DIGITAL DIALOGUE

China's Cyber Diplomacy: A Primer

Nikolay Bozhkov
March 2020

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Abstract

Key points

1 Introduction 3

1.1 Threat landscape and commercially motivated cyber espionage 4

1.2 Recent activity and shifting rationale 4

1.2.1 Uptick in cyber espionage activities after 2015 6

2 China's approach to cyberspace: main priorities 10

2.1 Control of information flows 12

2.2 Economic modernisation 13

2.3 Network resilience and reducing reliance on foreign technologies 15

2.4 Normative power 16

2.5 Cyber superpower 18

3 Legal, regulatory and institutional landscape 22

3.1 Legal and regulatory landscape 22

3.2 Institutional landscape and key stakeholders 25

3.2.1 Governmental actors 25

3.2.2 Private sector 28

3.2.3 Research institutes and academia 29

4 China's approach to cyber diplomacy: objectives and practice 30

4.1 Participation and positions adopted in international cyber debates 30

4.1.1 Internet governance 30

4.1.2 Cybernorm building debates 32

4.1.3 International law 35

4.1.4 Confidence Building Measures 38

4.1.5 Capacity building 38

4.2 Relations with regional actors and organisations 39

5 Priorities and strategy for Sino-European engagement in cyberspace 41

5.1 Overall EU priorities and cooperation with China 41

5.2 China's engagement with the EU and EU member states 42

5.2.1 Track 1 dialogues with China 44

5.2.2 Track 1.5 and 2.0 dialogues with China 46

6 Pushback against Huawei and Chinese tech suppliers 47

6.1 Risks 49

6.1.1 Cyber espionage and cybersecurity risks 50

6.1.2 Strategic autonomy 52

6.2 Implications 52

6.2.1 Redoubling of "indigenous innovation" 52

6.2.2 Corporate uncertainty 53

7 Priorities and strategy for engagement: shadings and closing the gaps 54

About the author 57

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author.

Acknowledgments

The author would like to thank Alice Ekman and Patryk Pawlak for their substantive and invaluable feedback on earlier drafts of this paper. Special appreciation is extended to Christian Dietrich for his extensive work on the graphics.

Abstract

This paper offers a comprehensive analysis of China's evolving approach to cyberspace domestically and its efforts to recast debates on cyber diplomacy internationally. It teases out how multifold priorities and foundations, predicated on the notions of the supremacy of the state as the sole guarantor of security in the cyber domain and the primacy of regime security, exhibit themselves in China's engagement with global cyber norms-building initiatives. It likewise addresses the overarching geopolitical and geoeconomic drivers of Chinese cyber domain policy focused on the restructuring of the economy toward self-reliance and innovation-led growth, the reducing of dependence on foreign technologies to secure and control key supply chains and the enhancing of China's discursive rulemaking influence. This paper analyses the principal instruments, strategies, and core rhetoric vehicles used to elevate China to a status of a "cyber superpower" in the digital realm. It explains how and why ideas like cyber sovereignty and "information security" are leveraged by the Chinese government in various multi- and minilateral fora to pull other actors closer to its orbit, and into fidelity and acquiescence with its idiosyncratic interpretation of international law, its vision of reforming global Internet governance, and its information security-centric regulatory landscape. In addition, this paper contextualizes China's efforts at cyber diplomacy against the backdrop of the US-led pushback against Huawei and traces the genesis and evolution of the Sino-European engagement on cyber affairs. Identifying existing knowledge, perception and conceptual gaps, this *Digital Dialogue* finds signs of China being both a challenger of the status quo and a constructive stakeholder in global cyber debates.

Key points

- The "rise of China" in cyberspace represents much more than the development of a sophisticated state-aligned cyber espionage apparatus. It is in many ways more about the ability of the PRC to transform national companies into champions, and in turn, expand their global reach and competitiveness. China-nexus industrial cyber espionage operations must be contextualized as single - but central - components of a broader state-driven strategy designed to restructure the main drivers of economic growth. The preference for this option is likely going to persist in the near term as increased global pushback against forced technology transfers by China continue to close off other routes of foreign intellectual property acquisition.
- China's approach to cyber diplomacy is driven by the overarching objective of becoming a "cyber superpower" in the economic, normative, military and commercial realms - one that harnesses the power of digital technologies and innovation to achieve global technological leadership and modernise economic development. State-subsidised plans form the primary basis of accomplishing this but are not the only tools at the one-party regime's disposal.
- The imperatives of one-party regime's narrative control - and maintaining social stability and regime continuity - permeate, shape and condition China's domestic information security-focused approach to cyberspace and its engagement in global cyber initiatives.
- China's cyber affairs legal and regulatory landscape is sweeping and institutionally complex, consisting of guidelines, plans, opinions, standards focused on cybersecurity, development and capacity building, and has a wide range of stakeholders.
- China's efforts at cyber diplomacy have become increasingly proactive and global in nature, seeking to promote its institutional power and normative influence over the overall development and governance of cyberspace. China's diplomatic quest has focused on increasing appeal for China's vision of cyber sovereignty and building a coalition of like-minded nations favourable to state-centric models of international cyber negotiations and Internet governance.

- China's political discourse on cyber affairs remains inherently grounded in historic distrust towards the international legal regime and deep-seated tension between China and Western neoliberal interests.
- The official Chinese line regards the application of international humanitarian law as being tantamount to legitimising conflict in the cyber domain, pleading for the demilitarisation of legal approaches to cyber domain. China has expressed support for the principles of the UN Charter and regards sovereignty as a primary rule of international law, advocating for the inherent right of states to administer their domestic cyberspace according to domestic law and political culture.
- The EU's engagement with China has been primarily focused on socio-economic issues related to cybersecurity, the digital economy, market access reciprocity and intellectual property safeguards. However, as the EU recalibrates its priorities toward China, diplomatic discussions are increasingly going to address more structural issues.
- The disentangling of supply chains with Chinese suppliers risks consolidating digital spheres of influence across the East-West divide. While this might prove beneficial for enhancing Europe's domestic industrial bases, the decoupling contradicts with broader objectives of compelling structural reforms to the PRC's state capitalism model and eradicating discriminatory market access policies. In contrast to comprehensive exclusionary measures, the EU's risk-based and network resilience-based approach to this issue may succeed in addressing both geoeconomic and cybersecurity issues related to Huawei.

1 Introduction

Few other aspects have permeated social life and interstate relations as thoroughly as the Internet and digital communication technologies. In China, the advent of digital technologies has amplified traditional challenges to the one-party regime and (re)shaped the governing elite's threat perceptions. This has been reflected in the Chinese understanding of "information/ICT security", which embodies different political imaginations of what the role of states in the governance of cyberspace should be and how this space should be governed. Whereas neoliberal models promote multi-stakeholderism with the state as a shaper or facilitator of public policy, the Chinese vision advocates for lifting governments' top-down decisionmaking power over a territorialised cyberspace.

China's growing international presence and a remarkable rise in science and technology have had profound geopolitical and economic ramifications. Similarly, developments in cyber affairs taking place in China produce a ripple effect on global cybersecurity policy. In part, this stems from the fact that China has the most Internet users in the world - 829 million according to official estimates in 2019[1] - and a rapidly expanding digital economy. Chinese Internet giants, such as Alibaba, Didi, Tencent and Baidu, are also increasingly able to rival those in Silicon Valley in terms of market value[2] and influence in the global tech landscape. According to Echo Wall, China was reported to be second only to the United States for so-called "unicorns" - "private companies valued at over $1 billion - with the latest data showing China already has 206 unicorns.[3]

Domestically, the People's Republic of China's (PRC) approach to cyberspace is driven by two imperatives: a technological imperative of ensuring long-term growth founded on innovation, and a political drive of maintaining the "orderly" flow of information within cyberspace to safeguard regime legitimacy and social stability. China's approach is further defined by the overarching goal of transforming the country into a normative, military and commercial "cyber superpower" that harnesses the power of digital technologies and innovation to achieve global technological leadership. These goals have provided the major impetus for an ongoing global campaign of industrial cyber espionage originating on the Mainland.

The "rise of China" in cyberspace therefore represents much more than the development of state-aligned offensive network capabilities or a sophisticated cyber espionage apparatus. It is in many ways more about the ability of the PRC to transform national companies into champions, and in turn, viable market players in the computing marketplaces on par with Western high-tech behemoths.

Turning the focus outwards, China's approach to international cyber diplomacy has been historically grounded in the national aim of the "great rejuvenation of the Chinese nation" after the perceived "century of humiliation". It is driven by the aspiration to "catch up and surpass" the West across the normative, economic, technological and political realms (弯道超车 and 跨越发展) and secure an equal place at the decision-making table as a rule-maker. In international cyber debates, the PRC has vehemently emphasised the binding principles of international law as enunciated in the UN Charter, elevating principles such as sovereignty and sovereign equality, the peaceful settlement of disputes, non-use of force, non-interferences, mutual respect over the Charter's "purposes" of self-determination of the peoples and human rights.[4] Moreover, China has expressed strong support for multilateral intergovernmental institutions as key fora to garner support for the negotiation of a binding treaty on

[1] "China has 829 mln online users: report." *Xinhua News Agency*, 28 Feb. 2019, http://www.xinhuanet.com/english/2019-02/28/c_137857753.htm

[2] "America V China: The Battle for Digital Supremacy." *The Economist*, 15 Mar. 2018, https://www.economist.com/news/leaders/21738883-americas-technological-hegemony-under-threat-china-battle-digital-supremacy

[3] Chen Jibing. "Piling Into the Lead." *Echowall*, 13 Nov. 2019, https://www.echo-wall.eu/chinese-whispers/piling-lead

[4] Judge Xue, Hanqin, and Elizabeth Wilmshurst. *China and International Law: 60 Years in Review*. International Law Summary, 8 Mar. 2013, https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/080313summary.pdf

information security that enshrines its territorial-based vision pertaining to the governance of cyberspace. The country's cyber diplomacy has been underpinned by substantial investments in capacity building in developing and emerging economies, which combine the exportation of China's domestic legal system with the "internationalisation" (走出去) of Chinese-made technology to new export markets.

1.1 Threat landscape and commercially motivated cyber espionage

In 2017, China's top cybersecurity risk-monitoring authority - the Chinese National Computer Network Emergency Response Technical Team and Coordination Centre (NCNERTTC) - reported 17.5 million cyberattacks on public and private Chinese entities,[5] critical infrastructure operators and data centres. The WannaCry ransomware infected more than 30,000 Chinese organisations and the growing proliferation of IoT devices has led to a spike in cyberattacks of "over 950 percent between 2014 to 2016".[6] China's Computer Emergency Response Team (CNCERT/CC)'s Cybersecurity Report of July 2019[7] maintains that in 2018, the organisation handled 106,000 cybersecurity incidents impacting data integrity or systems availability, with the majority of observed incidents being spear-phishing operations, website defacements, account takeovers, and DDoS attacks. While CNCERT/CC observed a 46.5 percent decrease in the number of "attacks" against government websites in 2018, the report notes an increasingly "growing number of cybercrimes", targeted intrusion operations and strategic compromises taking advantage of disclosed software vulnerabilities.

1.2 Recent activity and shifting rationale

Public reporting singles out China as a key source of global cyber insecurity, owing to the high number of cyber exploitation campaigns originating from its territory. FireEye has observed the activities of over 70 groups based in China - criminal, military and intelligence actors, civilian contractors, patriotic hackers - suspected to have varying "level[s] of state direction or support [for state interests]" from Beijing.[8] The threat actor landscape in China remains non-monolithic and opaquely state-linked, characterised by dynamic and continuously evolving relationships between actors and state bodies across spectrums of direct government sponsorship and independent moonlighting action. Threat actors, myriad in terms of organisation, nature and interests, may at times align for a common goal which could be state-sponsored or state-mandated. Nevertheless, the existence of a vast number of threat groups and proxies formally disconnected from the party-state apparatus underscores the profoundly blurred role of "state power [...] at the heart of [Chinese] threat ecosystem",[9] not least providing the Chinese government with a significant amount of plausible deniability to pursue broader objectives. Cyber operations originating from China fall within four interlocking baskets: **industrial espionage** to, *inter alia*, sustain top-down economic objectives linked to "self-reliance" in high-tech, military application technologies, and telecommunications (the 13th Five-Year Plan, Made in China 2025), or investment projects such as the Belt and Road Initiative; **domestic operations** to preserve the ruling power of the CCP with an emphasis on "CCP narrative control" or territorialised information monitoring; **geopolitical and foreign policy operations** (e.g. cyber-enabled intelligence collection) in line with "flashpoint" disputes and

[5] Cao, Yin. "Cybersecurity Threat Could Cause Damage 'Beyond Imagination'." *China Daily*. 6 Dec. 2017, http://www.chinadaily.com.cn/china/2017-12/06/content_35228255.htm

[6] Cadell, Cate and Nick Macfie. "China Rolls Out National Cyber Threat Response Plan". *Reuters*. 27 Jun. 2017, https://www.reuters.com/article/us-china-cyber-idUSKBN19I11J

[7] "国家互联网应急中心 [2018 China Information Security Report]." *The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC)*, 17 July 2019, https://www.cert.org.cn/publish/main/46/2019/20190717075521797368911/20190717075521797368911_.html

[8] FireEye iSight Intelligence. "Red Line Drawn: China Recalculates Its Use of Cyber Espionage." *FireEye Threat Research*, 20 Jun. 2016, https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html

[9] Fraser, Nalani, et al. "APT41: A Dual Espionage and Cyber Crime Operation." *FireEye Threat Research*, 7 Aug. 2019, https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

ongoing debates, such as the South China Sea or the US-China trade war; and cyber activities in the **military realm** for tactical and/or strategic advantage (e.g. reconnaissance and strategic collection).

However, cyber exploitation operations coming out of China must be contextualised as single components of a broader state-driven industrial policy designed to restructure the drivers of China's economic growth. Threat actors have shown a continued focus on cyber exploitation targeting a wide range of verticals, aligned with industrial policy programmes, particularly the high-tech and telecommunications, pharmaceuticals, energy and aviation sectors and the defence industrial base in South and Southeast Asia, Japan, Taiwan, Hong Kong, South Korea, Europe and the United States. Corporate or technical information stolen through cyber means could be operationalised for the development of strategically autonomous "secure and controllable" network systems and supply chains with reduced reliance on foreign technologies. Weaning China off its dependence on foreign suppliers of digital and communications technologies is perceived as being integral for the regime's broader survivability goals, national security and, by extension, protection from foreign interference in cyberspace. Those in Zhongnanhai, the Chinese governing elite's compound in Beijing, believe that increases in Chinese domestic national champions' innovative edge would eventually be converted into a modernised Chinese military and economy. In this sense, **comprehensive economic objectives linked to "self-reliance" and indigenous innovation** (自力更生 and 自主创新), **and corresponding industrial plans, incentivise Chinese actors' illicit practices beyond the Mainland**. As Chinese private or state-owned companies are encouraged to improve their indigenous innovative capacity and global competitiveness and reduce their reliance on foreign know-how by engaging in forced technology transfers through all possible means,[10] many actors opt-in for the cyber-enabled industrial espionage route.[11] As a result, Chinese cyber operations, both state- or commercially-backed, show a continued focus on targeted network intrusions against wide-ranging industrial sectors of importance for industrial policy programmes (e.g. Made in China 2025) or geo-economics initiatives (e.g. the Belt and Road Initiative). In the context of industrial policies, cyber-enabled acquisition, assimilation and absorption of foreign intellectual property is perceived as a valuable way to fast-forward the expansion of companies' competitiveness overseas, regardless of the Herculean task of capturing the tacit contexts surrounding proprietary information.

Chinese threat groups demonstrate a strong preference for carrying out targeted intrusions against victim organisations' communications data, sensitive business negotiation information, proprietary intellectual property, such as product design and engineering specifications, operational information, product manuals, production and assembly data. Based on industry reports, rather than seeking destabilisation or coercive effects, the majority of known cyber intrusion campaigns by Chinese threat groups has been primarily designed to support domestic "national champions" by providing them with foreign know-how to enable their efforts at market internationalisation in "strategically important" industrial sectors. Sensitive product line or trade information gained through cyber intrusions has been used to alter Chinese national champions' business behaviour, improve their "indigenous innovation" prowess or gain advantage during trade negotiations in such a way as to increase the domestic industry's global competitiveness as mandated by strategic industrial plans.

CrowdStrike has exposed a long-running coordinated cyber campaign by Ministry of State Security (MSS)-aligned APT26 threat actors against several foreign manufacturers of the indigenous C919 passenger aircraft in order to reduce reliance on foreign technologies and enable domestic commercial

[10] The Office of the United States Trade Representative (USTR). Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfers, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974. Section 301 of the US Trade Act of 1974, 27 Mar. 2018, pp. 1-215, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/march/section-301-report-chinas-acts

[11] Alternatively, obtaining foreign technology takes place through legitimate business and commercial practices, such as the direct buying out intellectual property via mergers and acquisitions (M&As), mandating technology transfers as part of market access bargaining chips via joint ventures and licensing, and others.

aviation rivals to grow more globally competitive.[12] Similarly, between 2011 and 2017, MSS-affiliated APT3 actors stole proprietary "files containing commercial business documents" and secret trade data related to GPS, energy and transportation technologies from large US companies that is assessed to "have assisted [Chinese] competitor in developing, providing and marketing a similar product without incurring millions of dollars in research and development costs".[13] Moreover, intelligence collection or espionage targeting NGOs, civil societies and governments' networks around the globe have co-existed with industrial espionage. However, these types of campaigns pertain to political and strategic imperatives to control and shape the narrative about the regime's rule, gain a foothold in a high-value network for reconnaissance or pursue coercive effects against foreign government entities through doxing or theft of sensitive data.

1.2.1 Uptick in cyber espionage activities after 2015

Based on existing evidence provided by the private cybersecurity industry, Chinese state-linked industrial cyber espionage campaigns **never came close to ceasing cyber network exploitation**. Rather, they benefited from refinement in tradecraft, a more streamlined organisation and a narrowed mission focus. In November 2018, Rob Joyce - formerly the White House's Cybersecurity Coordinator - declared that hacking groups originating in China, such as APT40[14] and APT10,[15] have continued carrying out cyberattacks targeting American companies in direct violation of the 2015 Xi-Obama cyber espionage agreement that neither government would "conduct or knowingly support" the cyber-enabled theft of trade secrets and confidential business information "with the intent of providing competitive advantages to their companies or commercial sectors,[16] and subsequent endorsements of this norm made by China at various multilateral and bilateral fora.[17]

The US National Counterintelligence and Security Center's 2018 report asserted that China continues to present a threat to "intellectual property through cyber-enabled means" as demonstrated by suspected China-nexus threat actors campaigns (e.g. APT10, APT3, APT26, APT41) to fulfil collection requirements of the Ministry of State Security in line with China's military and economic strategy objectives and initiatives. APT26 has reportedly carried out an extensive intellectual property cyber exploitation campaign targeting Western turbine engine technology in order to enable the domestic production of the C919 passenger jet,[18] while PKPLUG has targeted countries and regions involved in Beijing's Belt and Road Initiative.[19] Similarly, APT41 sub-groups have sought to exfiltrate sensitive intellectual property in a wide range of sectors to support Chinese industrial policies, like the 13th Five-Year Plan,[20] and APT31 threat actors have allegedly compromised the National Association of Manufacturers (NAM) internal networks in 2019 to gain an advantage within the context of US-China trade negotiations.[21]

---

[12] Kozy, Adam. "Turbine Panda, China's Spies & Passenger Jets - Part 1." *Crowdstrike*, 14 Oct. 2019, https://www.crowdstrike.com/blog/huge-fan-of-your-work-part-1/

[13] The US Department of Justice *US Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage*. 27 Nov. 2017, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

[14] Plan, Fred, et al. "APT40: Examining a China-Nexus Espionage Actor." *FireEye Threat Research*, 4 Mar. 2019, https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

[15] Cybereason. *Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers*. 25 June 2019, https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

[16] The White House. "FACT SHEET: President Xi Jinping's State Visit to the United States." *Office of the Press Secretary*, 25 Sept. 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[17] Volz, Dustin. "China Violated Obama-Era Cybertheft Pact, US Official Says." *Wall Street Journal*, 8 Nov. 2018, https://www.wsj.com/articles/china-violated-obama-era-cybertheft-pact-u-s-official-says-1541716952

[18] Kozy, Adam. "Turbine Panda".

[19] Hinchliffe, Alex. "PKPLUG: Chinese Cyber Espionage Group Attacking Asia." *Palo Alto Networks Unit 42*, 3 Oct. 2019, https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/

[20] Fraser, Nalani, et al. "APT41: A Dual Espionage".

[21] Bing, Christopher. "Exclusive: US Manufacturing Group Hacked by China as Trade Talks Intensified." *Reuters*, 14 Nov. 2019. https://www.reuters.com/article/us-usa-trade-china-cyber-exclusive-idUSKBN1XN1AY

China's cyber espionage apparatus

Suspected China-nexus groups and their possible strategic intent

Circles refer to advanced persistent threat groups (APT) identified, by the original industry sources, as having a nexus to China. Based on their campaign activities, those actors' operational focus and targeting patterns are driven by multifold collection requirements in support of bolstering domestic manufacturers' expansion, domestic control, long-term state-led economic objectives, and current geopolitical events.

Note that neither the threat actors nor their targeting rationales are monolithic, and rigidly aligned to state interests. Rather, this threat landscape is evolving and dynamic, operationally, strategically and institutionally.

This list is non-exhaustive, and solely based on open-source reporting. Note that may be overlaps between different actors, clusters and activities, and that institutional affiliations are exclusively based on evidence of criminal indictments by the US Department of Justice.

