SPECIAL REPORT

ASPI

October 2013

Compelled to control

Conflicting visions of the future of cyberspace

Dave Clemente

The contest for power in cyberspace is of growing concern for states and their citizens, whose daily lives are increasingly reflected in the digital domain. The ease and low cost of networking are driving dramatic expansions of connectivity, yet the interdependencies and potential risks of that expansion are often poorly understood.[1] In addition, the challenges of encouraging digital innovation while maintaining the stability of cyberspace are beyond the capabilities of any single country.

Governments are struggling to understand the political and social implications of a world where everyone is connected all the time, and where disruptive technologies can be developed and disseminated without government permission. This environment is strained further by the fact that competition on the global stage is mediated increasingly through digital means, as states attempt to leverage their technical strengths (including military and commercial strengths) for political advantage. States busy negotiating and manoeuvring among themselves often perceive civil society perspectives to be a footnote or an annoyance.

This paper looks at the desire among states for greater control over the digital domain. It begins by considering the convergence of controlling desires among the major cyberpowers, and then examining some of the main dynamics of the Russian and Chinese positions. Both those countries are attempting to shape the international dialogue on cyberspace to suit their preferences. Their positions are examined relative to each other and to the Western consensus—defined as 'the views on use and governance of the internet that have emerged in the USA, UK and other like-minded states—a system of views which forms an unstated but nonetheless tangible concurrence'.[2] The paper analyses the potential implications of those positions for the global internet and the impact that developing countries may have on the dialogue.[3]

Convergence of control

While there are significant and self-evident differences between the authoritarian and liberal positions described here (which themselves encompass a broad range of countries and perspectives), there's a danger of gradual—and illiberal—convergence between the governments of major cyberpowers, such as the US, the UK, Russia and China, on the levels of internet control they want. In other words, while the desired ends—or strategic outcomes—may vary widely among the dominant actors, there's a growing resemblance between ways and means—the policies, procedures and resources—that those actors and their allies deem necessary for protection from cyber insecurity.

The Western consensus is currently receiving significant public scrutiny, due in large part to the intelligence documents leaked by Edward Snowden and the highly controversial actions they revealed.[4] This has exposed well-established patterns of activity and has in many ways confirmed what was already suspected, and more. For a variety of reasons, a number of liberal democratic countries have gradually constructed cybersecurity policies and legal principles that appear to border on the illiberal, and for which little or no consent has been sought from the voting public. Those actions, and the policies that underpin them, have the potential to erode trust and create long-term damage to the domestic and international credibility of these countries. They may sway undecided countries in illiberal directions, and have sobering implications for the health of civil society and privacy rights around the globe.

Most importantly, these actions risk lending credence to a narrative of moral equivalence between countries such as the US and Russia—countries that would otherwise be positioned at the opposite ends of many international debates. Many observers will be tempted to think that there's little to distinguish the behaviour of liberal and illiberal governments in cyberspace, and in some cases they'd be correct. In addition, long-term damage is likely to be done to the current Western-dominated model of internet governance (which includes government and non-government actors), effectively leaving it open to challenge by state-dominated models. Whose model of internet governance has the potential to see widespread international adoption?

It would be deeply damaging if the main cyberpowers coalesce around common visions of intrusive domestic digital control, leaving developing countries with the option to join the crowd or the minority. There's a pressing need to counter illiberal tendencies, especially when fear of insecurity is greatest. Sustained action among liberal governments and civil society around the world is necessary to counter these tendencies, closely scrutinise political desires for control and mastery of the digital domain, and preserve the creativity and dynamism made possible by an internet that's free in both perception and reality.

A Russian perspective

The Russian Government position on 'information security' differs significantly from the Western stance on 'cybersecurity'. Whereas Western states acknowledge the threat from malicious code and craft policies and doctrine to defend themselves, they don't seek to control or otherwise restrict flows of information within or across domestic borders. The Russian conception of information security encompasses far more than cybersecurity. First, Russia views uncontrolled information as a potential threat to the state and society. This is an issue of national sovereignty and requires control of the national 'information space'. Second, the information doesn't necessarily have to come from the internet. It doesn't even have to be digital, and could also come from radio, TV or newspapers.

