Norwegian Institute of International Affairs

Policy Brief
[2 / 2017]

China's cyber sovereignty

Niels Nagelhus Schia and Lars Gjesvik

Overview

This policy brief analyses China's ambitions for imposing and strengthening the concept of cyber sovereignty in international negotiations on topics related to cybersecurity and Internet governance (IG). The presentation proceeds through four interconnected steps:

1. brief introduction and background to the Chinese 'cyber sovereignty' concept
2. China's role in defining, developing, and promoting this concept in international politics
3. international responses to the Chinese use of the concept of cyber sovereignty, and how this should be seen in conjunction with current trends in Chinese foreign-policy strategies
4. the use of cyber sovereignty in diplomacy, and how China uses this concept to counter Western dominance in cyberspace.

Thus, the policy brief offers a brief examination of how the Chinese idea of state sovereignty in cyberspace influences how China positions itself in international negotiations with regard to issues such as security, economy and trade, and soft power (diplomacy/governance).

1) The Chinese Cyber Sovereignty Concept

Cyber sovereignty is a concept distinct from the more familiar term 'cybersecurity'. Whereas the latter concerns protecting the infrastructure and processes connected to the Internet, cyber sovereignty focuses on the information and content provided by the Internet. As presented in Lindsay (2015) China's cyber sovereignty concept is based on two key principles:

1. Unwanted influence in a country's 'information space' should be banned. In effect this would allow countries to prevent their citizens from being exposed to ideas and opinions deemed harmful by the regime.

2. Shifting the governance of the Internet from current bodies which include academics and companies, to an international forum such as the UN. This move would also entail a transfer of power from companies and individuals to states alone.

2) China's role in defining, developing, and promoting cyber sovereignty

The emergence of a clear Chinese stand on cyber sovereignty is in line with the broader trends of the country's foreign policy. After years of low-key foreign policy, China's emergence as a more assertive power over the last decade has become evident, not least in the cyber-area. What was once a domain where US companies could operate freely while Chinese ones played catch-up has been replaced by increasingly vocal disagreements on how it should be managed. (Raud 2016)

For China, cyber sovereignty is a part of the larger field of information security which is critical for maintaining its core values. China's concept of cyber sovereignty concerns its need to control narratives about the country, nation, and the party. This is a holistic approach that does not distinguish the challenges of maintaining the actual infrastructure of the Internet from the content and information that flow through it. The focus is on control and management over the Internet and its content. In this way, cyber sovereignty propels cyber security as a means of maintaining cyber sovereignty in China.

China has seen an explosive rise in net connectivity: whereas only 10% of the population had access to the Internet 10 years ago, the figure now exceeds 50% – more than 700 million netizens. (Stratfor 2016) As information about the state of affairs to an increasing degree comes from the Internet and smartphones, the Chinese leadership feels a growing need to control this information flow. Dependence on Western-made technologies is seen as a gigantic weakness that foreign actors can exploit. Managing this, and achieving greater technological independence, is therefore seen as crucial for China to remain fully independent. (Raud, 2016)

Contrary to the popular belief of China as an offensive cyber-power intent on raiding industrial secrets from the West, the main concern of the Chinese government is domestic stability. The diversity and size of the country makes controlling information and managing unrest a highly pressing issue, and cybersecurity is no exception – not least as information dissemination moves from stationary sources like network stations and newspapers, to more fluid sources like blogs and the social media (Stratfor 2016). In late December 2016, the CAC (Cyberspace Administration of China) presented a new strategy for the cybersecurity. This included a warning that internet usage for 'treason, secession, revolt, subversion or stealing or leaking of state secrets would be punished', also warned against anyone working with outside forces trying to subvert Chinas autonomy (Kleinwachter 2017).

