Law Traps Russia's Activists in Limbo," *The Moscow Times*, 21 August 2014. Available online: <http://www.themoscowtimes.com/opinion/article/blogger-law-traps-russia-s-activists-in-limbo/505628.html>.

4 For more information, see: Chun Han Wong, "China Adopts Sweeping National-Security Law," *Wall Street Journal*, 1 July 2015. Available online: <http://www.wsj.com/articles/china-adopts-sweeping-national-security-law-1435757589>.

1. Internet Plus: Technology at the Centre of Chinese Politics

Rogier Creemers

Sources:

Chen Qiqing, "Accelerate the Construction of a Social Credit System", *Study Times*, 24 February 2014.⁵

"Ministry of Foreign Affairs' Law and Treaties Department Head Huang Huikang: Strengthen International Exchange and Cooperation in the Cyber Area", *Xinhua*, 5 October 2012.

Wang Kongxiang, "Using the Principles of International Law to Govern the Internet", *Zhongguo shehui kexue bao*, 16 January 2015.⁶

Wu Zhenghua, "We Can Absolutely Not Allow the Internet to Become a Lost Territory of People's Minds", *PLA Daily*, 12 May 2015.⁷

Zhao Zhoujian and Xu Zhilian, "Information Technology Development Trends and Ideological Security", *Red Flag Manuscripts*, 2014/14.⁸

Introduction

In March of this year, Chinese premier Li Keqiang unveiled Internet Plus (互联网+, *hulianwang+*), whose aim, he said, would be to integrate mobile internet, cloud computing, big data, and the "internet of things" with modern manufacturing in a way that would encourage the substantial expansion of e-commerce.⁹ Another benefit would be to enhance the international presence of China's internet companies and hardware manufacturers.

Since then, there has been steady progress. In May, China's State Council published a new policy document outlining how it planned to stimulate e-commerce by reducing barriers to entry, lightening fiscal burdens, increasing financial support, and improving the competitive environment.¹⁰ By

5 Chen Qiqing is an economist and director of the Central Party School of the Communist Party of China, in Beijing.

6 Wang Kongxiang is a law scholar at the University of International Relations in Beijing.

7 Wu Zhenghua is a commentator at *PLA Daily*, the newspaper of the People's Liberation Army (PLA).

8 Zhao Zhoujian and Xu Zhilian are analysts at the National Defence University (NDU) in Beijing.

9 2015年政府工作报告, *2015 nian zhengfu gongzuo baogao* (2015 Government Work Report). Presented to the National People's Congress on 3 March 2015. Available online: <http://lianghui.people.com.cn/2015npc/n/2015/0305/c394298-26642056.html>.

10 国务院关于大力发展电子商务加快培育经济新动力的意见, *Guowuyuan guanyu dali fazhan dianzi shangwu jiakuai peiyu jingji xin dongli de yijian* (State Council Opinions concerning Powerfully Developing E-Commerce and Accelerating the Fostering of New Economic Drivers). Promulgated on 4 May 2015. Available online: http://www.gov.cn/zhengce/content/2015-05/07/content_9707.htm.

2025, it said, it envisaged a thriving modern e-commerce system, privately owned and controlled by Chinese citizens.

That same policy document goes on to assign responsibility for a whole range of different tasks to a multitude of ministries and other regulatory bodies, with the result that a torrent of detailed implementation plans and new management regulations can be expected in the coming months. The Ministry of Commerce has already taken the lead in drafting a follow-up plan for the development of both rural and cross-border e-commerce.¹¹ It has also published an Internet Plus logistics plan, to support the development of delivery systems in rural areas and internationally.¹² And to ensure that the network is capable of transmitting the increased quantities of data these plans will generate, the State Council has called for a rapid upgrade of the country's internet infrastructure, projecting investment of 700 billion yuan during 2016 and 2017.¹³

It's no surprise that these projects have been enthusiastically welcomed by industry leaders. For instance, Pony Ma (Ma Huateng), CEO of social media company, Tencent, told this year's "two sessions" – as the annual Chinese People's Political Consultative Conference (CPPCC) is more commonly known – that Internet Plus would help to reduce "information asymmetries" and transaction costs, increasing productivity and driving innovation.¹⁴ In the eyes of Alibaba CEO, Ma Yun, Internet Plus means opportunities for traditional industries to expand and improve their businesses using new information technologies.¹⁵ Most significantly, it will make a major contribution to economic growth. According to McKinsey, the internet will contribute up to 22% of China's GDP growth up to 2025, and increase productivity in that period by a similar rate. In 2025, the report forecasts that the internet could add 10 trillion yuan to GDP, equivalent to the current GDP of Australia. It will also improve the efficiency of public services, by providing, for example, up to 610 million yuan in savings in healthcare alone.¹⁶

11 "11 Major Policies Published in 20 Days – Stable Growth Policies Intensively Raise Stakes," *Xinhua*, 25 May 2015. Available online: http://news.xinhuanet.com/fortune/2015-05/25/c_127837197.htm.

