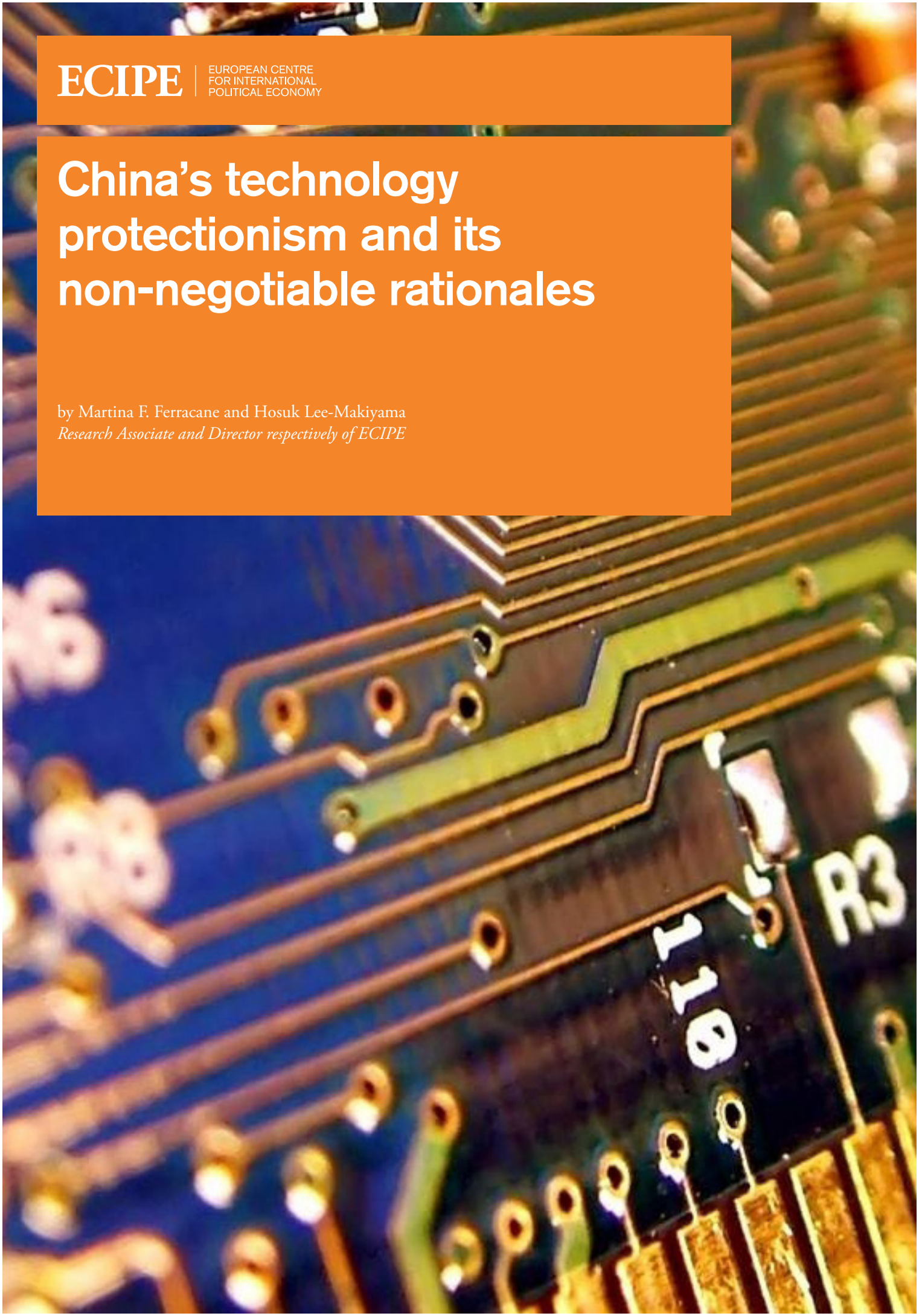
ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

China's technology protectionism and its non-negotiable rationales

by Martina F. Ferracane and Hosuk Lee-Makiyama
Research Associate and Director respectively of ECIPE



1. INTRODUCTION: CHINA'S DIGITAL DILEMMA

With more than 700 million internet users, a foreign exchange reserve of 3 trillion USD, leading manufacturers like Huawei and Lenovo, and the emergence of online services like Baidu, Alibaba and Tencent, China has all the components to become a global player in the internet economy. Yet it is not. Although the Chinese economy is overall more open since its accession to the World Trade Organisation in 2001 and its entry into the open trading system, there are still important exceptions: The internet economy and the ICT sector are but an intricate web of regulations which are increasingly tightening.

China is in a dilemma the Roman historian Livy famously described as «unable to neither bear its ills nor its cure».”

China imposes more trade and investment barriers, discriminatory taxes, and information security restrictions than any other country by a vast margin. Moreover, China's legal and technical infrastructure for online censorship remains pervasive and blocks not just politically sensitive content, but also the majority of foreign commercial platforms and intermediaries. China's rationale for these restrictions is increasingly complex, and not merely about shielding the country from security threats or foreign competition. In some cases, restrictions are deemed necessary to defer challenging reforms: The Chinese economy is constantly on the verge of market failure that is avoided through government interventions and short-term restructuring. A user-driven internet economy hampers the ability to deploy such short-term fixes, forcing the Chinese leadership to deal with the underlying causes. In other words, opening up the internet brings about many belated structural reforms.

Although China's technology restrictions allow the Chinese leadership to protract economic and political reforms, inaction also comes at a cost: Further digitalisation is necessary to spur consumption, improve industrial productivity and revitalise export competitiveness. China's engine for economic growth – ample labour supply and investments – has already run its course. Demographics are putting an upward pressure on wages, while investments (eclipsing nearly half of China's GDP) are ending up in non-productive use.

This is why China is in a dilemma the Roman historian Livy famously described as “unable to neither bear its ills nor its cure”. On one hand, opening up its digital economy necessitates a number of destabilising reforms, especially if they entail fiscal decentralisation or changes in its constitutional structure; on the other hand, deferring reforms worsens the dangerous economic slowdown, that is certain to lead to social unrest too.

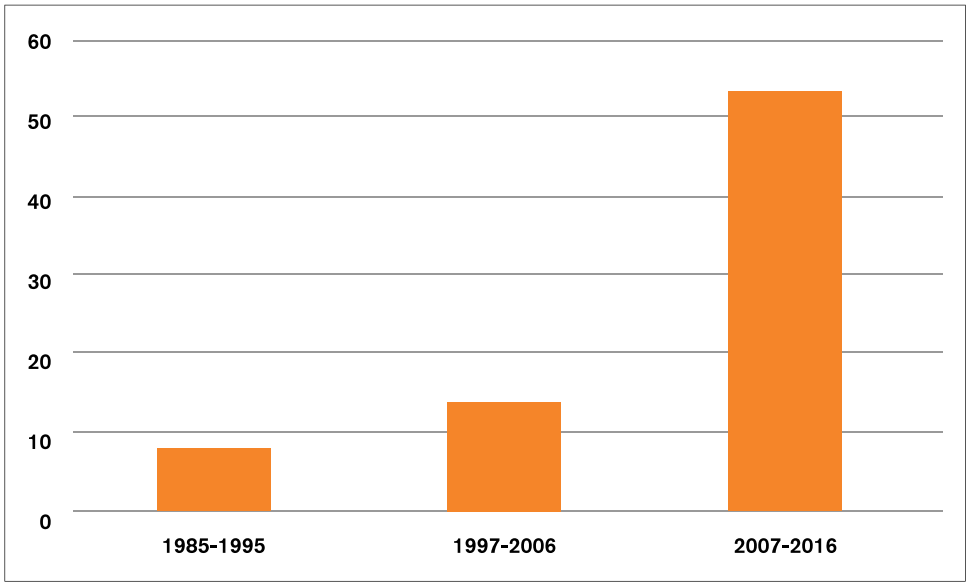
China's trading partners – the leading online service and technology exporters in Europe, Japan and the US – are caught in a similar Livian dilemma: As it stands, China's trading partners lack any effective leverage against China's digital protectionism besides “reciprocity” – i.e. closing their own economy in retaliation. However, such cause of action is contrary to the long-term goal of integrating China and the emerging markets into an open economic order.

2. THE RAPID EVOLUTION OF DIGITAL BARRIERS

Sixteen years after China's entry into the WTO, the Chinese business environment is inarguably improving, and the use of mobile and internet services has improved social and commercial interactions within China. This development is evident from a number of trade and business metrics (e.g. the World Bank's Doing Business index). However, this progress is contrasted by an increasingly intricate web of regulations that inhibit foreign participation in the China's digital economy, and discrimination of online services compared to their brick and mortar equivalents.

