TRAMPLED ORCHID: INTERNET FREEDOM IN HONG KONG

DECEMBER 2021

CIRA

CENTER FOR INTELLIGENCE RESEARCH AND ANALYSIS

SOSi

CHALLENGE **ACCEPTED**

About SOS International

Since 1989, SOS International (SOSi) has provided specialized services supporting the national security interests of the United States and the security and stability needs of its allies. SOSi advances public safety and national security through innovative research, analysis, and applied technology. SOSi conducts research and analysis in key areas of defense and intelligence work, provides high-level systems engineering services to selected national and homeland security organizations, and produces hardware and software products for government and commercial consumers.

About CIRA

SOSi's Center for Intelligence Research and Analysis (CIRA) is a leading national security think tank serving the U.S. government, Fortune 500 companies, and the broader Washington foreign policy community. Staffed by an experienced team of analysts with both deep subject matter expertise and advanced foreign language skills, CIRA provides cutting-edge research, analysis, and operational capabilities to both government and private-sector clients.

Comments may be sent to SOSi's Director of Intelligence Integration, Dr. James Mulvenon.

Dr. James Mulvenon
Director, Intelligence Integration
Intelligence Solutions Group
SOS International, LLC
2650 Park Tower Drive, Suite 300
Vienna, VA 22180
TEL: 571-421-8359
Email: James.Mulvenon@sosi.com

TABLE OF CONTENTS

LIST OF ACRONYMS

Abbreviation	Definition
AAE	Asia-Africa-Europe
AAG	Asia-America Gateway
ADC	Asia Direct Cable
APCN	Asia-Pacific Cable Network
APG	Asia Pacific Gateway
AS	Autonomous System
ASE	Asia Submarine-cable Express
ASN	Autonomous System Number
BGP	Border Gateway Protocol
BND	Bundesnachrichtendienst
BRI	Belt and Road Initiative
C2C	City-to-City
CAC	Cyberspace Administration of China
CCP	Chinese Communist Party
CDN	content delivery network
GovCERT.HK	Government Computer Emergency Response Team Hong Kong
CFIUS	Committee on Foreign Investment in the United States
CISA	Cybersecurity and Infrastructure Security Agency
CITIC	CITIC Group Corporation
CLS	cable landing stations
CMHK	China Mobile Hong Kong
CMI	China Mobile International
CNCERT/CC	National Computer Network Emergency Response Technical Team/Coordination Center
CoI CSD	Collaboration Team of the Cybersecurity Division
CSL	Cybersecurity Law
CSTCB	Cyber Security and Technology Crime Bureau
CUHK	Chinese University of Hong Kong
DDoS	Distributed Denial of Service
DNS	domain name system
DNSSEC	domain name system security extensions
DPI	Deep Packet Inspection
EAC	East Asia Crossing
EDSP	electronic data storage providers
FEA	FLAG Europe Asia
GCBD	Guizhou-Cloud Big Data
GDP	Gross Domestic Product

GDPR	General Data Protection Regulation
GFW	Great Firewall
GIRO	Government Information Security Incident Response Office
HCG	Hong Kong Communications Group
HK	Hong Kong
HKBN	Hong Kong Broadband Network
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre
HKCT	Hong Kong Cable Telecommunications
HKCTV	Hong Kong Cable Television Ltd
HKIRC	Hong Kong Internet Registration Corporation Limited
HKISPA	Hong Kong Internet Service Providers Association
HKIX	Hong Kong Internet Exchange
HKPF	Hong Kong Police Force
HKSAR	Hong Kong Special Administrative Region
HKT	Hong Kong Telecom
HSBC	Hong Kong and Shanghai Banking Corporation
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol secure
IAP	Internet Access Providers
IBX	business Internet exchanges
ICSO	Interception of Communications and Surveillance
ID	identification
IDS	intrusion detection systems
IILG	Internet Infrastructure Liaison Group
IP	Internet Protocol
ISIRT	Information Security Incident Response Teams
ISP	internet service providers
IT	information technology
ITSC	Information Technology Services Center
IXP	Internet exchange points
LAN	Local Area Network
LEA	law enforcement authorities
LLC	limited liability company
LT2P	Layer 2 Tunneling Protocol
MIIT	Ministry of Industry annd Informization Technology
MLPS	Multi-Level Protection System
MPS	Ministry of Public Security
MSS	Ministry of State Security
MTR	Mass Transit Railway