12 "互联网+流通"行动计划, "*hulianwang + liutong*" *xingdong jihua* ("Internet Plus Logistics" action plan). Promulgated on 15 May 2015. Available online: <http://dzsws.mofcom.gov.cn/article/zcfb/201505/20150500972952.shtml>.

13 国务院办公厅关于加快高速宽带网络建设推进网络提速降费的指导意见, *guowuyuan bangongting guanyu jiakuai gaosu kuandai wangluo jianshe tuijin wangluo tisu jiangfei de zhidao yijian* (State Council Secretariat Guiding Opinions concerning Accelerating the Construction of High-Speed Broadband Networks and Stimulating the Increase of Network Speeds and Reduction of Costs). Promulgated on 16 May 2015. Available online: http://www.gov.cn/zhengce/content/2015-05/20/content_9789.htm.

14 Li Yuan, "Internet Plus' Will Become Innovation Engine", *Guangming Daily*, 9 March 2015. Available online: http://news.gmw.cn/2015-03/09/content_15035152.htm.

15 "Internet Plus in Ma Yun's Eyes", *CZTV*, 22 April 2015. Available online: <http://n.cztv.com/news2014/895942.html>.

16 "China's digital transformation: The Internet's impact on productivity and growth", McKinsey Global Institute, July 2014.

A new attitude to the role of information technology

These are the most recent in a series of measures that have radically overhauled China's policy apparatus in order to exploit the potential of new technologies. Up to now, the internet has been regarded by China and its government regulators as primarily a platform for communication. However, with the advent of Web 2.0 technology, the "internet of things", mobile and wearable gadgets, and ubiquitous connectivity, the internet has moved to the nexus of different policy considerations. These have moved far beyond the dissemination of information to include economic growth, innovation and development, as well as questions of national security, governance, and social management.

Politically, this shift was underlined by the establishment

of the Central Leading Group for Cybersecurity and Informatization (中央网络安全和信息化领导小组, *Zhongyang wangluo anquan he xinxihua lingdao xiaozu*) in February 2014, and the new prominence of the Cyberspace Administration of China (CAC).¹⁷ The former, however, was not really transformative in institutional terms. The new Leading Group was, in fact, a reconstitution of the previous premier-level Leading Group for National Informatization (国家信息化领导小组, *Guojia xinxihua lingdao xiaozu*), with a very similar membership.¹⁸ Equally, many of the economic and technological reform measures announced since the establishment of the leading group are the continuation of agendas developed over the longer term.

However, the importance of these moves can be found in the signal they send about the prioritisation of cyberspace and China's ambition to become a leading global power in this field. In his speech at the establishment of the Leading Group, Xi Jinping called for China's transformation from a "large internet country" (网络大国, *wangluo daguo*) to a "strong internet country" (网络强国, *wangluo qianguo*), a subtle change of message that has both domestic and international relevance.¹⁹

17 The Chinese name of this department is *Guojia hulianwang xinxi bangongshi* (国家互联网信息办公室). Its original English name was the direct translation: State Internet Information Office. This English name was changed in the summer of 2014. The Chinese name remained the same.

18 A membership list can be found in James Lewis and Simon Hansen, "China's cyberpower: International and domestic Priorities," *Australian Strategic Policy Institute*, 12 November 2014. Available online: <https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities>.

19 "Xi Jinping: Build Our Country from a Large Internet Country into a Strong Internet Country," *Xinhua*, 27 February 2014. Available online: http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

With the advent of Web 2.0 technology, the "internet of things", mobile and wearable gadgets, and ubiquitous connectivity, the internet has moved to the nexus of different policy considerations.