This increasing number of discriminatory measures is symmetrical across the value chain, from upstream to downstream – from infrastructure and mobile equipment that carries the digital backbone to downstream online services, apps and the cloud – and the measures affect production as well as usage by public and private sectors.

FIGURE 1: NUMBER OF MEASURES RESTRICTING ICT AND DIGITAL TRADE IN CHINA, 1985-2016



Source: Digital Trade Estimates Database, May 2017

As evident, the number of barriers against the ICT and the online market is substantially increasing (figure 1). Some of the measures actually pre-date the time of public commercial use of the internet and before a proper ICT structure (with the use of PCs, broadband and mobile networks) took hold of the economy. Such regulations were designed for an offline world, but provided legal ground for later invented technologies. For example, the State Security Law (passed in 1993) provides the state security organs with access to any information or data held by an entity in China whenever they deem it necessary.[1] Without doubt, the scope of the State Security Law has grown exponentially in the digitalisation era.

However, the majority of the restrictions in China were introduced in the last decade, as 54 (out of 76 identified in total) were implemented after 2007, with 27 new measures in the last three years alone, where the majority concerns usage and transfer of electronic data (Figure 2). Other commonly used policies in the regulatory toolbox relate to national standards and intellectual property rights (IPRs), as well as restrictions on tariffs, trade defence and internet content access. Fewer measures are found in business mobility and competition policy. But the number of measures alone does not always provide a full picture of the actual restrictiveness applied.

Regardless of the policy field the restrictions occur, some objectives are recurring to justify these restrictions. A common objective relates to the implementation of a national industrial policy, with a clear goal to encourage the emergence of national champions. Although the history of Asian industrialisation shows that such protectionism tends to be phased out, as competitive

[1] Article 11 of the State Security Law stipulates that "where state security requires, a state security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual". In addition, Article 18 stipulates that "When a State security organ investigates and finds out any circumstances endangering State security and gathers related evidence, citizens and organizations concerned shall faithfully furnish it with relevant information and may not refuse to do so".

producers emerge and the economy transitions into export orientation, China's case may be different: Not all of China's national champions are destined for export orientation. Some policies are intended to protect purely inward-looking state-owned enterprises (SOEs) and public investments by various investment vehicles controlled by provincial and municipal governments.

FIGURE 2: NUMBER OF DISCRIMINATORY MEASURES CURRENTLY IN FORCE IN CHINA, 1985-2016

Source: Digital Trade Estimates Database, ECIPE, May 2017

China has also a number of measures with the objective to support public safety and morals, especially for the public use of the internet. Such restrictions have a long history in China, going back to government control of publishing and trade in printed matter, traditionally retained to control public opinion. Moreover, the fourth recurring objective is national security – which has justified the enactment of an increasing number of measures affecting supply of equipment, software and services into China's business and government sector.

3. MEASURES SUPPORTING INDUSTRIAL POLICY

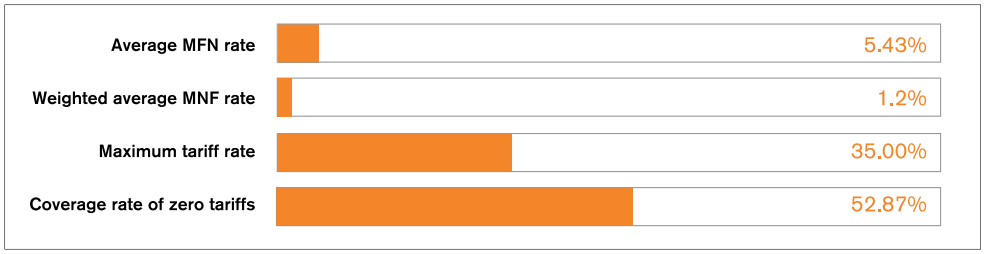
China has embarked on a comprehensive national plan to promote the internet and ICT sector, with the current five-year economic plan until 2020 being called 'Internet Plus', that depends heavily upon the internet and technology to reinvigorate a slowing economy. With increased R&D spending but decreasing its dependency on foreign imports and non-domestic innovations, the new five-year plan also echoes strongly import-substituting industrial plans like 'Made in China 2025' for local manufacturing and the National IT Development Strategy to secure core ICT technologies, such as semiconductors and enterprise software, and turn towards export-orientation.

At best, the government-led industrial planning in China (and elsewhere) has had an ambiguous track record. Policies that promote specific industries, technologies or firms are prone to fail, as policymakers act from limited information and knowledge in areas of rapid and unexpected technological change. National industrial policies are often captured by uncompetitive actors backed by powerful regional or special interest, making old-fashioned industrial policy a self-defeating exercise of sub-optimal allocation. As cost-effective access to ICT equipment and intermediary goods and services are important for all economic sectors, import substitution affects the competitiveness of the Chinese economy as a whole.

China is hardly the first or the last country to pursue an industrial policy objective through a mercantilist trade policy. Currently, the policies tariffs applied on digital goods being imported to China are similar to the levels applied in India, but higher than those applied in the vast majority

of developed and emerging economies at the equivalent level of development as China.[2] Thanks to China's participation in the ITA agreement and its expansion in 2016, the coverage of products with zero-tariffs is relatively high (52.9 percent). However, the country has tariff peaks of 35 percent applied to certain ICT products and inputs, including lithium batteries (that are subject to comprehensive Chinese government support), electric parts, wirings and any type of audio-visual devices (music players and televisions).

FIGURE 3: TARIFFS APPLIED ON DIGITAL GOODS IN CHINA[3]



Source: UNCTAD TRAINS Tariff data

Although the use of trade defence instruments in the ICT sector is rare globally, China imposes anti-dumping duties on several products, such as optical fibres (from the European Union, Japan, Korea, India and the United States). Import licensing procedures apply to chemicals, machinery and components used by the ICT industry are also subject to archaic customs inspection management.[4] On the export side, China imposed a set of quantitative restrictions through the export duties and quotas on rare earth metals used in electronic components,[5] resulting in a WTO ruling in 2014. These measures are directly or indirectly retaliatory to a heightened geopolitical situation where China used its supply-chain control during a time of territorial and trade disputes.

Similar to many jurisdictions, China's public procurement framework contains an active "Buy Chinese" policy to support national production. Yet, unlike other such policies that work on a negative list basis (i.e. generally open to non-nationals besides explicit exceptions), China's public procurement policy operates on a positive list basis, where foreign entities are only allowed in explicitly stated exceptions. China's public procurement measures go beyond what is deemed justified by security concerns, and have clear commercial objectives. It is also reported that central and local entities tend to implement these provisions in sweeping manner, going beyond the discrimination required by law, and there are also reports of insufficient notification of public tenders.[6]

China has also non-fiscal policies and strategies linked to its restrictive public procurement. One such example is its support for indigenous innovation, where only enterprises having the status of a national legal person can apply for accreditation of a product in the ICT sector, which serves

---

2. Lee-Makiyama, *Future-proofing World Trade in Technology*, ECIPE, 2011
3. ECIPE DTE covers Argentina, Austria, Australia, Belgium, Brazil, Brunei, Bulgaria, Canada, Chile, China, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Ecuador, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Pakistan, Panama, Paraguay, Peru, The Philippines, Poland, Portugal, Romania, Russian Federation, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Kingdom, United States, Vietnam.
4. See MOFCOM *Notice 97/2013*. December 31, 2013. Ministry of Commerce (MOFCOM); also *Notice of the Customs Tariff Commission of the State Council on the Tariff Execution Plan* (Shui Wei Hui [2013] No.36)
5. Including graphite, cobalt, copper, lead, chromium, magnesia, talcum, tantalum, tin, antimony and indium. Some of these raw materials (e.g. graphite, copper, tin, and indium) are used to produce smartphones and batteries.
6. ECORYS, *Evaluation of the EC Market Access Partnership. In-depth assessment of the functioning of the local Market Access Team in China*, Rotterdam, August 25, 2012

as a guidance to government purchases.[7] In order to be accredited, a product must have been manufactured by an entity that has full ownership of intellectual property rights in China, either by creating the rights or by acquiring them.