According to a former KGB official:

> [Russia looks] at information security from the international point of view, from the perspective of protecting national interests. It's not about the technology only (i.e. the protection of computer networks, commanding systems and so on). But it's also the political–ideological area—combating the misuse of information technology to undermine the political situation, and creating confrontational relationships.[5]

Russia continues to engage in a lengthy attempt to promote this all-encompassing vision of information security to sympathetic countries around the globe. A significant initiative came in September 2011, when Russia and China (along with Tajikistan and Uzbekistan) jointly produced the International Code of Conduct for Information Security.[6] At the same time, Russia released the Draft Convention on International Information Security. Taken together, the two documents propose to significantly strengthen the power of the state in cyberspace vis-a-vis non-government actors, many of which contribute substantially to global internet governance. Organisations such as the Internet Engineering Task Force and ICANN (the Internet Corporation for Assigned Names and Numbers) are largely ignored, as the preamble to the code of conduct states that 'policy authority for internet-related public issues is the sovereign right of States.'[7] States would also agree to not 'carry out hostile activities or acts of aggression', although how that would be enforced isn't specified.

The code of conduct and draft convention are tools for promoting a vision of robust state control in cyberspace. In the Russian context, this is enacted through an authoritarian mentality that's become entrenched among Russian political elites, as Vladimir Putin has alternated from President to Prime Minister (and back again) over the past 13 years.

There's significant friction between this and the Western stance, which is more accepting of non-government influences in internet governance. Two main differences are apparent, the first political and the second technical:

> First, they are at odds with Western principles in some of their key areas such as 'national information space' (also described as network sovereignty), state management and governance of the internet, and the threat from hostile content as well as hostile code. Second, they are also dissonant with the everyday work of Russian commercial internet service providers and domain name authorities, who on a daily basis work to ensure the free and unobstructed flow of information across national borders simply because this is how the internet presently works in real life, as opposed to how some sections of Russia's security elite would wish it to work.[8]

While neither proposal has gained traction beyond its authors, they're significant attempts by non-Western states to shift the narrative on personal online freedom towards a state-led and controlled perspective. They

provide an alternative vision for undecided countries that may lean naturally towards state-dominated models of governance, and that side with Russia and China in decrying the destabilising potential of the internet and cyberspace more broadly.

At the domestic level, and contrary to popular opinion, social media platforms in Russia are generally permitted freedom of expression.[9] In addition, 'there is no overt censorship of social media, as there is in China; at the same time there is investment in monitoring and seeding software.'[10] However, it's easy to see how an abundance of caution and a nuanced understanding of the government's red lines contribute to self-censorship. In Russia this caution is magnified by the hazards, which have included severe beatings or assassination, of writing stories that are unfavourable to the government or corporations.[11] The fear of online instability fuelled by journalists or social media, and its influence on policymakers, shouldn't be underestimated. For example, as the Arab Spring unfolded, the optimistic perspective of Russian bloggers and independent media outlets diverged significantly from the position of the Russian Government, with the latter framing it as a cautionary tale of subversive online activity that could be used against Russia.[12]

In this environment, the introduction of increasingly intrusive online surveillance has been justified in order to mitigate the threats of terrorism, criminality and general instability. The Russian surveillance program, known as SORM (System for Operative Investigative Activities), has the power to remotely and automatically gather information from all communications media in Russia and store it for several years. Internet and telecom service providers are required to pay for the installation of surveillance boxes in their networks, which only the authorities can access.[13] Use of the internet in Russia is growing rapidly, and the SORM system is being strengthened to compensate. Nearly 60% of Russians now use the internet once a week or more, compared with less than 10% in 2006 and only 3% in 2001.[14] This growth in connectivity is likely to continue, in line with intrusive government efforts to monitor and control the Russian national information space.

A Chinese perspective

As a signatory with Russia to the International Code of Conduct for Information Security, China has a stated interest in promoting national sovereignty in cyberspace. Both countries are closely engaged in all major international debates on topics such as internet governance, cybercrime, state-sponsored espionage, and offensive actions in cyberspace.