Internationally, it echoes calls for greater cybersovereignty and the development of a sophisticated system that is proof against potential foreign interference. The claim that "foreign hostile forces" (外国敌对势力, *waiguo didui shili*) are scheming to Westernise and divide China is a well-rehearsed refrain in elite speeches,²⁰ Party documents,²¹ and the party press.²² As a result of the Snowden revelations, deepening Sino-US tensions over cybersecurity, and the US indictment of five PLA officers on suspicion of cyberhacking, China has sought to reduce its reliance on foreign software and hardware by removing certain foreign suppliers from government procurement lists.²³ It has also instituted a security review for overseas companies.

Domestically, China has tightened control over social media, reduced the volatility of the microblogging website Weibo (China's equivalent of Twitter), and become more proactive about the use of information technologies for social management.

How is international internet engagement discussed in China?

While public discourse about China's stance on the global nature of the internet is relatively consistent when it comes to basic principles,²⁴ there are many different shades of opinion when it comes to identifying the threats that China faces and the potential countermeasures to be taken. There are some outspoken voices, for example inside the People's Liberation Army (PLA) and associated bodies, such as the National Defence University (NDU), that have sought to raise the profile of threats to China from abroad. NDU analysts Zhao Zhoujian and Xu Zhilian, for example, decry the fact that, in their opinion, the Chinese state is insufficiently proactive in anticipating the risks presented

20 Hu Jintao, "Resolutely Walk the Path of Socialist Cultural Development with Chinese Characteristics, Striving to Construct a Strong Socialist Culture Country", Speech at the 6th Plenum of the 17th Party Congress, 18 October 2011. Translation available online: <https://chinacopyrightandmedia.wordpress.com/2012/01/04/hu-jintaos-article-in-qiushi-magazine-translated/>.

21 关于当前意识形态领域情况的通报, *Guanyu dangqian yishixingtai lingyu qingkuang de tongbao* (Communiqué on the current state of the Ideological Sphere), 22 April 2013. Translation available online: <https://chinacopyrightandmedia.wordpress.com/2013/04/22/communiqué-on-the-current-state-of-the-ideological-sphere-document-no-9/>.

22 Sanglin Feng, "Cyber-sovereignty symbolizes national sovereignty", *PLA Daily*, 20 May 2015. Translation available online: <https://chinacopyrightandmedia.wordpress.com/2015/05/20/cybersovereignty-symbolizes-national-sovereignty/>.

23 "Symantec and Kaspersky Added to the List of Prohibited Domestic Security Software", *Xinhua*, 4 August 2014. Available online: http://news.xinhuanet.com/info/2014-08/04/c_133529593.htm; Paul Carsten, "China drops leading tech brands for certain state purchases," *Reuters*, 27 February 2015. Available online: <http://www.reuters.com/article/2015/02/27/us-china-tech-exclusive-idUSKBN0LV08720150227>.

24 Michael Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, 42, 2013. Available online: http://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf.

by information technology, and too reticent about using technology to mitigate those risks. Referencing solar-powered drones that can stay aloft indefinitely, as well as Google's Project Loon,²⁵ Zhao and Xu raise the spectre of foreign-owned drones circling China's borders to provide uncensored internet access to its citizens. *PLA Daily* commentator, Wu Zhenghua, claims that foreign forces could "use this convenient tool of the internet to build 'value traps', implement a 'cultural Cold War', and foster 'a fifth column'. Insults to leaders, vilification of heroes, ridicule of the system, and attacks against the army, may be said to have reached a state of unbridled brazenness, making the internet into a 'concession' to peddle Western ideology." This plays into the narrative – already widespread as a result of Document 9²⁶ – that the internet has become a channel through which foreign powers can engage in ideological infiltration.

More moderate voices, such as the University of International Relations law scholar Wang Kongxiang, propose that the internet should be regulated according to the "basic principles" (基本原则, *jiben yuanze*) of international law. These should include the principles of national sovereignty, non-interference in internal affairs, non-militarisation of cyberspace, peaceful resolution of international disputes in cyberspace, and international cooperation. This largely reflects the five principles of peaceful coexistence in cyberspace that China's envoy, Huang Huikang, delivered at the 2012 Budapest Convention on Cyberspace, and thus China's official diplomatic agenda.