Although the goal of these policies is to encourage domestic innovation and to build national champions by providing financial incentives, non-resident foreigners must effectively appoint an officially designated Chinese to act as agent in patent application processes, or pay into a local joint-venture to have access to China's public procurement market. Another fiscal measure supporting indigenous innovation is a preferential regime of corporate taxation for 'high-tech' firms. Chinese companies categorised as 'hi-tech' pay a lower corporation income tax rate of 15 percent, compared to the statutory rate of 25 percent given the company is registered in China and has a certain portion of R&D activities conducted in China.[8] One of the companies that benefitted from the regime is Alibaba. Additionally, tax rebates are offered for self-produced software reducing the effective VAT payments to about 3-6 percent.[9]

The above-mentioned measures are designed to limit foreign participation on the domestic market. However, other policies are export-contingent, with the purpose of facilitating exports on a discriminatory basis. China Ex-Im Bank, China Development Bank and Sinosure offer their export credit and insurance schemes to natively Chinese companies only, excluding foreign-owned producers in China. Although export credits and insurances are permitted per se under WTO rules, they may have trade distorting effects and it is not given that these credits are always WTO compliant.

"The extent to which China applies its trade policy to support its industrial objectives is unprecedented."

China has to date avoided a legal case on its export credits, as the country has not established a commercial interest reference rate (CIRR) for its currency, avoiding comparisons that would indicate subsidised loans below the reference rate. Also, the interest rates are individually set for each export arrangement, and remain undisclosed, or local governments allegedly assume the liabilities of the company.[10] Nonetheless, nearly half of China's Ex-Im credits are classified as 'High and New Tech Products' or electronics. In order for foreign-invest firms (whose products are manufactured in China) to benefit from these rates, they must sell out to a local partner and form a joint venture. Additionally, one of the main conditions stipulated in the terms of export credit is that local content should be above 60 percent of the contract value, effectively making export credits also a local content requirement.[11]

China's industrial policies may have the same 'soft' mercantilist objectives as other major economies, like the US' "Buy America" policy, or the EU tariff protection on consumer electronics. However, the extent to which China applies its trade policy to support its industrial objectives is unprecedented. Furthermore, China's fiscal and procurement policies (where both local production and nationality are pre-requisites for qualification) are unique in their discretionary power to select winners, and per default discriminate foreign participation.

---

7 Chow, *China's Indigenous Innovation Policies and the World Trade Organization*, 34 Northwestern Journal of International Law & Business. 81, 2013

8 China-Briefing, *China's Tax Incentives for High-Tech Enterprises*, August 8, 2013: http://www.china-briefing.com/news/2013/08/08/chinas-tax-incentives-for-high-tech-enterprises.html

9 EUSME Centre, *ICT Market in China*, 2011: http://www.iberchina.org/files/china_ict.pdf

10 Lee-Makiyama, *Chasing Paper Tigers: Need for Caution and Priorities in EU Countervailing Duties*, ECIPE, 2011

11 OECD, *Chinese Export Credit Policies and Programmes,* Working Party on Export Credits and Credit Guarantees, TAD/ECG(2015)

4. MEASURES FOR INFORMATION CONTROL AND PUBLIC ORDER

There are reports of how the Chinese internet is increasingly plural and inclusive. A majority of bloggers expressing political opinion is also critical of the government, which also serves as an effective safety vent to release the pressure for its citizens. However, China also maintains the most effective control the internet and its usage by the public: A nationwide blocking, filtering and monitoring system delays or interrupts access to international websites through the Great Firewall of China (GFW), also known domestically as the "Golden Shield". This system is based on centralised control over international gateways, filtering online content or blocking access entirely to some of the most common websites on the public internet, and the authorities have also shut down online access to entire communications systems in response to specific events, notably imposing a 10-month internet blackout in the Xinjiang Uighur Autonomous Region in 2009 to quell "social unrest".[12]

Such disproportionate blackouts are nowadays rare, and would most likely backfire amongst China's mobile users today. Yet, most web applications are still blocked and the video-sharing platform Youtube and social media sites like Facebook, Twitter, Google+ and Foursquare remain inaccessible. New services that are introduced on the global internet are blocked by default, and the list of blocked services grows incessantly: Document-sharing applications like Google's cloud storage and other Google applications like Calendar and Translate became inaccessible in June 2014; a month later, KakaoTalk and Line, two South Korean messaging apps, were disrupted by Domain Name System (DNS) tampering and http-request filtering for users based in China. Beijing informed Seoul it had blocked access to the apps, claiming terrorist organisations were using them to incite attacks and spread bomb-making instructions.[13] Since 2012, the GFW has also started to block Virtual Private Networks (VPNs), commonly used to circumvent the GFW. Users on blogs, microblogs, instant-messaging services, forums and comment sections are now also required to register with their real names and avoid spreading content that challenges national interests.[14]

"Chinese online censorship has some commercial rationale but it is ultimately a question of control."

China's online blockages are affecting services originating from overseas, while their domestic counterparts with identical functionalities are not. This is particularly evident from the asymmetrical treatment of e.g. domestic search engines (which are closely supervised), while foreign search engines are simply blocked. There are indications that Chinese online censorship has a commercial rationale,[15] making it vulnerable for a WTO challenge, but ultimately – China's internet management system is a question of control to maintain order.

The Great Firewall, whose existence had neither a legal basis nor was officially admitted, has transitioned into *ex ante* license regime for providing online content in China. The Internet Content Provider (ICP) license is required to operate any website in China, applying to both domestic and foreign businesses.[16] However, licensees must admit to Chinese jurisdiction, establish locally and prevent inappropriate content from circulating as part of licensing requirements. Sina – the leading online media content provider, and owner of Weibo microblogging platform – had its

---

12. Freedom House, *Freedom on the Net Report: China*, 2014

13. Segal, China, *Encryption Policy, and International Influence*. A Hoover Institution Essay. Series Paper No. 1610.

14. Standing Committee of the National People's Congress, *Decision on Strengthening Online Information Protection*, December 28, 2012

15. Hindley, Lee-Makiyama, *Protectionism Online*, ECIPE, 2009

16. State Council, *Telecommunications Regulations of the People's Republic of China*. Decree of the State Council of the People's Republic of China No. 291, September 25, 2000

online publication license revoked in 2014 for allegedly having spread online publications with banned content.[17]

The imperative to maintain information control stretches also to the telecommunication sector, where all the operators have remained under government ownership. The prohibition of foreign investment in "internet publishing" in the 2015 Foreign Investment Industrial Guidance Catalogue follows the same rationale, and is reaffirmed in a new set of guidelines published in March 2016 that impose strict guidelines on what can be published online and how the publisher should conduct business in China, while "foreign joint ventures and cooperative ventures, and foreign business units shall not engage in online publishing services".[18] These guidelines also require any publisher of online content, including "texts, pictures, maps, games, animations, audios, and videos" to store their "necessary technical equipment, related servers and storage devices" in China.[19] In 2017, the Cyberspace Administration of China (CAC) released additional regulations that extend restrictions on what news can be produced and distributed by online platforms.[20] The new regulations require all services – including all political, economic, military, or diplomatic reports or opinion articles, whether they feature on blogs, websites, forums, search engines, instant messaging apps or any other platforms – to be managed by party-sanctioned editorial staff. Such staff has to be approved by the national or local government internet and information offices, while their workers must receive training and reporting credentials from the central government.[21]

The public safety objective is explicitly spelled in a number of recent laws. A new counter-terrorism law of 2016 requires companies to monitor user behaviour to ensure public safety.[22] Telecom and internet services providers must establish content monitoring and network security programs, and adopt precautionary measures to prevent the dissemination of information on extremism, report terrorism information to the authorities in a timely manner. In addition, they have to keep original records, and promptly delete such messages to prevent further circulation. The same law requires providers of telecommunication, internet and financial services to conduct identity checks of their customers or clients, and refuse to provide services to those that decline to provide such information. Another law on mobile apps, or "Mobile Internet Application Programs"[23] requires app providers to monitor online content and keep records of user violations and report them to the relevant government authorities.[24]

The new laws for online services and apps are in addition to the existing requirements for internet intermediaries, who are already given responsibility to monitor the behaviour of users on their platforms.[25] The extended liabilities have also started to apply to cloud service providers through an amendment of criminal code where failure to implement adequate measures leading to "illegal use of internet" was defined as being accomplice of committing internet crime. These

---

17. Reuters, *Sina shares fall after China strips its licence in web porn crackdown*, April 24, 2014

18. State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) and Ministry of Industry and Information Technology (MIIT), *Administrative Regulations for Online Publishing Services ("Online Publishing Regulations")*, February 14, 2016

19. QUARTZ, *Beijing is banning all foreign media from publishing online in China*, February 18, 2016

20. Cyberspace Administration of China (CAC), State Council Information Office (SCIO) and Ministry of Industry and Information Technology (MIIT), *Provisions on the Management of Internet News Services*. May 2, 2017

21. Reuters, *China tightens rules on online news, network providers*, May 2, 2017

22. Standing Committee of the National People's Congress, Counterterrorism Law of the People's Republic of China, *Order of the President of the People's Republic of China No. 36*, December 27, 2015

23. Cyberspace Administration of China (CAC), *Administrative Provisions on Information Services of Mobile Internet Application Programs*, June 28, 2016

24. Library of Congress, *China: Cyberspace Administration Releases New Rules on Mobile Apps*. July 26, 2016

25. Beijing Copyright Bureau, *Guiding Framework on the Protection of Copyright for Network Dissemination.* April 28, 2011; Standing Committee of the National People's Congress, *Decision on Strengthening Online Information Protection*, December 28, 2012

instances provide legal grounds for prosecuting developers, providers or even hosts of circumvention tools.[26]

"This control has been increasingly decentralised from the Great Firewall to non-government actors, by shifting from censorship to intermediary liability."