NFV	Network Function Virtualization
NGO	non-governmental organization
NPC	National People's Congress
NPCSC	National People's Congress Standing Committee
NS	National Security
NSL	National Security Law
OFCA	Office of the Communications Authority
OGCIO	Office of the Government Chief Information Officer
OONI	Open Observatory of Network Interference
PCCW	Pacific Century CyberWorks
PCPD	Office of the Privacy Commissioner for Personal Data
PDPO	Personal Data Privacy Ordinance
PPS	pre-paid SIM
PPTP	point-to-point tunneling protocol
PRC	People's Republic of China
RMB	Renminbi
FNAL/RNAL	Flag North Asian Loop/Reach North Asian Loop
RPKI	Resource Public Key Infrastructure
SASAC	State-owned Assets Supervision and Administration Commission
SBO	Service-Based Operators
SPMC	Secure Multi-party Computation
SDH	Synchronous Digital Hierarchy
SFC	Securities and Futures Commission
SIM	Subscriber Identification Module
SJC	South-East Asia Japan Cable System
SMW3	Sea-Me-We 3
SOC	security operations center
SSP	SIM service plan
TCD-CCB	Technology Crime Division of the Commercial Crime Bureau
TCP	Transmission Control Protocol
TEE	Trusted Execution Environment
TGN-IA	TGN-Intra Asia Cable System
TKO	Tseung Kwan O
TVH	Thailand-Vietnam-Hong Kong
UCL	Universal Carrier License
URL	Universal Resource Locator
VNF	Virtual Network Functions
VPN	Virtual Private Network
Xdef	National Internet and Information Security Defense Summit

This page left intentionally blank.

1.0 INTRODUCTION AND KEY FINDINGS

On June 30, 2020, the Standing Committee of the National People's Congress of the People's Republic of China (PRC) passed the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (中華人民共和國香港特別行政區維護國家安全法, hereinafter Hong Kong National Security Law, 香港國家安全法), a draconian and broadly-worded measure targeting secession, subversion, terrorist activities, and collusion with foreign forces. The new law gives the PRC and Hong Kong Special Administrative Region (HKSAR) governments expansive new powers and allows China's security forces to openly operate in Hong Kong. While its effects on the ongoing popular protests against increasing PRC control were immediately visible, the law also raises pressing questions about the future of Internet freedom in Hong Kong. What strategic rationales in Beijing and Hong Kong are driving restrictions on Internet freedom? Which Hong Kong organizations would be responsible for managing and enforcing restrictions at present and into the future? What parts of Hong Kong's Internet infrastructure could be vulnerable to future Internet restrictions, and what possible mechanisms might be employed to constrain Internet freedom in Hong Kong?

This report answers these questions in four sections, using a range of publicly available information sources in Chinese and English. First, it describes the People's Republic of China (PRC) and Hong Kong leadership's views on Internet freedom and the importance of controlling Internet content. Next, the report identifies and summarizes key organizational actors responsible for implementing crackdowns on Internet freedom in Hong Kong and describes critical infrastructure that might prove vulnerable to these crackdowns. Finally, the report concludes with an assessment of various mechanisms for restricting internet freedom in Hong Kong.

The report's key findings are as follows:

- On an infrastructural level, connections to Chinese state-owned telecom giants and reliance on Hong Kong and China markets are the two most important risk factors that indicate whether a telecommunications service provider is likely to cooperate with Chinese government censorship or surveillance requests.
- Most of Hong Kong's Internet infrastructure—including mobile networks, fixed line broadband networks, and submarine cable systems—is controlled by companies that are either highly intertwined with Chinese state-owned telecoms or completely dependent on the Hong Kong and China markets. Only the data center market in Hong Kong is dominated by foreign companies.
- The four most prominent approaches to restricting Internet freedom in Hong Kong are legal pressure, real name registration, data localization, and control over Internet exchange points. Additional methods include the use of virtualized middleboxes and the technical blocking of circumvention tools.
- Given the predicted high rate of compliance with the government, authorities are likely to rely largely on legislative rather than physical methods of Internet restriction in Hong Kong. This is expected to include legal pressure on companies to cooperate with the Hong Kong National Security Law and

increasing de-anonymization of Internet behavior through real-name registration compliance.