There are also similarities in the way both countries view the threat from uncontrolled information:

> Russia and China seem to favour the use of the term control to a much greater extent than the United States. This difference is often reflected in internal debates and the need to restrict freedom on the web. Another common point is that both nations have developed long-term cyber plans. For China it is the Informatization Development Strategy and for Russia it is the Doctrine of Information Security.[15]

Yet, while they broadly agree on the desirability of state control and sovereignty over the internet, there are significant differences, particularly related to the challenges of implementing that vision. China's population (1.34 billion) is nearly ten times larger than Russia's (142 million), and includes a vibrant and expanding middle class that increasingly expects social and economic opportunities to continue to grow. Beijing views the greater use of information technology, or the 'informatization' of Chinese society, 'as a means to ensure sustained economic growth, compete globally in the information technology realm, and ensure national security. Informatization relies on information security systems that can support economic restructuring and national security.'[16]

From exploiting commercial opportunities to reducing cybercrime and maintaining national security and stability, the challenges faced by Beijing are relevant to its trading partners and allies around the globe in a way that eclipses Moscow's reach. This is a challenge for Chinese politicians and securocrats, who embrace authoritarianism but are often forced to be responsive to the demands of an increasingly empowered citizenry. Social media are often mentioned as barometers of public engagement and provide new ways to organise collectively to expose corruption, while at the same time government organs monitor and filter online communication in an attempt to maintain stability and harmony. Citizens' demands often gather momentum online before moving to the street, and they're occasionally successful when exposing the misdeeds of low- or mid-level officials. However, when criticism is directed at Communist Party leaders, or when collective action in the physical world is encouraged, the security response tends to be swift and uncompromising.[17]

The Communist Party's stated goals of maintaining political stability and single-party rule while opening China's economy

even further to global market forces are particularly difficult. Officials often cite foreign influence (particularly political influence) as a destabilising factor, and one that requires the steady, correcting hand of the state.[18] The oft-invoked metaphor of the 'Great Firewall' is only partly accurate—Chinese Government strategies of control and coercion are more nuanced than popularly believed:

> Firewall-type activity does indeed describe aspects of the Chinese approach to the internet. But it's been obvious for a while that the subtlety of the regime's approach to managing the network has gone way beyond the binary allow/disallow nature of the firewall metaphor. There are still occasional 'completely and immediately delete' instructions to website editors, but because of the rapid growth of social media the Chinese have realised that blanket bans have become a kind of nuclear option and that a more graduated approach is required.[19]

This nuanced system has been likened to a waterworks or a hydraulic project: 'Water, in this view, is both vital and dangerous: it has to be managed.'[20] Enough information has to be allowed to circulate to satisfy enough of the people enough of the time, while not endangering the positions of the political elite. This fits the Party's broader political strategy of moving China down the path of becoming a 'rich, strong country'.[21] The system of control is laborious but delicate, given the ease with which ordinary citizens can now make their voices heard. No longer is the elite political class the only voice that speaks for China on the international stage. It's now possible for external observers to gain a far more nuanced and subtle perspective of how non-elite groups in China engage in international and domestic debates (including those related to information security) and with each other.[22]

Hacking-related tensions between China and the US have increased to a level that's now worthy of attention from leaders of both countries, and although dialogue among senior officials is a positive step there's no guarantee it will produce a mutually agreeable outcome. While US officials and US-based companies such as Mandiant have made frequent and increasingly specific accusations about cyberattacks emanating from China, Beijing has only recently allowed officials to make statements that go beyond repetitive denials and the standard line that 'China is also a victim of cyberattacks.' A more nuanced strategy appears to be emerging, as the old language is coupled with emphasis on 'common exploration and cooperation' (in particular with the US) in order to reduce mutual mistrust.[23] In addition, organisations such as the China Computer Emergency Response Team are highlighting specific details of hacking against Chinese networks in an attempt to provide tangible evidence of cyberattacks against China.[24]

Chinese and Russian oppositional stances to Western models of internet governance have so far tended to attract the expected supporters, for example from post-Soviet states. The International Code of Conduct has received minimal international support, and the December 2012 World Conference on International Telecommunications (which dealt in part with aspects of internet governance) ended in an impasse.[25]

But China is making progress on other fronts. It appears to be gaining confidence in its ability to negotiate with the US as an equal on issues related to cybersecurity and internet governance. This may be partly due to improved internal coordination among government ministries in Beijing, owing to the frequency at which cybersecurity is now discussed at senior levels. That confidence is apparent on other sensitive issues as well, including during the highly disciplined negotiations with the US State Department over Chinese dissident Chen Guangcheng, who escaped house arrest and took refuge in the US Embassy in Beijing in April 2012.[26] This internal political coordination and professionalisation are likely to improve over time, as China's interests grow and become truly global.