Many of the restrictions imposed on the grounds of public order are easily defined as trade barriers as they discriminate between like services providing similar content. The only differentiator is whether the authorities can exercise control over them or not. Needless to say, domestic service or app providers tend to fall under the former, and foreign market actors tend to fall under latter. However, this control has been increasingly decentralised from the Great Firewall to non-government actors, by shifting from censorship to intermediary liability extended to developers, operators and hosts with little or no prospect of legal certainty or rule of law – and through this decentralisation, China has successfully avoided a legal challenge in the WTO.

This leaves only one avenue open for foreign apps and services, namely domestic reforms. However, unlike many other market restrictions, public order measures are less likely to be reformed unilaterally, or be conceded in trade and investment negotiations with third countries. After all, none of the foreign online services, apps or intermediaries has ever seen bans being lifted once they have been blocked. Moreover, as new information services are invented, they are automatically added to the list of blocked services in China. This is evident from how the list of blocked services expanded incrementally from web portals such as search engines, to encompass translation and cloud storage services. These measures designated to uphold public order are a near *fait accompli* and subsequently foreign online services providers have either decided to leave, or share their technology with a local Chinese competitor in a joint venture as a price to remain on the market.

5. MEASURES SUPPORTING CHINA'S FISCAL AND SOE STRUCTURE

Aside from social networks, messaging and other services that distinctively feature social interaction between citizens that unsettles the authorities' need for information control, Chinese online service and app markets are seemingly arbitrary. For example, there is no ban on car-sharing services like Uber or its local Chinese partner Didi Chuxing, whereas such services were blocked or severely limited in a number of European jurisdictions. Outside of social networks and information services, a large variety of consumer apps are still accessible.

Aside from the hurdle set by government information control, the second major determinant to whether a sector of an economy remains open to foreign and private entities in China has always been whether there are state-owned enterprises operating in the area. The digital economy is no exception. Although car sharing, gaming or restaurant reviews are typically not areas where SOEs are operating, over $300 billion have been channelled into 780 different technology venture capital (VC) funds by China's local and central governments that invest in various internet startups. These VCs often take minority shares along with private VCs to secure public R&D subsidies and provide "good governance". The distinction between a private entity and an SOE will be much less clear-cut for future generation of Chinese tech firms, or how the government will act to protect public investments in case there is an asset bubble.

To date, China's internet SOEs traditionally reside further 'upstream' – i.e. amongst telecom operators and networks. Although the telecom market operates as a market economy from the consumer perspective, it has yet to be fully liberalised. An incumbent SOE is designated to

---

26. *Ninth Amendment to the Criminal Law*, August 29, 2015; English version accessed at: http://www.chinalawtranslate.com/criminallawam92/?lang=en

dominate the market for each product: For example, China Telecom holds half of the market shares of the fixed broadband market, but is only the third largest mobile services provider in the country. Market competition between Chinese SOE operators is a recent phenomenon, as the state authorities did not cede price controls until 2014. Politics still dictates business terms: For example, in 2014, the Chinese government could agree and implement a settlement on the precise market share the European manufacturers should receive in a tender by China Mobile to avoid anti-dumping measures in the EU.[27] According to the U.S. Trade Representative, the Ministry of Industry and Information Technology (MIIT) has not rescinded an internal circular issued in 1998 instructing telecommunications companies to buy components and equipment from domestic sources, whereas the supposedly competing operators also centralise their purchases through their SOE holding companies.[28]

"The distinction between a private entity and an SOE will be much less clear-cut for the future generation of Chinese tech firms."

Foreign ownership in basic telecommunication services – meaning fixed line, mobile and broadband – is formally capped at 49 percent.[29] However, as all network providers are SOEs, and there are no more licenses issued, foreign participation is non-existent. China also imposes strict limitations on companies that wish to offer voice-over-IP (VoIP) services in the country, and compete with its SOEs, similar to other countries, e.g. Mexico and Germany, who also sought to protect the revenues of incumbent operators. China includes VoIP on the list of value-added telecom services (VATS) that require a license to operate. Moreover, a traditional operator license (a Basic Telecommunication Service license) is necessary in order to interconnect VoIP services with the public switched telecommunications network.[30] Foreign investment in VATS is capped at 50 percent,[31] and foreign VoIP services have been forced to partner with local telecom operators. Moreover, the formation of such a joint venture must be approved by both the MIIT and the Ministry of Commerce (Mofcom). In other words, foreign VATS are forcefully "compensating" for the revenues that they may be eroding from the owners of the old telecom infrastructure, or that local players cannot provide.

The term 'value-added telecommunication services' is an overarching one that includes, among other sectors, online database storing and searching; electronic data exchange, online data processing and transactions processing, domestic multiparty communication services, IP-VPN, ISP, ICP and video teleconferencing; it also include business services like cloud computing, data centre services and call centre services – in other words, any type of services where the state-run incumbents may perceive as a competitor. To date, only one category of VATS was opened up for wholly-owned subsidiaries in 2015 (through MIIT Circular 196), namely e-commerce. China still considers online retail of physical goods to be a telecom service that requires a telecom license, but has reversed its previous limitation on wholly-owned subsidiaries by foreigners. The first license to a wholly foreign-owned subsidiary was issued one year after the circular, to the Japanese retailer Heiwado. And as so happens, none of the Chinese e-retail giants – like Alibaba and JD.com – are state-owned, and have reached a sufficient level of internationalisation.

There are also other examples of China's inadequate reforms blocking foreign participation. China accounts for over half the world's mobile payments and three-quarters of online lending.

---

27. Oliver, *EU and China agree truce on trade disputes*, Financial Times, October 20, 2014

28. USTR, National Trade Estimates, 2014; see also annual reports of China Telecom and China Unicom in 2011

29. State Council, *Provisions on Administration of Foreign-Invested Telecommunications Enterprises*. Decree of the State Council of the People's Republic China No.333, December 11, 2001

30. USTR, *Section 1377 Review On Compliance with Telecommunications Trade Agreements*, 2015

31. State Council, *Provisions on Administration of Foreign-Invested Telecommunications Enterprises. Decree of the State Council of the People's Republic China No.333*, December 11, 2001

Innovative Chinese fintech actors can be very powerful, like Ant Financial which is valued at $60 billion on par with Switzerland's largest bank, and together with WeChat and AliPay (chats and e-commerce apps expanding into payments) fill a retail market that traditional Chinese banks are unable to fill. However, China's banking system is fragile, due to poor credit rating instruments and securitisation of assets. There are uncertainties regarding China's non-performing loans (NPLs) that range between 1.74 percent and 6 percent,[32] much owed to SOEs and regional investment vehicles controlled by provincial governments. Similar to the telecoms, Chinese banks – many of them owned or collated with local government interests – are under competitive pressure and required by regulators and stakeholders alike to generate top line growth. Moreover, the banking system is central to governing the economy, and to prevent influx of hot money that can overheat the economy.

Local governments operate SOEs and invest in private entities for a number of reasons, but primarily two: Firstly, regional governments engage in business and investments to compensate for their lack of ability to raise taxes, which is an exclusive competence of central government defined in a intricate and politically sensitive power-sharing balance between the executives in the centre and the kingmakers in the regions; secondly, these vehicles support local social goals, such as higher labour participation rates. The result is a banking system that is constantly on the verge of a crisis and requires constant monitoring and political or market interventions by Beijing. China's reluctance to liberalise 'fintech' applications, or even the simple payment solutions,[33] must be seen in the light of its frail condition of the banking system, its stakeholders and its role in China's unreformable fiscal system. It is not unforeseeable that China's fintech boom could come to a halt at the best of traditional banking – and in any case, foreign participation seems unlikely.