National security espionage

Strategic access

Counterintelligence and targeted surveillance

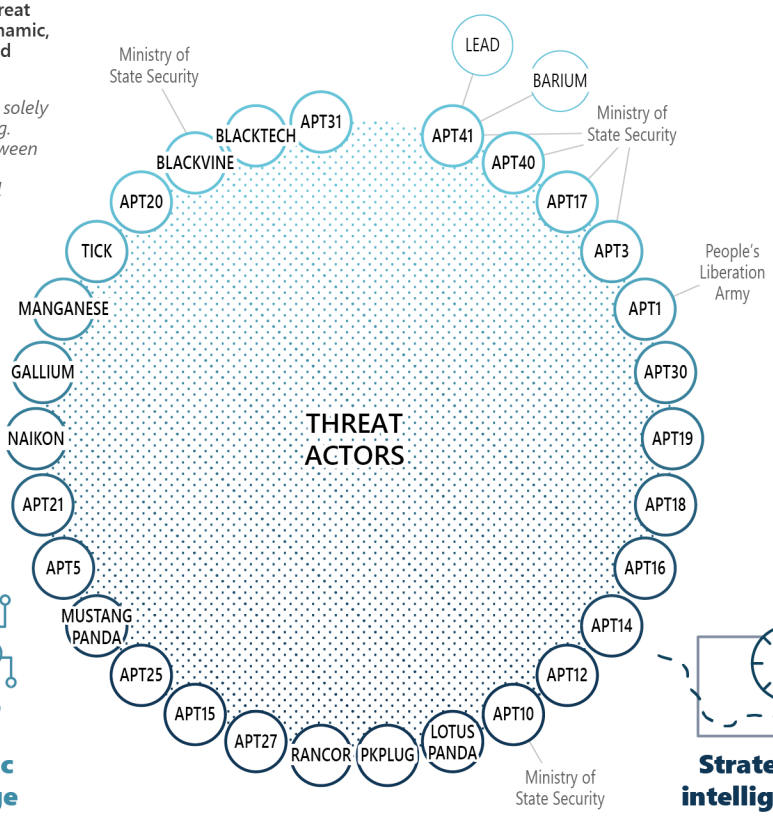
Office of Personnel Management (OPM)
Anthem Inc.
Marriott International
Equifax

Upstream data entries

Telecoms
Managed Service Providers (MSPs)
Internet Service Providers (ISPs)
data centers
law firms

Internal politics, 'social stability' and CCP narrative control

Hong Kong
Taiwan
Macau
Xinjiang Province
Tibet



Economic espionage

Directed collection

Bilateral trade and foreign policy negotiations

State-subsidised strategic economic plans and 'core' technologies

self-reliance and indigenous innovation
"secure and controllable" supply chains

Business negotiations involving domestic manufacturers

Infrastructure investment projects and the Belt and Road Initiative (BRI)

Strategic intelligence collection

Positional access

Military intelligence objectives related to the South China Sea

Development of indigenous (dual-use) maritime, aerospace, defense technologies

Regional power projection

Data: FireEye, 2020; Palo Alto Unit42, 2020; Microsoft, 2019; Symantec, 2019; SecureWorks, 2019; US Department of Justice, 2018; Trend Micro, 2019; Fox-IT, 2019, Crowdstrike, 2019

Based on industry reports, other China-based advanced persistent threat actors - such as THRIP, KEYBOY, APT40, APT41 and APT27 - conduct cyber exploitation operations in pursuit of strategic and positional access intelligence collection operations, particularly targeting defence industrial bases and dual-use military application technologies, such as satellite operators, telecommunications and maritime security/communication.[22] While the APT40 group's targeting focus has focused almost exclusively on naval technologies against the backdrop of territorial disputes in the South China Sea, APT41, THRIP and APT10 actors have recently conducted cyber espionage operations near the backbone of global communications by targeting telecommunications operators and managed service providers.[23] These campaigns likely serve multi-faceted industrial/commercial and (military) intelligence requirements, and are simultaneously aimed at exfiltrating intellectual property theft and obtaining intelligence and personally identifying information for the purposes of secondary operations. In July 2017, Germany's domestic intelligence agency complained about the damaging effects of (Chinese) cyber espionage on German industry against the backdrop of a growing number of cyber operations targeting the German Ministry of Foreign Affairs and German military research institutes critical of China's political leadership.[24] Similarly, the 2018 annual report by Dutch intelligence agencies asserts that intrusions carried out by Chinese hacking groups continue to cause significant economic damage by exfiltrating sensitive "confidential information [and intellectual property] with a substantial economic value" from the energy, chemical and high-tech sectors.[25]

Significantly, in December 2018, the United Kingdom, the United States and other members of the Five Eyes alliance issued coordinated high-confidence intelligence assessments attributing Cloud Hopper, "one of the most significant and widespread" cyber espionage campaigns "since at least 2016", to a hacking group acting on behest of the Ministry of State Security.[26] Cloud Hopper was an industrial cyber exploitation campaign that targeted intellectual property and trade secrets of companies across a wide range of countries in Europe and Asia and in the US. The hacking group behind the campaign - dubbed APT10 or Stone Panda - leveraged supply chain and "living off the land" attack vectors to compromise some of the largest managed and cloud service providers in the world[27] - hence the name of the campaign - as gateways to valuable intellectual property in the financial, healthcare, oil and gas, manufacturing, biotechnology and other sectors considered strategic by the Chinese government.[28]

Although refraining from calling out the Chinese government directly, other nations (Japan and Germany) supported the Five Eyes-coordinated attribution and the members of the intelligence alliance's broader attempt to solidify the norm against commercially motivated cyber espionage that emerged in 2015.[29] While not the sole contributing factor, the widespread publicity caused by this incident, in addition to its large size and scale, might have also provided the final impetus necessary for

[22] US National Counterintelligence and Security Center (NCSC). "Foreign Economic Espionage in Cyberspace." 26 Jul. 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

[23] Leong, Raymond, et al. "MESSAGETAP: Who's Reading Your Text Messages?" *FireEye Threat Research*, 31 Oct. 2019, https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html, Symantec Threat Intelligence. "Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies." *Symantec*, 19 Jun. 2018, https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

[24] Shalal, Andrea. "Germany Big Target of Cyber Espionage and Attacks: Government Report". *Reuters*. 4 Jul. 2017, https://www.reuters.com/article/us-germany-espionage-idUSKBN19P0UC

[25] Corder, Mike. "Dutch Intel Agency: Volume, Complexity of Cyberattacks Rises." *Associated Press*. 6 Mar. 2018, https://www.apnews.com/542b83152b174570b2ec97efd77874ae

[26] U.K. Foreign & Commonwealth Office, National Cyber Security Centre (2018). "UK and allies reveal global scale of Chinese cyber campaign." 20 Dec. 2018, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign

[27] Stubbs, Jack, et al. "Stealing Clouds." *Reuters*. 26 Jun 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

[28] Insikt Group, and Rapid7. "APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign." *Recorded Future*, 6 Feb. 2019, https://www.recordedfuture.com/apt10-cyberespionage-campaign/

[29] "G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015." *Council of the European Union*, 16 Nov. 2015, http://www.consilium.europa.eu/en/press/press-releases/2015/11/16/g20-summit-antalya-communique/

practical **political action within the EU -** the establishment of a targeted EU sanctions regime to deter and respond to external cyber threats agreed in May 2019.

Several underlying reasons might explain the shift from the slowdown in activity following the 2015 Xi-Obama bilateral accord to the apparent **resumption of Chinese state-supported espionage** after 2016.

First, the brief decline in activity coincided with the creation of the **Strategic Support Force** (SSF; **战略支援部**) which brought about internal streamlining[30] and reorganisation of (previously misaligned) responsibilities, mission objectives and targeting priorities between the two most relevant actors responsible for cyber operations in China - the PLA and the MSS.[31] In effect, the establishment of the SSF split up industrial cyber exploitation from activities falling under the label of "cyber warfare" between the two CCP organisations. More specifically, the MSS has limited its focus to (cyber-enabled) "foreign intelligence, political dissent, and economic espionage", leaving reconnaissance, "military intelligence and warfighting" to the People's Liberation Army.[32] The new division of labour induced by the creation of the SSF has triggered an evolution in economic espionage groups' operational sophistication but leaves unanswered questions regarding the mechanics of the interaction between military bodies like the SSF and other entities with cyber mandates, such as the MPS and the CAC.

The SSF's organisational streamlining and division of labour has resulted in incremental increases in Chinese cyber espionage campaigns' tradecraft marked by novel and more creative tactics, techniques and procedures. MSS-linked cyber espionage operators have secured persistent access to victim organisations through compromises in third-party trusted supply chains and have stepped up the use of stealthy living-off-the-land initial infection vectors.[33] According to industry reporting, Chinese state-sponsored advanced persistent groups have departed from historically less sophisticated and "noisy" behaviour through steady investment in developing custom malware for privilege escalation, lateral movement and network reconnaissance, as well as improvements in command-and-control infrastructure.

Second, the uptick in cyber espionage originating from China has been conditioned by the dynamics of the **US-China trade war**. The return of hacking could be linked to the tenacity of the US administration to decouple the US economy from Chinese technological dependence in the wake of the PRC becoming a prominent challenger for global leadership in next-generation technologies and innovation.

The Trump Administration has sought to curtail the flow of American intellectual property to China by weaving together a wide array of restrictive measures including criminal indictments, naming-and-shaming, trade sanctions and other non-tariff economic coercive measures. It announced in 2018 a whole-of-government initiative to counter Chinese industrial (cyber-enabled) espionage, forced technology transfers, state-backed foreign investment in the high-tech sector and economic coercion.[34] Furthermore, the drive to publicly expose and sanction Chinese state entities for cyber espionage activities has significantly accelerated since the first indictment of Chinese PLA officers in 2014. The US Department of Justice has indicted several entities linked to the Ministry of State Security for industrial

[30] Costello, John K., and Joe McReynolds. "SSF Structure and Components", *China's Strategic Support Force: A Force for a New Era*. National Defense University Press, 2018.
[31] Costello, John K., and Joe McReynolds, "Remaining Challenges."
[32] Costello, John K., and Joe McReynolds, "Remaining Challenges."
[33] Fraser, Nalani, et al. "APT41: A Dual Espionage". Marc-Etienne M.Léveillé, and Mathieu Tartare. "Connecting the Dots: Exposing the Arsenal and Methods of the Winnti Group." *ESET WeLiveSecurity*, 14 Oct. 2019, https://www.welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/. See the SHADOWPAD, SHADOWHAMMER, and CCLEANER intrusion campaigns.
[34] The US Department of Justice. "Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage." 1 Nov. 2018, https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage

cyber espionage. Moreover, Chinese high-tech suppliers have been the subject of restrictive trade measures, export controls, exclusionary bans and FDI restrictions.

Yet, the acquisition of foreign technology is critical for Beijing's objective of sustaining the transformation of China's economy and securing control over "core technologies" (核心技术). Technology acquisition is often accomplished through legitimate business practices, such as mergers and acquisitions or joint ventures, but also through illicit means like cyber-enabled industrial espionage. The adoption of more stringent approaches to tackling Chinese forced foreign technology transfers, albeit necessary, has in effect closed off the legitimate routes of foreign know-how acquisition, hence hampering Chinese firms' capacity to acquire technology through other means. Cumulatively, the sealing of the business route and the (re)structuration of the SSF has encouraged more Chinese hacking groups to (re)intensify their efforts to conduct cyber-enabled intellectual property theft to help fuel China's economic development.

2 China's approach to cyberspace: main priorities

The complexities of China's social, political, institutional and economic context make it challenging to construct, implement and enforce international cybernorms of responsible state conduct in cyberspace. This stems from difficulties in determining the degree of state direction and control over entities involved in cyber exploitation operations. Most importantly, this stems from the CCP's profound embeddedness in the economy and the all-encompassing, expansive notion of national security enshrined in government and statutory legal frameworks.

CCP's embeddedness in the economy: The CCP exercises control across the whole spectrum of the public-private system and "the institutional fabric of society".[35] The CCP, the PLA, state-owned and non-state private enterprises, local and top governmental bodies and organs are deeply interwoven in a centralised party-state system. Industry sources and the US Department of Justice have exposed several targeted intrusions campaigns conducted by suspected contractors of the MSS. To clarify, APT10 activity targeting global Managed Service Providers (MSPs) has been associated with a company Huaying Haitai Science and Technology Development Company acting at the behest of the Tianjin Bureau of the MSS.[36] A similar contractor structure existed between APT26 operators and the Jiangsu Province MSS,[37] APT17 and information technology companies acting as fronts for the Jinan Bureau of the MSS,[38] and the deep linkages between the Ministry of State Security, the APT3 and active defence lab sponsored by China Information Technology Evaluation Center (CNITSEC) and the notorious Chinese firm Boyusec.[39]

The enmeshed nature of party-state control in the economy therefore blurs the dividing lines between "state and market actors, interests, and motivations".[40] This might present challenges for the effective

[35] Williams, Robert D. "The 'China, Inc+' Challenge to Cyberspace Norms." Hoover Institution Working Group on National Security, Technology, and Law, *Aegis Series Paper No. 1803*, 22 Feb. 2018, https://www.hoover.org/research/china-inc-challenge-cyberspace-norms

[36] The US Department of Justice. Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information. 20 Dec. 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[37] The US Department of Justice. Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years. 30 Oct. 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

[38] "APT17 Is Run by the Jinan Bureau of the Chinese Ministry of State Security." *Intrusion Truth*, 24 July 2019, https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/

[39] Insikt Group. "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3." *Recorded Future*, 17 May 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/

[40] Williams, Robert D. "The 'China Inc+' Challenge."

application of existing "traditional Western legal constructs", particularly (punitive) legal rules and measures that rely on a clear-cut distinction between state and non-state actors.[41]

These issues are accentuated in the cyber domain, where governmental policies to promote "military-civil integration"[42] further exacerbate the murkiness between state and private relations.[43] Close linkages between for-profit hacking groups, state intelligence agencies and moonlighting civilian/private actors - visible across the domain but very pronounced in China - make it difficult to ascertain the nature of state sponsorship involved in cyber espionage or its degree of direction or control.[44]

In addition, *the far-reaching and historically broad definition of national security* affords the CCP the legitimacy and legal grounds to constitute "virtually any objective" as "within the realm of [its] national interests",[45] including cyber-enabled intellectual property theft to sustain the national security goals of ensuring "secure and controllable" supply chains and an innovation-driven economic growth. National security "with Chinese characteristics" - as incorporated in statutory laws - is of sweeping vision and scope, extending beyond the concept's traditional confines to capture "core interests", such as cultural security, public opinion, social order and stability, cultural security and regime legitimacy.

Article 2 of China's National Security Law of 2015 (国家安全法) defines the concept as the absence of external and domestic threats to the "regime, sovereignty, unity, territorial integrity, the welfare of the people", the continued socio-economic development and "the ability to maintain a sustained state of security".[46] "China's Peaceful Development" - a white paper published by the State Council in 2011 - also refers to China's form of government and "political system", "national reunification [...] and overall social stability" as "core interests" of the state to be resolutely defended at all costs.[47] Tracing the genealogy of "national security" to today, current international demands for structural reforms to China's economic model and the exerting of pressure on state-backed and subsidised Chinese telecommunications giants have been construed as encroaching on China's core interests of "economic sovereignty"[48] and the national industry's burgeoning ability to capture large swaths of the global technology supply chain.[49]

"Without cybersecurity, there is no national security, and without informatisation, there is no [economic] modernisation [没有网络安全就没有国家安全，没有信息化就没有现代化]", announced Xi in 2014.[50] For the party-state, cyberspace represents a double-edged sword sitting at the nexus of three concerns for the CCP: regime legitimacy, national security and technological-economic dependence. On the one hand,

[41] Williams, Robert D. "The 'China Inc+' Challenge."
[42] "Xi Jinping's Speech at the National Cybersecurity and Informatization Work Conference." *China Copyright and Media*, 22 Apr. 2018, https://chinacopyrightandmedia.wordpress.com/2018/04/22/xi-jinpings-speech-at-the-national-cybersecurity-and-informatization-work-conference/, Triolo, Paul, et al. "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities." *DigiChina*, New America, 1 May 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/
[43] Jiang, Jie. "China Unveils Its First Civil-Military Cybersecurity Innovation Center." People's Daily, 28 Dec. 2017, http://en.people.cn/n3/2017/1228/c90000-9309428.html
[44] Segal, Adam. "Chinese Cyber Diplomacy in a New Era of Uncertainty". Hoover Institution Working Group on National Security, Technology, and Law, *Aegis Series Paper No. 1703*, 2 June 2017, https://www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty
[45] Segal, Adam. "Chinese Cyber Diplomacy".
[46] National Security Law of the People's Republic of China, *Ministry of National Defence of the People's Republic of China,* 3 Mar. 2017, http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm
[47] "China's Peaceful Development", *The State Council of the People's Republic of* China, 6 Sep. 2011, http://english.gov.cn/archive/white_paper/2014/09/09/content_281474986284646.htm
[48] "述评：美国发动对华贸易战的五大世界性危害 [Commentary: The Five Major Global Harms of the United States Launching a Trade War against China]." *Xinhua News Agency*, 25 May 2019, http://xhpfmapi.zhongguowangshi.com/vh512/share/6159262
[49] Xu, Qiyuan. "Opinion: What Is China's Core Economic Interest in Trade War?" *Caixin Global Limited*, 28 Sept. 2018, https://www.caixinglobal.com/2018-09-28/opinion-what-is-chinas-core-economic-interest-in-trade-war-101331152.html
[50] "President Xi Jinping's views on the Internet". *China Daily*. 14 Dec. 2015, http://www.chinadaily.com.cn/china/2015-12/14/content_22706973.htm

Beijing considers digital technologies as vital fuel for the country's economic rise in the next few decades. Above all, new technology is essential to extend the Party's rule, strengthen central control over individual lives, and cultivate a public opinion environment consistent with Party objectives.[51] On the other hand, new and powerful ways of disseminating information amplify age-old challenges to the regime's hold on power and its legitimacy. Cyberspace offers novel opportunities for "colourful" resistance movements critical to the regime to coalesce, form opposition movements and even mobilise against the regime's continuation of power.

For this reason, the CCP leadership conceptualises two types of "cyber threats":

- **threats through cyberspace**, or forms of cyber-enabled operations that have the potential to undermine social stability or subvert the regime's legitimacy and hold on power through the manipulation of information;
- **threats to cyberspace**, or "conventional-style" cyber capabilities that disrupt, damage, sabotage, subvert, destroy or interfere with the functioning of computer and network systems, critical infrastructure or data.

2.1 Control of information flows

First, the Chinese leadership is most wary of the implications of weaponised information, given the fact that "political stability is [perceptibly considered as] the basic precondition for national economic development and the happiness of the people".[52] The governing elite thus perceives the ability **to control the flows of information and manage content within China** as a necessity to ensuring the government's survival and for shaping narratives about the state and the Party in its favour. The goals of retaining the party-state's hold on power and extending its capacity for centralised control lie at the heart of China's domestic and international cyber domain policy. Official CCP cyber diplomacy discourse constitutes information being as potentially threatening to the one-party regime's narrative and its grasp on power, given the country's distinctive "political-cultural [and governance] context", which is historically characterised by a "tension" between "centralisation, hierarchy and order" and "decentralisation, rebellion and disorder".[53] In effect, "information security" has manifested in specific technological practices, such as restricting access to foreign websites (Google, Wikipedia, Twitter, Facebook, YouTube, among others), filtering content and managing and/or suppressing "negative" online public opinion and "energy"[54] on various platforms through the Great Firewall.

Chinese policymakers conceptualise cybersecurity as all-encompassing and expansive, often through the prism of communication and *information security*. Content, ideas and information circulating within Chinese cyberspace take precedence over external threats to networks infrastructure, which remain nonetheless subsumed under this concept. The constellation of referent object of cybersecurity - i.e. that which is threatened - and Beijing's security logic are broad and far-reaching, predominantly focused on the political implications of weaponised information to undermine regime continuity and social stability. Beijing has sought to define the problem of **information or ICT security** as distinctively different from the notion of "cybersecurity", expanding beyond technical infrastructure risks to broader

[51] Creemers, Rogier, et al. "Translation: China's New Top Internet Official Lays out Agenda for Party Control Online." *DigiChina*, New America, 24 Sept. 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-top--official-lays-out-agenda-for-party-control-online/

[52] "National Cyberspace Security Strategy." *Cyberspace Admiration of China, Office of the Central Leading Group for Cyberspace Affairs,* China Copyright and Media, 27 Dec. 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspacesecurity-strategy/

[53] Creemers, Rogier. "Cyber-Leninism: History, Political Culture and the Internet in China." *SSRN Electronic Journal*, Apr. 2015, 2.

[54] Creemers, Rogier, et al. "Translation: China's New Top Internet Official."

"political, economic, military, social, cultural [...] types of problems created by the misuse of information technology".[55]

2.2 Economic modernisation

Second, **cybersecurity** is a central component of China's next-generation **economic modernisation** strategy, which is conceived as indivisible elements like "two wings of a bird".[56] The 13th Five-Year Plan for Science and Technology Development of 2016 puts ICT as "the highest priority sector" of sustainable economic development. Accordingly, this sector attracts a tremendous amount of state-led and private investment owing to its significance for achieving the underlying objective of "digitising" the Chinese society and economy - the **moving away from labour-intensive manufacturing to innovation-driven economic modernisation** (often referenced as "informatisation" [信息化] in official discourse).[57]

This economic postulate associated with cyberspace is vital for ensuring CCP political legitimacy in the wake of the Chinese economy's slowdown and its transitioning towards higher-value products and services. Economic modernisation is therefore a centrifugal force driving China's industrial policy planning, cyber espionage operations and global decoupling within the context of US-China trade negotiations.

The underlying logic is that China faces an "innovation imperative" - "a pressing need to "upgrade the technological sophistication" of the economy through innovation and the creation of homegrown new advanced technologies.[58] From Zhongnanhai's vantage point, this imperative is vital for resolving structural economic challenges, moving up the economic value chain and ensuring sustained long-term economic growth. China is vehemently responding to this imperative to move past the current stage of industrialisation and combining this with a concurrent pursuit for capturing a larger share of global ICT supply chains. Adherent to the self-reliance mantra, the government is actively seeking to spur "innovation" by using direct state subsidies, developing homegrown technologies, implementing non-tariff market access barriers, boosting its own R&D spending and foreign direct investment and incentivising (il)legitimate means of acquiring intellectual property. Strategic plans actively leverage these instruments for the purpose of shielding domestic manufacturers from foreign competitors, particularly through specific joint venture requirements, foreign equity and contractual limitations, administrative licensing, forced technology transfers and other non-tariff cooperative arrangements.[59] Zhongnanhai has vowed to continue funding basic research and original innovation - financially and through institutional restructuring and overhauling - as well as through the cultivation of talent through recruitment and education.[60]

By enhancing their ability to innovate, Chinese high-tech enterprises are expected to be able to "replace [with homegrown alternatives] their foreign competitors on the domestic market and increasingly [...]

---

[55] United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security." annex, U.N. Doc. A/61/161, 18 Jul. 2006, https://undocs.org/A/61/161.

[56] "Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference." *Ministry of Foreign Affairs of the People's Republic of China*, 16 Dec. 2015, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

[57] "The 13th Five-Year Plan For Economic and Social Development of the People's Republic of China 2016-2020", *Central Committee of the Communist Party of China*, April 2016, http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf

[58] Kennedy, Andrew B., and Darren J. Lim. "The Innovation Imperative: Technology and US-China Rivalry in the Twenty-First Century." *International Affairs*, vol. 94, no. 3, May 2018, pp. 553-72.

[59] Zhou, Qian. "How to Read China's New Law on Foreign Investment." *China Briefing*, 31 Oct. 2019, https://www.china-briefing.com/news/read-chinas-new-law-foreign-investment/, "Law of the People's Republic of China on Chinese-Foreign Equity Joint Ventures." *Ministry of Commerce of the People's Republic of China*, 30 Nov. 2005, http://english.mofcom.gov.cn/article/policyrelease/Businessregulations/201303/20130300045777.shtml

[60] "中共中央印发《深化党和国家机构改革方案》[The Central Committee of the Communist Party of China Issued the 'Deepening Party and State Institution Reform Plan']." *State Council of the People's Republic of China*, 21 Mar. 2018, http://www.gov.cn/zhengce/content/2018-03/24/content_5277121.htm

on global markets".[61] President Xi himself has repeatedly emphasised the significance of "shaking off" the PRC's dependence on foreign know-how and China's drive of increasing control over core technologies through "self-reliance"[62] and "indigenous innovation" (自主创新)[63] within the context of a prolonged Sino-Chinese trade war and emerging supply chain decoupling. The Shanghai Cooperation Organisation-led Code of Conduct, presented to the UN General Assembly in 2015, maintains this perception by purporting that single-country dominance in critical infrastructures or emerging technologies' supply chains could threaten other states' sovereign right to establish territoriality and sovereign borders in administering the cyber domain.[64]

According to Xi Jinping, the shift away from a labour-intensive, manufacturing-based economy necessitates the "prioritisation of higher-quality drivers of economic development".[65] Core tenets of accomplishing this vision include the building up of the domestic ICT industry, especially in sectors such as artificial intelligence, cybersecurity, cloud computing, nanotechnology and Big Data. President Xi has also signalled that scaling up China's digital economy - moving forward the process of "deep integration of the Internet, big data and artificial intelligence with the real economy" - "will further advance indigenous innovation. In short, accelerating China's genuine capacity to innovate and produce homegrown R&D while reducing foreign dependence is irreplaceable for Xi's vision of boosting the country's overall market, diplomatic and technological global power.[66] Still, according to reports, Chinese innovation through R&D investment still faces fundamental problems. While the Chinese government has consistently maintained a high rate of R&D investment growth, the vast majority of invested funds have been devoted to technology application rather than discovery and basic research.[67]

The "Made in China 2025" (MIC2025) science and technology development strategy issued in 2016 is a prime example of how this aspiration translates into (industrial) policy. The MIC2025 blueprint is saturated with the phrases "indigenous innovation" and "self-sufficiency", setting up explicit market shares for Chinese companies' quest for "global market dominance" in the high-tech sector and a "cyber superpower" status.[68] As a prime example of China's extensive state-led policy for boosting indigenous innovation, Made in China 2025 highlights the Chinese government's "strive to control essential core technology" and its desire to "build independent development capacities in [...] strategic [...] areas related to the national economy and industrial security".[69]

However, there is no single strategy, guidance document or action plan that forms a monolithic Chinese top-down state-led industrial policy. Instead, a plethora of strategic documents and plans, in addition to private initiatives, form China's complex tech-related governance system. Those include, for instance, the Belt and Road and Digital Silk Road strategies, China's National Strategy for Innovation-Driven

[61] The Office of the United States Trade Representative (USTR). "Findings of the Investigation Into China's Acts, Policies, and Practices".
[62] "Xi Stresses Nation's Self-Reliance." *Ecns*, 27 Sept. 2018, http://www.ecns.cn/news/politics/2018-09-27/detail-ifyyknzp7230181.shtml
[63] "Speech at the Work Conference for Cybersecurity and Informatization." *China Copyright and Media*, 19 Apr. 2016, https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/
[64] United Nations General Assembly, "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." annex, U.N. Doc. A/69/723, 13 Jan. 2015, https://undocs.org/A/69/723.
[65] Wubbeke, J., et al. *Made in China 2025: The Making of a High-Tech Superpower and Consequences For Industrial Countries.* MERICS Papers on China No. 2, Mercator Institute for Chinese Studies, https://www.merics.org/en/papers-on-china/made-china-2025
[66] "What did Xi Jinping say about cyberspace?". *China Copyright and Media*, 19 Oct. 2017, https://chinacopyrightandmedia.wordpress.com/2017/10/19/what-did-xi-jinping-say-about-cyberspace/
[67] Kensaku Ihara. "Taiwan Loses 3,000 Chip Engineers to 'Made in China 2025.'" *Nikkei Asian Review*, 3 Dec. 2019, https://asia.nikkei.com/Business/China-tech/Taiwan-loses-3-000-chip-engineers-to-Made-in-China-2025; Chen Jibing. "Piling Into the Lead."
[68] The Office of the United States Trade Representative (USTR). "Findings of the Investigation Into China's Acts, Policies, and Practices".
[69] Wubbeke, J., et al. "Made in China 2025".