- Indicators of escalating legal pressure include higher rates of unexplained website removals, permanent or longer website blocks, or coordinated website blocks. Legal pressure on entities comes in waves that could emerge with little warning.
- Indicators of escalating efforts to enforce real name registration could include new laws or regulations that enforce de-anonymization in phases. Real name registration is likely to be encumbered by long, drawn-out regulatory and legal processes; past efforts have taken 18 months or more for implementation.
- Data localization as a means of restricting Internet freedom would require a significant departure from Hong Kong's existing policy trajectory, and the regulatory process for doing so would likely take longer than 12 months to implement.
- Control over Internet exchange points could occur without legal or regulatory proceedings and with little advance warning, especially if the National Security Law is interpreted broadly to seize control. Indicators that these points were being used for restrictions on Internet freedom include announced infrastructure updates leading to changes in filtering methods, security systems, or data storage, or significant traffic slowdowns suggesting installation of new restriction hardware.
- Chinese scholars are studying increasing virtualization of HK networks and infrastructure and virtualized middle boxes for censorship.
- Removal of virtual private networks (VPNs) from app stores would depend on the cooperation of tech companies, foreign and domestic. Blocking VPNs is less likely to be effective and will incur significant costs to the business environment.

The report assesses the four main methods for restricting Internet freedom in Hong Kong as follows in the table below.

TABLE 1: ASSESSMENT OF MECHANISMS FOR RESTRICTING INTERNET FREEDOM IN HONG KONG

	Legal Pressure	Real Name Registration	Data Localization	Control over IXPs
Feasibility	High	Medium	Low	Medium
Affordability	High	Medium	Low	Medium
Effectiveness	Medium	Medium	Medium	High
Implementation Speed	High	Low	Low	High
Political Concordance	High	Medium	Low	Medium

2.0 PRC AND HONG KONG VIEWS ON INTERNET FREEDOM

The Chinese Communist Party (CCP) considers control over China's Internet ecosystem to be a vital guarantee of its rule over China and characterizes its governance of the country's Internet as an extension of the nation's sovereignty. Beijing views the governance of the Internet as rule over a cyber society (网络社会) vulnerable to Western infiltration and must therefore be isolated and protected.[1] Specifically, the CCP believes significant domestic unrest and instabilities like the 2009 unrest in Xinjiang and the 2014 Hong Kong protests were mobilized by the Internet with the assistance of foreign influence. As such, regulating the Internet is no longer merely a domestic, administrative matter but a highly political and transnational affair involving Chinese sovereignty and regime security.[2]

2.1 "THERE IS NO NATIONAL SECURITY WITHOUT NETWORK SECURITY": THE CCP AND INTERNET REGULATION

The CCP enforces its control over China's Internet using a patchwork of regulations and legal measures. China had few Internet regulations before 2000, which allowed the Chinese Internet to develop relatively freely. This began to change between 2000 and 2013, when several administrative organizations implemented specific but low-level rules and regulations, which were disorganized and arose *sui generis* (自成体系) compared to those of other countries.[3] During this period, the Internet was loosely regulated by comparatively broad and vague restrictions like the "*Nine Forbidden*" (九不准) content categories laid out in Article 13 of the Interim Provisions on the Administration of Internet Websites Engaging in News Publication Services (互联网站从事登载新闻业务管理暂行规定).[4]

The establishment of the Ministry of Industry and Information Technology (MIIT, 工业和信息化部) in 2008 and the Cyberspace Administration of China (CAC, 国家互联网信息办公室)[1] in 2011 marked a more systematic attempt by the CCP to control, govern, and censor the Internet,[5] characterized by a proliferation of legal measures and rules designed to restrict Internet freedom. Beginning in 2014, the Chinese central government began to assert more systematic governance of the Internet through the creation of the Cybersecurity and Informatization Leading Small Group (网络安全和信息化领导小组), which was later upgraded to a commission and run by the CCP Central Committee's Office of the Central Cyberspace Affairs Commission (中共中央网络安全和信息化委员会办公室), chaired by Xi Jinping himself.[6] While the Cybersecurity Law (网络安全法) implemented by CAC in 2017 does not specify restrictions on internet content, its general provisions categorically prohibit use of the Internet to engage in illegal activities.[7] In 2019, CAC issued Provisions on Ecological Governance of Network Information Content (网络信息内容生态治理规定) that further expanded the "*Nine Forbidden*" content categories