Some telecoms, internet and financial services in China provide a stark contrast to the industrial policy of other Asian economies on their trajectory path, where they caved in for international pressure, and opened up their home markets once the local players were competitive enough to internationalise. Unlike some Chinese SOEs that are currently gearing up for internationalisation in sectors like construction, aerospace, high-speed trains or semiconductors – most Chinese SOEs or publicly invested firms operating in fintech, cloud or telecom services are unlikely to turn to export orientation, as they either lack competitiveness or the regulatory compliance to operate outside of China. In other words, SOEs will continue to be pervasive for internet and telecom sectors, and Chinese investment protectionism is less likely to cease in these sectors than in others - as that entails as far deeper reforms of China's fiscal system and relinquishing of the government control of the information and financial system.

6. REGULATORY MEASURES RELATED TO NATIONAL SECURITY

The Chinese government gives primacy to its security interests and puts such considerations above any other policy objectives. In that regard, Chinese government behaves exactly like any other government, acting in support of its core national interests. However, China as an emerging world power is the only genuine challenger to the post-Cold War order. Security threats against China are of different magnitude than any country, with the possible exception of the US. At the same time, the "safety margin" that China has put in place on the commercial market for the sake of national security is wider and more comprehensive than those deployed by other countries against China.

As so often, a number of regulations and national strategies overlap in the security realm. At the core of China's security measures, China's extensive central government spending of at least 14 percent of GDP ($US 1.5 trillion) is a veritable leverage: The Multi-Level Protection Scheme (MLPS) introduced by the Ministry of Public Security in 2007 (also known as Classified Pro-

32. China Banking Regulatory Commission, *The CBRC Released Supervisory Statistics of Q4 2016*, 2016

33. WTO, *China—Certain Measures Affecting Electronic Payment Services*, DS413

tection of Information Security) governs public procurement,[34] and the scheme is a blanket ban on foreign ICT products in what it classifies as 'critical infrastructure' – MLPS requires all IT systems in China to be classified on different levels of security, from one to five (with the most sensitive systems designated as level five) and bars any projects graded level three and above from incorporating foreign suppliers. In such cases, IT systems must solely contain products developed by Chinese ICT suppliers, and key components made from Chinese intellectual property.

"The explicit goal is to make the entire Chinese digital environment, commercial and public, secure and controllable'."

Although similar provisions for national security exist in other countries, the scope of MLPS is wider due to the prominent role of the public sector in the China's economy. Government agencies, financial sector, telecom companies, the domestic energy and power grid, educational institutions, and healthcare providers have all issued requests for proposals (RFPs) incorporating MLPS requirements at level three or higher. The product scope of MLPS is also expanding with evolving technology – an example is public tenders for antivirus software in 2014 where all foreign security providers (such as Kaspersky and Symantec) were excluded from the list for national security reasons. Only five Chinese providers, i.e. 360, Jiangmin, Rising, Kingsoft, and KILL, were approved.[35] In comparison, the US government agencies still deploy China-made products or suppliers, including Lenovo, but keep network equipment out of their commercial infrastructure. In Europe, Chinese suppliers compete on equal terms in public procurement or in building their network infrastructure – and neither the US nor the EU deploy the broad and sweeping definitions of what is deemed as critical infrastructure for their national security.

The Chinese rationale to protect national security also includes common commercial products. In 2014, the Central Government Procurement Centre banned Windows 8 from all government computers without providing any reasons for its decision.[36] Moreover, the powerful National Development and Reform Commission (NDRC) and the Ministry of Finance ban the purchase of certain foreign IT products for selected government procurement lists, including ten Apple products, such as iPads and MacBooks. A separate procurement list includes some Apple computers that departments can continue to buy on a smaller scale, i.e. purchases totalling less than 1.2 million yuan ($195,000). Products from Dell Inc., Hewlett-Packard Co. and even the Chinese maker Lenovo were also included on both lists. This ban applied to all central Communist Party departments, government ministries and local governments.[37]

But China's quest for safety margins goes beyond just public procurement of ICT suppliers. The explicit goal is to make the entire Chinese digital environment, commercial and public, 'secure and controllable' - which is also the name of the guiding policy since the Xi administration was sworn in. In the wake of Secure and Controllable policy framework, China has implemented a new comprehensive National Security Law that foresees the rollout of a "secure and controllable" internet infrastructure, by screening purchases, investments and supply chains. The official Xinhua news agency reported that the new law (signed personally by President Xi Jinping) would establish "mechanisms to censor items that have or may have an impact on national security, including foreign investment, particular materials and key technologies".[38] The law appears ambiguous about how the new requirements will be implemented, and it has raised concerns related to legal uncertainty for businesses. It is this ambiguity that gives all policymakers – China and

---

34. Ministry of Public Security, *Multi-Level Protection Scheme (MLPS), also known as Classified Protection of Information Security*, June 22, 2007
35. China Digital Times, *China Bars Foreign Antivirus as Cybersuspicion Deepens*. August 5, 2014
36. China Digital Times, *Questions Remain After Chinese Hacking Indictments*, May 20, 2014
37. Bloomberg,. *China Said to Exclude Apple From Procurement List*, August 6, 2014
38. Xinhua, *Xinhua Insight: China adopts new law on national security*, July 1, 2015

elsewhere – the freedom to discriminate despite identical conditions.

As seen from the new national security laws, China puts a national security dimension specific to this sector to its foreign investment caps, where the prior objectives were mainly fiscal and developmental. But prior to the new law, China already imposed general screening of foreign investment,[39] where foreign-capital enterprises are blocked from investing if they are deemed to injure "China's sovereignty or social and public interests", endangering China's national security, or "not in keeping with the requirements of China's national economic development". Also, when a foreign investor intends to obtain the actual controlling rights of a domestic enterprise and if any key industry is concerned, or if such investment has an impact or may have an impact on the national economic security, the parties concerned shall file an application to Mofcom.[40] If the parties concerned fail to apply but the acquisition has had or may have a serious impact on the national economic security, the Mofcom may demand the parties concerned to terminate the transaction or transfer the relevant equities, or take other effective measures to eliminate the acquisition impact on the national economic security. To date there are no cases of investments in the telecom/ICT sector being blocked on national security grounds – but, as the Beijing issued the new Cybersecurity law, it restates that this rationale exists and is strong in the tech sector.

Internet and cross-border data flows pose a very specific cyber security issue, which is in the public debate wrongly conflated with protection of privacy. China imposes overlapping horizontal and sector specific restrictions related to processing electronic data, both on personal information and non-personal. Generally, China imposes a requirement to localise data where companies must store any data they collect in China on servers physically located in the country. These requirements have been implemented since the early 1990s, despite not being formalised in written law and recognised as a *de facto* obligation.[41] Another recent law derived from the Secure and Controllable policy formalises this overarching data localisation requirement.[42] The new Cybersecurity Law, which entered into force in June 2017, includes requirements for personal information of Chinese citizens and 'important data' collected by 'key information infrastructure operators' (KIIOs) to be kept within the borders of China. If there are business needs for the KIIOs to transfer this data outside of China, security assessments must be conducted. The definition of KIIOs remains to be finalised,[43] providing another example of ambiguity that could provide the policy space for discrimination.

In addition to horizontal regulations, there are also a number of onerous, sectoral regulations: Sensitive data such as personal information collected by commercial banks and population health information must be stored, handled and analysed within the territory of China, and is not allowed to be transferred and stored overseas.[44] Online maps are required to set up their server inside of the country and must acquire an official certificate.[45] Finally, China also instituted in 2016 a licensing system for online taxi companies, which requires them to host user data on Chinese servers.[46] China also conditions all transfer of personal data abroad to express consent

---

39. Ministry of Commerce (MOFCOM), article 5 of the *Rules for the Implementation of the Law of the People's Republic of China on Foreign-capital Enterprises*, April 12, 2001

40. Ministry of Commerce (MOFCOM), State-owned Assets Supervision and Administration Commission of the State Council, State Administration of Taxation, State Administration for Industry and Commerce, China Securities Regulatory Commission and State Administration of Foreign Exchange, art. 12 of the *Interim Provisions on Mergers and Acquisitions of Domestic Enterprises by Foreign Investors*, Order No.10, 2016

41. Business Roundtable, *Promoting Economic Growth through Smart Global Information Technology Policy. The Growing Threat of Local Data Server Requirements*. July 2012

42. Standing Committee of the National People's Congress, *Cybersecurity Law*, November 7, 2016

43. DLA Piper, *Data Protection Laws of the World: China*

44. People's Bank of China, *Notice to Urge Banking Financial Institutions to Protect Personal Financial Information*, January 21, 2011.

45. State Council, *Map Management Regulations*, December 14, 2015.

46. Ministry of Transport, Ministry of Industry and Information Technology, Ministry of Public Security,

of the data subject as well government permission or explicit regulatory approval,[47] whereas only the former is needed in even most data-restrictive jurisdictions.