Development,[70] the 13th Five-Year Plan for economic/social development[71] and informatisation,[72] military-civilian fusion initiatives,[73] a multitude of AI development plans,[74] Internet Plus[75] and others.

2.3 Network resilience and reducing reliance on foreign technologies

Third, Beijing is increasingly worried about **the potential for cyberattacks on governmental and private networks** to disrupt critical infrastructure or services in times of conflict, suspend economic growth or cause physical-economic destruction that prevents China's future rise during peacetime. They are also particularly sensitive to their industry's dependence on foreign technology suppliers for network equipment, industrial control systems and other security products, as illustrated by President Xi's statement that "the fact that core technology is controlled by others is [China's] greatest hidden danger".[76] Given the importance to national security, and in the aftermath of the 2013 Snowden leaks exposing the US government's global surveillance programme PRISM,[77] one of Beijing's top priorities has been to secure cybersecurity supply chains by **diminishing dependence on foreign suppliers** of network equipment, digital platforms and "core technologies of key fields" which remain "under others' control".[78] This CCP perception of external cyber threats - both within the semantic/content and technology layers of cyberspace - provides a significant impetus for China's massive state-led investment in "self-reliance" industrial policies.

The Arab Spring, the 2013 Snowden revelations and high-profile incidents, such as the 2009 Stuxnet attack, the WannaCry ransomware of 2017 and operations against the DNC/DNCC, have provided Beijing with hard evidence of cyberattacks' increasingly real potential to produce political, social and economic disruption and interference. Achieving self-reliance through an indigenous supply chain is therefore also necessary for ensuring technological autonomy from Western manufacturers, both commercially and in military technologies. Motivated by a desire to shield communication channels from foreign intelligence services interception, Beijing has invested heavily in the build-up of indigenous dual-use technology product lines of strategic importance, particularly communication networks, undersea fibre-optic cables and satellite navigation systems (especially the BeiDou Navigation Satellite System and the Belt and Road Space Information Corridor).[79] The goal of achieving greater strategic

---

[70] 中共中央 国务院印发《国家创新驱动发展战略纲要》 [The State Council of the Communist Party of China Released "Outline of the National Innovation-Driven Development Strategy"]. 19 May 2016, http://www.xinhuanet.com//politics/2016-05/19/c_1118898033.htm

[71] "Goals, Missions of China's New Five-Year Plan." *China Daily*, 5 Mar. 2016, http://www.chinadaily.com.cn/business/2016-03/05/content_23749530.htm

[72] "国务院关于印发'十三五'国家信息化规划的通知（国发〔2016〕73号）[Notice of the CPC State Council the '13th Five-Year National Informatization Plan']." *The State Council of the People's Republic of China*, 15 Dec. 2016, http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm

[73] "国防科工局发布2017年军民融合专项行动计划 [National Defence, Science and Security Bureau Releases Special 2017 Military-Civil Integration Action Plan]." *The State Council of the People's Republic of China*, 23 June 2017, http://www.gov.cn/xinwen/2017-06/23/content_5204695.htm#1

[74] "国务院关于印发新一代人工智能发展规划的通知（国发〔2017〕35号）[Notice of the State Council of the Communist Party of China on the Issue of a New Generation 'Artificial Intelligence Development Plan']." *The State Council of the People's Republic of China*, 8 July 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

[75] "国务院关于积极推进'互联网+'行动的指导意见（国发〔2015〕40号）[Guiding Opinion of the State Council of the CPC on Actively Promoting the 'Internet+' Plan]." *The State Council of the People's Republic of China*, 4 July 2015, http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm

[76] "Speech at the Work Conference for Cybersecurity and Informatization."

[77] "NSA Slides Explain the PRISM Data-Collection Program." *The Washington Post*, 6 June 2018, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

[78] "President Xi Says China Faces Major Science, Technology "Bottleneck"". *Xinhua News Agency*, 1 June 2016, http://www.xinhuanet.com/english/2016-06/01/c_135402671.htm

[79] "China Is Building a New Silk Road, and This One Is Digital." *World Economic Forum*, 18 Aug. 2018, https://www.weforum.org/agenda/2018/08/china-is-building-a-new-silk-road-and-this-one-s-digital/, "China to Promote Space Cooperation for UN Sustainable Development." *Xinhua News Agency*, 24 Apr. 2019, http://www.xinhuanet.com/english/2019-04/24/c_138006139.htm

autonomy in both the cyber and kinetic technology realms is strategic in the context of China's growing regional security role and the PLA's ongoing efforts to **modernise China's armed forces**.

2.4 Normative power

A crucial fourth priority for the Chinese government related to the cyber domain is in the normative realm. Specifically, Beijing seeks to **promote China's institutional power and normative influence over the overall development and governance of cyberspace**. More internationally oriented, this central pillar of Chinese cyber diplomacy entails the promotion of the idea of cyber sovereignty (网络主权) and a multilateral model of Internet governance.

The core values of the multi-stakeholder cyberspace governance mode favoured by the EU - underscore the economic benefits of cyberspace and the norms of openness (of connection and access), inclusiveness (of a wide range of heterogeneous stakeholders) and freedom (e.g. from censorship). In stark contrast, China advocates for a more significant "recognition of sovereign rights [...] and **a greater role for sovereign states** in Internet governance"[80] to further legitimise the curtailing of the free dissemination of information and online expression within China. Beijing's special attention to the principle of cyber sovereignty subordinates cyberspace to the interests and values of the state. The elevation of this concept over other principles has, in turn, justified the sustaining of infringements upon privacy and human rights through content-filtering systems like the Great Firewall, which have consistently operationalised the idea of a controllable and manageable cyberspace. China is among the states that emphasise a central role for national security and the supremacy of state actors - along with their priorities, interests and security logic - in administering cyberspace and information technology. This model of risk and threat management is at odds with the bottom-up approach to Internet governance that is historically espoused by liberal Western regimes.[81] Official Chinese cyber discourse contends that the "transformation of the global Internet governance system" - "characterised by Western hegemony - could only take place with the widespread adoption of "cyber sovereignty" (网络主权).

The notion describes the idea of respecting the right of individual nation-states to "independently choose their path of cyber development, the model of cyber regulation and Internet public policies"[82] and "administer cyberspace in accordance with [national] law" and their distinct political-cultural contexts and legal frameworks. The cyber sovereignty idea also includes the right to "exercise jurisdiction over ICT infrastructure, resources and activities within their territories" and the protection of ICT security "to safeguard citizens' legitimate rights and interests in cyberspace".[83] In other words, according to this territorialised vision of cyberspace, governments are to be afforded the right to exert their political and cultural sovereignty into cyberspace to defend their domestic national interests and national sovereignty. States are called upon to formulate and enforce public policies, "laws and regulations concerning cyberspace" based on their "national circumstances".[84]

Sovereignty - as an organising principle of China's efforts - embodies the idea that national governments are free to erect borders in cyberspace in a way that is similar to the physical world. Much like actual borders, Beijing's reading of the idea empowers governments to monitor and sanction

[80] Hampson, Fen Osler, and Michael Sulmeyer. "Getting Beyond Norms: New Approaches to International Cyber Security Challenges". *Special Report, Centre for International Governance Innovation*, 7 Sep. 2017,https://www.cigionline.org/publications/getting-beyond-norms-new-approaches-international-cyber-security-challenges

[81] Each state is seen as having the legitimate right to fully manage and administer its own sovereign spaces according to its own domestic law, rules, norms, and political culture. Although the importance of nonstate actors in maintaining the Internet is recognised and their role to 'participate' in governance is reaffirmed, Beijing believes states should have a louder voice.

[82] "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference."

[83] "International Strategy of Cooperation on Cyberspace", *Information Office of the State Council of the People's Republic of China*, 2 Mar. 2017, http://www.scio.gov.cn/32618/Document/1543874/1543874.htm

[84] "National Cyberspace Security Strategy."

external and internal data flows with the help of tools, such as the Great Firewall. Cyber sovereignty serves to legitimise Beijing's own sweeping surveillance and censorship policies, practices and acts, as well as new legal frameworks that run contrary to the liberal values of multi-stakeholderism and the neoliberal model of cyber governance.

Beijing has maintained this territorialised approach to governing cyberspace since the beginning of international discussions on "the field of ICTs in the context of international security". Under the auspices of the United Nations, China has repeatedly insisted that the Internet should be subject to "domestic legislation" and that traffic in cyberspace should be controlled "under the premises of national sovereignty and security" taking into account "historical, cultural and political differences among countries".[85]

Moreover, China advocates for all nation-states to "participate in the international cyberspace governance on an equal footing". Official documents and speeches call upon states with advanced technology to refrain from pursuing "cyber hegemony", interfering in "other countries' internal affairs", "engag[ing] in, connive[ing] at or support[ing] cyber activities that undermine other countries' national security",[86] or leveraging technological or institutional dominance to "undermine the security of other countries' ICT product and service supply chain[s]".[87]

Therefore, cyber sovereignty could similarly be understood as a diplomatic quest to "shape the nature of statehood" in the field of cyber diplomacy towards an alternative model of governance and regulation that is more control- and state-focused.[88] Beijing's proactivity in international cybersecurity negotiations in recent years - manifested by, for instance, the sponsoring of the Codes of Conduct and the open-ended working group draft resolution at the General Assembly - has aimed at increasing emerging countries' appeal to China's vision to build a coalition of like-minded nations that "subscribe to its policies" in order to "gain de jure international support for [...] its de facto Internet censorship policies".[89] As contended by Xi himself, the "Chinese way" aspires to "blaz[e] a new trail for other developing countries to achieve modernisation", allowing them to "speed up their development" by use of new technologies "while preserving their independence".[90]

Beijing's preference for a cyber sovereignty-based model, which some might say has also gained some traction in the West, simultaneously builds support for diminishing perceived Western hegemony within the global governance system while reinforcing China's leadership role internationally. Significantly, the promotion of Chinese ideas in the ideational realm has taken place in tandem with the export of Chinese surveillance technologies and networking equipment in countries, such as Tanzania, Ecuador and Zimbabwe and the internationalisation of China's domestic legal system to places like Vietnam.

Drawing upon the historical experience of centuries of humiliation and profound distrust in the status quo, official discourse builds a narrative of China as a champion of plurality. Beijing lists the promotion of a "fair" and "equal" Internet governance system as one of its strategic goals of cyber diplomacy. The prevalence of concepts, such as "hegemony", "equality" and the "digital divide", in official cyber-related discourse underscore the need for political solutions to rebalance global governance and the perceived centre-periphery division therein. The official line highlights the widening "digital divide among

[85] United Nations General Assembly, U.N. Doc. A/61/161.
[86] "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference."
[87] "International Strategy of Cooperation on Cyberspace".
[88] Zeng, J., Stevens, T., and Yaru Chen. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty.'" *Politics & Policy* 45 (3): 432-64., 2017.
[89] Lewis, Dev. "China's Global Internet Ambitions: Finding Roots in ASEAN"., *ICS Occasional Papers No. 4*, Institute of Chinese Studies, July 2017, https://www.icsin.org/uploads/2017/10/06/c460b9acb99e603970132f5ecffd4ef9.pdf
[90] "Socialism with Chinese Characteristics Enters New Era: Xi." *Xinhua News Agency*, 18 Oct. 2017, http://www.xinhuanet.com/english/2017-10/18/c_136688475.htm

countries and regions"[91] in technological capacity, the institutional hegemony of technologically advanced countries in the current system and rising "unilateralism" across the globe.

2.5 Cyber superpower

The fifth key component of the Chinese government's approach to cyber diplomacy is the strategic ambition of becoming a **cyber superpower "across multiple axes"**[92] **-** a great power able to reach "general parity with other national powers in digital technology".[93] First invoked in a seminal speech by Xi Jinping in 2014,[94] this strategic vision denotes everything from building up advanced digital infrastructure to enhancing China's role in global cyber-related norm- and rulemaking.

As with other Chinese concepts, "cyber superpower" (网络强国; also linked to science and technology superpower 科技强国) blends strategic/military objectives of an ICT-enabled military modernisation with commercial interests - such as increasing China's "Internet market capabilities" and the computing industry's global competitiveness - and political-social aspects related to the economic potential of a digitised society. In the long run, Beijing presumes that becoming a great power in cyberspace could help it build a more modern, self-reliant, globally competitive and prosperous market economy. Similarly, realising this vision would revamp China's military with state-of-the-art technology and replace dependence on foreign powers by integrating technology that is "secure" because it is "controllable", which would ultimately bolster China's regional security presence. Moreover, the normative dimension of this exhortation signifies the PRC's intention of gaining a leading voice in international cyber affairs negotiations and its pursuit of a norm-setting position commensurate with its size and relative power.

A central feature of being a "cyber superpower" is the promotion of China's normative vision and agenda-setting power in international cyber debates.[95] The Chinese government under Xi believes that becoming a rulemaker and normsetter present powerful mechanisms towards shaping others' behaviour in cyberspace in China's favour.

Beijing has demonstrated a preference for state-centric models of cyberspace negotiations within the framework of the UN, especially the United Nations Telecommunications Union (ITU), the UN Governmental Group of Experts (UNGGE) and the UN General Assembly.[96] Intergovernmental forums would provide China with a platform "to mobilise the votes of developing countries" that are supportive of exercising greater political authority over Internet traffic.[97]

At the Wuzhen World Internet Conference in 2015, President Xi Jinping charted out the general direction of China's international cyber diplomacy as being underpinned by four principles "to reform the Internet governance system" and five propositions "to jointly build a community of shared future in cyberspace".[98] The four principles advocate for a reform based on open cooperation, cyber sovereignty,

---

[91] "International Strategy of Cooperation on Cyberspace".

[92] Creemers, R., et al. "Lexicon: 网络强国 Wǎngluò Qiángguó." *DigiChina*, New America, 31 May 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/

[93] Webster, Graham. "Testimony Before the US-China Economic and Security Review Commission", US-China Economic and Security Review Commission, Hearing on 'US Tools to Address Chinese Market Distortions', 8 Jun. 2016, https://uscc.gov/sites/default/files/USCC-Webster-Written-FINALSUBMIT.pdf

[94] "Central Leading Group for Internet Security and Informatization Established". *China Copyright and Media*, 1 Mar. 2014, https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/

[95] "International Strategy of Cooperation on Cyberspace".

[96] "International Strategy of Cooperation on Cyberspace."

[97] Segal, Adam. "When China Rules the Web: Technology in Service of the State", *Foreign Affairs*, September/October 2018, Council on Foreign Relations, 13 Aug. 2018, https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web

[98] "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference."

peace and security and "building a good order".[99] The five propositions specify the need for the international community to work towards guaranteeing cybersecurity and promoting the digital economy and innovation, an online cultural exchange and a more inclusive Internet governance system. The National Cybersecurity Strategy, released by the Cyberspace Administration of China (CAC) in 2016, and the International Cooperation of Cooperation on Cyberspace, jointly issued by the Ministry of Foreign Affairs and the CAC in 2017, further set out China's general approach to international cyber affairs policy by defining specific foreign policy goals and action points.

The International Strategy stipulates the key thematic areas and strategic objectives underlying China's participation in international multilateral processes and other bilateral, regional and "minilateral" dialogues and cooperation mechanisms. China has specifically mentioned its own Wuzhen Summit, the ARF, the SCO, FOCAC, APEC, G20 - and above all, bilateral partnerships - as key tribunes for the promotion of its normative views.

According to the International Strategy, China's cyber diplomacy objectives would revolve around:

- **Safeguarding sovereignty and security** by strongly emphasising that investments in cyberdefence could maintain peace and security in cyberspace, but also by adherence to peacetime law and the principles enshrined in the UN Charter (sovereignty and sovereign equality, peaceful settlement of disputes, non-use of force, non-interference), and by use of confidence building measures, such as "consultation and mediation mechanisms to forestall and avoid conflict";[100]
- **Developing a system of international rules** by maintaining stability in cyberspace as a discursive and norm entrepreneurship power and seeking to create and implement universally accepted international legal rules and norms of responsible state behaviour under the auspices of the UN;
- **Promoting "fair" Internet governance** and advocating for a shift towards more inclusive, democratic, transparent, but also a more intergovernmental cyber domain governance system;
- **Protecting legitimate rights and interests of citizens** by enforcing a "rules-based", "domestic" cyberspace in which citizens' rights and fundamental human rights are to be balanced against other priorities, such as the maintenance of social "order" and safeguarding "national security and public interests";[101]
- **Promoting cooperation in the digital economy** by pushing forward the development of digital technologies and innovation to shift the drivers of economic growth, while bridging the "digital divide" through capacity building in developing countries;
- **Building platforms for cyber culture exchange** between nation-states.

The strategy sets out concrete action points for the achievement of the above-listed strategic goals, emphasising the need for the negotiation of a new cybercrimes and cyber terrorism treaty as well as new "global legal instruments" signed by states to replace existing frameworks that, according to Beijing, have become "obsolete". In addition, Beijing seeks to accelerate law enforcement cooperation, information-sharing and the provision of training and capacity building in emerging economies. The government also underscores its support for international cooperation on cybercrimes and terrorism at the UN within the Commission on Crime Prevention and Criminal Justice (CCPCJ), the United Nations Office on Drugs and Crime (ODC), the ASEAN Regional Forum (ARF) and the BRICS organisation. China also vows to remain actively engaged in capacity building in developing countries through bilateral

[99] "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference."
[100] "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference."
[101] "International Strategy of Cooperation on Cyberspace."

programmes and initiatives, such as the Digital Silk Road and the Belt and Road Initiative. The emphasis of capacity building is put on critical information infrastructure protection, information-sharing and exportation of legislative and technological expertise.

Table 1. Selected speeches, documents and regulations guiding China's approach to cyberspace. Authors' compilation.

Year	Title	Institution
Seminal speeches and interventions on global cyber issues		
Oct. 2011	66th Session of the General Assembly on Information and Cyberspace Security, *United Nations (A/C.1/66/PV.17)*	Ministry of Foreign Affairs / H.E. Ambassador Wang Qun
Feb. 2014	Central Leading Group on Cybersecurity and Informatization	Xi Jinping
Jun. 2014	Opening Ceremony of the International Workshop on Information and Cyber Security	Ministry of Foreign Affairs / Vice FM Li Baodong
Dec. 2015	Opening Ceremony of the Second World Internet Conference	Xi Jinping
Apr. 2016	Work Conference for Cybersecurity and Informatization	Xi Jinping
Oct. 2017	19th Party Congress	Xi Jinping
Dec. 2017	Fourth World Internet Conference	Wang Huning / Standing Committee
Apr. 2018	National Conference on the Work of Cybersecurity and Informatization	Xi Jinping
Sep. 2019	General Debate in the First Session of UN OEWG, *United Nations*	Wang Lei / Coordinator for Cyber Affairs, MFA
Oct. 2019	Sixth World Internet Conference	Wang Lei / Coordinator for Cyber Affairs, MFA
National strategies and white papers		
Jun. 2010	The Internet in China	State Council
May 2015	China's Military Strategy	State Council
Dec. 2016	National Cyberspace Security Strategy	Cyberspace Administration of China (CAC)
Mar. 2017	International Strategy of Cooperation on Cyberspace	Cyberspace Administration of China (CAC) / Ministry of Foreign Affairs
Jul. 2019	China's National Defense in the New Era	State Council

Year	Title	Institution
Initiatives, position papers and interventions at the United Nations		
Jul. 2007	Report of the Secretary-General *(A/62/98)*	Ministry of Foreign Affairs
Sep. 2011	International Code of Conduct for Information Security *(A/66/359, draft proposal)*	Ministry of Foreign Affairs
Jan. 2015	International Code of Conduct for Information Security *(A/69/723, draft proposal)*	Ministry of Foreign Affairs
Sep. 2019	Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security	Ministry of Foreign Affairs
Laws, regulations, and top-level design strategic economic/industrial plans		
May 2015	Made in China 2025	State Council / Ministry of Industry and Information Technology (MIIT)
Jul. 2015	National Security Law	NPC Standing Committee
Jul. 2015	Internet Plus	State Council
May 2016	National Strategy for Innovation-Driven Development	State Council
June 2016	Military-Civilian Action Plan for 2017	State Council / Central Committee and Central Military Commission
Dec. 2016	13th Five-Year Plan for Economic and Social Development, 13th Five-Year Plan for Informatisation	Central Committee
Jun. 2017	Cybersecurity Law	NPC Standing Committee, Cyberspace Administration of China (CAC)
Jun. 2017	National Intelligence Law	NPC Standing Committee
Jul. 2017	National Informatization Development Strategy 2006-2020	State Council

3 Legal, regulatory and institutional landscape

3.1 Legal and regulatory landscape

The Cybersecurity Law (CSL; 网络安全法) that came into force in June 2017 operationalises cyber sovereignty and grants the CCP the power to control foreign ICT companies and firewall off its Internet. Besides the CSL, China has drafted, or has already implemented, a wide-ranging system of overlapping regulations that act in concert to bolster the government's control and monitoring of the entire digital ecosystem "from the [physical] infrastructure that undergirds the Internet to the flow of data and the dissemination of information online".[102]

The Chinese system of digital technologies governance "meshes security-focused laws", for instance, the National Intelligence Law (国家情报法), the Counterterrorism Law (反恐怖主义法) and the National Security Law - with a variety of "development-focused" guiding strategies, plans and standards on ICTs, AI, big data, cybersecurity and others.[103] Like the EU Joint Communication on "Building strong cybersecurity for the EU",[104] national CCP strategies serve as high-level blueprints to guide both the political and technical enforcement of regulations and standards[105] transposed by (local government) policymakers. The National Cyberspace Strategy of 2016, the 2017 International Strategy for Cooperation in Cyberspace, the 13th Five-Year Plans on Science & Technology and the "Standing Committee Regulations on Strengthening Network and Information Security" are illustrative examples.[106]

In contrast with EU legislation, the CSL's scope is sweeping and comprehensive. As an "umbrella" law, CSL encompasses regulatory equivalents of the EU's NIS Directive, GDPR, the Cybersecurity Act, as well as regulations on "disinformation" and online platforms content management.

In terms of structure, the CSL is comprised of an interlocking matrix of rules pertaining to online content management, critical information infrastructure protection (NIS), data protection and cross-border data flow management (GDPR), network products and services management (NIS), technical standardisation and certification (Cybersecurity Act) and coordination of cybersecurity incidents emergency responses, critical information infrastructure protection and cyberdefence (NIS). The CSL is better conceived as a centrepiece regulation from which other, more granular measures and standards flow. It should be viewed as an accompanying plan in the enforcement and implementation of overall cyber affairs policy, rather than a standalone piece that forms the whole of Chinese cyberspace-related regulation.

Key CSL provisions include:

- Disclosure of Sensitive Information, Aggressive Data Localisation and the Cybersecurity Review Regime. Under the **Personal Information and Important Data Protection System** and the Critical Information Infrastructure Security Protection System (**CII**), foreign ICT companies and network system operators wishing to operate in the Chinese market in the all-encompassing "critical information infrastructure" sector are required to store, process and manage specific types

[102] Sacks, Samm. "Beijing Wants to Rewrite the Rules of the Internet". *The Atlantic*, 18 June 2018, https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/

[103] Sacks, Samm, et al. "Beyond the Worst-Case Assumptions on China's Cybersecurity Law." *DigiChina*, New America, 13 Oct. 2017, https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/; Triolo, Paul, et al. "China's Cybersecurity Law One Year On." *DigiChina*, New America, 30 Nov, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/

[104] Joint Communication to the European Parliament and the Council on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN (2017) 450 final, European Commission, Brussels, 13 Sep. 2017.