[1] This office is also known as the CCP Central Committee's Office of the Central Cyberspace Affairs Commission (中共中央网络安全和信息化委员会办公室).

into "*Eleven Forbidden*" content categories that defined the parameters of acceptable Internet expression for China's residents.[89]

"Eleven Forbidden" Content Categories in Chinese Internet Content[1011]
1. Violate the fundamental principles set forth in the Constitution (反对宪法所确定的基本原则的);
2. Jeopardize national security, divulge state secrets, subverts state power, or undermine nation unity (危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的);
3. Damage the dignity or interests of the state (损害国家荣誉和利益的);
4. Distort, defame, desecrate, or deny the deeds and spirit of heroes and martyrs, and insult, defame, or otherwise infringe upon the name, portrait, reputation, or honor of a hero or a martyr (歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的);
5. Advocate terrorism or extremism, or instigate any terrorist or extremist activity (宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的);
6. Incite ethnic hatred or discrimination, or undermine ethnic solidarity (煽动民族仇恨、民族歧视，破坏民族团结的);
7. Sabotage state religious policies, or propagate heretical or superstitious ideas (破坏国家宗教政策，宣扬邪教和封建迷信的);
8. Spread rumors to disturb economic and social order (散布谣言，扰乱经济秩序和社会秩序的);
9. Disseminate obscenity, pornography, force, brutality, and terror or crime-abetting (散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的);
10. Humiliate or defame others or infringe upon their reputation, privacy, and other legitimate rights and interests (侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的); and
11. Other content as prohibited by laws or administrative regulations (法律、行政法规禁止的其他内容).[1213]

Beyond a patchwork array of legal regulations and measures intended to restrain Internet freedom in China and protect the Party's rule, the CCP also relies upon the chilling effect of self-censorship in shaping the online behavior and opinions of China's Internet users. Xi himself has stressed the importance of self-policing and distributed responsibility for Internet regulation, proclaiming that in order to increase China's internet governance capability, it needs to "form a comprehensive Internet governance structure led by Party Committees, managed by the government, monitored by the society, and with the participation of self-disciplined netizens combining with economic, legal, technological, and other means."[14] This Internet governance model places the Party (through CAC) and government in leading positions, providing top-level policy design and coordinating subordinate administrative bodies and other entities. State-owned organizations and enterprises act as monitoring and approval authorities for online content, while Internet platform companies act as the "suppliers" that conduct Internet content review and

filtering, and ordinary Internet users conduct "mutual supervision" (相互监督) in a form of self-governing society.[15]

Party authorities and scholars from mainland China have extended these perspectives to Hong Kong's Internet ecosystem and view the city's Internet as a tool for dangerous anti-government mobilization. Some Chinese writers explicitly characterized Hong Kong's "Occupy Central" (占中) protests in 2014 as an unwelcome outcome of new media presence on the Internet where "a few new media representatives were used by Western political powers."[16] Others argued that social platforms have become a medium for Hong Kong's pro-independence elements, harboring cyber warriors (网军) and illegally mobilizing society and colluding with foreign forces.[17] A 2020 research article went further, arguing that the Internet was flooded with "aggressive opinions" of the Hong Kong [pro-democracy] opposition (香港反对派), had become "a tool to control public opinion," and was using Hong Kong pro-democracy opposition to remotely control the violent crowds through social media, specialized social software, or information spread on the Internet in the 2019 Hong Kong protests.[18] These detailed views reflect top-down opinion: Xi Jinping proclaimed in a thinly veiled 2016 reference to Hong Kong unrest that "the Internet is not a territory of outlaws, and any behavior using the Internet to spread any rhetoric of overthrowing the state, instigating religious extremism, promoting national separatism, and inciting violent terrorist activity shall be resolutely stopped and cracked down upon."[19]