In recent years Beijing's approach towards dissenters has become markedly stricter. As the regime's hold over the population has tightened, so have policies regarding cyberspace (Financial Times 2016). Cyberspace policies, which had long been piecemeal and incoherent, have become more uniformed and controlled from the very top (Inkster 2016). In that regard 2014 may mark a watershed: that year saw the formation of the leading small groups of Central Internet Security and the Information Leading Group, both chaired by President Xi Jinping. That the sitting president chairs a leading small group sends a strong signal on China's deep commitment to the issue. In that year the first annual World Internet Conference was held, the main arena where China promotes its foreign policy and stance on cyber security. (Raud 2016)

In 2015, cyber sovereignty was described by Lu Wei, then head of Cyberspace Administration of China (CAC), as the difference between a 'multi-stakeholder' and a 'multilateral' approach. Basically, the difference boils down to what extent the primacy of the state is valid in the cyber domain. (Lu Wei 2015) The concept is a key part of Chinas broader cyber policy, and has been promoted from the highest levels. In a speech held in 2015, Xi Jinping warned the world about the destabilizing prospects of not allowing countries to govern their own cyberspace according to their own rules (Xi Jinping 2015). However, in late 2016, Beijing's stance seemed to soften slightly when Chinese officials introduced and recognized the term 'multi-party governance' as their alternative to the 'multi-stakeholder' concept (Kleinwachter 2017). This 'softer' idea of cyber sovereignty is re-stressed in the 2017 'International Strategy of Cooperation on Cyberspace' which emphasizes the need for both multilateral governance of the Internet, and multi-party participation in this governance – including companies, organizations, and technological communities.

This uncertainty indicates a fundamental dilemma facing Chinese policymakers. The Internet is perceived as a huge threat to Chinese stability, but also as necessary for the country's development goals. Striking the right balance between openness and repression is a delicate issue. One of the main ways China has tried to balance these two concerns has been by promoting domestic companies and giving them a stake in the regime. Notable business figures, like as Alibaba-founder Jack Ma, has been accorded a role in forming and promoting Chinese policies (Lindsay 2015).

3) International responses

International responses to China's attempts to apply the cyber sovereignty concept in practice have been overshadowed in the West by Chinese industrial espionage and hacking, even though cyber security concept might have far greater importance in the future (Inkster 2016, 14). Indeed, the concept has been attracting greater attention recently, with the USA expressing concerns that China uses its policies as a cover for censorship, protectionism and espionage. It has been noted, for instance, that 'In June 2015, China passed the National Security Law with the stated purpose of safeguarding China's security, but it included sweeping provisions addressing economic and industrial policy. China also drafted laws relating to counterterrorism and cybersecurity in 2015 which, if finalized in their current form, would also impose far-reaching and onerous trade restrictions on imported ICT products and services in China' (Aaronson 2016)

The introduction of legislation that allows the government enhanced control over the Internet is not, exclusive to China or other authoritarian regimes. Russia, Iran and Saudi Arabia have also taken steps in that direction – but so have European countries such as the UK, Poland and Hungary, indicating that the clear democracy–non-democracy divide might not be as applicable as it seemed just a few years ago (Kleinwachter 2017). This control approach has also found favour in developing countries, who see themselves at a digital disadvantage and vulnerable to globalization (Inkster 2016, 10). That being said, there is still a distinct line between the countries that seek an open Internet and those who want it to be under stricter control, but this gap may be closing in some areas. Some issues, such as companies aiding the government when requested, are high on the agenda in the USA as well. An example of this is the FBI–Apple encryption case, where the agency wanted the company's assistance in hacking the phone of an arrested terrorist (Stratfor 2016). US companies have also increasingly turned to the government to protect them from foreign intrusion into their networks (Aaronson 2016).

The Chinese concept has encountered deep scepticism among some NGOs. Prior to the 2015 World Internet Conference, Amnesty International called on companies to take a stand and denounce the Chinese position, stating that talks about sovereignty were in fact an 'all-out assault on internet freedoms' (Amnesty 2016). Freedom House has consistently ranked China as one of the worst, and sometimes the worst, country with regard to internet freedom. The strategy of pursuing cyber sovereignty, and the ways it is applied, have been seen as the main reasons why China is considered worst in class (Freedom House 2016).

4) Cyber sovereignty in diplomacy, and how China uses it to counter Western cyber dominance

Beijing's position in international diplomacy has changed from a more passive and reactive approach in the past, to the current stance which is largely proactive and seeks to influence the shaping of the global agenda (Inkster 2016, 109). Chinese tactics for furthering these aims can be summarized as leveraging the large user community to gain concessions, build and support domestic companies, advocate the concept of cyber sovereignty in international for a, and constructing information networks in the developing world (ibid.,

15). Another important, and unorthodox, tool has been the swarming of the agenda – notably with the 2015 meeting of the Internet Engineering Task Force, where China sent 40 delegates whereas most Western countries sent only one or two (ibid. 120).