[105] Standards should be understood as guidelines, aiming at facilitating the successful and consistent implementation of higher-level policies *within* China. As a result, standards function as instruments to execute higher-level legal frameworks and compliance with domestic legislation.

[106] Sacks, Samm, et al. "Beyond the Worst-Case Assumptions".

of data in China and undergo security reviews (CRR, see below) that expose their "sensitive intellectual property (IP) and source code" as part of "verification and testing" procedures.[107] The security reviews are designed to evaluate the implications of cross-border data transfers on national security, "the people's livelihood", "economic development and social and public interests".[108]

- The Cybersecurity Multi-Level Protection System (**MLPS**) is a compliance mechanism according to which enterprises deemed to be critical infrastructure operators "would be subject[ed] to enhanced monitoring by the MPS [Ministry of Public Security] and third-party [security] certification". Moreover, MLPS specifies "domestic encryption requirements" which might in practice compel companies to disclose encryption keys.[109] MLPS and CII interlock with the **Cybersecurity Review Regime (CRR)**, administered by the Cyberspace Administration of China. CRR examines the "supply chains of network and product service providers" by use of security reviews with an extensive scope that focus on products' implications on national security.[110] CSL regulations are complemented by a variety of other, more granular measures building on specific issues, such as disclosures of cyber threat information.[111]
- The Internet **Information Content Management System** "tightens controls over online activities" and seeks to "attach an activity to users' offline identities", further granting the government the capacity to censor information deemed harmful. The System imposes "self-regulation [requirements] on intermediaries", platforms, networks and other actors operating on China's Internet.[112] To access China's market, domestic and foreign platforms, private firms, service providers or intermediaries therefore have to comply with the CCP's policies regarding control of the dissemination of online information. The securing of this objective - shaping, controlling, monitoring and censoring online public spaces - requires the indispensable co-optation, or cooperation, of Chinese Internet firms. The entrenchment of the so-called "networked authoritarianism"[113] works not only through a stringent system of intermediary liability, but also by imposing "corporate [...] [and] national responsibility" (互联网企业的国家责任) to Internet companies to supervise and sustain "the healthy development of the Internet".[114] The Chinese stringent regulatory environment in China also saddles domestic companies "with baggage that [other firms] operating within liberal democracies do not have", exposing Chinese businesses to increased levels of resistance, suspicion and scrutiny.[115]

[107] Sacks, Samm and Manyi Kathy Li. *How Chinese Cybersecurity Standards Impact Doing Business in China*. CSIS Briefs. Center for Strategic and International Studies (CSIS), 2 Aug. 2018, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china
[108] Sacks, et al. "Beyond the Worst-Case Assumptions".
[109] Sacks and Li, How Chinese Cybersecurity Standards
[110] "Interim Security Review Measures for Network Products and Services", *China Copyright and Media*, 4 May 2017, https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/
[111] 李勤. 网信办发布《网络安全威胁信息发布管理办法(征求意见稿)》及答记者问 [CAC Issued the "Administrative Measures on the Release of Cyber Threat Information (Draft for Comments)" and Answering Reporters' Questions]. 20 Nov. 2019, https://www.leiphone.com/news/201911/fOKyhRO6PstGnwKh.html
[112] Webster, Graham. "Testimony".
[113] MacKinnon, Rebecca. "China's 'Networked Authoritarianism.'" *Journal of Democracy*, vol. 22, no. 2, 2011, pp. 32-46.
[114] "Xi Jinping's Speech at the National Cybersecurity and Informatization Work Conference."
[115] Potter, Robert."PacNet #45 - Cybersecurity: The China Problem", Commentaries, *Pacific Forum*, 27 June 2018, https://www.pacforum.org/analysis/pacnet-45-cybersecurity-china-problem

- The **Personal Information and Important Data Protection System**, modelled on the GDPR, regulates the collection, storage and sharing of personal and corporate data.[116] The Data Protection System includes, among other things, data localisation requirements and policies to restrict cross-border data transfers. The standard **Personal Information Security Specification,** in effect as of May 2018,[117] and the Draft Privacy Impact Assessment Guide[118] further set out the procedures for consent to access of data and enforce responsibilities on companies to provide personally identifying information on users.
- The **Cross-Border Data Transfer Regime** imposes restrictions on the flow of data to and from China. It includes strict requirements for data localisation, especially for companies deemed to be critical infrastructure operators in exchange for market access.
- As in the NIS Directive, the **Cybersecurity Incident Management System,** the Public Internet Cybersecurity Threat Monitoring and Mitigation Measures,[119] issued in 2018, and several other cybersecurity standards schemes lay out the foundations for a system for coordinating incident responses, incident vulnerability "discovery and reporting management" and the development of "threat information-sharing platforms".[120]

Overall, CSL effectively functions as a non-tariff market access barrier for foreign software, hardware or network equipment-specific companies.[121] CSL demonstrates that playing by Beijing's rules - in other words, complying with standards which may often be at odds with enterprises' values or interests - is necessary to access the Chinese market. Requirements for data localisation, restrictions on cross-border data transfers and intrusive security reviews may expose firms' proprietary business information, intellectual property or personally identifying data to Chinese intelligence authorities.

In addition, the Ninth Amendment to the Criminal Law of the People's Republic of China of November 2015 tackles cybercrime offences. The Amendment extended criminalisation to cyber acts - breaches of information, dissemination of illegal information, the fabrication and spreading of "false information" and the sale or illegal use of personal information - and imposed responsibilities on Internet service providers (ISPs) to prevent cybercrime. The amendment also allows the court to levy hefty penalties against ISPs for failing to comply with national regulations on cybersecurity or providing deliberate assistance to criminals.[122]

It is worth noting several factors that could hamper China's overall objectives related to cyberspace. China's sovereignty-based approaches to governance require the continuous application of censorship to stifle the free flow of information, necessitating the increasing codification of such measures into repressive cybersecurity laws and regulations. This runs counter to the distributed nature of the Internet and the inherently cross-border and open environment promoted by this medium communication. It

[116] Mingli Shi, et al. "Translation: China's Personal Information Security Specification." *DigiChina*, New America, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/

[117] Sacks, Samm. "China's Emerging Data Privacy System and GDPR", Center for Strategic and International Studies (CSIS), 9 Mar. 2018, https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr

[118] Mingli Shi. "Translation: Principles and Criteria from China's Draft Privacy Impact Assessment Guide." *DigiChina,* New America, 13 Sep. 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-principles-and-criteria-from-chinas-draft-privacy-impact-assessment-guide/

[119] "Public Internet Cybersecurity Threat Monitoring and Mitigation Measures", *China Copyright and Media*, 9 Aug. 2017, https://chinacopyrightandmedia.wordpress.com/2017/08/09/public-internet-cybersecurity-threat-monitoring-and-mitigation-measures/

[120] Triolo, Paul, et al. "China's Cybersecurity Law".

[121] Yang, Yuan. "China's cyber security law rattles multinationals", *Financial Times*, 30 May 2017, https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996

[122] "Ninth Amendment to the Criminal Law of the People's Republic of China | Congressional-Executive Commission on China." *The Congressional-Executive Commission on China*, 1 Nov. 2015, https://www.cecc.gov/resources/legal-provisions/ninth-amendment-to-the-criminal-law-of-the-peoples-republic-of-china

also comes with increasing domestic and international reputational risks, both for the Chinese government and commercial businesses.

Furthermore, the success of economic objectives enshrined in China's cyberspace policy could be hampered by the rollout of a market discriminatory governance regime. Strict national data localisation requirements, all-encompassing intelligence laws and the exposure of foreign corporations to market discrimination measures reinforce suspicion of China's business environment. In the long run, the strict regulatory environment might decrease the market's appeal and end up being detrimental for Chinese high-tech suppliers' market expansion beyond the Mainland's borders.

3.2 Institutional landscape and key stakeholders

Please note that the sections below provide a non-exhaustive list of selected Chinese-based actors, senior officials, private organisations, think tanks, research institutes[123] and government agencies dealing with cyber diplomacy. Due to continuous institutional shifts, changes in governmental agencies' supervisory powers and an ever-expanding cyber domain academia and research field in China, this selective list is of limited scope and scale, and only reflects information provided in public reporting.

3.2.1 Governmental actors

Since 2014, the Chinese government has been engaged in the process of streamlining and consolidating the political-institutional environment in which China's cybersecurity policy operates. Aiming to streamline the ability of the CCP to steer policy from the top, Beijing has purposefully implemented "fixes" - "institutional shuffles, power shifts, reorganisation of priorities and the creation of new political organs - to tackle a sprawling bureaucracy, growing turf wars over responsibilities, deep fragmentation, issues with power-sharing and operational conflicts. Despite these efforts, the weaknesses in the Chinese cybersecurity institutional system - opaqueness and fragmentation - remain apparent.

To improve coordination, the State Council announced that the **Central Commission for Cybersecurity and Informatization** (中央网络安全和信息化委员会; led by President Xi) is now the centralised decisionmaking body on cyberspace and ICT affairs that charts out the official line for cybersecurity policymaking, strategy, planning and resources.[124] These prescriptions, in turn, trickle down to the local level through a system of policy documents designed to implement the top-level vision and planning. The centralisation of China's cyberspace governance apparatus is, above all, designed to cement and consolidate political power into the hands of the CCP and to concentrate the party-state's capacity to guide changes through top-down decisionmaking.

More importantly, the move underscored the prioritisation of cybersecurity in the administration's future policy direction. Elevating the previous Central Leading Group for Cyberspace Affairs to the status of a Central Commission took place within the broader context of President Xi's efforts to centralise and streamline overlapping and ineffective bureaucracy related to cyberspace policy. The shift, therefore, reflects an "urgent priority among the senior leadership to settle turf battles among actors such as the Ministry of Public Security (MPS；公安部), the Ministry of Industry and Information Technology (MIIT; 工业和信息化部), and the Publicity [Propaganda] Department of the Central Committee of the CCP [中共中央宣传部]".[125] As with other CCP organs, the CCCI's full member list is not yet public and readily available,

[123] For more information on defence-related research institutions dealing with cyberspace, and their suspected state affiliation, please consult Joske, Alex. *The China Defence Universities Tracker*. 25 Nov. 2019, https://www.aspi.org.au/report/china-defence-universities-tracker

[124] Note that the Central Committee for Cybersecurity and Informatization is sometimes referred to as Central Commission for Cyberspace Affairs.

[125] Creemers, Rogier, et al. "China's Cyberspace Authorities Set to Gain Clout in Reorganization." *Digi China*, New America, 26 Mar. 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/

vice chairs of the new Commission include Premier Li Keqiang and Politburo Standing Committee Member Wang Huning.[126] Moreover, in May 2019, **Sheng Ronhua** assumed the role of deputy head of both the Central Commission for Cybersecurity and Informatization and the Cyberspace Administration of China,[127] while former director of the Commission and head of CAC - the notorious Lu Wei - was sentenced to 14 years in prison for bribery.[128]

The **Cyberspace Administration of China** (国家互联网信息办公室) is a "one structure, two nameplates" entity[129] that implements, but also shapes, most tenets of China's cybersecurity policy. CAC also serves as the secretariat of the CCCI to which CAC is directly subordinate.[130] In other words, CAC - the leading Chinese institution responsible for cybersecurity and cyber diplomacy - is the functional office of the Central Commission. Despite having a pivotal role, CAC is far from being the only actor with cybersecurity responsibilities. Other actors - the MSS, the Ministry of Public Security (MPS), the Ministry of Industry and Information Technology (MIIT), the Ministry of Propaganda, intelligence agencies, intra- and inter-agency bodies and standardisation committees - share other technical and political ICT-sector responsibilities.

As of 2018, China has a new cyber czar, **Zhuang Rongwen**, a close ally of President Xi, who has assumed the role of the new head of CAC.[131] That the CAC continues to be headed by a senior propaganda official reflects the organisation's - and by extension the government's - primary focus on monitoring and policing the dissemination of online content and the strengthening of the Party's capacity to exercise (ideological) control over the Internet. Network security also remains a priority, albeit a secondary one. Related to this, in a 2018 essay in the leading Party theory journal, *Qiushi*, the new chief of CAC stressed the "Party's leadership over the governance of the Internet" and committed to increasing control over online information as a core instrument of Party indoctrination.[132] Xu Lin, who is Mr Zhuang's predecessor, will now head the State Council Information Office, which is the CCP's external "propaganda arm"[133] supervised by Premier Li Keqiang.

Wang Huning is the vice chair of the Central Commission for Cybersecurity and Informatization, a member of the Politburo Standing Committee and a close adviser to Xi Jinping. Wang spoke at the Wuzhen Internet Conference in 2017 on the importance of norm building, international cooperation and exchange, expertise sharing in the digital economy sphere, e-commerce and cross-border flows.[134]

---

[126] Triolo, Paul, et al. "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies'."

[127] "盛荣华任中央网络安全和信息化委员会办公室副主任--组织人事 [Sheng Ronghua Becomes Deputy Director of the Office of the Central Cyberspace Affairs Committee [under CAC]]." *People's Daily*, 16 May 2019, http://renshi.people.com.cn/n1/2019/0516/c139617-31088831.html

[128] "中宣部原副部长鲁炜受贿案一审宣判 [Lu Wei, Former Vice Minister of the Publicity Department of the Communist Party of China, Sentenced in the First Instance]." *Disciplinary Inspection Committee of the Central Committee of the Communist Party of China*, 26 Mar. 2019, http://www.ccdi.gov.cn/yaowen/201903/t20190326_191195.html

[129] "中共中央印发《深化党和国家机构改革方案》[The Central Committee of the Communist Party of China Issued the 'Deepening Party and State Institution Reform Plan']." *The State Council of the People's Republic of China*, 21 Mar. 2018, http://www.gov.cn/zhengce/content/2018-03/24/content_5277121.htm

[130] Creemers, Rogier, et al. "China's Cyberspace Authorities Set to Gain Clout in Reorganization."

[131] Zhou, X. and Chi-yuk Choi. "Beijing names new Internet watchdog as China keeps door closed to global tech giants", *South China Morning Post*, 1 Aug. 2018, https://www.scmp.com/news/china/policies-politics/article/2157762/beijing-names-new-internet-watchdog-china-keeps-door

[132] Gan, Nectar. "Cyberspace controls set to strengthen under China's new Internet boss", *South China Morning Post*, 20 Sep. 2018, https://www.scmp.com/news/china/politics/article/2164923/cyberspace-controls-set-strengthen-under-chinas-new-internet

[133] Gan, Nectar. "China names former Internet tsar Xu Lin as new international propaganda chief", *South China Morning Post*, 21 Aug. 2018, https://www.scmp.com/news/china/policies-politics/article/2160623/china-names-former-internet-tsar-xu-lin-new

[134] Webster, Graham, et al. "Wang Huning's Speech At the 4th World Internet Conference in Wuzhen." *DigiChina*, New America, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/wang-hunings-speech-4th-world-internet-conference-wuzhen/

China's institutional cybersecurity environment remains layered, complex and fragmented. Recent shuffles have aimed to facilitate shared common goals and mitigate turf wars between ministries, which often have their own agendas and interests.

The **Ministry of State Security** (安全部) The MSS has a "double" mandate of foreign intelligence (counterintelligence, counterespionage) and domestic (politically motivated) intelligence.[135] MSS' primary focus lies in ensuring domestic stability. The Ministry collects intelligence on internal and external targets and threats, as part of counterterrorism and anti-radicalisation initiatives. It also has an integral role in the security reviews mechanism. Crucially, with the creation of the Strategic Support Forces (SSF; 战略支援部队), an effort to reorganise the use of offensive cyber capabilities within China between the military and civilian intelligence agencies, highly operationally sophisticated groups affiliated with the Ministry of State Security are now responsible for industrial cyber exploitation operations. Recent indictments and exposed espionage campaigns have all been associated with intelligence operatives working for the MSS, which is itself a non-monolithic actor. It should be noted that the MSS operates at the national, provincial and local levels, where "many of [its entities], especially at the provincial and local levels, include organisations with valid public missions to act as a cover for MSS intelligence operations".[136]

The **Ministry of Public Security** (公安部) has a security and law enforcement mandate directed at ensuring public social order both offline and online. The MPS is partially responsible for implementing Internet traffic control in China, in concert with the MIIT, which regulates access, and the MSS, which monitors content. The MPS focuses on combating cybercrime and cyber terrorism, curbing the use of VPN services to circumvent the Great Firewall and is responsible for critical infrastructure protection together with the CAC.

The **Ministry of Industry and Information Technology** (MIIT; 工业和信息化部) has a mandate to "regulate ICT sector industrial policy" manifested in initiatives, such as Made in China 2025, Internet+ and others.[137] The MIIT manages China's telecommunications, ICT and network infrastructure. Although one of the most important ministries in relation to the cyber domain, its role in China's cybersecurity policy has weakened since 2018 as the CAC's role has taken off.[138]

The **National Information Security Standardization Technical Committee (Technical Committee 260**, or **TC260)** is the leading ICT evaluation and testing standardisation body. Its role on policy is high and stems from its integral role in enforcing Cybersecurity Law across lower levels - to organisations, private companies and governmental organs - by use of implementing guidelines, technical measures, compliance frameworks and standardisation plans. China's cybersecurity standardisation framework is comprised of several other less authoritative, or more specialised, standardisation committees, such as the Communication Standardization Association (CCSA) and the Cryptography Industry Standardisation Technical Committee (CISTC).

The **Ministry of Foreign Affairs** (国外交部) - particularly the Arms Control and Disarmament (军控司) and the Department of Treaty and Law (条约法律司) - covers cyber diplomacy and international "rulemaking" for cyberspace. The MFA, co-author of China's 2017 strategy on international cooperation in cyberspace, is the executive of China's cyber diplomacy official party policy line. MFA representatives from the Department of Arms Control and Disarmament have led and coordinated China's efforts at two parallel UN First Committee processes, and have represented Beijing's views at all previous iterations of the Group of Government Experts between 2004 and 2019. Additionally, MFA coordinates the PRC's Track 1 cyber dialogues with senior officials from the European Union (e.g. the EU-China Cyber

[135] Insikt Group. "Recorded Future Research Concludes."
[136] Insikt Group. "Recorded Future Research Concludes."
[137] Triolo, Sacks, Webster and Creemers. "China's Cybersecurity Law."
[138] Creemers, Triolo, Sacks, Lu and Webster. "China's Cyberspace Authorities."

Taskforce). It co-organises and oversees Track 1.5 discussions (e.g. the Sino-European Cyber Dialogue) and often plays the role of 'facilitator' in bilateral dialogues about cyberspace.

The **People's Liberation Army of China** (中国人民解放军) was formerly responsible for industrial cyber-enabled espionage (notably, the Third Department of the PLA General Staff Department). Nowadays, the newly created PLA Strategic Support Force oversees China's development of its offensive intrusion capabilities, cyberdefence, military intelligence and cyber exploitation reconnaissance. As a result of the (PLA)SSF reforms initiated in 2015, which united space, cyber and information warfare capabilities, the PLA now has a narrowed focus on reconnaissance and conflict scenario cyber intrusions and critical infrastructure defence.

There are only semi-authoritative statements on the PLA's doctrinal thinking on the use of cyber capabilities in a warfighting scenario, specification of thresholds that could trigger countermeasures or the mechanics of its cyber deterrence policy. Semi-official statements have shown that the PLA conceived cyber capabilities as low-cost, high-impact effects that could serve a supportive and adjunct function to conventional military action. In response to a perceived cyber arms race and militarisation of cyberspace, the PLA's 2019 White Paper calls for accelerating the build-up of offensive and defensive cyber capabilities "consistent with China's international standing and its status as a major [cyber superpower]".[139] Additionally, the PLA vows to improve the "informatisation" of its armed forces and its "cyber border defence" and network intrusions situational awareness capacities in order to better maintain state security, "national sovereignty, information security and social stability".[140]

The **Cybersecurity Association of China (CSAC; 国网络空间安全协会)** was established in 2016 as a CCP-led industry association to transmit policy ideas downstream and to provide practical support across the government-industry nexus in China's ICT-related legal regime. CSAC provides support for the implementation of information control measures, the security of network products and services and the promotion of China's domestic ICT industry.[141]

The **National Computer Network Emergency Response Technical Team/Coordination Center of China** (CNCERT or CNCERT/CC): China's CERT is now subordinated to the CAC (previously by the MIIT). Much like CERTs in Europe, CNCERT is responsible for (emergency) incident response, coordination, prevention and detection, the protection of critical information infrastructure and security testing of public institutions' and governmental bodies' networks. Like ENISA, CNCERT deals with improving China's overall cybersecurity posture.[142] In addition, the National Computer Network and Information Security Management Center (NCNISMC), which is closely associated with CNCERT, allegedly holds technical responsibilities for the deployment and maintenance of China's censorship system (the Great Firewall of China).[143] Given its subordinate position to the CAC, this means that the regime's censorship apparatus will now be administered directly by the Cyberspace Administration of China and the Central Commission for Cybersecurity and Informatization, comprised of several members of the Standing Committee and President Xi himself.

3.2.2 Private sector

Qihoo 360 is China's leading private cybersecurity company. It operates China's first civil-military cybersecurity innovation centre, under the supervision of the Central Commission for Integrated Military

[139] "China's National Defense in the New Era." *Ministry of National Defence of the People's Republic of China*, 24 July 2019, http://eng.mod.gov.cn/publications/2019-07/24/content_4846452.htm
[140] "China's National Defense in the New Era."
[141] Robert O'Brien. "What to Make of the Newly Established CyberSecurity Association of China." *Center for Strategic and International Studies*, 25 May 2016, https://www.csis.org/analysis/what-make-newly-established-cybersecurity-association-china
[142] "The National Computer Network Emergency Response Technical Team/Coordination Center of China, About Us." *The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT-CNCERT/CC)*, 2019, https://www.cert.org.cn/publish/english/index.html
[143] Marczak, Bill, et al. "China's Great Cannon." *The Citizen Lab*, 10 Apr. 2015, https://citizenlab.ca/2015/04/chinas-great-cannon/

and Civilian Development "and related military bodies".[144] Together with other private Chinese cybersecurity companies, Qihoo plays a vital role in building up China's "cyberdefence systems for military-related Internet services" and serves an integral threat intelligence role enhancing the PLA's situational awareness regarding cyber threats.[145] Zhou Hongyi (CEO of Qihoo 360) has previously highlighted the importance of civil and military integration and cooperation in the field of cyberdefence.

BATJ - Baidu, Alibaba, Tencent, JD.com (or China's GAFA): These are China's national champions in the digital sphere. They compete with American companies in terms of value and influence and play a vital role in the management and control of public information spaces.

3.2.3 Research institutes and academia

The think tanks below have varying degrees of contact with China's foreign policy apparatus. Nonetheless, they provide policymakers with expert opinions and input regarding overall policy. Leading Chinese foreign policy organisations and agencies, such as the Ministry of Foreign Affairs, the Ministry of State Security, military organisations, local governments and the Party itself, all administer bespoke research institutes, which submit input across levels of policymaking.

The **China Institutes of Contemporary International Relations (CICIR)** is a think tank directly affiliated with the Ministry of State Security. It deals with foreign policy and international relations and frequently engages with foreign think tanks in Track 1.5 dialogues. CICIR holds consistent channels of policy recommendation with higher levels of policymaking.

The **Shanghai Institute for International Studies (SIIS)** is a think tank that researches foreign policy and has ties to China's Ministry of Foreign Affairs and the Shanghai Municipality.

The **China Institute of International Studies (CIIS)** is affiliated with the Ministry of Foreign Affairs.

The **Chinese Academy of Social Sciences (CASS)**, subordinate to China's State Council, is the largest government think tank in the country.