2.2 THE VIEW FROM HONG KONG

The Hong Kong Special Administrative Region (HKSAR, 香港特别行政区) apparently agrees with the CCP's assessments. Less than a week after the Hong Kong National Security Law passed on June 30, 2020, the Hong Kong government issued a set of new Implementation Rules for Article 43 of the Law (國家安全法第四十三條實施細則), demanding that all local and foreign-owned online publishing platforms in Hong Kong provide data, remove content, or restrict access to users upon request, which prompted numerous foreign companies such as Facebook, WhatsApp, Google, Twitter, Signal, Zoom, Microsoft, and Telegram to temporarily stop responding to the city's requests for information on users.[20]

Hong Kong officials regard their sweeping power over Hong Kong's Internet as a mandate from the Chinese central government enacted out of grave concern for national security and a duty to maintain the "one country, two systems" constitutional principle. Before the passage of the Hong Kong National Security Law in June 2020, Hong Kong officials lacked the legal framework to act on national security issues. In a letter to all Hong Kong citizens on May 29, 2020, urging the city to support the upcoming Hong Kong National Security Law, Hong Kong Chief Executive Carrie Lam (林鄭月娥) underscored that Hong Kong was unable to use its legislative competence under Article 23 of the Hong Kong Basic Law (香港基本法) to enact matters on national security and public safety even 23 years after returning to China and would remain unable to do so in the foreseeable

future.[21] The Hong Kong National Security Law changed that status quo, giving Hong Kong officials a legal pathway to act in defense of national security broadly defined.

Hong Kong officials' intent to regulate the Internet is clear. The swift promulgation of the Implementation Rules for Article 43 suggests the Hong Kong authorities likely coordinated with the Chinese government in advance to draft internet policing and surveillance policies. Hong Kong has since reiterated its commitment to widespread Internet control. On April 2021, accompanied by the PRC's Director of the Liaison Office of the Central People's Government in Hong Kong (中央政府駐港聯絡辦公室), who stated that "the central government always suits the action to the word" on matters of national security, Lam explicitly asserted that Hong Kong will strengthen its supervision and management of its schools, media, the Internet, and other issues related to national security.[22] Chapter II of the Supplement to Carrie Lam's 2021 Policy Address further states that the HKSAR has been undertaking new initiatives to strengthen cyber and data security and includes indications that the government plans to pass Hong Kong's own cybersecurity law, impose network security obligations on internet providers, and strengthen Hong Kong's critical information infrastructure on cybersecurity issues. [23]

2.3 THE LEGAL FOUNDATIONS OF AN INTERNET CRACKDOWN

All legal mechanisms for restricting Internet freedom in Hong Kong must abide by the provisions of the Hong Kong Basic Law (香港基本法), which was adopted by the Standing Committee of the PRC National People's Congress (NPCSC, 全国人民代表大会常务委员会) in 1990 and took effect in July 1997.[24] The Basic Law replaced Hong Kong's colonial constitution of the Letters Patent and the Royal Instructions, has constitutional status, and takes precedence over all other Hong Kong laws.[25] The Basic Law provides several provisions for fundamental rights and freedom. In particular, Article 30 of Hong Kong Basic Law stipulates that "the freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences."[26]

The Hong Kong Legislative Council has enacted several laws that regulate protection of privacy and freedom on the Internet through Article 75 of the Basic Law, which allows the Council to make its own rules as long as they do not contravene the Basic Law itself.[27] For instance, the Hong Kong Bill of Rights Ordinance (香港人權法案條例), incorporating the International Covenant of Civil and Political Rights, created a general "right of privacy" protecting individuals from arbitrary or unlawful governmental interference with their privacy.[28] The Personal Data (Privacy) Ordinance (PDPO, 個人資料（私隱）條例) protects an individual from collection of personal data by means that are "unfair" in the circumstances of the case, even if the means are lawful. [29] Article 24(c) of the Telecommunications Ordinance (電訊條例) prohibits telecommunications providers from willfully transmitting any message or willfully intercepting, detaining, or delaying any

message, and Article 27 prohibits any person from removing or interfering with a telecommunications installation with intent to intercept or discover the contents of a message.[30] The Interception of Communications and Surveillance Ordinance (ICSO, 截取通訊及監察條例) provides statutory foundation and due process for the authorization and regulation of interception of communication and covert surveillance conducted by law enforcement agencies of serious crimes and protection of public security.[31]