Long-term Implications

In the past 20 years, a full one-third of the world's population, or 2.5 billion people, have been connected to the internet, but that pales in comparison with the change that awaits us in the next 20 years.[27] The private sector understands this well, having been the main driver of global digital interconnection, but governments are still coming to terms with the permissionless innovation permitted by digital technologies. Cyberspace is agnostic in this process, serving as a magnifying glass for pre-existing social, economic and political realities.

Government investment in tools that facilitate greater surveillance and control of cyberspace, including offensive 'cyberweapons', appears to dwarf similar investment in technologies and policies that can expand global internet connectivity in a vibrant and sustainable way.[28] In other words, the national security priorities of several select actors trumps the stability of the global Internet. Social concerns regarding online privacy and individual freedom are also being challenged. This is, after all, a domain ideally suited for observation and surveillance, whether by intelligence

agencies trying to improve their situational awareness or by companies trying to persuade potential consumers to part with their money.

The long-term risks of controlling behaviour could be significant. They include undermining the creativity and permissionless innovation inherent in the internet, as governments in newly connected countries invest in technology meant to protect the state against their citizens. It could also erode trust between allies and trading partners and hasten the fracturing of the internet along commercial or political fault lines. The international debate over how cyberspace should be governed is perhaps the most contentious and far-reaching contest for digital power, and in relative terms it's just begun. An international perspective is crucial, as it's increasingly beyond the ability of any single state to dominate cyberspace, no matter how hard some may try.

The dominant Western narratives on cyberspace (such as that technology is an inherently liberating force) are highly malleable, and often fall victim to internal dissonance and contradiction. The US Government isn't the only one (Western or otherwise) struggling to present and maintain a consistent and coherent narrative in the face of technological change and disruption, but it's one of the most visible. The US State Department's internet freedom agenda is a potentially useful mechanism for promoting liberal values, and also does no harm to US tech giants that benefit from increasing global connectivity. However, US claims to support freedom (already weakened by the so-called War on Terror) have been undermined further by recent revelations of large-scale internet surveillance by the US and its allies.

Convergence between the major cyberpowers on the methods and tools of digital control could mean the Western consensus becomes less liberal, while countries such as China and Russia could soften their authoritarian stances mildly in recognition that too much overt control can be economically damaging (for example, by discouraging foreign investment). Among all the major actors, this would probably manifest through greater coercion and covert online surveillance (compared to today), as well as an increasingly militarised posture towards digital threats.

While the rhetorical justification for this shift would be couched in the now-familiar language of protection against threats such as foreign terrorists, in practice it would permit vastly increased domestic situational awareness. Adopted at scale (that is, among the major states), it would have significant negative implications for the health and development of the internet. It would likely influence the digital development of countries that are just beginning to experience the benefits of digital connectivity and may be undecided about taking an authoritarian or liberal stance towards cyberspace.

Drawing distinctions

There's no complete convergence between these actors on the tools of online control; nor is that likely, given the difference in social and political structures.[29] There are tangible and enduring differences between the Russian and Chinese stances on the one hand and the Western consensus on the other hand. They include relative levels of individual freedom vis-a-vis the state, as well as states' adherence to the rule of law. For example, one recent US intelligence leak—that of Presidential Policy Directive 20, which sets the guiding principles for a range of offensive and defensive cyber operations—demonstrated exceptionally close attention to legal oversight (although one might question how effectively this works in practice, and across the intelligence community as a whole).[30]

There's no question that both the perception and the reality of individual freedom and state adherence to the rule of law are more robust among the Western nations than in China and Russia. The quest for national sovereignty in cyberspace is another difference. The Western consensus doesn't openly claim that the internet should be controlled, although some countries would very much like to surveil all of it. The question is, what factors may change that? If countries such as the US and UK had far less capability to monitor the global internet, would they, too, begin to explicitly advocate closer government control and sovereignty in cyberspace?

These differences are some comfort, but don't fully explain the motivations for states to compete in cyberspace. Social and, more importantly, economic factors are exerting pressure on the international dialogue. Those factors must be taken into account when interpreting government positions on, for example, internet governance, intellectual property rights, or offensive military actions in cyberspace.

From an economic perspective, the global financial crisis hasn't been kind to many Western states. The growing prosperity of China has benefited many of them, but Beijing's military growth is a primary area of concern due to its potential for regional destabilisation. Cyberspace may reduce the relevance of time and space, but countries in the Asia–Pacific region, such as Australia, Japan and South Korea, have understandable concerns about the intentions of their largest neighbour.