The **China Academy of Information and Communications Technology (CAICT)** is the Ministry of Industry and Information Technology's think tank. The CAICT provides research input to the Chinese ICT industry on major top-down regulations and plays a role in the assessment of enterprises' compliance with governmental testing and certification frameworks. The CAICT supports "strategy and policymaking" programmes (Made in China 2025, Internet Plus, Broadband China) by producing white papers and carrying out "in-depth [studies] and foresighted planning" on the impact of emerging technologies on China's digital economy.[146] Significantly, the CAICT is integral for the implementation of major cyber-related policy initiatives and regulations by virtue of it being a member of TC260 working groups on cybersecurity standardisation. It is also a leading "third-party technical organisation" tasked with implementing the Cybersecurity Review Regime of the Cybersecurity Law.[147] The Academy is also a key member of the IMT-2020 5G Promotion Group, which was a key partner in the 2015 Joint Declaration between the EU and China on developing 5G network technology.[148]

---

[144] "China Unveils Its First Civil-Military Cybersecurity Innovation Center." *People's Daily*, 28 Dec. 2017, http://en.people.cn/n3/2017/1228/c90000-9309428.html

[145] "China Unveils Its First Civil-Military."

[146] "Profile of the China Academy of Information and Communications Technology (CAICT), Profile." *The China Academy of Information and Communications Technology (CAICT)*, 2019, http://www.caict.ac.cn/english/intro/201804/t20180428_161365.htm

[147] Paul Triolo, and Graham Webster. "Profile: China Academy for Information and Communications Technology (CAICT)." *DigiChina*, New America, 16 Oct. 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/profile-china-academy-information-and-communications-technology-caict/

[148] "The EU and China Signed a Key Partnership on 5G, Our Tomorrow's Communication Networks." *European Commission*, 28 Sept. 2015, https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5715

The **Chinese Academy of Military Sciences of the People's Liberation Army (CAMS)**, the **China Institute for International Strategic Studies (CIISS)** and the **National Defence University (NDU)** are think tanks that deal with strategic and security issues under the PLA. The NDU often publishes on AI and cyberdefence.

4 China's approach to cyber diplomacy: objectives and practice

4.1 Participation and positions adopted in international cyber debates

Beijing's insistence on state-centric models of governance and intergovernmental cyber domain negotiations seeks to boost the top-down power of the (sovereign) state, along with its state security interests and political imperatives, relative to other (non-governmental) actors.[149] Although Beijing recognises the importance of private companies and technical communities in contributing to the growth and maintenance of the Internet, it still believes that governments should have a leading voice and retain their top-down steering capacity.[150]

Furthermore, other concepts raised by Beijing in international discussions revolve around promoting disruptive reforms to the Internet governance status quo, which is discursively perceived as a vehicle for advancing Western states' institutional monopoly, hegemony and neoliberal political ideology. The CCP discourse generally construes the international governance and legal regimes as remnants of a time when China did not hold the institutional and technological position enabling it to decide on global rules due to its stage of development. Key reforms, therefore, could boost China's and developing countries' international voice, which would subsequently allow them to exert their sovereignty, cultures, political contexts and interests in deciding how cyberspace is administered.

4.1.1 Internet governance

The Chinese government is committed to shaping international debates on norms of responsible state behaviour in cyberspace. The World Internet Conference, launched in 2014,[151] was designed to counter efforts by the US and like-minded allies to proliferate their definitions and expectations of (ir)responsible behaviour in cyberspace, propagate multi-stakeholder Internet governance initiatives and saturate discourse with discussions on digital human rights. The Wuzhen Summit, a showcase of China's Internet vision and high-tech sector power, serve to promote an alternative model for "cyberspace order and governance", while at the same time highlighting the fact that playing by Beijing's cyber governance rules is the only road to admission to its vast market.

The cyberspace wing of Chinese public diplomacy has long been engaged in a campaign of "reforming by de-Americanising" the existing cyber-related international governance system and norms building processes. In conjunction with an institutionalising process of China's cyber diplomacy, meaning the establishment of new dedicated agencies and positions and the implementation of domestic organisational reforms, the PRC has gradually broadened its participation in various issue-based, multi-stakeholder forums such as the IANA, the ICANN, the IETF and the IGF. Increasingly cognisant of the rising stakes in Internet governance, Chinese diplomats have concentrated their efforts on disrupting

[149] "Xi sets path for cyberspace to take." *China Daily*, 23 Apr. 2018, http://www.chinadaily.com.cn/a/201804/23/WS5adce162a3105cdcf6519be5.html
[150] "International Strategy of Cooperation on Cyberspace".
[151] "About WIC", *World Internet Conference*, Cyberspace Administration of China, 10 Nov. 2015, http://www.wuzhenwic.org/201511/10/c_46113.htm

Washington's monopoly over critical Internet infrastructure by "politicising" technical matters. The US relinquishing regulatory control over the IANA under pressure from Beijing is a case in point.[152]

Since 2012, Beijing has been pushing to bring Internet governance under the framework of the UN. At the 2012 World Conference on International Telecommunications ITU in Dubai, China, Russia, Saudi Arabia and several other signatories sought to elevate the role of the ITU over bottom-up institutions (like the IETF) by expanding the ITU and member states' authority over Internet traffic/resources and policymaking.[153] The proposal for an update to the legally binding International Telecommunications Regulations (ITR) treaty could have legitimised governmental censorship and surveillance practices and would have undermined the ICANN's multi-stakeholder role in the allocation and management of the DNS system had it not been withdrawn.[154] Still, 89 out of 193 states signed the controversial update aimed at extending governmental control over the Internet. Countries including the US, Canada and France fundamentally disagreed with proposed amendments that would have empowered the ITU to cover "a range of [...] governance functions" that were previously reserved for non-governmental stakeholders.[155] In November 2018, at the ITU's 20th Plenipotentiary Conference (PP-18) in Dubai, member states of the ITU re-elected Houlin Zhao, a Chinese national, as the Secretary General of the Union for his second four-year term, set to end on 1 January 2023.

Beyond the creation of the open-ended working group process under the First Committee of the UN General Assembly, China's most ambitious attempts at normsmaking comprised of two proposals to the General Assembly - tabled in 2011 and 2015 together with Russia and Shanghai Cooperation Organisation (SCO) members[156] - of a draft International Code of Conduct for Information Security. Following the guidelines of the Yekaterinburg Agreement of 2009, the SCO Code of Conduct framed potential cyber threats "in the context of international security" as issues of "information security", i.e. the use of information communication technologies to destabilise, interfere, attack or sabotage other nations' social-political and economic security and public order. The proposal was modelled on the principle of the sovereignty of states over cyberspace, requiring states to protect their "information spaces" and "critical information infrastructure" by imposing strict national legislation and regulation. The Codes further reinforced suspicion towards the Sino-Russian definition of information security and triggered criticisms that if such a regulation were adopted, it would provide authoritarian regimes with the legal foundation to arbitrary curtail and restrict the free flow of information and freedom of speech. Moreover, sceptical of the role of non-state and private actors in existing multi-stakeholder processes, the 2015 Code of Conduct also sought to establish "multilateral, transparent and democratic international Internet governance mechanisms" that empower governments to determine Internet-related public policy. Comparably, in 2016, BRICS members argued for reinforcing the decisionmaking power of governments as the primary creators and operators of cyberspace-related policy, diminishing the role of other non-state stakeholders to that of providers of input on decisions.[157]

[152] The Economist. "Why is America giving up control of ICANN?" *The Economist*, 30 Sep. 2016, https://www.economist.com/the-economist-explains/2016/09/29/why-is-america-giving-up-control-of-icann

[153] Blue, Violet. "WCIT-12 Leak Shows Russia, China, Others Seek to Define 'Government-Controlled Internet.'" *ZDNet*, 8 Dec. 2012, https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-Internet/

[154] In addition, China has been active in meetings and groups under international organisations tasked with shaping the future of technical standards pertaining to ICT, especially in the technological areas of Internet of Things and 5G.

[155] Kehl, Danielle, and Tim Maurer. "Did the U.N. Internet Governance Summit Actually Accomplish Anything?" *Slate Magazine*, 14 Dec. 2012, https://slate.com/technology/2012/12/wcit-2012-has-ended-did-the-u-n-internet-governance-summit-accomplish-anything.html

[156] United Nations General Assembly, U.N. Doc. A/69/723.

[157] "8th BRICS Summit - Goa Declaration", *BRICS 2017*, 16 Oct. 2016, https://www.brics2017.org/English/Documents/Summit/201701/t20170125_1410.html

4.1.2 Cybernorm building debates

As one of the first movers in the field, diplomats from the People's Republic participated in all five editions of the UN Group of Government Experts (UNGGE) from 2004 to 2017. Beijing is also a major player in the two new parallel processes at the UN tasked with studying ICTs in the context of international peace and security.

It was only in 2013, at the third meeting of the UNGGE, that governmental experts reached a consensus that international law - and the UN Charter in particular - is applicable to "information security" and states' conduct in cyberspace.[158] What's more, the 2013 report explicitly recognised that the principle of sovereignty and that "the international norms and principles that flow from it apply to [s]tates' conduct of ICT-related activities", including that states have a sovereign right to exercise control and enjoy jurisdiction over cyber infrastructure "within their territory".[159] The participating states also reached an agreement to continue working towards developing "common understandings" on norm maintenance - "how [the agreed] norms shall apply" - "and to carry out further norm formation over time given the "unique attributes" of information and communications technology. In China, the 2013 report was considered consistent with the official party-state line, as it acknowledged a favourable reading of the principle of state sovereignty and underscored the fact that the novelty of the cyber domain might require the identification of new norms regulating states' behaviour in the future.

As a signatory to the most recent consensus report reached within the framework of the UNGGE, China endorsed 11 non-binding norms and principles of responsible state behaviour in cyberspace, later reaffirmed by the G20.[160] Parties agreed to, among other things:

- exercise due diligence by not "knowingly" allowing their territories to be used for/in internationally wrongful cyber acts. They would do so by taking resilience measures to protect critical infrastructure from cyber intrusions and by responding to others' requests to "mitigate" malicious cyber acts emanating from their territory, "taking into account [...] sovereignty";
- refrain from carrying out or supporting cyber operations that could damage, disrupt or destroy critical infrastructure;
- refrain from targeting computer emergency response teams' networks;
- cooperate with others in developing confidence building stability measures to prevent conflict, increase predictability and promote peace and security in cyberspace;
- exchange information on vulnerabilities and abide by a duty to assist injured states whose critical infrastructure is being attacked;
- maintain the integrity and security of ICT supply chains and prevent the proliferation of malware tools and techniques;
- to protect human rights and fundamental freedoms online.[161]

The 2013 report was crucial in clarifying how the existing international legal regime applies to the use of cyber capabilities. In addition to noting selected international humanitarian law principles' applicability to cyber scenarios, the report reaffirmed that the UN Charter applies in its entirety, including the right of states to exercise their inherent right to take measures consistent with the Charter and their responsibilities to respect and protect human rights and fundamental freedoms. States should not use - or allow their territory to be used by - proxies formally outside of governments to commit

[158] United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." U.N. Doc. A/68/98, 24 June 2013, http://undocs.org/A/68/98

[159] United Nations General Assembly, U.N. Doc. A/68/98.

[160] "G20 Leaders' Communiqué Antalya Summit."

[161] United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", U.N. Doc. A/70/174, 22 July 2015, http://undocs.org/A/70/174

malicious cyber acts and should bear responsibility for operations legally attributed to them under the general standards of the law on state responsibility.

Yet, parties across the East/West divide fundamentally disagree over their views on the type of law appropriate for governing state behaviour in cyberspace (peacetime law vs. law of armed conflict; new vs. existing) and the mechanics of concrete principles and legal rules for specific cyber domain scenarios. The existence of two camps with fundamentally divergent views on international law ultimately led to the collapse of the UNGGE mechanism in 2017.

However, in December 2018, the General Assembly established two new processes to discuss the actions of states in cyberspace in the context of international security at the First Committee.[162] The Russia-sponsored resolution, supported by China, establishes an open-ended working group (OEWG) that expands participation to potentially every member state of the UN.

From 2019 to 2021, the OEWG is tasked with building upon past normmaking, including by revision, working towards the enforcement of existing norms of responsible behaviour in cyberspace and identifying new rules of behaviour in the sphere of information security. Founded on the language of past UNGGEs, the OEWG draft resolution promotes an additional set of "duties and rights" which elevate the role of governments in cyberspace governance through the language of "information/ICT security".

Within the UN context, China also voted against a parallel US-led draft resolution - subsequently adopted by the First Committee - for a resolution on "advancing responsible State behaviour in cyberspace in the context of international security". In addition to the open-ended working group, the US-sponsored resolution establishes a new Group of Governmental Experts limited to 25 members, one of which is the People's Republic of China. The UNGGE's mandate includes further clarifying how international law applies to cyberspace, whereby individual states are requested to submit their legal reasoning regarding cyber acts and identifying ways to improve compliance with existing norms. China's decision not to support a new round of the UNGGE at the 73rd session of the General Assembly might have been facilitated by its growing distrust towards Washington, the impasse of previous UNGGEs, reluctance to crystallise legal reasoning on cyberspace and a desire to maintain strategic ambiguity or involve more like-minded states in normsbuilding initiatives.

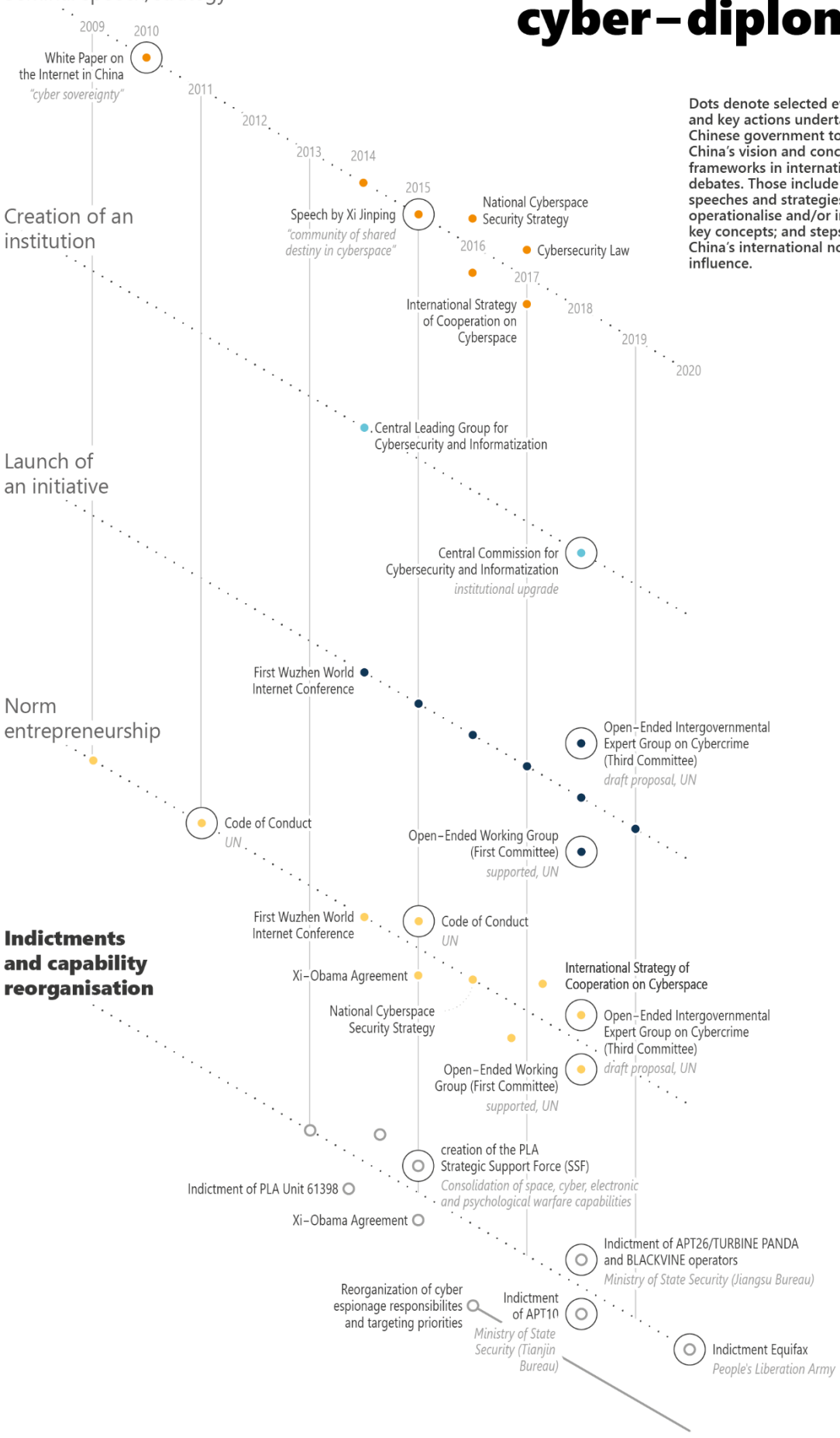
In the context of China's campaign to boost the role of the UN in international cyber debates, the existence of two new processes could be perceived as advantageous to China's cyber diplomacy strategy. The Third Committee's adoption of a resolution to "propose new national and international legal or other responses to the use of information and communications technologies for criminal purposes" is also well-aligned with Beijing's objective of developing new international legal instruments on cybercrime to compete with the Budapest Convention.[163]

[162] United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security." revised draft resolution, U.N. Doc. A/C.1/73/L.27/Rev.1, 29 Oct. 2018, https://undocs.org/A/C.1/73/L.27/Rev.1.; United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security." Resolution adopted by the General Assembly on 5 December 2018, U.N. Doc. A/RES/73/27, 11 Dec. 2018, https://undocs.org/A/RES/73/27; for the voting sheets, please see United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security." Report of the First Committee, U.N. Doc. A/73/505, 19 Nov. 2018, https://undocs.org/A/73/505.

[163] United Nations General Assembly, "Countering the use of information and communications technologies for criminal purposes." draft resolution, U.N. Doc. A/C.3/74/L.11, 11 Oct. 2019, https://undocs.org/A/C.3/74/L.11;

Cyber diplomacy

Brief history of Chinese cyber-diplomacy



Dots denote selected events by year and key actions undertaken by the Chinese government to promote China's vision and conceptual frameworks in international cyber debates. Those include major speeches and strategies; measures to operationalise and/or institutionalise key concepts; and steps to bolster China's international normative influence.

Data: United Nations, 2020; Shanghai Cooperation Organization, 2010; International Telecommunication Union, 2015; Ministry of Foreign Affairs of the People's Republic of China , 2016; World Internet Conference, 2019; The White House, 2015; Cyberspace Administration of China, 2017; European External Action Service, 2012; Council of the EU, 2015; Mandiant, 2013; US Department of Justice, 2020; Cyberspace Administration of China, 2019; Ministry of National Defense of China, 2016.

4.1.3 International law

The vision of a comprehensive cyber superpower extends far beyond the mere technological capability to great power competition within the **normative, discursive and ideational realm**. Xi asserted in 2016 that a core element of China's international ambition is enhancing the country's global discursive voice, its influence and its "right to speak" (话语权) in international standard-setting and rule- and norm-formation debates to help generate an international cyberspace order conducive to China's foreign policy and national interests.[164] Beijing values its involvement in the shaping of standards and expectations of (un)acceptable behaviour in the cyber domain as an instrumental strategic advantage.

Xi recognised that, even in cyberspace, the strategic competition between powerful states entails a "game" comprised of both material and ideational factors, where the relative distribution of power is determined by the ability of states to maintain a technological lead and instil homegrown standards, ideas and "discourse power".[165] In the context of the growing competition over ideas in international debates, the CCP Central Committee has called upon China to exert more "productive" power in the sphere of international law to advance China's interests going forward.[166] Following this logic, Chinese diplomats, lawyers and scholars are urged to participate in the formulation of "international [legal] norms" and rules through "'legal methods' with Chinese characteristics" to bolster Beijing's "discursive power and influence in international legal affairs".[167]

Technical communities, governmental agencies and nominally private organisations are incentivised to increase their participation in the global emerging technologies standardisation landscape. Standard-setting promotion in international bodies such as the ITO, IEC and ISO[168] sits at the core of the Made in China 2025, the Digital Silk Road and China Standards 2035[169] industrial policies. This serves a multifaceted objective: On the one hand, standardsmaking is intended to realise the nation-wide effort of achieving self-reliance and a leadership role on the international high-tech stage. Closely related to this, the internationalising of Chinese standards is also essential for sustaining national ICT champions' efforts to move up strategic value chains - from "third-tier" manufacturers to "first-tier" standard-setters - in international trade of advanced technologies.[170] Beyond advancing China's normative power, the shaping of global tech standards is further considered advantageous because it opens opportunities for

[164] Office of the Central Cyberspace Affairs Committee. 习近平：加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力 [Xi Jinping: Accelerating Indigenous Innovation Information Technology and Making Efforts to Build a Network Power]. Cyberspace Administration of China, 9 Oct. 2016, https://web.archive.org/web/20190115054041/http://www.cac.gov.cn/2016-10/09/c_1119682237.htm

[165] "打造中国网络空间国际话语权 [Building China's International Cyberspace Discourse Power [Right to Speak]"." *Information Office of the State Council of the People's Republic of China*, 14 Nov. 2016, http://webcache.googleusercontent.com/search?q=cache%3Awww.scio.gov.cn%2Fzhzc%2F10%2FDocument%2F1519386%2F1519386.htm&rlz=1C1GCEB_enBE813BE813&oq=cache%3Awww.scio.gov.cn%2Fzhzc%2F10%2FDocument%2F1519386%2F1519386.htm&aqs=chrome..69i57j69i58.919j0j4&sourceid=chrome&ie=UTF-8.

[166] "CCP Central Committee Decision Concerning Some Major Questions in Comprehensively Moving Governing the Country According to the Law Forward." *China Copyright and Media*, 28 Oct. 2014, https://chinacopyrightandmedia.wordpress.com/2014/10/28/ccp-central-committee-decision-concerning-some-major-questions-in-comprehensively-moving-governing-the-country-according-to-the-law-forward/

[167] "CCP Central Committee Decision Concerning Some Major Questions."

[168] Shi-Kupfer, Kristin, and Mareike Ohlberg. *China's Digital Rise*. MERICS Papers on China, Mercator Institute for China Studies (MERICS), pp. 1-58, https://www.merics.org/en/papers-on-china/chinas-digital-rise

[169] *国家标准委：正制定《中国标准2035》[National Standards Committee: Developing "China Standard 2035"]*. 10 Jan. 2018, http://www.xinhuanet.com/fortune/2018-01/10/c_129787658.htm

[170] "重视标准是'中国制造'走向世界的必经之路_要闻_新闻 [Attaching Importance to International Standards Is the Only Way for 'Made in China 2025' to Go Global]." *The State Council of the People's Republic of China*, 12 Feb. 2015, http://www.gov.cn/xinwen/2015-02/12/content_2818351.htm

concurrent expansion of Chinese firms' commercial power and the internationalisation of Chinese-made technology to new export markets.[171]

Beijing's **approach to the application of international law** in cyberspace remains highly selective and purposefully limited. It is characterised by a strong preference for specific primary legal principles enshrined in the Charter at the expense of "the rest of the international law" and the "[full] implications of accepting the UN Charter's application to cyberspace".[172] Efforts to explain how laws on the use of force, self-defence, state responsibility and international humanitarian law apply to cyber acts and capabilities became a sticking point at the latest round of the UNGGE. Fierce criticism from China, Russia, Cuba and others ultimately resulted in a short-lived collapse of the mechanism. Fundamental differences of opinion between the two camps zeroed in on the question of "whether cyberspace should remain an exclusively non-military domain" governed by peacetime legal frameworks or whether cyberspace should be subjected to the laws of armed conflict.[173]

The Chinese position was characterised by a reluctance to crystallise the precise ways in which existing customary and international treaty law might govern the cyber domain. The Sino-Russian camp repeatedly disagreed over the adequacy of applying existing law regulating the resort to force and the law of armed conflict in cyber scenarios. Beijing fundamentally opposed the idea that the current framework of international legal rules can appropriately outlaw malicious cyber operations and allow states to mount proportionate (cyber-enabled) responses to protect themselves from harmful activities.

Current laws are perceived as unsuitable for regulating the complexity and novelty of cyber acts, requiring the international community to work towards negotiating a new multilateral treaty dedicated to cyberspace and its "unique attributes" rather than continue relying on a soft law/norms approach. According to Beijing, the departing point of international cyber discussions should begin with surmising ways to use information and communications technology infrastructure in peaceful scenarios rather than during conflict, hence the preference for examining matters of international peace in and security of cyberspace through the lens of peacetime law.

The official Chinese line regards the application of the law of self-defence, the general rules of state responsibility and international humanitarian law principles - specifically those of proportionality, necessity, distinction, neutrality and collateral damage - as tantamount to legitimising conflict in the cyber domain and the offensive use of cyber capabilities instead of prohibiting them altogether.