The Hong Kong National Security Law was also passed by the NPCSC,[32] bypassing the normal conventions that constrain the introduction of new laws and kicking off a new era of restrictions on Internet freedom in Hong Kong. According to Article 18 of the Hong Kong Basic Law, the laws in force in the HKSAR shall be the Basic Law, the laws previously in force in Hong Kong, and the laws enacted by the legislature of Hong Kong.[33] Chinese national laws and regulations are generally not applied to the HKSAR. However, Article 18 of the Hong Kong Basic Law provides an exception allowing the NPC Standing Committee to add to or delete from the list of national laws in Annex III of the Basic Law, as long as the change concerns defense, foreign affairs, or other matters outside the limits of the autonomy of Hong Kong, and they consult with the Basic Law Committee.[34] This mechanism was used to bypass the Hong Kong legislature to pass the Hong Kong National Security Law. At around 6 P.M. local time on June 30, 2020, immediately after the passage of the law, NPCSC listed the Hong Kong National Security Law in Annex III of the Hong Kong Basic Law. The HKSAR Chief Executive Carrie Lam promulgated the law in the HKSAR Gazette (香港特別行政區政府憲報) under Article 18 of the Basic Law some five hours later.[35]

The legality of the Hong Kong National Security Law has been a point of contention widely discussed by legal and international affairs academics, practitioners, and politicians domestically and globally. Skeptics have argued that Article 23 of the Hong Kong Basic Law explicitly attributes the legislative competence for such a law to the Legislative Council of the HKSAR, and that Beijing has limited legislative authority vis-à-vis Hong Kong inasmuch as it can only alter national laws related to defense, foreign affairs, and other matters outside the limits of the HKSAR.[36] Critics also claim that criminal offences are vaguely defined in the Hong Kong National Security Law and could be used for politically motivated criminal prosecution, undermining privacy and freedom of speech, as well as curtailing judiciary independence, under the pretext of national security. This concern is heightened by the protective principle of the law, which allows the Chinese and Hong Kong authorities to regulate extraterritorial conduct by foreigners or non-residents.[37]

In response to these detractors, at least one prominent supporter of the Hong Kong National Security Law has argued that its passage fills a regulatory gap to restore public order exposed when a 2003 attempt to pass a national security law failed.[38] Beijing argues that it is entitled and obliged to do just that.[39] For example, the vice chairman of the Hong Kong Bar Association, Paul Lam Ting-kwok (林定國), asserted that Article 23 only delegates a part of legislative competence on national security to HKSAR, an

extremely unique situation under the one country, two systems (一國兩制) constitutional principle; the language of Article 23 should not be regarded as the Chinese central government relinquishing its power to legislate in Hong Kong on the grounds of national security.[40] Lam further claimed that since both Hong Kong Basic Law and National Security Law were adopted by the NPCSC, they should be considered at the same hierarchical level, such that the Basic Law comprises constitutional, general principles of law, and the National Security Law details special provisions for the Basic Law.[41]

2.4 AN EMPHASIS ON ENFORCEMENT

Legal contention aside, the Hong Kong Police Force (HKPF, 香港警務處) has garnered attention for requesting user data or removals of Internet content from Internet providers long before the enactment of the Hong Kong National Security Law. During previous unrest in Hong Kong, the HKPF attempted to restrict Internet content, often without legal basis. Between February 2013 and February 2014, the HKSAR registered 5,507 requests for Internet user data and content deletion, the vast majority of which (4,557) came from the HKPF with requests to "prevent and detect crimes involving high technology and Internet crime," very few of which had obtained court warrants.[42]