China is today effectively hermetically sealed when it comes to cross-border data flows. The State Security Law requires that the state security organ should always be permitted to accede, when necessary, to any information held by companies in China.[48] Unlike other jurisdictions, there is no due process of warrants or other jurisdictional checks in order to access electronic communications. In addition, the recently adopted Counterterrorism Law requires Internet Service Providers (ISPs) and the telecommunication sector to "provide technical support and assistance, such as technical interface and decryption, to support the activities of the public security and state security authorities in preventing and investigating terrorist activities".[49] Furthermore, ISPs are already keeping records of each service user's time spent online, user account, IP address or domain name, phone number and other information for 60 days and provide that information to the authorised government authorities when required.[50] ISPs are also required to cooperate with the government and provide technical support upon inquiry from the authorised government authorities.

Finally, China's also links its technical standards to national security objectives. Most technical standards in China differ from those implemented or agreed internationally, and China applies strict licensing schemes for telecommunications equipment and other ICT products where standardisation is essential for interoperability. China enforces three licensing regimes: the Radio Type Approval (RTA), the Network Access License (NAL) and the China Compulsory Certification (CCC), in conflict with China's WTO obligations of limiting imported products to no more than one conformity assessment scheme. Moreover, all testing for the CCC mark must be conducted in China. These tests can cost up to $35,000,[51] which is particularly prohibitive to ICT firms who can have portfolios of hundreds of products. Moreover, the aforementioned Cybersecurity Law adds an additional layer on top of the licensing scheme through a specific security review for a list of ICT products that was revealed in June 2017.[52] According to the first list released, the products that need to pass mandatory certification and inspection by related agencies (e.g. CAC, the MIIT, and Ministry of Public Security, and other national-level certification institutes) are network critical equipment like routers and servers and online security products, including firewalls, data back-up machines and secure database systems.

Ministry of Commerce, State Administration for Industry and Commerce, and General Administration of Quality Supervision, *Interim Measures for the Administration of Online Taxi Booking Business Operations and Services*, July 28, 2016

47. General Administration of Quality Supervision, Inspection and Quarantine of China and Standardization Administration of China, Article 5.4.5. of *Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems*, November 5, 2012

48. Article 11 of the the State Security Law stipulates that 'where state security requires, a state security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual'; Article 18 states that 'When a State security organ investigates and finds out any circumstances endangering State security and gathers related evidence, citizens and organizations concerned shall faithfully furnish it with relevant information and may not refuse to do so'; see also Wang, *Systematic Government Access to Private-Sector Data in China*, International Data Privacy Law, 2/4 2012

49. Inter alia *Military Programming Law*, Law No. 1168 , 2013 in force in France since January 201550 Standing Committee of the National People's Congress, Counterterrorism Law of the People's Republic of China. Order of the President of the People's Republic of China No. 36. December 27, 2015

50. Standing Committee of the National People's Congress, *Counterterrorism Law of the People's Republic of China. Order of the President of the People's Republic of China No. 36*. December 27, 2015

51. State Council, article 14 of the *Regulation on Internet Information Service of the People's Republic of China*, Decree of the State Council of the People's Republic of China No. 292. September 25, 2000; Standing Committee of the National People's Congress, article 10 of the Decision on Strengthening Online Information Protection, December 28, 2012

52. See FCC filing by Telecommunication Industry Association, 2011 accessed at: http://www.tiaonline.org/gov_affairs/fcc_filings/documents/P%20Telecommunications%20Industry%20Association%201377%20Report.pdf

In addition to technical standards and security screening, China is developing and mandating 'national' algorithms for its encryption technology that differ from global standards.[53] Although a globally accepted standard for encryption often exists (e.g. 3GPP for 4G communication), ZUC is *de facto* often required in order to enter the Chinese market, along with extensive testing requirements. The Chinese government began regulating encryption in 1999 when it banned foreign encryption products, deemed all commercial encryption a state secret, and all production and sales of commercial encryption products were monopolised by relevant government authorities (State Encryption Management Bureau and the Office of State Commercial Cryptography Administration).[54] The rules also required that the strength of encryption systems not surpass a level set by the state regulator.[55] More recently, new standards are being developed in technical committees that are closed to foreign participation. The Chinese government has also supported the development of mandated domestic radio frequency identification (RFID) standards without international participation or consensus, despite the fact that global standards for RFID already exist.[56]

"In a world where everything is seen through a national security prism, restrictions on public procurement, privacy or standards turn non-negotiable".

In conclusion, there is little evidence that these measures on the grounds of national security will be revoked or softened given the hard political objectives behind them, as long as there is a geopolitical detente in the cyberspace between the global powers.

An increasing number of product restrictions in China were originally fiscal or technical in their nature, but have been conflated with security objectives. In such cases, security objectives tend to overtake the original intentions of commercial protectionism. Whereas commercial objectives are possible to negotiate, national security is often not: In a world where everything is seen through a national security prism, restrictions on public procurement, privacy or standards turn non-negotiable. Restrictions on the grounds of national security are never put up for negotiation – by China or any party – during trade negotiations and strategic economic dialogues, as security is governed by an entirely different government apparatus, and increased economic cooperation does not eradicate the perceived threats.

7. CHINA'S ABILITY TO UNDERTAKE MARKET REFORMS

In all fairness, many of China's technology restrictions are also implemented by other countries – but no country imposes them simultaneously, or in such disproportionate and opaque manner as China. Nor is China the first Asian economy to embark on a mercantilist path to growth by limiting imports. However, not all of China's restrictions on internet or the ICT sector have the exclusive objective to support exports, but also to defer structural and governance reforms. Some of the most draconian and disproportionate measures are imposed to protect the country against internal and external threats. On such occasions, the rationale behind China's technology protectionism is uniquely Chinese without precedence in Asia, explained by its unique governance structure and its emergence as world's second superpower.

This uniqueness is also why much of the criticism of protectionism has fallen to deaf ears in

---

53. Article 23 of the *Cybersecurity Law*; also, MIIT, Catalogue Critical Networking Equipment and Products Designed for Network Security

54. MIIT and the State Encryption Management Bureau informally announced in early 2012 that only domestically developed encryption algorithms, such as ZUC, would be allowed for use in the network equipment (mobile base stations) and mobile devices comprising 4G TD-LTE networks in China.

55. Segal, A., *China, Encryption Policy, and International Influence*. A Hoover Institution Essay. Series Paper No. 1610

56. *inter alia*, complaint by TIA (Telecommunication Industry Association) in USTR 2013 NTE Report

Beijing. At best, they seem condescending or oblivious to the challenges China is facing going forward – and these challenges are manifold, and they all have a bearing on China's ability to open up and digitalise. Aside from security and public order, digitalisation also touches on China's most difficult challenge, namely the economy. While the Chinese economy has shown spectacular growth for the last two decades, managing the slowdown of the Chinese over-leveraged economy is no easy task. To begin, despite the recent turn in demographics, Chinese state planners must still generate nearly 20 million new jobs per year to maintain current unemployment rates.[57] In order to generate new jobs and to escape the middle-income gap, China is bound to upgrade its services sector, which in turn could only happen through opening up its ICT sector to improve its productivity. Clearly, China's reliance on technology transfer via joint ventures and domestic innovations has not been enough to mitigate the slowdown. And China's social contract with its citizens is not built on a welfare state, but on low taxation and full employment, achieved through an ever-growing GDP. As most of the population lacks a social safety net, failing the ongoing challenge to digitalise China's service sectors will have social ramifications, at least in the medium term.

"Failing the ongoing challenge to digitalise China's service sectors will have social ramifications."

The economic challenges facing China also highlight a much broader issue, which concerns governance. The digital economy operates on a user-centric and demand-driven peer-to-peer or "bottom-up" approach, rather than the traditional supplier-centric top-down model. Thus, online services require open data, financial and logistical flows in every direction. Such openness challenges the way China is currently governed, why the ongoing experiment of Chinese fintech and mobile payments cannot lead to further internationalisation of the Chinese financial system without substantial reforms. While the interaction between the government and business is gradually evolving into an investor relationship, the ties between the executive branch and the private sector are actually being strengthened, encouraged by recent economic and industrialisation plans.

Removing some restrictions designed to protect such SOEs or public investments could upset the political balance between the regions and Beijing – a power equilibrium that even predates modern China – and fundamental to its unitary governance. Foreign participations in telecoms, mobile payments, cloud services and social media let go of the political governance of information and social interactions, deemed essential for maintaining public order. These are immediate and short-term risks to its stability that the Chinese governance model cannot bear.