The final part of this strategy involves building coalitions and partnerships to counter the perceived US dominance in the field (Inkster 2016, 15). Traditionally the concept of cyber sovereignty was linked to the more repressive of Middle Eastern regimes, and as such it did not figure greatly in the wider world. China's adopting this agenda marked the first time a major power supported the idea of cyber sovereignty. Other major authoritarian countries, such as Russia, have in the past taken a somewhat incoherent and at times liberal stance towards internet autonomy, but in recent years they have moved towards the Chinese position (Burgman 2016).

The Snowden revelations in 2013 provided a boost for the cyber sovereignty movement, as it showed how user data could be, and were, utilized for espionage purposes. Some of the goals of the cyber sovereignty movement, like storage of user data within each country, have been favoured by non-authoritarian countries such as Brazil and Germany. This has also allowed China and its allies to frame the counter-arguments against the cyber sovereignty movement as a smokescreen for what they see as the real goal: allowing the NSA access to user-data. (Schneier 2015, 187–188)

China has promoted its agenda in various diplomatic settings, trying to establish a broad coalition of states that agree on the principle. The 2016 BRICS summit in Goa underlined the primacy of states in developing the agenda, while also admitting that other stakeholders deserved a say and a voice in the process (Kleinwachter 2017). Another arena where China has pushed its agenda is the Shanghai Cooperation Organization (SCO), a still-expanding group of China, Russia, and several Central Asian countries. The main position taken by these countries is the primacy of the nation state, and its applicability in the cyber realm as well (Raud 2016).

Framing the issue of potential US interference is both a strategy and a real concern. One of the major fears is of the West, and the USA particularly, advocating its own interests through the superficially 'neutral' Internet. According to this logic, NGOs and Western media are engaged in undermining governments not to the West's liking. Such thinking is in part based on recent history – like Colin Powell's infamously telling NGOs they were a 'force multiplier' during the Iraq War. Statements like this have stoked the fears of authoritarian regimes that Western civil society is in fact little more than an extended propaganda arm. Washington is also keen on US companies contributing to the national interest when this is deemed necessary, reinforcing the idea that the Internet is partly a tool of the USA (Malcolmson, 2016).

Fang Binxing, credited as the creator of China's famous Great Firewall, presented this view in his remarks to the China–Russia forum on Internet sovereignty in 2016. He claimed that the fact that much of the Internet infrastructure was located in the USA meant that Internet governance today was under US control. The point is not to add the concept of government control to the Internet of today, but to force the USA to share the control that it already has. By framing the issue in this manner, China seeks to establish a narrative wherein state power already exists in the cyber realm, but where the USA is a hegemon. Establishing national sovereignty would therefore not be about the issue of censorship of the Internet, but about including more actors than the USA in its governance (Malcolmson 2016). This argument is in line with broader trends in Chinese foreign policy calling for a 'democratization of international relations' – moving away from the perceived Western dominance of international affairs towards a more inclusive order with greater respect for autonomy and the internal affairs of states (Xinhua Net 2014).

The 'US dominance' of the Internet does reflect some basic facts, but the influence is subtle and done with a 'light touch'. The various actors involved in its governance collaborate through their own perceived self-interest in spreading a way of governing that is inherently Western. Moreover, the idea of a globalized integrated world is (or at least was) seen as being in the US interest (Lindsay 2015). The diplomatic strategy utilized by China has already scored some minor victories. The Obama administration's decision to move the regulatory Internet Assigned Name Authority out of the chamber of commerce and to the international community has by some been credited to the effective diplomacy of China and Russia (Lindsay, Cheung, Reveron 2015).

An issue to watch is the potential for a turf war between the multi-stakeholder approach of the ICANN and the intergovernmental approach of the ICU (a UN sub-body). There has been tentative agreement on the sharing of responsibilities since 2014, but 2016 saw some developments that might hint at a less certain future (Kleinwachter 2017). Another pressing issue, with uncertain consequences, has been the debate about the alleged hacking of the 2016 US presidential elections and how this will influence perceptions of information sovereignty in the West.