China is aiming for digital connectivity on a scale never before attempted. This will bring significant benefits but also permit the development of new tools of control that can be tested and exported to other authoritarian countries (which are just now getting connected). Western countries—the innovators and early developers of the internet—no longer have the option of dominating the internet governance debate by force of numbers. Who gets to define what the 'real internet' is, when China has as many internet users (about 564 million) as all of North America and Latin America combined? [31]

Some differences aren't as significant as they may appear. Governments are trying to catch up with the pace of change in cyberspace, and that could result in behaviours that appear different on the surface but hide similarities beneath. Adopting divergent positions and using strong rhetoric are popular options, for example when Russia wishes to distinguish itself from the US position on internet governance, or when the US wishes to claim the lead on 'internet freedom'. Below the surface lie common concerns about the internet as a threat to domestic security and stability, particularly because of the malign foreign influences that it may propagate, or because it's a challenge to entrenched political interests.

Conclusions

The challenges that lie ahead are significant. They go beyond domestic politics and will influence the international debate on topics such as internet governance, digital security standards, privacy rights, intellectual property protection, and individual and journalistic freedoms. For newly connected countries, the obvious route will be to adopt positions similar to those of the major actors, such as the US, the UK, Russia or China, and attempt to gain maximum situational awareness of their domestic networks.

While the positions of the major actors fall on a spectrum of control, there's a danger of that spectrum narrowing as illiberal convergence takes hold. Where undecided countries ('swing states') decide to place themselves on the spectrum depends on factors such as the economics of connectivity (is it cheaper to route traffic through specific countries?), the diversity of telecom providers, and of course on the level of domestic public engagement on issues of privacy and security.

Authoritarian governments will, at least in the short term, find it easier to persuade the swing states of the hypocrisy of the Western model of cybersecurity. From a political perspective, they'll find willing ears among governments that already have authoritarian tendencies and among leaders who are looking to solidify their political control. From an economic perspective, they'll gain traction with states that are contemplating major investment in such things as national broadband networks and are wavering between procurement from Chinese, US or European telecom giants.

Liberally minded states will find it more difficult to sustain their self-created image as the ethical stewards of the internet. They'll come under increasing challenge from illiberal and undecided states in multilateral forums such as the Seoul Conference on Cyberspace, the Internet Governance Forum, the International Telecommunication Union and ICANN. Western companies will come under much closer scrutiny when attempting to enter new markets. They're likely to more strongly resist the cooperative and coercive measures of Western governments. One example of this are the efforts by the US and UK signals intelligence agencies to influence the development of global digital security standards, thereby creating security vulnerabilities that allow for greater surveillance of online communication believed to be secure by individuals, businesses and other governments.[32] This desire for unlimited access to the world's data is eroding trust in Western tech giants, who have been forced to comply with demands from Western governments.[33]

Many governments and corporations are pursuing aspirations to control cyberspace. Despite political initiatives for internet freedom, or commercial initiatives to promote 'frictionless sharing' of the details of our lives, very few actions are based on purely altruistic motives. Many organisations are adapting to the changing digital environment and are using economic, social and political levers to enable or enhance their power. In many cases, that control requires the sacrifice of freedoms on the altar of security. And, although steps such as those are rarely so explicit, they're exceedingly difficult to reverse.

The desire for unfettered government and corporate access to and control of information should be resisted strongly by all who aspire to live in a liberal society, and who believe that democracy and ubiquitous surveillance are incompatible. All internet users are implicated in this process, although many don't realise it as they move through cyberspace leaving a trail of digital debris. These are challenges not only for the citizens of developed countries, who have become familiar with digital technologies, but also for the next several billion internet users (and more), who have yet to be connected.

Gone are the days when powerful Western nations could draw a clear dividing line between the behaviour of liberal and authoritarian states in cyberspace. It will require

sustained effort to raise public awareness, roll back government control, and reclaim the ground that's been lost to fears of terrorism and worries over diminishing national power. This process will be lengthy, and there's no single optimal balance between digital freedom and control. Each society must adapt its use of cyberspace to its societal norms, but as this process takes place, illiberal tendencies and their short- and long-term consequences should be recognised and challenged, and openness, transparency and public discussion of these issues should be encouraged.

Unlocking the potential of the information age requires more than bits and bytes. It needs committed individuals working to harness the power of those (agnostic) bits and bytes for the benefit of all users.