Since the Hong Kong National Security Law was introduced in 2020, the HKPF has further focused on enforcement operations on the Internet as a matter of declared policy. The then-head of the HKPF Chris Tang Ping-keung (鄧炳強) added "liabilities" to the existing language of "risks associated with the Internet and social media" in the 2020 Commissioner's Operational Priorities (2020 年警務處處長首要行動項目), signaling HKPF's shifting focus to Internet governance from conventional cybersecurity and technology crimes.[43] After his promotion to become the head of the HKSAR Security Bureau, Tang amplified Lam's rhetoric that Hong Kong's social media and Internet lack supervision and announced that LIHKG (連登討論區), Hong Kong's largest forum website, will be the focus of its investigation for illegal posts and information.[44] Echoing Lam's 2021 Policy Address, Tang stated the Hong Kong authority expects the Legislative Council (LegCo, 立法會) to work on a legislative proposal for a cybersecurity law to regulate Internet providers under Article 23 of the Hong Kong Basic Law due to the increase in cyberattacks in recent years.[45]

This shifting emphasis in enforcement is also reflected in the HKPF's technical elements. The new head of the HKPF, Raymond Siu Chak-yee (蕭澤頤), stated that the force will "expand its intelligence network and keep an eye on whether anyone incites violence on the Internet."[46] The HKPF has been expanding its Cyber Security and Technology Crime Bureau (CSTCB, 網絡安全及科技罪案調查科), a HKPF organ staffed with more than 350 personnel, growing the technology crime team, the cybersecurity team, and the Internet intelligence team, which targets individuals' Internet and social media activities for surveillance purposes.[47] In January 2021, the then-head of the HKSAR Security Bureau, John Lee Ka-chiu (李家超), stated that while the Interception of Communications and Surveillance Ordinance (截取通讯及监察条例) applies to all kinds of electronic

information, including social media platforms, all national security-related interceptions and surveillance are governed by the Implementation Rules for Article 43 of NSL, an entirely separate mechanism that eliminates the need for prior judicial approvals. [4849]

As Hong Kong authorities move to establish sufficient legal justification to restrict and monitor Hong Kong's Internet, they must also articulate and enact practical implementation measures. The remainder of this report addresses the key components needed to implement surveillance and censorship in Hong Kong's Internet ecosystem, covering the key organizations that would be involved in such activities, summarizing critical parts of Hong Kong's Internet infrastructure that could be targeted, and describing a variety of possible mechanisms for restricting or limiting Internet freedom in Hong Kong.

3.0 KEY ORGANIZATIONS

Much of the legal scrutiny of recent restrictions on Internet freedom in Hong Kong focuses on the Hong Kong National Security Law, which was designed and actual enforced by a patchwork group of government organizations. Brief descriptions of these organizations follow below.

3.1 COMMITTEE FOR SAFEGUARDING NATIONAL SECURITY OF THE HKSAR

The Committee for Safeguarding the National Security of the HKSAR (香港特別行政區維護國家安全委員會舉行首次會議, or 國安委) was established under Article 12 of the National Security Law on July 3, 2020.[50] Article 14 lays out the role of the Committee, which is to:

1. "analyze and assess developments related to safeguarding national security in the HKSAR, make work plans and formulate policies for safeguarding national security in the HKSAR;
2. In order to safeguard national security, advance the development of the legal system and enforcement mechanisms of the HKSAR; and
3. Co-ordinate major work and significant operations for safeguarding national security in the HKSAR." [51]

The Committee is empowered to operate with little public scrutiny. Its actions are confidential, its decisions are not subject to judicial review, and individuals and entities are prohibited from interfering with the actions of the Committee.[52] The Committee is supervised by and accountable to the PRC government.[53] The PRC government also appoints a National Security Advisor, who serves as a non-voting delegate and advises the Committee.[54] The Committee can direct the Hong Kong Police Department's National Security Bureau (newly created under the Hong Kong National Security Law) to undertake actions related to protecting national security. The new office in the Justice Department of the HKSAR related to national security likewise must seek approval from the Committee. The Committee is also involved in approving judges who will be designated to deal with cases involving the endangerment of national security.[55] Chinese government offices stationed in Hong Kong and dedicated to protecting national security should work in tandem with the Committee to oversee and guide related work.[56]

The Committee is also empowered to vet the city's prospective leaders with its characteristic opacity. According to new election measures released by the PRC in 2021, the Committee has a role in vetting candidates for the legislative council. The Committee, according to investigations run by the Hong Kong Police Department's National Security Division, will determine whether a candidate meets the specified standards of loyalty to the PRC and other conditions. If they do not meet these standards, a copy of the relevant report will be forwarded to the election committee (a newly established body for vetting candidates).[57]

There has been no public information relating the Committee to Internet control laws directly, but the Committee's sweeping role in all personnel appointments, national security law cases, and police action indicates that it could influence related policy and enforcement. In particular, its ability to direct police investigations means that it could choose how the Hong Kong National Security Law is enforced—including the response to ISPs that refuse to cooperate with the government, or individuals who post illegal content online. Similarly, since the Justice Department's national security bureau must consult the Committee on decisions, it can determine how strictly Internet laws are enforced.