Things to watch for

- Whether China continues to open up space for non-state actors in its governance agenda. 2016 saw the inclusion of multilateralism in Chinese rhetoric, so whether China moves towards greater openness or more control in 2017 will be important.
- Whether the big hackings of 2016, especially the US election, will change the Western position. Information warfare and campaigns to influence democratic processes will probably continue well into 2017.
- Whether more powers will be shifted from current institutions to intergovernmental ones.
- The USA, with its intelligence partners, has until now enjoyed a major advantage over China and other countries due to its ability to monitor global networks. This advantage, while still significant, is eroding fast – especially in the developing world, where China has become the leading provider of the hardware and infrastructure needed for these networks. With this development continuing, the issue seems set to rise in importance in the years to come. (Inkster 2016, 15–17)

Sources

- Aaronson, Susan Ariel, 2016. 'The Great Moderation? China and the US in Cyberspace', http://www.chinausfocus.com/peace-security/the-great-moderation-china-and-the-us-in-cyberspace Accessed 13.01.2017

- Amnesty International, 2016. 'Tech Companies Must Reject China's Repressive Internet Rules'. https://www.amnesty.org/en/latest/news/2015/12/tech-companies-must-reject-china-repressive-internet-rules/ Accessed 10.01.2017
- Burgman, Paul Jr., 2016 "Securing Cyberspace: China Leading the Way in Cyber Sovereignty', 18.05.2016 http://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-in-cyber-sovereignty/. Accessed 13.01.2017
- Financial Times, 2016. 'Xi's China: Smothering Dissent', 27.07.2016. https://www.ft.com/content/ccd94b46-4db5-11e6-88c5-db83e98a590a Accessed 08.03.2017
- Freedom House, 2016. Freedom on the Net 2016, https://freedomhouse.org/report/freedom-net/freedom-net-2016 Accessed 13.01.2017
- Inkster, Nigel, 2016. China's Cyber Power. London: Routledge/IISS.
- International Strategy of Cooperation on Cyberspace, 2017. http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_2.htm 01.03.2017 Accessed 09.03.2017
- Kleinwachter, Wolfgang, 2017 'Internet Governance Outlook 2017'. http://www.circleid.com/posts/20160106_internet_outlook_2017_nationalistic_hierarchies_multistakeholder Accessed 13.01.2017
- Lindsay, Jon R. 2015. 'The Impact of China on Cybersecurity, Fiction and Friction', http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf Accessed 13.01.2017
- Lindsay Jon R., Tai Ming Cheung and Derek S. Reveron, 2015. China and Cybersecurity. Oxford: Oxford University Press.
- Lu Wei, 2014. 'Cyber Sovereignty Must Rule Global Internet', Huffington Post, 15.12.2014. http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html Accessed 10.01.2017
- Malcolmson, Scott, 2016.'How Russia and China are Cooperating to Dismantle America's Dominance of the Internet', Huffington Post, 05.05.2016. http://www.huffingtonpost.com/scott-malcomson/russia-china-internet_b_9841670.html
- Perritt, Henry H. 1998. 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance', Global Legal Studies Journal, 5(2): 423–42
- Raud, Mikk, 2016. 'China and Cyber: Attitudes, Strategies, Organisation', https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf Accessed 13.01.2017
- Sassen, Saskia. 1998. 'On the Internet and Sovereignty', Global Legal Studies Journal,.5(2): 545–59.
- Schneier, Bruce, 2015. Data and Goliath. New York: W.W. Norton
- South China Morning Post, 2017. 'The Who, What and Why in China's Latest VPN Crackdown, 26.01.2017,
- http://www.scmp.com/news/china/policies-politics/article/2065432/who-what-and-why-chinas-latest-vpn-crackdown Accessed 08.03.2017
- Stratfor Analysis, 2016. What the Great Firewall of China Can't Keep Out, 08.11.2016. https://www.stratfor.com/analysis/what-great-firewall-china-cant-keep-out Accessed 13.01.2017
- Xi Jinping, 2015. Speech to World Internet Conference. http://www.bbc.com/news/world-asia-china-35109453 and https://www.youtube.com/watch?v=GNR3MV9C2-Q Accessed 10.01.2017
- Xinhua Net, 2014. 'Chinese President Calls for Greater Democracy in Int'l Relations', 28.06.2014, http://news.xinhuanet.com/english/china/2014-06/28/c_133445551.htm accessed 08.03.2017

Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

About the authors:

Niels Nagelhus Schia is a Senior Research Fellow in the Security and Defence research group at the Norwegian Institute of International Affairs and programme manager for NUPIs Cyber Security Forum.

Lars Gjesvik is a Research Assistant in the Security and Defence research group at the Norwegian institute of International Affairs.

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no