Taken together, China short-term and long-term needs are an unsolvable digital dilemma – to borrow the words of the ancient historian Livy: China is unable to neither bear its ills nor its cure. On one hand, deferring market reforms worsens a dangerous economic slowdown that would destabilise the country. On the other hand, reforms could severely limit a governance model that is needed to maintain stability.

If the rationale of Chinese ICT restrictions were purely and exclusively commercial protectionism, these policies could be reformed as the country turns towards export-orientation, and grow sufficiently competitive – which is the case of China's liberalisation of online retailing. Alternatively, China would respond to the economic incentives or threats of retaliation that is put on the table by its trading partners. But – as we have seen – a multitude of rationales is behind China's digital policies, each of them potentially stronger than China's commercial objectives.

---

57. Krol, Lee-Makiyama, Macyra, *The International Services Agreement – from an European Vantage Point, ECIPE*, 2012

8. RESPONDING TO CHINA'S DIGITAL DILEMMA

It is not surprising therefore that a decade of strategic economic dialogue with China has yielded very little results. The fundamental problem is in how the other major technology suppliers – i.e. Europe, Japan and the US – have very few means to incentivise or confront China in a trade dialogue over commercial issues if China is driven by non-commercial objectives and concerns.

As economic negotiations merely led to *status quo* and further fragmentation of digital trade, China's trading partners turn to using sticks rather than carrots through 'reciprocity' – i.e. closing their own economy in retaliation. For example, the US and Australia restrict telecom equipment purchases from Chinese tech firms. In addition, the US also imposes a *de facto* investment ban for Chinese ICT firms through a Congressional review committee (Cfius), while the EU Member States have signalled their intention to follow suite. Another area considered for reciprocity is public procurement, as fiscal spending is at heart of a number of Chinese discrimination of foreign ICT firms. The US already imposes 'Buy America' policies more broadly, while the EU has attempted reciprocity, implicitly aiming at China.

Here is where China's trading partners are caught in a Livian dilemma of their own: Whether the West chooses negotiation or unilateral retaliation, both options are lead to an outcome that is contrary to the long-term goal of integrating China as a partner in an open economic order. Both approaches are effectively a dead-end. For example, if China's objective is genuinely to maintain public order, any trade incentives or retaliation are meaningless, as China is not presented with a credible incentive or threat to its stability. Similarly, China will not cease to impose its policy of 'secure and controllable' and its disproportionate safety margins on cyber security – as long as China finds the offensive capabilities of its geopolitical adversaries as superior, or if its internal processes of the government apparatus are too poor to deal with cyber threats in a more refined manner.

"Misreading the rationale of China's digital policies have led Brussels and DC analysts to prescribe policy responses that were sometimes unworkable or on occasion even counterproductive".

Moreover, China is not a singular and monolithic entity, but consists of diverse and multi-layered interests. China's main beneficiaries from free trade in the tech sector are primarily the major telecom and computer equipment manufacturers, who carry the brunt of the retaliation. These exporters may be subject of immense national pride, but not always the main beneficiary of all forms of Chinese protectionism and state aid. Meanwhile, industries that are still in the lesser developed stages of their internationalisation, such as the semiconductors or app developers, are immune to reciprocity. Such mismatch between retaliation targets and beneficiaries of protectionism has made economic retaliation politically and financially bearable for China. Similarly, if local governments see more business opportunities in local Chinese start-up scene rather than in Europe, stricter EU investment screening may be a price they are ultimately willing to pay for a bigger share of the investment opportunities at home.

Misreading the rationale of China's digital policies have led Brussels and DC analysts to prescribe policy responses that were sometimes unworkable at best, or on occasion even counterproductive with further loss in market access in China – as exemplified by EU attempts to impose anti-dumping duties on Chinese telecom equipment. Alternatively, they may provide political impetus for China's national security organs, industry or the provinces to 'resist interference' and 'external pressure', demanding Beijing to dig its heels deeper. As the old paradigm for dealing with China's digital policies has failed, Europe, Japan and the US must invent a new one for their future engagement.

Firstly, such new engagement can no longer be bilateral between China and each of its counter-

parts, as to date. This is not just a matter of a joint international coordination providing bigger leverage, but also the fact that China's major partners – Europe and the US in particular – are between them very different. Some sectors, in Europe and Japan are deemed sufficiently open to China, whereas US is closed. For example, having access to China's telecom and communication markets are primarily a European interest, from whom China wants very little. As a consequence, the major trade incentive for China to open EU telecom manufacturers is to gain access to the US telecom equipment market in return. Similarly, Europe which largely lacks a geopolitical footprint in Asia does not have an obvious geopolitical contention with China, but is nonetheless affected by cyber security laws resulting of China's issues with the US and its strategic allies. Over a number of issues, a different party must act to improve on someone else's concern with China. An internationally coordinated approach on multiple issues facilitates concessions across different beneficiaries, while making a direct confrontation more costly to all parties.

"An internationally coordinated approach on multiple issues facilitates concessions across different beneficiaries, while making a direct confrontation more costly to all parties."

Secondly, the current approach has failed because Europe, Japan and the US failed to recognise that many of the digital trade issues also arose from non-commercial rationales. China's internet management or cybersecurity laws have deep impact on trade, but their objectives were not exclusively about protecting local production. While past attempts by the EU and US to exercise pressure have been instrumental in opening up China to this point in a number of sectors, commercial gains could never fully offset existential political objectives on public order or security that exist in the digital economy. What China sees as a security issue can only be dealt with carrots and sticks that will have some consequences for China in that regard, either by actions that increases confidence and trust between the parties, or by facing an alternative scenario that puts China worse off than today. Financial and capital controls could only cease if the Chinese leadership perceives it maintains adequate market control, or face a risk of losing it. Although trade will remain a centrepiece of what China seeks from its partners, on a number of issues, more economic openness can only be achieved by deploying a broader catalogue of non-trade, i.e. strategic, financial and political incentives and affirmative pressure that corresponds to China's rationale for the protectionism in the first place.

Thirdly, by limiting the scope of digital trade to mere market access issues, China's digital protectionism was often downgraded below other pertinent market access issues – especially as the bilateral trade agenda with China is overburdened with a number of market access issues. The current approach also failed because the EU, the US, Japan and other free trade countries failed to realise that an open digital economy is also a high-stakes political issue for *them*. Governments that are proponents of free trade in the technology sector often failed to see the political importance of the open commercial internet – the platform that will dominate social and economic interaction – and the importance it plays in their own strategic agenda and economic statecraft. Meanwhile, China's political leadership recognised and acted firmly to control this evolution nearly two decades ago. —

LIST OF MAIN REGULATORY MEASURES CURRENTLY IN PLACE IN CHINA THAT INCLUDE A COMPONENT OF INCREASE IN COSTS OF ENGAGING IN DIGITAL TRADE:[58] [59]

Trade Defence:

1 MOFCOM Announcement No.9 of 2013 on Midterm Review Ruling on Dispersion Unshifted Single-Mode Optical Fiber. March 4, 2013. Ministry of Commerce (MOFCOM).

2 Final Ruling on Expiry Review of Anti-dumping Investigation into Imports of Paper for Electrolytic Capacitor Originating in Japan. April 19, 2013. Ministry of Commerce (MOFCOM).

Taxation:

3 Cai Shui [2014] No. 43. April, 29, 2014. Ministry of Finance (MOF) and the State Administration of Taxation (SAT).

4 Regulations on export credits of China Exim Bank and Regulations of Sinosure.

Public Procurement:

5 "Buy Chinese" policy informally implemented in public tenders. Since 1995.

6 Multi-Level Protection Scheme (MLPS), also known as Classified Protection of Information Security. June 22, 2007. Ministry of Public Security.

7 Hangjinhouqi County Government notice announcing 2013-2014 public procurement work. February 1, 2013. Inner Mongolia, China.

8 Online Statement by China Central Government Procurement Center on ban of Windows 8 from Central State Organs. May 20, 2014. China Central Government Procurement Center.

9 Result of the public tender for central government procurement of electronic information products of 2014 (Vol.21, GC-HJ140283). June 11, 2014. China Central Government Procurement Center.

10 Report by the National Development and Reform Commission of China and the Ministry of Finance introducing a ban on several IT products for central Communist Party departments, government ministries and local governments. July 1, 2014. National Development and Reform Commission of China (NDRC) and the Ministry of Finance.

11 Directive Number 618 "Notification Regarding the Launch of National Indigenous Innovation Product Accreditation Work for 2009". November 15, 2009. Ministry of Science and Technology (MOST), National Development and Reform Commission of China (NDRC) and Ministry of Finance (MOF).