Notes

1 Juliette Garside, 'Nasdaq crash triggers fear of data meltdown', *The Guardian*, 23 August 2013, www.theguardian.com/technology/2013/aug/23/nasdaq-crash-data.

2 Keir Giles, 'Russia's public stance on cyberspace issues', in C Czosseck, R Ottis, K Ziolkowski (eds), *4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2012, www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.

3 These positions exhibit characteristics that could be categorised broadly as (a) Russia—entrenched authoritarian; (b) China—responsive authoritarian; and (c) Western consensus—liberal/paternalistic.

4 Glenn Greenwald, Ewen MacAskill, Laura Poitras, 'Edward Snowden: the whistleblower behind the NSA surveillance revelations', *The Guardian*, 9 June 2013, www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance#start-of-comments.

5 Andrei Soldatov, Irina Borogan, 'In ex-Soviet states, Russian spy tech still watches you', *Wired*, 21 December 2012, www.wired.com/dangerroom/2012/12/russias-hand/all/.

6 Adam Segal, 'China and information vs. cyber security', *Asia Unbound*, Council on Foreign Relations, 2011, http://blogs.cfr.org/asia/2011/09/15/china-and-information-vs-cybersecurity/.

7 Nate Anderson, 'Russia, China, Tajikistan propose UN "code of conduct" for the net', *Wired*, 21 September 2011, www.wired.co.uk/news/archive/2011-09/21/code-of-conduct.

8 Keir Giles, 'Internet use and cyber security in Russia', *Russian Analytical Digest*, no. 134, 30 July 2013, www.css.ethz.ch/publications/pdfs/RAD-134.pdf, pp. 3–4.

9 Alexey Kovalev, 'Russians express their frustration with explosion in political satire', *The Guardian*, 22 December 2011, www.theguardian.com/world/2011/dec/22/russia-frustration-leadership-political-satire.

10 Keir Giles, 'Russian cyber security: concepts and current activity', *REP Roundtable Summary*, 6 September 2012, www.chathamhouse.org/events/view/185483.

11 Alexey Kovalev, 'The problem with journalism in Russia is not censorship; that would be easy to deal with', *journalism.co.uk*, 10 November 2010, www.journalism.co.uk/news-commentary/-the-problem-with-journalism-in-russia-is-not-censorship-that-would-be-easy-to-deal-with-/s6/a541438/.

12 Bruce Etling, 'The Russian media ecosystem and the Arab Spring', *Internet & Democracy Blog*, 18 May 2011, http://blogs.law.harvard.edu/idblog/2011/05/18/russian-media-ecosystem-arab-spring/.

13 Andrei Soldatov, Irina Borogan, 'In ex-Soviet States, Russian spy tech still watches you', *Wired*, 21 December 2012, www.wired.com/dangerroom/2012/12/russias-hand/all/.

14 Mark Adomanis, 'Russia's internet use is exploding', *Forbes*, 18 May 2013, www.forbes.com/sites/markadomanis/2013/05/18/russias-internet-use-is-exploding/.

15 Jon Lindsay, 'China and cybersecurity: political, economic, and strategic dimensions', report from workshops held at the University of California, San Diego, April 2012, http://igcc.ucsd.edu/assets/001/503568.pdf, pp. 21–22.

16 Mark A Stokes, LC Russell Hsiao, *Countering Chinese cyber operations: opportunities and challenges for US interests*, Project 2049 Institute, 29 October 2012, p. 3, www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-079.pdf.

17 'China's internet—a giant cage', *The Economist*, 6 April 2013, www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled.

18 Chris Buckley, 'China takes aim at Western ideas', *The New York Times*, 19 August 2013, www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hard-line-in-secret-memo.html.

19 John Naughton, 'The great firewall of China gets metaphorical', *The Observer*, 13 July 2013, www.theguardian.com/technology/2013/jul/14/china-great-firewall-put-out.

20 'For sensitive topics on which central media have already said something, … the instructions may say, "Reprint Xinhua [the official Chinese news agency] but nothing more." For topics that cannot be avoided because they are already being widely discussed, there are such options as "mention without hyping"; "publish but only under small headlines"; "put only on back pages"; "close the comment boxes"; and "downplay as time passes".'— John Naughton, 'The great firewall of China gets metaphorical', *The Observer*, 13 July 2013, www.theguardian.com/technology/2013/jul/14/china-great-firewall-put-out.