Nevertheless, when pressed on exactly how international law should apply and be enforced, China has, so far, remained non-committal. At a meeting of the United Nations Group of Governmental Experts (GGE) on cyberspace, convened to explore the application of norms in internet governance, China only reluctantly agreed to support the inclusion of existing international law in the group's report in 2013,²⁷ and seems to have withdrawn from that position at the most recent GGE meeting this year. Instead, it has concluded a mutual information security protection and cooperation treaty with Russia,²⁸ a country widely seen as the primary source of cybercrime, as well as political-

military espionage.²⁹ Cybersecurity was also mentioned as a point of cooperation in China's recent joint declaration on strategic partnership with Belarus.³⁰

Which internal aims does the sovereignty agenda protect?

These external security concerns produce increasingly ambitious internal goals. The Leading Group and the CAC have shown significant initiative in moving information technology to the centre of a renewed reform agenda, and seeking to transform social governance and political structures. Perhaps most important in this regard is the "social credit scheme" (社会信用体系, *shehui xinyong tixi*) announced by the State Council in July of 2014. While the first plan was relatively vague, it does indicate that the idea of a social credit scheme is to use big data technology and increasingly sophisticated algorithms to monitor the behaviour of Chinese citizens in private and public environments.³¹ The information such a system could collate would range from traffic violations to benefit fraud, the performance of medical and educational professionals, or the conduct of judicial and political officials.

In an article in *Study Times*, published by the Central Party School, Chen Qiqing wrote that the establishment of such a system was necessary in view of China's rapid social transformation, which had greatly increased the number of social transactions with strangers rather than acquaintances, leading to a decrease in trust and morality. To counteract this, Chen argues, it is necessary first to gather as much "credit information" as possible, using that credit information to incentivise individual behaviour, and ensure that individuals act in a trustworthy manner in commercial and social environments. The scheme also has explicit political relevance: it facilitates oversight of local officials by providing more convenient means of monitoring social outcomes in public services, and thus bypassing the internal party-state reporting system which is prone to interference.

25 Project Loon is a Google project aimed at providing wireless connectivity through an aerial network of balloons stationed in the stratosphere.

26 Document 9 is a secret party document, issued in April 2013, that listed seven kinds of discourse harmful to the PRC's ideological integrity. It also identified the internet and academia as the two main channels through which these risks entered China. Veteran journalist, Gao Yu, was sent to prison, allegedly for leaking the document. (See also footnote 15)

27 Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace", *American Foreign Policy Interests*, 2014, 36:5, pp. 322-331.

28 Interestingly, this treaty has, thus far, not received any significant attention in authoritative party media. The full text has also not been published in Chinese or English, although the Russian government has made it available online in Russian: <http://government.ru/media/files/5AMaccs7mSlXgbffUa785WwMwCABDJw.pdf>.

29 James Lewis, "Testimony: Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, Senate Foreign Relations Committee", 14 March 2015. Available online: http://www.foreign.senate.gov/imo/media/doc/051415_REVISED_Lewis_Testimony.pdf.

30 中华人民共和国和白俄罗斯共和国关于进一步发展和深化全面战略合作关系的联合声明, *Zhonghua Renmin Gongheguo he Bai Eluoshi Gongheguo guanyu jinyibu fazhan he shenhua quanmian zhanlüe huoban guanxi de lianhe shengming* (Joint Declaration of the People's Republic of China and the Republic of Belarus concerning Further Developing and Deepening the Comprehensive Strategic Partnership). 11 May 2015. Available online: http://www.81.cn/dblj/2015-05/11/content_6482368_2.htm.

31 社会信用体系建设规划纲要(2014—2020年), *Shehui xinyong tixi jianshe guihua gangyao* (Planning Outline for the Construction of a Social Credit System (2014-2020)), 14 June 2014. Translation available online: <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>.

Such systems have one fundamental requirement: it must be possible to identify who did what and where. To this end, the authorities have stepped up pressure to enforce real-name registration requirements for social media. In various ways, real-name regulations have been on the books for about a decade, but have rarely been consistently or effectively implemented.³² That now appears to be changing. It was reported in January 2015 that more than 80 percent of WeChat users had registered under their real identities.³³ Moreover, real-name registration obligations are not limited to online content. They are also required for the purchase of telephones, enabling the identification of online activities through individual pieces of hardware.³⁴ In February 2015, the CAC mandated a real-name registration system for all account-based online information services.³⁵ Nevertheless, strong public concern remains about the security of the data protection systems surrounding these systems, particularly in light of the fact that Chinese data protection regulations remain underdeveloped.³⁶