Investment:

12 Rules for the Implementation of the Law of the People's Republic of China on Foreign-capital Enterprises. April 12, 2001. Ministry of Commerce (MOFCOM).

13 Provisions on Administration of Foreign-Invested Telecommunications Enterprises. Decree of the State Council of the People's Republic China No.333. December 11, 2001. State Council.

14 Interim Provisions on Mergers and Acquisitions of Domestic Enterprises by Foreign Investors - Order No. 10 [2006] of the Ministry of Commerce. August 10, 2006. Ministry of Commerce (MOFCOM), State-owned Assets Supervision and Administration Commission of the State Council, State Administration of Taxation, State Administration for Industry and Commerce, China Securities Regulatory Commission and State

---

58. The detailed description of the measures can be found in the DTE database www.ecipe.org/dte/database

59. Measures that impact more than one policy areas are listed in all areas of interest.

Administration of Foreign Exchange.

15 Circular of the General Office of the State Council on the Establishment of Security Review System Regarding Merger and Acquisition of Domestic Enterprises by Foreign Investors. March 4, 2011. Ministry of Commerce (MOFCOM).

16 Foreign Investment Industrial Guidance Catalogue (as amended in 2015). March 13, 2015. National Development and Reform Commission of China (NDRC) and Ministry of Commerce (MOFCOM).

Intellectual Property Rights:

17 Copyright Law of the People's Republic of China (last amended by the Decision of February 26, 2010, by the Standing Committee of the National People's Congress on Amending the Copyright Law of the People's Republic of China). September 7, 1990. National People's Congress.

18 Multi-Level Protection Scheme (MLPS), also known as Classified Protection of Information Security. June 22, 2007. Ministry of Public Security.

19 Directive Number 618 "Notification Regarding the Launch of National Indigenous Innovation Product Accreditation Work for 2009". November 15, 2009. Ministry of Science and Technology (MOST), National Development and Reform Commission of China (NDRC) and Ministry of Finance (MOF).

20 MOFCOM conditional approval of Microsoft acquisition of Nokia. April 8, 2014. Ministry of Commerce (MOFCOM).

Data policies:

21 Law of the People's Republic of China on Guarding State Secrets. May 1, 1989. Standing Committee of the National People's Congress.

22 State Security Law. Order No. 68 of the President of the People's Republic of China. February 22, 1993. Standing Committee of the National People's Congress.

23 Regulation on Internet Information Service of the People's Republic of China. Decree of the State Council of the People's Republic of China No. 292. September 25, 2000. State Council.

24 Notice to Urge Banking Financial Institutions to Protect Personal Financial Information. January 21, 2011. People's Bank of China.

25 Guidelines for Personal Information Protection Within Public and Commercial Services 26

26 Information Systems. GB/Z 28828-2012. November 5, 2012. General Administration of Quality Supervision, Inspection and Quarantine of China and Standardization Administration of China.

27 Decision on Strengthening Online Information Protection. December 28, 2012. Standing Committee of the National People's Congress.

28 Law of the People's Republic of China on Protection of Consumer Rights and Interests. Order of the President of the People's Republic of China No. 7. October 25, 2013. Standing Committee of the National People's Congress.

29 Ninth Amendment to the Criminal Law of the People's Republic of China. November 19, 2015. Standing Committee of the National People's Congress.
Administrative Measures for Population Health Information (For Trial Implementation). May 5, 2014. China's National Health and Family Planning Commission.

30 Map Management Regulations. December 14, 2015. State Council.

31 Counterterrorism Law of the People's Republic of China. Order of the President of the People's Republic of China No. 36. December 27, 2015. Standing Committee of the National People's Congress.

32 Provisions on the Administration of Online Publishing Services. Order No. 5. February 4, 2016. State Administration of Press, Publication, Radio, Film and Television and the Ministry of Industry and Information Technology (MIIT).

33 Administrative Provisions on Information Services of Mobile Internet Application Programs.

June 28, 2016. Cyberspace Administration of China (CAC).

34 Interim Measures for the Administration of Online Taxi Booking Business Operations and Services. July 28, 2016. Ministry of Transport, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of Commerce, State Administration for Industry and Commerce, and General Administration of Quality Supervision.

35 Cybersecurity Law. November 7, 2016. Standing Committee of the National People's Congress.

Intermediary Liability:

36 Guiding Framework on the Protection of Copyright for Network Dissemination. April 28, 2011. Beijing Copyright Bureau.

37 Decision of the Standing Committee of the National People's Congress on Strengthening Online Information Protection. December, 28 2012. Committee Meeting of the National People's Congress Standing Committee.

38 Ninth Amendment to the Criminal Law of the People's Republic of China. November 19, 2015. Standing Committee of the National People's Congress.

39 Counterterrorism Law of the People's Republic of China. Order of the President of the People's Republic of China No. 36. December 27, 2015. Standing Committee of the National People's Congress.

40 Administrative Provisions on Information Services of Mobile Internet Application Programs. June 28, 2016. Cyberspace Administration of China (CAC).

Content Access:

41 Golden Shield (no legal text available). 1998. Ministry of Public Security.

42 Telecommunications Regulations of the People's Republic of China. Decree of the State Council of the People's Republic of China No. 291. September 25, 2000. State Council.

43 Opinions on Promoting Innovation and Development of Cloud Computing and Cultivating New Commercial Activities in the IT Industry. January 6, 2015. State Council.

44 Internet Domain Name Management Rules (Opinion-seeking Revision Draft). Proposed in March 25, 2016. Ministry of Industry and Information Technology (MIIT).

45 Notice on Regulating Cloud Computing Service Market Business Activities" (Draft Notice). November 24, 2016. Ministry of Industry and Information Technology (MIIT).

46 Provisions on the Management of Internet News Services. May 2, 2017. Cyberspace Administration of China (CAC), State Council Information Office (SCIO) and Ministry of Industry and Information Technology (MIIT).

Quantitative Trade Restrictions:

47 Notice of the Customs Tariff Commission of the State Council on the Tariff Execution Plan. Shui Wei Hui [2013] No.36. December 11, 2013. Customs Tariff Commission of the State Council.

48 MOFCOM Notice 97/2013. December 31, 2013. Ministry of Commerce (MOFCOM).

49 Joint Announcement [2015] No. 20 on Implementing Export Control over Dual-Use Unmanned Aircraft. June 25, 2015. Ministry of Commerce (MOFCOM), Customs, SASTIND, and General Armament Department of the People's Liberation Army of China.

50 China—Measures Related to the Exportation of Rare Earths, Tungsten, and Molybdenum. DS431, 432, 433. August 7, 2014. World Trade Organization.

Standards:

51 Provisions on the Management of Import of Radio Transmission Equipment (Radio Type Approval). January 1, 1996. State Radio Regulation Center (SRRC).

52 Network Access License. Since June 1, 2001. Ministry of Industry and Information

Technology (MIIT).

53 Regulations on the Administration of Commercial Encryption. 1999. China State Council Directive No. 273. State Council.

54 Regulation on Commercial Encryption. 1999. Office of State Commercial Cryptography Administration.

55 Implementation Rules for Compulsory Certification of Telecommunication Equipment - Telecommunication Terminal Equipments. December 7, 2001. Certification and Accreditation Administration of the People's Republic of China.

56 Implementation Rules for Compulsory Certification of Electrical and Electronics Products - Information Technology Equipments. August 6, 2007. Certification and Accreditation Administration of the People's Republic of China.

57 Revised Management Regulations for Compulsory Product Certification (CCC). July 3, 2009. Administration of Quality Supervision, Inspection, and Quarantine (AQSIQ).

58 WAPI Wireless Local Area Network (WLAN) standard. Since 2009. Unpublished requirement.

59 Informal announcement of the ZUC encryption standard. 2012. Ministry of Industry and Information Technology (MIIT) and State Encryption Management Bureau.

60 National Security Law. July 1, 2015. Standing Committee of the National People's Congress.

Online Sales and Transactions:

61 Telecommunications Regulations of the People's Republic of China. Decree of the State Council of the People's Republic of China No. 291. September 25, 2000. State Council.

62 Postal Law of the People's Republic of China. Order of the President of the People's Republic of China No. 12. April 24, 2009. Standing Committee of the National People's Congress.

63 Administrative Regulations for Online Publishing Services ("Online Publishing Regulations"). February 14, 2016. State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) and Ministry of Industry and Information Technology (MIIT).

64 Provisions on the Management of Internet News Services. May 2, 2017. Cyberspace Administration of China (CAC), State Council Information Office (SCIO) and Ministry of of Industry and Information Technology (MIIT).

ECIPE
EUROPEAN CENTRE
FOR INTERNATIONAL
POLITICAL ECONOMY