21 Kerry Brown, 'What do Chinese leaders want?', *The China Story*, 2013, Australian Centre on China in the World, www.thechinastory.org/agenda2013/what-do-chinese-leaders-want/.

22 Brown, 'What do Chinese leaders want?'.

23 'China denies role in cyber-attacks on United States: claim themselves victim of hacking', *The Economic Times*, 20 August 2013, http://articles.economictimes.indiatimes.com/2013-08-20/news/41429211_1_cyber-attacks-cyber-crimes-domain.

24 Li Xiaokun, 'China is victim of hacking attacks', *China Daily USA*, 5 June 2013, http://usa.chinadaily.com.cn/china/2013-06/05/content_16567196.htm.

25 Milton Mueller, *ITU phobia: why WCIT was derailed*, Internet Governance Project, 18 December 2012, www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/.

26 'Over the course of the negotiations, the Chinese never put any proposals on the table. Their role was strictly reactive. At the end of each meeting, Cui would leave to report the latest terms to Chinese leaders. At times, he would enter the next meeting having come directly from the compound reserved for China's highest leaders. "We would put something forward, and were getting answers back almost immediately from the highest levels," one senior administration official said. "I have never seen the Chinese government working this rapidly and efficiently."'—William Wan, 'Negotiations over dissident Chen Guangcheng offered rare glimpse into how China's leadership operates, US officials say', *The Washington Post*, 19 May 2012, http://articles.washingtonpost.com/2012-05-19/world/35455319_1_chen-guangcheng-fang-lizhi-negotiations/2.

27 'Internet World Stats data shows 34.3% penetration worldwide for mid-year 2012. For mid-year 2020, we predict Internet world penetration will be in the range of 75–85%. For the majority of developed countries, our forecast is a 90% Internet user penetration rate.'— 'Internet users in 2020', *The Internet World Stats Blog*, 15 April 2013, http://internetstatstoday.com/internet-users-in-2020/.

28 Barton Gellman and Greg Miller, 'U.S. spy network's successes, failures and objectives detailed in 'black budget' summary', *The Washington Post*, 29 August 2013, http://articles.washingtonpost.com/2013-08-29/world/41709796_1_intelligence-community-intelligence-spending-national-intelligence-program

29 'In the US and Western Europe, a law enforcement agency seeks a warrant from a court and then issues an order for LI to a network operator or internet service provider, which is obliged to intercept and then to deliver the requested information. In Russia, an FSB operative is also required to get an eavesdropping warrant, but he is not obliged to show it to anyone. Telecom providers have no right to demand that the FSB show them the warrant. The providers are required to pay for the SORM equipment and its installation, but they are denied access to the surveillance boxes.'—Andrei Soldatov, Irina Borogan, 'In ex-Soviet states, Russian spy tech still watches you', *Wired*, 21 December 2012, www.wired.com/dangerroom/2012/12/russias-hand/all/.

30 Dave Clemente, 'A measured US policy for cyber offence and defence?', *Chatham House Expert Comment*, 9 June 2013, www.chathamhouse.org/media/comment/view/192131.

31 Charlie Osborne, 'China's internet population surges to 564 million, 75 percent on mobile', *ZDNet*, 15 January 2013, www.zdnet.com/chinas-internet-population-surges-to-564-million-75-percent-on-mobile-7000009813/; Internet World Stats, 'The Internet big picture—world Internet users and population stats', 30 June 2012, www.internetworldstats.com/stats.htm.

32 James Ball, Julian Borger and Glenn Greenwald, 'Revealed: how US and UK spy agencies defeat internet privacy and security', *The Guardian*, 6 September 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

33 Allan Holmes, 'NSA Spying Seen Risking Billions in U.S. Technology Sales', *Bloomberg*, 10 September 2013, http://www.bloomberg.com/news/2013-09-10/nsa-spying-seen-risking-billions-in-u-s-technology-sales.html

About the author

Dave Clemente is a Research Associate with the International Security Department at Chatham House. His areas of expertise include technology and cyber security policy and US and UK security and defence policy. He is the author of *Cyber Security and Global Interdependence: What is Critical?* (Chatham House, 2013) and co-author of *Cyber Security and the UK's Critical National Infrastructure* (Chatham House, 2011) and *On Cyber Warfare* (Chatham House, 2010).

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au
ASPI-ICPC http://cyberpolicy.aspi.org.au

RRP $5.00 ISSN 2200-6648