China's zero-sum argument regarding the applicability of international law to cyber conduct is relatively straightforward: It pleads for the demilitarisation of legal approaches to the cyber domain as one of the staunchest critics of Washington's efforts to make "the shift from peace to armed conflict [...] too low".[174] At the 2017 round of the UNGGE, Washington was accused of promoting "war and the use of force" instead of peace and stability, and of perceptibly trying to "establish equivalence between the malicious use of ICTs and the concept of 'armed attack'" to give itself a legal license to resort to force pursuant of "the right of (collective) self-defence".[175] China adheres to the view that the application of the doctrine of self-defence - enshrined in the UN Charter and customary law - together with the law of armed conflict could provide technologically advanced countries' a legal license to wage cyber warfare and

[171] "Huawei Leverages Massive Patent Portfolio." *The Japan News*, 16 June 2019, https://web.archive.org/web/20190619010231/http://the-japan-news.com/news/article/0005812867

[172] Segal, "Chinese Cyber Diplomacy."

[173] Osula, Anna-Maria, and Henry Roigas. *International Cyber Norms: Legal, Policy & Industry Perspectives* (eds)., Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 119.

[174] Väljataga, Ann. "Back to Square One? The Fifth UN GGE Fails To Submit A Conclusive Report At The UN General Assembly", NATO Cooperative Cyber Defence Centre of Excellence, 1 Sep. 2017, https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/

[175] "71 UNGA: Cuba At The Final Session Of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context Of International Security", *Diplomatic Representations of Cuba Abroad*, 23 June 2017, http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information

impose arbitrary countermeasures on others, including (forcible) cyber countermeasures and reprisals pursuant the law of state responsibility. According to this logic, the explicit recognition of Art. 51 would incentivise "the use of cybermeans during a conflict" or non-cyber kinetic means " as a way to respond to the cyberconflict".[176]

This is rooted in a growing awareness of the damage that could be inflicted by cybermeans, particularly other states using offensive cyber capabilities to "incite social unrest", "interfere in internal political affairs", "subvert [the] regime" or harm "national political security and users' information security".[177] Accordingly, the CAC has also argued that demilitarisation is necessary within the context of an "aggravating arms race in cyberspace" and strategic competition for control over cyberspace.[178]

The explicit referencing of the rules of **international humanitarian law** to constrain cyberconflicts - specifically the principles of necessity, proportionality, neutrality and distinction - is similarly understood as giving a legal justification to military action by the use of ICTs and as an incentive for war. According to the Chinese position in international cyber debates, the focus on the law of armed conflict destabilises stability in cyberspace by presupposing and incentivising conflict and making unintended escalation more likely.

Beijing calls upon countries to observe the principles enunciated in Article 2 of the UN Charter, namely the sovereign equality of all states, the obligation to refrain from the threat or use of force against the territorial integrity or political independence of any state, the principles of non-intervention in matters within the domestic jurisdiction of any state and the peaceful settlement of disputes, and to reject "the Cold War" and "double standards" mentality.[179]

Advocating for the adoption of legal frameworks targeted at below-the-threshold activities in peacetime, particularly "information warfare campaigns", China's international cyberspace strategy mobilises a set of "hard" security solutions to deal with the perceived militarisation of cyberspace. Those solutions include developing cyberdefence, enhancing situational awareness on cyber threats and a modernisation of the armed forces through technological investments, institutional streamlining and the creation of a new dedicated "cyber force" within the PLA.[180]

Beyond bargaining chips in international negotiations, these debates framed as issues of international law reflect deeper security concerns. China might be wary of its cyber capabilities being unnecessarily curbed or of allowing others, namely the United States, to conduct destructive/disruptive cyber operations during an international armed conflict.

Beijing's distrust of the international legal regime, international law's inherent interpretive flexibility and the uncertainty of state practice are at the heart of the debate. Beijing might consider the space for elastic interpretation of the law of self-defence as excessively broad, despite the existence of a coherent body of related customs and case-law stipulating its utilisation. Supposed defensive operations against imminent attacks could be launched pursuant to anticipatory-, pre-emptive- or preventive-based justifications or idiosyncratic readings of the plea of necessity. Such woes are further reinforced by the absence of a proper definition of self-defence in cyberspace as well as states' evolving views regarding cyberspace and international law nexus. Similarly, the United States' denial of a gap between the use of force and an armed attack - the so-called equivalence doctrine - still makes it unclear what types of cyberattacks and threshold levels warrant resorting to the use of force as a response. The debate on sovereignty as a principle or a standard is also illustrative in this regard.

Further uncertainty could be introduced by the complexities of cyber operations' immediacy, the distributed geographies of cyber infrastructure and the blurred lines between military and civilian

[176] Grigsby, Alex. "The End of Cyber Norms." *Survival* 59(6): 109-122.
[177] Grigsby, Alex. "The End of Cyber Norms."
[178] "National Cyberspace Security Strategy."
[179] "International Strategy of Cooperation on Cyberspace".
[180] "International Strategy of Cooperation on Cyberspace".

targets, in addition to ambiguities related to ascertaining the sufficient level of severity, scale and scope warranting states to mount responses. Similar is the case with (cyber) countermeasures and the legality of *collective* responses with *(forcible)* effects contributed by non-injured states, which remain "ripe for interpretation by States".[181] While governments have largely restrained their operations below certain thresholds of severity, there are no stable modes of expected (un)acceptable behaviour yet.

Another fundamental difference between the two camps relates to the principle of sovereignty. Here, Beijing's position is clear - sovereignty is a primary rule of international law and each country has the sovereign right to manage and administer its domestic cyberspace according to domestic law and political culture without foreign interference. This is underpinned by the principles of non-interference and, in practice, by the enforcement of stringent cyberspace policy regulations that cumulatively restrict the free flow of information and stifle fundamental freedoms. China's view stands at odds with views of cyberspace as a global commons.

4.1.4 Confidence Building Measures

China's International Strategy on Cyberspace Cooperation contends that the PRC is committed to maintaining peace and stability in cyberspace through international cooperation on norms formation and the creation of confidence building measures. The foci areas of Chinese confidence building engagement include the establishment of predictability-increasing practical measures to prevent unintended conflicts, or arms races, and the proliferation of offensive cyber capabilities. According to the international strategy, new CBMs will also encompass measures to curb misuses of information communication technologies and ensure supply chain security in network equipment and industrial control systems. Furthermore, establishing an atmosphere of mutual trust and predictability would also require increasing transparency regarding states' deterrence and doctrinal strategies and clarification of legal principles' capacity to govern specific cyber acts.

4.1.5 Capacity building

Another key pillar of China's cyber diplomacy is capacity building in developing nations. Capacity building in digital technologies - network infrastructure, information systems, 5G, fibre optic and undersea cables and content filtering tools - serve the greater strategic purpose of convincing developing states to adopt the country's cyber domain ideas and concepts.[182] The Belt and Road Digital Economy International Cooperation Initiative, launched in 2017,[183] and "the Digital Silk Road" seek to internationalise Chinese technology made by state-owned or affiliated companies, including Huawei and ZTE, and in this way, embed Chinese technical standards and set up potentially favourable conditions for political cyber-enabled espionage.[184] In addition to infrastructure investment, capacity building also focuses on enhancing information-sharing capacities, cyberdefence personnel training and crisis management. In the long-run, Beijing hopes to leverage ICT infrastructure investment in developing nations for political purposes and to make sure that China is well-positioned to take advantage of the gradual realignment of power in the international order.

---

[181] Schmitt, Michael. "Estonia Speaks Out on Key Rules for Cyberspace." *Just Security*, 10 June 2019, https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/

[182] "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road", *National Development and Reform Commission (NDRC) of the People's Republic of China*, 28 Mar. 2015, http://en.ndrc.gov.cn/newsrelease/201503/t20150330_669367.html

[183] "Initiative on Belt and Road digital economy cooperation launched." *Information Office of the State Council of the People's Republic of China*, 4 Dec. 2017, http://www.scio.gov.cn/31773/35507/35520/Document/1612635/1612635.htm

[184] Joe Parkinson, et al. "Huawei Technicians Helped African Governments Spy on Political Opponents." *Wall Street Journal*, 15 Aug. 2019. *www.wsj.com*, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

In terms of regional distribution, Chinese state-owned or affiliated companies' investments concentrate on Africa,[185] South America, Central and Southeast Asia[186] through concrete projects, such as the China-ASEAN Information Port and the China-Arabia Digital Silk Road Ningxia Hub. Tanzania, for instance, was selected by Beijing as a "pilot country for China-Africa capacity building" in developing content controlling systems and a strict Internet regulatory legislative framework.[187]

4.2 Relations with regional actors and organisations

Cyber diplomacy has come to the forefront of China's growing multilateral, bilateral and regional commitments. The 2016[188] and 2017[189] summits of the BRICS strategic grouping underscored the asymmetric distribution of power in the existing Internet governance system by calling for democratic and fair participation of states. More recently, the 10th BRICS Summit Declaration of July 2018 highlighted the importance of intergovernmental cooperation within the framework of the UN "to develop a universal regulatory binding instrument on combatting the criminal use of ICTs".[190]

At the G20 level, China endorsed the G20 Finance Ministers and Central Bank Governors Meeting Communiqué in 2017,[191] accentuating the importance of cybersecurity to protect the resiliency of financial and informational systems. Similarly, at the G20 Osaka Leaders' Declaration of 2019, Beijing, together with other countries, committed to working towards enhancing cyber resilience.[192]

According to Xi Jinping, Russia is China's key strategic partner "of coordination" and a key like-minded partner in pushing forward the Sino-Russian notion of "information security" and maintaining "global strategic stability" amid a "complex and volatile international situation" of increased interference in domestic affairs.[193] In international cyber debates, the two countries emphasise the importance of sovereignty and non-intervention and share a profound distrust of "the current Western rules-based liberal order" and the United States' advocacy for "Internet freedom", often acting in concert and coordinating "counteraction" to American-led norms initiatives.[194] Besides their joint submission of two codes of conduct in 2011 and 2015, Moscow and Beijing also signed a "nonaggression" cyber pact in 2015[195] in which the two governments pledged to refrain from offensive cyber operations against each other and to promote a "multilateral" vision of Internet governance. The 2016 Sino-Russian Declaration on the Promotion of International Law reaffirms China's support for the principles of the UN Charter

[185] "Chinese firm hopes to wire continent with same strategy that boosted Internet access across China." *Global Times*, 13 Mar. 2017, http://www.globaltimes.cn/content/1037500.shtml

[186] "Key connectivity improvements along the Belt and Road in telecommunications & aviation sectors." *Ernst & Young,* China Go Abroad 4, Sep. 2016, https://www.ey.com/cn/en/services/specialty-services/china-overseas-investment-network/ey-key-connectivity-improvements-along-the-belt-and-road

[187] "Forum on China-Africa Cooperation (Beijing)." *Ministry of Commerce of the People's Republic of China*, 11 May 2017, http://english.mofcom.gov.cn/article/newsrelease/counselorsoffice/westernasiaandafricareport/201705/20170502573605.shtml

[188] "8th BRICS Summit - Goa Declaration."

[189] "BRICS Leaders Xiamen Declaration", *BRICS 2017*, 4 Sep. 2017, https://www.brics2017.org/English/Documents/Summit/201709/t20170908_2021.html

[190] https://www.mea.gov.in/bilateral-documents.htm?dtl/30190/10th_BRICS_Summit_Johannesburg_Declaration

[191] "Communiqué G20 Finance Ministers and Central Bank Governors Meeting", G20 Information Centre, 18 Mar. 2017, http://www.g20.utoronto.ca/2017/170318-finance-en.pdf

[192] "10th BRICS Summit Johannesburg Declaration." *Ministry of External Affairs of India*, 26 July 2018, https://www.mea.gov.in/bilateral-documents.htm?dtl/30190/10th_BRICS_Summit_Johannesburg_Declaration

[193] "Xi Jinping Meets with Secretary of the National Security Council Nikolai Patrushev of the Russian Federation." *The Ministry of Foreign Affairs of the PRC*, 2 Dec. 2019, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1721345.shtml; "中俄举行第十五轮战略安全磋商 杨洁篪同帕特鲁舍夫共同主持 [China and Russia Hold the 15th Round of Strategic Security Consultations Yang Jiechi Co-Chairs with Patrushev]." *People's Daily*, 5 Dec. 2019, http://cpc.people.com.cn/n1/2019/1205/c64094-31490568.html

[194] Broeders, Dennis, et al. "A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace." *The Hague Cyber Norms*, Nov. 2019, https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace

[195] Korzak, Elaine. "The Next Level For Russia-China Cyberspace Cooperation?" *Net Politics*, Council on Foreign Relations, 20 Aug. 2015, https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation

and the 1970 Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States.[196]

While both Zhongnanhai and Moscow identify "threats, concerns, concepts and opportunities in cyberspace" as being predicated on the implications of online content and information, the two states diverge on their doctrinal thinking regarding the underlying motivating factors behind cyber intrusions, with Russia "actively pursu[ing] destabilising abroad" and China investing in long-term "strategic stability and predictability".[197] Similarly, official Chinese discourse emphasises the need to reform the Internet governance system and a disruption of the status quo.

The inclusion of cyber affairs and Internet governance in China's diplomatic activities has served to bolster Beijing's leadership role in regional organisations such as the ASEAN Regional Forum (ARF), the Boao Forum for Asia, the Forum on China-Africa Cooperation (FOCAC), the China-Arab States Cooperation Forum, the Forum of China and the Community of Latin American and Caribbean States, the China-Japan-Korea Cyber Policy Consultation, the Asian-African Legal Consultative Organization, APEC and the BRICS.[198]

Cybersecurity also takes a central role in Sino-American bilateral relations. In the aftermath of the public exposure of PLA-linked APT1 cyber espionage operations, China and the United States agreed in 2015 not to "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage".[199] Beijing endorsed this nascent norm against commercial cyber-enabled espionage in bilateral accords with Canada[200] and Australia in 2017.[201]

The Xi-Obama Agreement against commercially motivated cyber exploitation also included commitments to enforce norms of responsible behaviour in cyberspace, create confidence building measures to prevent unintended conflict or escalation (a crisis hotline) and establish two high-level working groups to tackle cybercrime and advance information systems' resilience. The bilateral accord was later complemented by the Third US-China High-Level Joint Dialogue on Cybercrime that took place in 2016[202] and the Xi-Trump Agreement of 2017, in which the two parties agreed to set up the US-China Law Enforcement and Cybersecurity Dialogue (LECD) mechanism.[203] Moreover, the two great powers engage in Track 1.5 and Track II dialogues. The Centre for Strategic and International Studies (CSIS) and the MSS-affiliated China Institutes of Contemporary International Relations (CICIR) Track 1.5 dialogue, established in 2009, contributed to the cyber-related cooperation between the two countries by enhancing transparency and predictability when the DoJ indicted five PLA hackers.[204] Harvard's Belfer Center Track II "US-China Cyber Security Working Group" with the PLA-linked China Institute for International Strategic Studies (CIISS) similarly aims at preventing inadvertent conflict and increasing

[196] "The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law", The Ministry of Foreign Affairs of the Russian Federation, 25 June 2016, http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2331698

[197] "The Declaration of the Russian Federation and the People's Republic of China."

[198] "International Strategy of Cooperation on Cyberspace."

[199] The White House. "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference.", 25 Sep. 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint

[200] Fife, Robert and Steven Chase. "Canada and China strike corporate hacking deal." *The Globe and Mail*, 26 June 2017, https://www.theglobeandmail.com/news/politics/china-agrees-to-stop-conducting-state-sponsored-cyberattacks-targeting-canadian-private-sector/article35459914/

[201] Jamie Smyth. "Australia and China in Pact Against Cyber Theft." *Financial Times*, 24 Apr. 2017, https://www.ft.com/content/9df81164-28b5-11e7-9ec8-168383da43b7

[202] The US Department of Justice. "Third US-China High-Level Joint Dialogue on Cybercrime and Related Issues." 8 Dec. 2016, https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues

[203] LECD's objectives focus on advancing the norm against commercial cyber espionage; the duty to assist in cases of state-linked cyber incidents, emphasis on law enforcement cooperation; to advance the international normsmaking progress; and to engage in high-level dialogue on fighting cybercrime.

[204] "Track 1.5 US-China Cyber Security Dialogue." *Center for Strategic and International Studies (CSIS)*, 2019, https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity/track-1

predictability in cyberspace by use of scenario exercises. In addition, this dialogue provides a platform for scholarly exchange on other cyber domain-related issues, such as intellectual property theft and supply chain security.[205]

Since the Xi-Obama deal, industrial cyber espionage originating from China has taken centre stage in the escalating Sino-American trade war. In March 2018, the Office of the United States Trade Representative issued a "Section 301" report, which asserted that despite the Xi-Obama Agreement, China has continued to conduct "cyber intrusions into US commercial networks in line with Chinese industrial policy goals" incentivising (forced) technology transfers.[206] The report, using the Section 301 mechanism of the US Trade Act of 1974, justified the imposition of a first round of tariffs on Chinese exports. This was due to the cumulative effect of Beijing's cyber espionage and market discriminatory acts, practices and policies, which resulted in the forced acquisition of US intellectual property to sustain Beijing's economic objectives in strategic industries. The US administration, therefore, placed technology and cyber espionage at the heart of the US-China tariff escalation. In November 2018, the USTR issued an update to the Section 301 Report. USTR vowed to continue seeking structural market-opening reforms against China at the WTO and bilaterally.

5 Priorities and strategy for Sino-European engagement in cyberspace

5.1 Overall EU priorities and cooperation with China

In absolute terms, the People's Republic of China is the European Union's largest trading partner. China is its most significant source of imports and second-largest export market. The EU is second only to the United States as China's top trade partner.[207]

In the framework of the EU-China 2020 Strategic Agenda for Cooperation signed in 2013 - the strategy that guides comprehensive bilateral cooperation - the EU and China agreed to establish strategic partnership across a wide range of issues, including sustainable development, economic prosperity, global governance, foreign policy, security and peace.[208] In 2017, China and Europol reached an agreement known as the "Europol-China Strategic Cooperation Framework" to increase law enforcement cooperation directed at combating transnational crime.

The 2016 Joint Communication on "Elements for a new EU strategy on China", adopted by the High Representative, the European Commission[209] and the EU Council's Strategy on China[210] further clarified EU priorities vis-à-vis China. In line with the EU's overarching engagement strategy, it put special attention on human rights, the rule of law, social-economic issues, trade and investment and market access. The EU has repeatedly highlighted the need to curb industrial cyber espionage by intensifying cooperation with China on reforming the country's "protection and enforcement of intellectual property

[205] Voo, Julia. "Belfer Center Convenes US-China Cyber Security Working Group." *Harvard Kennedy School, Belfer Center for Science and International Affairs*, 3 May 2019, https://www.belfercenter.org/publication/belfer-center-convenes-us-china-cyber-security-working-group

[206] The Office of the United States Trade Representative (USTR). "Findings of the Investigation Into China's Acts, Policies, and Practices."

[207] European Commission. "China", DG Trade, Countries and regions Trade Policy, 16 April 2018, http://ec.europa.eu/trade/policy/countries-and-regions/countries/china/

[208] "EU-China 2020 Strategic Agenda for Cooperation." *European External Action Service*, Brussels, 23 Nov. 2013.

[209] "Joint Communication to the European Parliament and the Council on Elements for a new EU strategy on China." JOIN (2016) 30 final, *European Commission,* Brussels, 22 June 2016.

[210] "Council conclusions on EU Strategy on China." 11252/16, *Council of the European Union,* Brussels, 18 July 2016.

rights"[211] through mechanisms such as the Intellectual Property Rights Infringement Protection[212] and the EU-China Strategic Framework for Customs Cooperation on IPR for 2018-2020.[213] Underscoring the importance of intellectual property rights protection in Europe, and building on synergies with Japan and the USTR Section 301 Report, the EU has also launched a case at the WTO against China's "unfair [and forced] technology transfers" and discriminatory treatment of foreign companies.[214]

5.2 China's engagement with the EU and EU member states

The landmark 2015 Xi-Obama industrial cyber espionage agreement has served as a template for EU member states' cyber-related bilateral partnerships with China. Both the United Kingdom (2016)[215] and Germany (2015)[216] have convinced China to formally adopt a norm against cyber espionage in bilateral accords, commit to hold a regular dialogue on pertinent cyber issues and cooperate in the fields of incident mitigation, CERTs assistance, cybercrime and CBMs. European member states' diplomatic approach to China has therefore been more functional and in pursuit of concrete practical outcomes of benefit for both sides. From EU countries' vantage point, this type of functional cooperation with China is necessary as it transcends unsurmountable differences between the two sides' normative preferences, threat perceptions and security interests.

For decades, Sino-European Union relations have been characterised by consistently growing economic and cultural ties. Accommodating China's economic rise and appetite to shape international order has given rise to greater technological interdependence in tandem with tremendous new normative, security and political challenges. China's growing assertiveness - particularly its growing political reach in Europe, which is often perceived as a lever to undermine the cohesion of the Union - has eventually compelled the EU to fundamentally redefine its China strategy from an accommodation-based engagement policy towards one of balancing and "managed interdependence" in key strategic sectors and supply chains, with an emphasis on ensuring market reciprocity.[217]

2019 saw the European Union chart a new bolder course vis-à-vis China. In March 2019, weeks before the 21st EU-China Summit, and coming after recommendations made by the Federation of German Industries and other European actors (member states, other industry federations, etc.) earlier that year,[218] the European Commission published an official document ("EU-China - A strategic outlook") describing a new "EU policy shift towards a more realistic, assertive, and multi-faceted approach" to

[211] "Council conclusions on the EU Strategy on China."
[212] "EU-China Cooperation in IPR." *European Commission Taxation and Customs Union*, 17 Feb. 2017, https://ec.europa.eu/taxation_customs/business/customs-controls/counterfeit-piracy-other-ipr-violations/eu-china-cooperation-ipr_en
[213] European Commission. *Report on the Implementation of the EU Customs Action Plan to Combat IPR Infringements for the Years 2013/2017*. Report from the Commission to the Council and the European Parliament, COM(2018) 77 final, 22 Feb. 2018. , https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0077&from=EN
[214] "EU Launches WTO Case against China's Unfair Technology Transfers." *European Commission*, 1 June 2018, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1852
[215] U.K. Foreign & Commonwealth Office. "China-UK High Level Security Dialogue: Communique", Policy paper, 13 Jun. 2016, https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique
[216] Wu, Wendy. "Handshake to end the hacking: China and Germany pledge for peace in cyberspace by 2016." *South China Morning Post*, 10 Nov. 2015, https://www.scmp.com/news/china/diplomacy-defence/article/1877288/china-and-germany-aim-reach-commercial-cyberspying-deal
[217] Roberts, Anthea, et al. "The US-China Trade War Is a Competition for Technological Leadership." *Lawfare*, 21 May 2019, https://www.lawfareblog.com/us-china-trade-war-competition-technological-leadership
[218] "Strengthen the European Union to Better Compete with China." *German Industries (BDI)*, 10 Jan. 2019, https://english.bdi.eu/article/news/strengthen-the-european-union-to-better-compete-with-china/. In this influential policy paper, leading German business representatives call on the EU (and its member states, the German government in particular) to use its overall political and economic weight and become more assertive in resolving economic challenges posed by China's model of state capitalism and economy, systemic unfair trade practices and market discrimination.

dealing with China.[219] The EU asserts that despite China being a cooperation and negotiating "partner" with which the EU needs to (re)align objectives and strike a "balance of interests", the PRC has increasingly become a "systemic rival" and an "economic competitor" that leverages economic investment to achieve geopolitical gains, energetically pursues global "technological leadership" and seeks to export norms and forms of governance at odds with neoliberalism. Furthermore, the profoundly intertwined role of the CCP in China's economy and the opaque and highly blended divisions between the public and private spheres and the military have made Chinese technology a security risk for the EU in the "short to mid-term".