There are few voices at the moment opposing this more Sinocentric, control-orientated shift. A crackdown against reformist voices on social media that started in 2013 was followed by a campaign countering ideological deviance in universities in 2014. Equally, corporations seem little inclined to anger their regulators. As a result, few calls have emerged advocating a more cosmopolitan stance on the internet sovereignty agenda. One rare example of criticism came from Huawei executive, Eric Xu, who opposed the technological localisation measures taken by the leadership. "Even if you localise, make your own CPUs (central processing units), make your own operating systems, make your own database software, it would still be at a grade-school level, (with) your (security measures) transparent to the college students", Xu claimed, in an interview with Reuters. He also discussed the repercussions for international trade, arguing that a decision by China to close its borders might provoke Europe and the United States to do the same.³⁷

32 Johan Lagerkvist, "Principal-Agent Dilemma in China's Social Media Sector? The Party-State and Industry Real-Name Registration Waltz," *International Journal of Communication*, 6, 2012.

33 Liu Sha, "Govt Takes Down Illegal Websites," *Global Times*, 14 January 2014.

34 电话用户真实身份信息登记规定, *Dianhua yonghu zhenshi shenfen xinxi dengji guiding* (Telephone User Real Identity Information Registration Regulations). 16 July 2013. Translation available online: <http://chinacopyrightandmedia.wordpress.com/2013/07/16/telephone-user-real-identity-information-registration-regulations/>.

35 互联网用户账号名称管理规定, *Hulianwang yonghu zhanghao mingcheng guanli guiding* (Internet User Account Name Management Regulations), 4 February 2015. Translation available online: <https://chinacopyrightandmedia.wordpress.com/2015/02/04/internet-user-account-name-management-regulations/>.

36 "Online Real-name System: How Long Until the 'Virtual World' Does Not Become an 'Outlaw Land'?", *Xinhua*, 23 January 2015. Available online: http://news.xinhuanet.com/newmedia/2015-01/23/c_1114110521.htm.

37 Gerry Shih, "Huawei CEO says Chinese cybersecurity rules could backfire," *Reuters*, 21 April 2015. Available online: <http://www.reuters.com/article/2015/04/21/us-huawei-cybersecurity-idUSKBN0NC1G920150421>.

Conclusion

The internet has gained a new importance in Chinese domestic politics. It is seen as a powerful driver of economic reform to the extent that it allows China to climb up the value chain and facilitates expansion into rural areas. It also enables more effective social management by government, and realigns the central-local nexus within the party-state architecture. Nevertheless, there are international tensions, particularly in the relationship with the United States. Concerns about information and network security have driven China to pursue a policy of software indigenisation and to raise the requirements for foreign technology suppliers. They also fuel the hawkish voices that are already prominent in Chinese public discourse. If China and the international community wish to continue reaping the benefits of burgeoning technological change, it will be necessary to achieve some level of mutual co-operation that addresses China's security concerns while maintaining the operational openness and ethos of collaboration at the heart of the internet's architecture.

About the authors

Rogier Creemers is an associate scholar at the University of Oxford China Centre and the Centre for Socio-Legal Studies. His main research interests include Chinese internet policy and legal theory. His work has been published in academic journals such as the *China Journal* and the *Chinese Journal of Communication*. He has also appeared in *Foreign Policy*, the *Diplomat*, the *New York Times* and the *Financial Times*. He edits *China Copyright and Media*, a blog and database of Chinese policy documents. He can be reached at rogier.creemers@csls.ox.ac.uk.

François Godement is Director of the China & Asia programme and a senior policy fellow at the European Council on Foreign Relations. He is also an associate researcher at Asia Centre, a non-resident senior associate of the Carnegie Endowment for International Peace in Washington, D.C., and an outside consultant for the Policy Planning Staff of the French Ministry of Foreign Affairs. He can be reached at francois.godement@ecfr.eu.

Agatha Kratz is the chief editor of *China Analysis*, and an Associate Policy Fellow at the European Council on Foreign Relations's Asia & China Programme. She can be reached at agatha.kratz@ecfr.eu.

ECFR would like to thank Peter Cluskey for his help in preparing the text for publication.

This publication is edited in collaboration with Asia Centre.

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 2015

Contact: london@ecfr.eu, contact@centreasia.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 programmes 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 Carl Bildt, Emma Bonino 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, Sofia and Warsaw. 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 a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions.

www.ecfr.eu

This issue of China Analysis was produced with the support of the Calouste Gulbenkian Foundation and Stiftung Mercator.

www.gulbenkian.pt

www.stiftung-mercator.de