At its core, however, the EU's symbolic reorientation towards China was propelled by economic concerns stemming from the broader systemic and normative challenges mounted by China's state-interventionist model of governance to European liberal market economies.[220] China has received the label of a "strategic [economic] competitor for the EU", primarily owing to its discriminatory and market-distortive policies and for incentivising forced technology transfers. Increasingly able to undermine Europe's edge in technology, China's model of state capitalism has continuously mandated the forced transfer of European technology and intellectual property to China and has repeatedly enforced extensive restrictions on foreign companies' access to the Chinese ICT market through the use of non-tariff (market) barriers and unfair practices, such as limiting foreign access to state-funded industrial programmes to national companies. The wide range of discriminatory tools employed by the government has cumulatively boosted the domestic industry' competitive edge in global markets, allowing them to reap the benefits of the Chinese market's massive economies of scale.

Much like the US Trade Representative Section 301 report of 2018, the EU's "strategic outlook" report highlights the distortive effects of industrial policy instruments, such as "heavy [government] subsidies", state-owned or state-backed companies' investment practices and cyber-enabled intellectual property theft "on the EU internal market" and the bloc's innovative edge. By devoting massive amounts of direct government funds, extending domestic restrictions and promoting legitimate and illegitimate means of acquiring foreign know-how, the state's intervention-by-industrial policies have sought to alter competitive dynamics in the global high-tech marketplace in order to boost domestic companies' global competitiveness, control entire segments of global supply chains and capture more market share in strategic industries.

While in December 2018 China called on the EU to refrain from "politicising economic and trade issues", "ease its high-tech export control on China" and ensure a continued bilateral cooperation in innovation and scientific research, the Commission's report concludes that China has been reluctant to implement market-opening policies, hence failing to "reciprocate market access and maintain a level playing field" with EU counterparts.[221]

The EU also set forth 10 action points in several policy areas in pursuit of economic reciprocity objectives vis-à-vis China and a desire "to strengthen its industrial base". Those include, among other things, increasing the EU's economic leverage to negotiate market reciprocity, promoting procurement transparency and openness and demanding the Chinese government carry out structural and micro-level reforms addressing specific economic considerations. Informed by the dynamics of the US-China trade negotiations, the European Union has also taken practical steps towards redressing its security concerns related to 5G. The EU has done this by issuing cybersecurity guidelines[222] and tackling the distortive effects of state-led foreign investments in critical infrastructure and other strategic sectors by

[219] *EU-China - A Strategic Outlook*. Joint Communication to the European Parliament, the European Council and the Council, JOIN (2019) 5 final, European Commission, 12 Mar. 2019

[220] Small, Andrew. *Why Europe Is Getting Tough on China*. Apr. 2019. *Foreign Affairs,* https://www.foreignaffairs.com/articles/china/2019-04-03/why-europe-getting-tough-china

[221] "Full Text of China's Policy Paper on the European Union." *Xinhua News Agency*, 18 Dec. 2018, http://www.xinhuanet.com/english/2018-12/18/c_137681829.htm

[222] "European Commission Recommends Common EU Approach to the Security of 5G Networks." *European Commission*, 26 Mar. 2019, https://web.archive.org/web/20190326190621/http://europa.eu/rapid/press-release_IP-19-1832_en.htm

enforcing a framework for scrutinising Chinese investments in Europe in April 2019.[223] Apart from this, the EU outlined its own Europe-Asia strategy for developing global connectivity and infrastructure partnerships in 2018, aiming to ensure a level playing field for participating businesses by upholding the values of transparency, reciprocity and fairness.[224]

Overall, the EU's more critical stance before the 2019 summit has helped secure several concessions from the Chinese side. Concerning EU-China cooperation in cyberspace, the two sides will continue working towards implementing norms of responsible state behaviour under the EU-China Cyber Task Force framework and within parallel UN processes. While affirming that "there should be no forced technology transfers", the two sides also committed themselves to enhancing resilience against malicious cyber activities, including against cyber-enabled intellectual property theft. The two sides also committed to a concrete timeline to conclude the "EU-China Comprehensive Investment Agreement", for which "decisive progress" from the Chinese side - i.e. substantial market-opening reforms directed at ensuring a level playing field - will be required in 2019.[225] Furthermore, China and the EU are to cooperate on reforming the WTO, though this will be conditional on China reforming the discriminatory effects of industrial state subsidies and other related issues.

5.2.1 Track 1 dialogues with China

The ICT sector and "digital economy" - "in particular, cybersecurity-linked issues and market access reciprocity issues - are strategic priority areas of the EU's engagement with the PRC as manifested by the EU-China Cyber Taskforce, the EU-China ICT Dialogue, the High Level Economic and Trade Dialogue (HED) and DG CONNECT's expert group meetings on the economic impact of cybersecurity and the digital economy.[226]

The EU's cyber diplomacy towards China firmly adheres to the "strategic framework for conflict prevention and cyber stability". This includes: support for existing cyber-related international legal instruments and the application of current laws to govern cyber activities; the promotion for the development of universal norms, rules and principles of responsible state behaviour articulated by the UN Group of Governmental Experts, and their implementation; and the establishment of confidence building measures that enhance mutual trust, predictability and transparency between states, and their implementation. Increasing mutual trust in cyberspace through cooperation is a central objective of the EU-China 2020 Strategic Agenda for Cooperation.

The annual EU-China Cyber Taskforce - co-chaired by the European External Action Service and DG CONNECT on the EU side, and China's Ministry of Foreign Affairs and the CAC on the Chinese side - was launched in 2012 as the principal Track I mechanism to strengthen cooperation, mutual trust and understanding on cybersecurity issues. In addition, the Taskforce serves as a platform for legal and policy exchanges regarding the applicability of existing international legal principles on cyber affairs and discussions on cybernorm maintenance, privacy and human rights, intellectual property rights and ICT standardisation.[227] At the two most recent EU-China summits - in July 2018 and April 2019[228] - the two sides agreed to the "further development and implementation" of existing internationally accepted cybernorms, rules and principles for responsible state behaviour "as articulated in 2010, 2013, 2015

[223] "EU foreign investment screening regulation enters into force." *European Commission,* 10 Apr. 2019, http://europa.eu/rapid/press-release_IP-19-2088_en.htm

[224] "EU steps up its strategy for connecting Europe and Asia." *European Commission,* 19 Sep. 2018, http://europa.eu/rapid/press-release_IP-18-5803_en.htm

[225] "Joint Statement of the 21st EU-China Summit." *European External Action Service*, 10 Apr. 2019, https://eeas.europa.eu/delegations/china/60836/joint-statement-21st-eu-china-summit_en

[226] "Joint statement of the 20th EU-China Summit." *European External Action Service*, 17 July 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/48424/joint-statement-20th-eu-china-summit_en

[227] "Asia." *European Commission*, DG Connect, Digital Single Market Policy, 2019 https://ec.europa.eu/digital-single-market/en/asia

[228] "Joint Statement of the 21st EU-China Summit."

reports of the UNGGE" through the continuation of the EU-China Cyber Taskforce.[229] To complement this, the European Commission's DG CONNECT and the PRC Ministry of Industry and Information Technology (MIIT) have set up the EU-China ICT Dialogue and a non-governmental expert group, both tasked with studying the economic impact of cybersecurity challenges, ensuring market access reciprocity and strengthening the digital economy.[230]

Market access challenges generated by China's enforcement of non-tariff measures and its strict national regulatory environment were also discussed in the framework of the 7th EU-China High-Level Economic and Trade Dialogue.[231] The 8th EU-China Dialogue held in July 2017[232] reaffirmed bilateral commitments to implement reforms alleviating ICT-related market barrier issues that may arise due to national regulations,[233] in addition to reaffirming future technological collaboration in new technologies, such as 5G.[234]

High-level cyberspace-related dialogue between the EU and China, however - especially regarding international cyber stability - has produced limited results. This was due to almost irreconcilable divergences between the two sides regarding their approaches to Internet governance and how to regulate state behaviour in cyberspace. More specifically, China and the EU fundamentally disagree over the role of state actors in governing cyberspace, the maintenance of the "free, open and secure" Internet anchored in the protection of human rights and fundamental freedoms online and the adequacy of the existing international legal regime to effectively regulate cyberspace.

On the *substantive* level, China and the EU's positions diverge with respect to the role of governments in determining cyberspace policy. China advocates for a territorialised cyber sovereignty model with a strong role for governments in controlling a "Balkanised" cyberspace by way of national laws, "traffic rules" and content-filtering tools. It supports a top-down "multilateral" or "multi-party" model of Internet governance with governments in the driver's seat. The EU strongly favours a bottom-up model of Internet governance, in which multiple stakeholders - responsible for the creation, maintenance or operation of Internet services and infrastructures such as technical communities, engineers, private industry, civil society and individuals - work together to develop a regulatory environment over cyberspace. The role of the state is that of a shaper and a facilitator. The EU's core ideal of a free, open, stable, secure Internet has been anchored in the protection of online human rights and fundamental freedoms, respect for international law and existing legal instruments and the values of market openness and reciprocity.

As to how international law applies to cyberspace, there remain fundamental divides. China adopts the view that the principles enshrined in the UN Charter apply to cyberspace. The law of armed conflict or law of countermeasures have limited applicability and even appropriateness in the cyber domain. The EU, as a unitary actor, is a strong proponent of the general and universal application of the current international legal regime to cyberspace. EU member states such as France, Estonia, the United Kingdom, the Netherlands and Germany have enunciated their legal opinions illustrating their understanding of the applicability of international law in this domain, crystallising *opinio juris* and state practice.

---

[229] "Joint statement of the 20th EU-China Summit."
[230] "List of Outcomes of the 19th China-EU Summit." *The State Council of the People's Republic of China*, 4 June 2017, http://english.gov.cn/premier/news/2017/06/04/content_281475676073214.htm
[231] "EU and China discuss economic and trade relations at the 7th High-level Economic and Trade Dialogue." *European Commission,* DG Trade, 25 June 2018, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1873
[232] "8th EU-China ICT Dialogue." *European Commission*, DG Connect, 11 July 2017, https://ec.europa.eu/digital-single-market/en/blog/8th-eu-china-ict-dialogue-11-july-2017
[233] "EXCITING - EU-China study on IoT and 5G 2016 to 2018." *European Commission*, 2019, https://cordis.europa.eu/project/rcn/205946_en.html
[234] "The EU and China signed a key partnership on 5G, our tomorrow's communication networks." *European Commission,* 28 Sep. 2015, http://europa.eu/rapid/press-release_IP-15-5715_en.htm

Procedurally, Beijing advocates the development of a new multilateral treaty negotiated by states within the framework of the UN to regulate the specific features of cyberspace. In contrast, the EU has been strongly disinclined to support the development of a new treaty process. It believes existing international customary and general international law are adequately capable of governing the use of ICTs. In addition, the EU appears to be very prescient about the challenges linked to treatymaking processes, rightly expecting difficulties in building consensus on primary issues like scope, jurisdiction and leading principles.

The EU promotes existing mechanisms to address specific issues, such as the CoE's Budapest Convention on Cybercrime. To facilitate new measures for long-term stability and security in cyberspace, the EU has favoured a soft law norms approach at the United Nations, but also bottom-up norm formation initiatives. In the EU's view, the creation, cascading and maintenance of norms represent the most appropriate way to address new challenges, transcend political differences and solidify standards of behaviour.

5.2.2 Track 1.5 and 2.0 dialogues with China

As with a range of other policy areas, the European Union has taken a socio-economic approach to cybersecurity, the digital economy and information communication technologies, understanding cyberspace as an enabler for social, political and economic development.

At the unofficial level, the "expert group meeting on the economic impact of cybersecurity challenges and digital economy" held in May 2018 - organised by EU Directorate Generals CONNECT and TRADE, cooperating with the European External Action Service (EEAS) and the Ministry of Industry and Information Technology of China - charted out the future of an EU-China industry and academia-driven cooperation expert platform that seeks to examine the economic impact of national cybersecurity and digital economy regulatory policy on each partner country's ICT market. Areas of focus include issues like the economic impact of restricting cross-border data transfers and implementing data localisation requirements, forced technology transfers and ICT certification systems' impact on national security consideration. Above all, the Track 1.5 format aims at improving Sino-European reciprocity regarding market access.

In addition, there are several annual Track 1.5/2 formats addressing specific issues of international stability in cyberspace. The Sino-European Cyber Dialogue (SECD) was launched in 2014 between the MSS-affiliated China Institutes of Contemporary International Relations (CICIR) and The Hague Centre for Strategic Studies (HCSS) in cooperation with the Chinese government (MFA, MIIT, CAC) and the European External Actions Service. The 7th meeting of April 2018 aimed to reduce misperceptions and increasing predictability and transparency "of both [EU and China's] approaches to cybersecurity through the implementation of confidence building measures" and the identification "of potential practical cooperation, particularly on international law and norms of responsible state behaviour in cyberspace".[235] The SECD format, like the official EU-China Cyber Taskforce, has expanded well beyond international stability-increasing measures to include norms of responsible state behaviour, international law and the implementation of confidence building measures. SECD functions as an umbrella track 2 dialogue platform as it includes discussions on Internet governance, cyber deterrence and doctrinal thinking and cyberspace regulatory developments. CICIR is also a partner organisation in Track 1.5 dialogues in the "US-China Cyber Security Dialogue" organised by the Center for Strategic & International Studies (CSIS)[236] and the International Institute for Security Studies (IISS)-CICIR Cyber Dialogue in Europe.

[235] "7th Sino-European Cyber Dialogue (SECD) takes place in Geneva." *The Hague Centre for Strategic Studies*., 7 June 2018, https://hcss.nl/news/7th-sino-european-cyber-dialogue-secd-takes-place-geneva
[236] "Track 1.5 US-China Cyber Security Dialogue."

Furthermore, the EU Institute for Security Studies (EUISS), together with the Geneva Centre for Security Studies (GCSP) and China Institutes of Contemporary International Relations (CICIR) convened the first meeting of the annual Sino-European Expert Working Group on the Application of International Law.[237] The working group provides a platform for European and Chinese legal experts to exchange views on how international law rules and principles could govern specific scenarios, recent developments and past cyber operations against critical infrastructure or related state practice. In particular, the specialised expert working group aims at fleshing out the legal concepts, explanations, and modes and styles of reasoning with respect to international law's applicability in cyberspace and the permissibility of specific actions, responsibilities and protective measures. Engaging in a serious dialogue on these specific issues could increase transparency and mutual trust about European and Chinese legal reasoning, especially if conceived as a legal confidence building measure conducive to stability and security in cyberspace. Discussions within the framework of this mechanism at the unofficial level could potentially produce a sifting-through effect to official Track 1 dialogue on international law between government officials, particularly as the new round of the UNGGE calls upon states to submit their official legal positions on cyberspace.

6 Pushback against Huawei and Chinese tech suppliers

The Trump Administration has recently manoeuvred to lead a 5G supply chain "decoupling" campaign with Chinese manufacturers of strategic technologies in order to resolve perceived national security risks and accelerate the unravelling of "interlocking supply chains and trading relationships" resulting from the two economies' entanglement in the past 30 years.[238]

In May 2019, after the US-China trade negotiations had reached yet another impasse, the White House made two significant moves targeted at Chinese high-tech suppliers: First it barred foreign companies identified as posing national security risks from selling in the US market, then it blocked domestic exports of technology to Huawei without specific licenses.

The first move - an **executive order** "on Securing the Information and Communications Technology and Services Supply Chain"[239] - gave the US government broad powers to restrict any US acquisition or transaction of technology that is linked to a "foreign adversary" and deemed to represent a risk to "national security", critical military and civilian infrastructure or the "digital economy" of the United States.[240] Situated in the ongoing US-China technology/trade confrontation and seemingly directed at China, the order broadly defines "foreign adversary" as any company, person or country intending to conduct harmful activities against national security, critical infrastructure or the digital economy of the United States.[241] It delegates to the Department of Commerce the authority to identify foreign adversaries and block any transactions involving ICTs "designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary".[242]

---

[237] "Sino-European Expert Working Group on the Application of International Law in Cyberspace, 29-30 April 2019, Beijing." *Geneva Centre for Security Policy*, 5 June 2019, https://www.gcsp.ch/global-insight/sino-european-expert-working-group-application-international-law-cyberspace

[238] Lim, Darren, and Victor Ferguson. "Huawei and the Decoupling Dilemma." *Lowy Institute, The Interpreter*, 28 May 2019, https://www.lowyinstitute.org/the-interpreter/huawei-and-decoupling-dilemma

[239] The White House. *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. 15 May 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

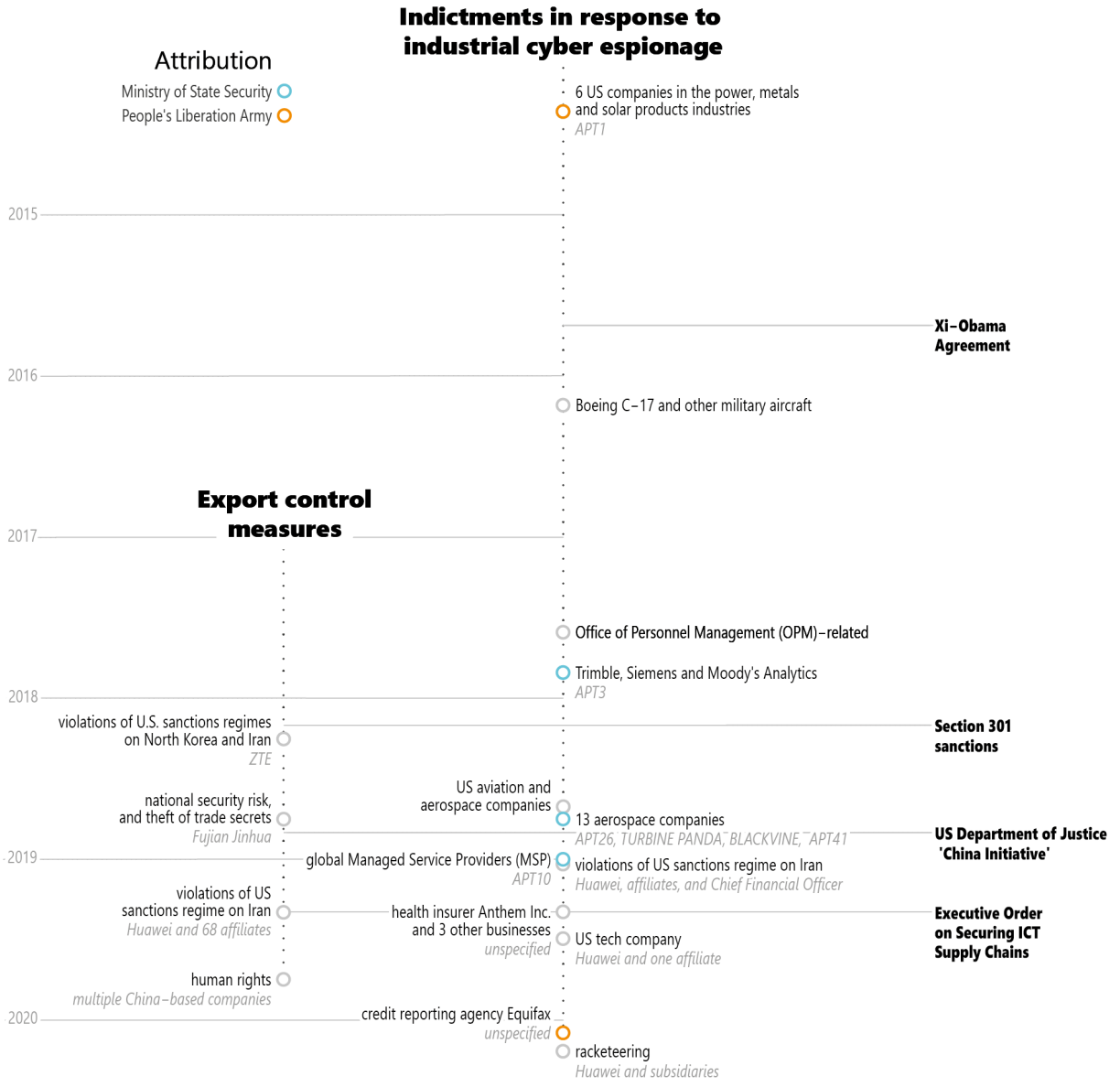
[240] The White House. Executive Order on Securing the Information and Communications Technology and Services Supply Chain.

[241] Webster, Graham. "It's Not Just Huawei. Trump's New Tech Sector Order Could Ripple through Global Supply Chains." *Washington Post*, https://www.washingtonpost.com/politics/2019/05/18/its-not-just-huawei-trumps-new-tech-sector-order-could-ripple-through-global-supply-chains/

[242] "The Trump Administration's Approach to Huawei Risks Repeating China's Mistakes." *Slate Magazine*, 21 May 2019, https://slate.com/technology/2019/05/u-s-china-huawei-executive-order-foreign-adversary-national-security.html

Timeline of indictments and export control measures against Chinese actors

Adopted by the US Departments of Justice and of Commerce



Data: US Department of Justice, 2020; US Department of Commerce, 2019; White House, 2019; Office of the US Trade Representative, 2019

In a second powerful move, the Department of Commerce announced "Huawei Technologies and 68 non-US affiliates" as a new addendum to the Export Administration Regulation's **entities list**, hence blocking the transfer of non-licensed US technology to the Chinese nominally private juggernaut.[243] The move was founded on prior indictments against the Shenzhen-based company for its alleged violation of the US secondary sanctions regime against Iran, construing the business practices of the firm as a national security risk. This move ratcheted up pressure on China by building upon a cumulative set of tech-related export control measures targeted at other Chinese high-tech companies and individuals in the recent years, such as the companies ZTE and Fujian Jinhua.

In effect, the adoption of an export control regime against Huawei - a manufacturing behemoth in (critical) telecom equipment that has enormous market share on the global marketplace across the entire value chain - meant that the company's access to vital US technology supplies, innovation capacity, advanced components (like semiconductor chips) and the Android smartphone operation system could be cut off.[244]

Furthermore, the US has sought to galvanise the support of like-minded allies to implement national security-based country-of-origin restrictions or bans against Huawei's and other Chinese tech suppliers' 5G infrastructure. Several countries have already halted the use of Huawei components in their "core" networks. Others have proceeded to bar the Chinese company from supplying the entire technology stack of their 5th-generation communication networks. Mirroring the United States, Five-Eyes members Australia and New Zealand have effectively barred Huawei from participating in the rolling out of 5G, referencing national security concerns and the firm's links to the CCP.[245] Similarly, Japanese, Czech, French and Polish carriers have partially halted Huawei and ZTE's involvement in the rollout of their (core) 5G networks due to top-down bans, cybersecurity risks and espionage concerns.[246] Others, such as the UK and Germany, have taken non-exclusionary, risk-based approaches to the supply of 5G technology.

6.1 Risks

The pushback against Huawei has been primarily driven by a fear of falling behind China in next-generation technologies and the transformative impact of the technology itself. Many experts anticipate a ground-breaking impact of 5G on the way future society, industry and military function and depend on networked communications. As a critical infrastructure, 5G promises greater speed and stability, minimal latency, enhanced access to larger amounts of data and the capacity to handle massive numbers of devices concurrently. It is expected that 5G will enable, among other things, new types of near-instantaneous, industrial-scale machine-to-machine communication and will therefore underpin the future development of advanced automation, robotics and artificial intelligence.[247]

The Chinese company is in the spotlight due to its meteoric rise as a dominant market player in next-gen 5G technology and its "first-mover advantage", which could potentially secure Beijing the upper hand geopolitically in the long run.[248] Beset by controversy and still heavily dependent on foreign companies for advanced components (memory, semiconductors, data converters), quantitative metrics show that Huawei - a partially state-built "national champion" – "holds a leading market share on the next-generation technologies marketplace. Huawei and its subsidiaries hold the world's top 5G patent

[243] "Addition of Certain Entities to the Entity List (Final Rule), Effective May 16, 2019." *Bureau of Industry and Security (BIS)*, US Department of Commerce, 16 May 2019, https://www.bis.doc.gov/index.php/all-articles/17-regulations/1555-addition-of-certain-entities-to-the-entity-list-final-rule-effective-may-16-2019
[244] Webster, Graham. "It's Not Just Huawei."
[245] Williams, Robert, and Preston Lim. "Huawei Arrest Raises Thorny Questions of Law Enforcement and Foreign Policy." *Lawfare*, 7 Dec. 2018, https://www.lawfareblog.com/huawei-arrest-raises-thorny-questions-law-enforcement-and-foreign-policy
[246] "Huawei 5G in Europe and Beyond." *Carnegie Endowment for International Peace*, https://carnegieendowment.org/publications/interactive/huawei-timeline
[247] "The Geopolitics of 5G." *Eurasia Group*, 15 Nov. 2018, https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g
[248] "The Geopolitics of 5G."

owner and standard-setter spot as the largest telecom infrastructure supplier".[249] Unmatched by competitors at price, Huawei components underpin critical infrastructure around the globe. The company offers a broad range of competitive, cost-effective products across the entire design-deployment-application 5G ecosystem and enjoys a high and diversified market penetration rate, at least in Europe.[250]

Crucially, the "case against Shenzhen" masks fundamental issues of trust in China's legal and political environment and its state-dominated economic development model, where the party-state apparatus has deeply intertwined itself in the private sector. In addition, new measures are also driven by strategic autonomy woes, (cyber)security risks and a rivalry over the consolidation of digital spheres of influence in 5th-generation networks across the East-West divide.

Huawei has become a sticking point in the broader technological competition among states. Technology supply chains originating in China are increasingly politicised as major national security risks. Much like how the Snowden revelations provided fuel Beijing's quest for "secure and controllable" indigenous technologies in Chinese (semi)official political discourse, concerns over Huawei serve to legitimise actions - renationalisation of supply chains for critical technologies and consolidation of domestic industrial bases - against a dissenter of the liberal economic order. When viewed through the prism of Western states, Huawei's 5G is construed as a threat to military and critical infrastructure, national security, system-level economic structures (like the high-market), intellectual property and strategic autonomy.

6.1.1 Cyber espionage and cybersecurity risks

For many states, President Trump's recent executive order hits at the crux of the issue - that the integration of Huawei technologies in domestic critical infrastructure risks exposing Western networks to the long arm of Chinese intelligence services in peacetime, during a conflict or in the increasingly grey area in between.[251] By gaining a legitimate foothold in the 5th-generation backbone, and by allegedly planting backdoors or leaving vulnerabilities deliberately unpatched,[252] Huawei's access might present state-linked actors with a unique array of tools for leverage or coercion through cyber espionage, subversion or even sabotage. The potential for a foreign company leveraging 5G network systems for industrial or politically motivated espionage represents a principal concern for many states as this practice could erode economic competitiveness, compromise military advantages and undermine political cohesion or national security.

This concern - that Chinese telecom companies could function as vehicles for commercial/military espionage - can be traced back to 2012, when a US government report concluded that "Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat".[253] Despite the absence of declassified evidence that clarifies Huawei's complicity in state-backed cyber espionage, the company was allegedly involved in the hack of the African Union (AU), where it exploited its position as a main ICT service and equipment provider.[254] Similarly, the latest report by the UK's Huawei Cybersecurity Evaluation Centre (HCSEC) has found the existence of "serious [cybersecurity]

[249] IPlytics. *Who Is Leading the 5G Patent Race? A Patent Landscape Analysis on Declared 5G Patents and 5G Standards Contributions*. Nov. 2019, pp. 1-14. , https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf

[250] Duchâtel, Mathieu and François Godement. "Europe and 5G: The Huawei Case - Part 2." *Institut Montaigne*, June 2019, https://www.institutmontaigne.org/en/publications/europe-and-5g-huawei-case-part-2

[251] Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2018, xi.

[252] *Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2019*. A report to the National Security Adviser of the United Kingdom, Mar. 2019, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

[253] Webster, Graham. "What the Huawei Executive's Arrest Could Mean for the US-China Trade Talks." *Slate Magazine*, 7 Dec. 2018, https://slate.com/technology/2018/12/huawei-arrest-meng-wanzhou-us-china-trade-war-tariffs-analysis.html

[254] "The African Union Headquarters Hack and Australia's 5G Network." *Australian Strategic Policy Institute (ASPI) The Strategist*, 12 July 2018, https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/

vulnerabilities and issues" in Huawei-made networking products that could be exploited by malicious actors, in addition to poor "cybersecurity quality" in its software products line.[255] Huawei and ZTE have also been subjected to indictments and export controls for their alleged engagement in cyber-enabled *intellectual property theft* against Western companies and trade violations of sanctions regimes against Iran and North Korea.

National security woes are inextricably linked to the nature of the Chinese party-state. Particularly relevant are the blended relationship between public-private and civil-military, the deep embeddedness of CCP interests and priorities in the economy and the existence of an institutionalised framework for political-legal influence and coercion over the technology industry. China's unique political-legal environment could enable the party-state apparatus to pressure suppliers of critical and network infrastructure to conduct activities, such as cyber espionage, for its benefit, thereby cultivating a network of proxies with "deep ties to the Chinese government and the military" with state-shaped objectives.[256]

The global pushback against Huawei's 5G symbolises the broader competition over "economic models" and styles of decisionmaking.[257] The Shenzhen-based giant is a prominent commercial representative of a political-economic culture that has simultaneously relied on the liberal economic order as well as state-based decisionmaking and subsidising to fuel its growth. China's governing elite mobilises a specific regime-oriented information security logic to administer the use of digital technologies within its territory that runs at odds with neoliberal norms.

While the Chinese private sector is not solely comprised of state agents, the defining features of the party-state - along with the CCP's adherence to a regime-oriented security logic and endorsement of a "rule *by* law" method of governance - remain a powerful force driving Western nations' distrust of Chinese ICT manufacturers.

According to the PRC's statutory law provisions (particularly Articles 7, 12 and 14 of the 2017 National Intelligence Law), private Chinese enterprises, such as Huawei, could be compelled to "support, assist and cooperate [with]" intelligence agencies carrying out intelligence-gathering for the purposes of the all-encompassing concept of "national security".[258] Companies could be required to grant state actors access to internal "communications" networks - abroad or on the Mainland - and have no effective legal remedies in case of abuse by state security authorities or if providers breach (or refuse to comply with) their Counterespionage Law-mandated obligations to provide the necessary "facilities or other assistance".[259] Article 28 of the CSL declares that "network providers shall provide technical support and assistance to the public [and state] security organs" carrying forth "work to protect national security".[260] What's more, the National (State) Security Law of 2015 - an "umbrella law" that defines national security as an all-encompassing concept - stipulates that private enterprises have the "responsibility and obligation to preserve national security" by, *inter alia*, cooperating with public, state and military organs and providing "conditions" and "other assistance" for facilitating "national security efforts".[261] Besides the legal framework, the party-state has also tightened control over "national champions" through the

[255] Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2019.
[256] Isaac Stone Fish. "Even If Trump Trusts Huawei, Here's Why America Shouldn't." *Washington Post*, 5 July 2019, https://www.washingtonpost.com/opinions/2019/07/05/even-if-trump-trusts-huawei-heres-why-america-shouldnt/
[257] "How 5G Will Shape Innovation and Security: A Primer." *Center for Strategic and International Studies (CSIS)*, 6 Dec. 2018, https://www.csis.org/analysis/how-5g-will-shape-innovation-and-security
[258] Clarke, Donald C. "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law." *SSRN Electronic Journal*, Mar. 2019, https://www.ssrn.com/abstract=3354211
[259] "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws." *Australian Strategic Policy Institute (ASPI) The Strategist*, 12 Sept. 2018, https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/
[260] Clarke, Donald C. "The Zhong Lun Declaration."
[261] Pieke, Frank, et al. *Chinese Telecommunication Companies: Political and Legal Vulnerabilities and How Europe Should Deal with Them*. MERICS Policy Brief, Mercator Institute for China Studies, 13 Mar. 2019, pp. 1-8., https://www.merics.org/en/policy-brief/chinese-telecommunication-companies

integration of party "committees, cells and secretaries" as policymaking supervisory mechanisms and, crucially, as force multipliers of CCP power.[262]

The above provisions are further reinforced by the fact that by virtue of the party-state, judicial power in China is "subordinate to the executive and the latter to the Party".[263] This affords state authorities with opportunities to operate beyond the law and structures the system to favour political over commercial interests. As Article 4 of the sweeping National Security Law stipulates, "national security work" must adhere to the Chinese Communist Party leadership, whose political or security interests trump all other objectives.[264] Ultimately, party rule has "absolute leadership over [all] political and legal work".[265]

6.1.2 Strategic autonomy

The case against Huawei's 5G has blended economic and national security risks. From the vantage point of European states, Huawei's 5G technology can be construed as a systemic risk to their "strategic autonomy" and technological independence.[266] The EU Commission has advocated a risk-based "diversity of suppliers" approach to the rollout of 5th-generation networks.[267] Although critical of Chinese industrial policies and their discriminatory effects, the EU has recognised that this issue requires a careful balancing act between the potential national security risks of Huawei's critical infrastructure equipment, foreign technology dependence and the values of corporate autonomy and independent decisionmaking that might be infringed upon with comprehensive market-wide bans. Within this balancing act, however, lie opportunities for increasing the economic competitiveness of European firms in high-tech and for further strengthening the European industrial base and innovation edge.[268]

6.2 Implications

6.2.1 Redoubling of "indigenous innovation"

Against the backdrop of a spiralling US-China technology leadership competition in 2018, China's governing elite continued to champion the core CCP sloganeering of "self-reliance through indigenous innovation".[269] President Xi asserted that "self-reliance" is a necessary strategic road to take, given "rising unilateralism and protectionism" that make it harder for China to obtain "key technology [...] internationally".[270] Xi reiterated his country's commitment to taking the initiative in science and technology, becoming *the* "leading player in technology" and "guarantee[ing] China's development" through technological self-reliance and homegrown innovation "for key and core technologies".[271]

For the governing elite inside Zhongnanhai, international pressure exerted on Huawei in 2018 has highlighted the Chinese ICT industry's excessive reliance on advanced foreign technologies, serving as

[262] Pieke, Frank, et al. Chinese Telecommunication Companies: Political and Legal Vulnerabilities.
[263] Duchâtel, Mathieu and François Godement. "Europe and 5G: The Huawei Case - Part 2."
[264] Pieke, Frank, et al. Chinese Telecommunication Companies: Political and Legal Vulnerabilities.
[265] "中共中央印发《中国共产党政法工作条例》[The Central Committee Issues 'Regulations on Political and Legal Work of the Chinese Communist Party']." *The State Council of the People's Republic of China*, 18 Jan. 2019, http://www.gov.cn/zhengce/2019-01/18/content_5359135.htm
[266] "Cybersecurity of 5G Networks." *European Commission Digital Single Market*, 26 Mar. 2019, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks
[267] "Cybersecurity of 5G Networks."
[268] "Strategic Autonomy in the Digital Age High-Level Hearing." *European Political Strategy Centre*, 17 Dec. 2018, https://ec.europa.eu/epsc/events/strategic-autonomy-digital-age_en
[269] "Mao Redux: The Enduring Relevance of Self-Reliance in China." *Macro Polo*, 25 Apr. 2019, https://macropolo.org/analysis/china-self-reliance-xi-jin-ping-mao/
[270] "Mao Redux."
[271] "Seizing Core Technologies: China Responds to US Technology Competition." *China Leadership Monitor*, no. 61, Fall 2019, pp. 1-12.

a rallying point to double down on efforts to boost the Chinese industry's innovation edge and their economic competitiveness on the market of critical technologies. At the May 2019 meeting of the PRC State Council, Premier Li Keqiang announced the expansion of government industrial policies to the homegrown semiconductor industry, particularly the development of semiconductor *technology*, including manufacturing and chip design services.[272] Furthermore, Huawei is "similarly pushing innovation in [...] the most advanced technology sectors globally, including new chip designs, systems architectures, software, and artificial intelligence".[273] Arm China - a key player in the drive for semiconductor technology self-sufficiency - has similarly moved to develop its chip designs and infrastructure intellectual property.[274] The firm is currently licensing "processor technology architectural frameworks" and "advanced memory" from British and Asian suppliers but will also begin developing its semiconductor chips and smartphone operating system.[275] Owing to the extraterritorial reach of US restrictive measures and EU regulations, Huawei and other Chinese high-tech suppliers should be expected to double-down on their efforts of expanding investments markets beyond the United States and the EU, particularly to emerging economies.

6.2.2 Corporate uncertainty

Although the long-term implications of the disentangling of American and Chinese technological supply chains are unclear, in the short run, exclusionary measures against Huawei might generate uncertainty on the global computing market. This is due, in particular, to the complexity of the technological ecosystem, the interlinked nature of globalised value and innovation chains and the economies of scale in the high-tech sector, upon which Chinese and foreign companies are all deeply (inter)dependent.

Moreover, the knowledge that Chinese supply lines could be cut off at any time - via an addendum to an entities list or through economic sanctions - could destabilise high-tech value chains in the short-term. In the long run, it may cause a loss of trust between suppliers. More broadly, "the tactical advantages of prioritising national security concerns in economic policymaking" could temporarily alleviate concerns, however such decisions could inadvertently generate a crisis of confidence "in free markets" themselves.[276]

"Decoupling" contradicts with the more crucial objective of leveraging Huawei - and Chinese suppliers - to compel structural economic reforms to the PRC's "state-dominated economic model" and discriminatory market access policies.[277] Incentivising such deep, structure-level liberalising economic reforms in China, however, would mandate pulling the country closer to the liberal economic order - that is, "deepening [its] integration with [...] global markets" rather than disentangling them.

[272] "China Doubles Down on Industry Subsidies: No Exit." *China Law Blog*, 27 May 2019, https://www.chinalawblog.com/2019/05/china-doubles-down-on-industry-subsidies-no-exit.html
[273] "US-China Supply Chains and Innovation: The Risks the Huawei Hawks Don't Understand." *SupChina*, 18 June 2019, https://supchina.com/2019/06/18/u-s-china-supply-chains-and-innovation-the-risks-the-huawei-hawks-dont-understand/
[274] Cheng Ting-Fang. "Beijing's Latest Tech Ally in US Clampdown: Arm China." *Nikkei Asian Review*, 4 Dec. 2019, https://asia.nikkei.com/Economy/Trade-war/Beijing-s-latest-tech-ally-in-US-clampdown-Arm-China
[275] "Huawei Confirms It Has Its Own OS on Back Shelf as a Plan B." *South China Morning Post*, 14 Mar. 2019, https://www.scmp.com/tech/big-tech/article/3001685/huawei-confirms-it-has-built-its-own-operating-system-just-case-us
[276] Lim, Darren, and Victor Ferguson. "Huawei and the Decoupling Dilemma."
[277] Lim, Darren, and Victor Ferguson. "Huawei and the Decoupling Dilemma."

7 Priorities and strategy for engagement: shadings and closing the gaps

The material characteristics and networked character of cyberspace make international engagement with China technically and politically unavoidable. Despite ideological divergences, China's policymakers recognise that states face common security risks in cyberspace. The PRC's strategy on cyber diplomacy, for instance, hints at a desire to move forward **international cooperation between technical communities on narrowly defined operational matters of cybersecurity**, such as investigating the trans-national technical effects of high-profile incidents, building network security resilience between CERTs and sharing incident response best practices and related policy research. Zooming in on such functional areas of engagement avoids having to reconcile ideological divides regarding visions of the role of the state in governing cyberspace. A bottom-up cooperation environment driven by technical communities could indirectly facilitate the building of issue-specific consensus, which over time could accrue benefits for the stability of cyberspace or transform into high-level commitments. Best practice workshops with technical experts from relevant bodies could also shed more light on the Chinese institutional chain of command and incident response landscape - at a time when a high degree of opacity continues to envelop official Chinese institutions.

In the short to medium term, engagement with China will need to move toward a greater focus on **developing practical trust- and predictability-enhancing confidence building measures** aimed at diminishing escalatory risks associated with the "fog of war" related to cyberconflict. Such engagement will play to the EU's strengths, and reinforce its position as a prudent international player that continues to invest in de-escalation efforts. Track 2 civilian-military dialogues, doctrinal and strategic thinking exchanges or table-top exercises or formal initiatives on cyberdefensive decisionmaking could aid in minimising misperception, prevent unintended escalation and increase behavioural visibility in cyberspace, if - and only if - the exchange is reciprocal, and provided that both sides are equally prepared to exchange views and non-operational information.

(Re)engagement will also benefit from the **channelling of more resources toward contextualising China's approach to cyberspace,** particularly taking into account China's distinctive political context and **existing knowledge, perception and conceptual gaps** about Beijing's idiosyncratic vision of the cyber domain and its specific socio-legal and corporate environment.

Better contextualising and understanding Beijing's behaviour in cyberspace on both the cyber threat and international political landscapes, through experts area studies and sectorial working groups (China studies scholars, experts on cyberspace, international legal experts and others), is key to closing these gaps and identifying issues for cooperation.Chinese cyber-related policies have no value bereft of the historical, economic, political, social, institutional and security context into which these are embedded. The Great Firewall, cyber-enabled forced technology transfers, industrial policies, the notion of cyber sovereignty and Beijing's sponsorship of the codes of conduct or the OEWG are deeply encoded in the country's political culture environment, historical experiences and distinctive corporate-political power relationships. These take place in accordance with pre-existing security logics and evolving regional and global security aspirations, dynamic institutional shifts, internal power struggles between local governments and other governmental organs and shifting threat perceptions. Cyberspace and ICTs are not mere instrumentalities of the party-state, but also shapers and co-producers of the policies and actions undertaken by Zhongnanhai in the cyber domain. Filling existing knowledge gaps about Beijing's intentions, ideological "speech" shades of meaning, policy developments, as well as its reactions to major policy moves within the EU (the EU cybersanctions regime and GDPR), is a necessary tool for a more efficient and functional engagement with China.

In this sense, a nuanced understanding of the multifaceted and evolving role of the Party apparatus in China's economy and the private sector is vital for grasping the gist and broader rationale behind

malevolent cyber operations stemming from the country. Researchers should explore opportunities for new analysis on how China's uniquely blended institutional context affects the design and enforcement of international legal rules and norms on responsible state behaviour in cyberspace and what measures could be taken to transcend emerging issues. This might entail further fleshing out a taxonomy of the intricate relationship between external proxies, threat groups, private companies, intelligence agencies and governmental bodies in the context of cyber espionage in order to develop new analytical paradigms on the degrees of state sponsorship or the nature of linkages across the civil-military-government nexus (see civil-military fusion; 军民融合). Keeping apprised of China's shades and complexities could enhance the effectiveness of existing instruments, such as the EU Cyber Diplomacy Toolbox and cybersanctions regime and help forge unforeseen synergies between the full spectrum of tools at the EU's disposal.

In a similar vein, procuring objective expertise on the domestic legal and political institutionalised channels for party-state political influence over Chinese private companies, but also the available modes of resistance to "state security", could refine discussions on exclusionary bans of high-tech suppliers, both within China and abroad.

The **European engagement strategy vis-à-vis China might also benefit from a stronger engagement on managing cyber-enabled risks to system-level structures,** such as the financial system and the digital market. Such cyber threats are of interest to both sides. Such engagement work would take place in the normative realm, where engagement would focus on cascading and internalising nascent cybernorms about the integrity of financial data, the protection of financial systems and the countering of disruptions to financial institutions and services.

Co-opting China, the second-largest economy relying heavily on the existing global economic rules-based order, to reach "critical mass" in the internalisation of these types of norms might be a promising avenue of cooperation, owing to its ability to build synergies on a shared interest and its potential transcendence of broader value differences and divergences. Norm-formation related to financial systems - as an example of key critical infrastructure - could pave the way for further progress in the development of other norms beyond critical infrastructure.

Moreover, international cooperation would enhance trust in the global financial system, which is a prominent target of malicious cyber activity. Achieving effective movement across this specific normative lifecycle would, however, require concrete deliverables and compliance oversight mechanisms, which in conjunction would work against one of the most fundamental and destabilising capacities of cyber threats: the degradation of trust. What's more, securing China's normative support regarding the protection of the financial system and institutions from cyber threats might signal to other actors that China is involved in building concrete sets of appropriate behaviour that place the financial system out of bounds in strategic contestation.

Bottom-up, expert-driven joint research groups on international law and definitional gaps[278] could help reduce misunderstandings and fill the existing knowledge vacuum regarding Beijing's official legal reasoning on legal frameworks for state response and the conditions for restraint, state responsibility and attribution. This bottom-up approach will accrue benefits for European governments by elucidating key concepts and acknowledging the existence of definitional gaps in international law or the cyber domain more broadly from the very beginning of track 1 and 1.5 engagement. Scholarly exchanges, especially those entailing case studies and offering reasoning on specific cyber scenarios, could help crystallise a distinctive Chinese reading of concepts like "stability in cyberspace" or a "holistic approach to cyberspace". At the very least, they would provide detailed views on the applicability of specific fields of international law to cyberspace. Owing to close linkages between research institutes

[278] Ekman, Alice, "'Definition Gap': Shaping Global Governance in Words." *The ASAN Forum*, 4 Nov. 2017, http://www.theasanforum.org/china-and-the-definition-gap-shaping-global-governance-in-words/

and Beijing's policymaking circle, such joint research groups could potentially spill over into more practical engagement between relevant bodies.

On the EU side, such exchanges would help facilitate European policymakers' deciphering of Chinese cyber diplomacy clouds of discursive meaning in international cyber debates. Track II dialogues studying the evolution of cyber diplomacy processes through focused strategic discussions on how to reconcile or find convergences between parallel, UN-based cybernorms mechanisms are also notable venues for cooperation between European and Chinese diplomats. Such opportunities might be especially promising given China's preference for the United Nations as the central platform for international cyber-related decisionmaking.

At the same time, the EU may consider a more assertive stance toward China in normative debates on cyber diplomacy and ICTs, insisting upon greater procedural transparency and substantive clarification at a time when the EU-China dialogue remains tremendously asymmetric in terms of access to information. To this aim, the EU can build on its existing long-running **socio-economic approach to cybersecurity cooperation with an emphasis on the economic benefits of cybersecurity, 5G, the digital economy** and other emerging technologies. The EU has already put in place numerous economically focused cooperation initiatives, both at the senior and lower levels, to study the economic benefits of a free and open digital market and the negative impact of non-tariff barriers and discriminatory market access measures. Although symbolic, the EU has already secured concessions from China on specific outcomes and timelines regarding these trade issues and intellectual property rights protection, the reform of the WTO, the discriminatory impact of industrial subsidies, forced technology transfers and FDI.

Further economic cooperation should move toward building on these while seeking to identify corporate structures in China - private enterprises, corporate bodies, affiliates or broader organisations - which are aligned with the EU's stance of espousing free-market principles and global economic competitiveness. This involves **seeking to reinforce their positions** and playing to their strengths.

Against the backdrop of the shifting EU policy direction and rhetoric towards China, the endorsement of the EU joint toolbox on 5G risk mitigation,[279] and inherent systemic and normative differences between the two sides, 2020 promises to be a consequential year in EU-China relations. The two sides are expected to hold their annual summit at the end of March in Beijing, and a special Leipzig summit, hosted by Germany in September with leaders of the 27 EU member states and Xi Jinping.[280] In addition, the upgraded 17+1 meeting, now chaired by Xi Jinping, will gather China and 17 central and eastern European states' leaders around the table as part of the "year of Europe for China".[281] As both Beijing and Brussels aspire to be more assertive players in ongoing global cyber debates, these high-level meetings will invariably place cybersecurity and digital issues high on the agenda.

[279] "Secure 5G networks: Commission endorses EU toolbox and sets out next steps". *European Commission*, 29 Jan. 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123.
[280] Wu, Wendy. "China and EU May Hold Summit at End of March, Ahead of '17+1' Meeting". *South China Morning Post*, 13 Jan. 2020, https://www.scmp.com/news/china/diplomacy/article/3045845/china-and-eu-may-hold-summit-beijing-end-march-ahead-171
[281] Wu, Wendy. "China Ready to Turn Its Attention to Europe in 2020". *South China Morning Post*, 26 Nov. 2019, https://www.scmp.com/news/china/diplomacy/article/3039267/china-ready-turn-its-attention-europe-2020-us-trade-deal-gets.

About the author

Nikolay Bozhkov is a cyber threat analyst at NATO's cyber defence section and was formerly a trainee at the EU Institute for Security Studies. At the Institute, he provided research support for the EUISS Task Force on Cyber Sanctions and coordinated its activities. He is co-author of the *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace (2019)*. In the framework of the EU Cyber Direct Project, he was closely involved in research on international law and norms in cyberspace as well as China's digital policies. Nikolay obtained his master's degree in international security from Sciences Po Paris with a specialisation in Chinese studies and research methods. For his master's thesis, he examined China's evolving political discourse and strategic thinking on cyberspace. He can be found on Twitter at @nbozhkoff.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

DIGITAL DIALOGUES

are a series of research papers providing an overview of selected issues, policies and institutions of the EU's main strategic partners.

EU CYBER DIRECT

This project is funded by the European Union.