The Committee is chaired by Hong Kong's Chief Executive, Carrie Lam, and includes Chief Secretary for Administration Matthew Cheung Kin-chung (張建宗), Financial Secretary Paul Chan (陳茂波), Secretary for Justice Teresa Cheng (若驊資), Secretary for Security John Lee (李家超), Commissioner of Police Tang Ping-keung (鄧炳強), Deputy Commissioner of Police (National Security) Edwina Lau (劉賜蕙), Director of Immigration Au Ka-wang (區嘉宏), Commissioner of Customs and Excise Hermes Tang (鄧以海), and Director of the Chief Executive's Office Chan Kwok-ki (陳國基), who serves as the secretary general of the committee.[58] The Committee appointed Luo Huining (駱惠寧), who is the Director of the Liaison Office of the HKSAR, as a National Security Advisor, a non-voting role established in Article 15 of the Hong Kong National Security Law.[59]

3.2 OFFICE OF THE COMMUNICATIONS AUTHORITY

The Office of the Communications Authority (OFCA) is the main enforcement unit for telecommunications and broadband regulations, including unlicensed service provisions and failures to abide by conditions of service. OFCA, with the Communications Authority, will be the investigation and enforcement unit for rules like Hong Kong's new SIM-card real-name registration law.[60] OFCA will perform the on-the-ground work engaging stakeholders and operators to prepare to abide by the real-name regulations.[61] OFCA may also be involved in ensuring that UCLs and other ISPs follow government orders to censor content. They are the unit that licenses ISPs, so they may be asked to suspend licenses if there are violations (though OFCA and the Communications Authority are not directly referenced in the Implementation Guidelines of the NSL).[62] OFCA, as the main government agent to liaise, consult with, inspect, and govern telecommunications and broadband providers, is likely to be highly involved in ensuring compliance with any censorship or surveillance laws through drafting specific "codes of practice," responding to complaints, inspecting physical locations, and suspending licenses.

The Communications Authority was established in 2012 under the Communications Authority Department's Regulations (通訊事務管理局條例), which dissolved the previous Telecommunications Authority and Broadcasting Authority and reformed the organization as the Communications Authority.[63] The OFCA was established under provision 16 as an

organization that supports the director-general of the Communications Authority.[64] The main roles that the OFCA undertakes are:

1. "Dealing with and managing telecommunications services and broadcasting services.
2. Managing Hong Kong's wireless frequency.
3. Provide consultation, planning, and assistance services to the government regarding telecommunications, broadcasting, and anti-spam messages.
4. Supervise implementation standards and serve as the government representative in international affairs.
5. Enforce regulations regarding unsolicited electronic messages; and
6. Ensure the telecommunications industry and the broadcasting industry adopt fair commercial tactics and advance fair competition."[65]

There are five main offices under the OFCA: the regulation work office, the implementation office, the marketplace and competition office, the broadcasting work office, and the support office.[66]

OFCA publishes an annual work report of its main initiatives. In 2021, it planned to focus on 5G expansion (in cooperation with other departments), rolling out high-speed Internet to rural areas, monitoring Internet land usage, re-assigning the mobile service spectrum, and regulating telecom and broadband services and equipment.[67] Its daily business centers on granting licenses and enforcing permits and regulations, including physical telecom infrastructure construction guidelines and spectrum usage rules. It ensures that providers abide by service contracts and communicate about terminations of service with customers.[68] OFCA has a supervisory and enforcement role for all broadband and telecom-related services in Hong Kong.

The Communications Authority and OFCA often have overlapping roles in enforcing broader regulations authored by the legislative council.[69] Both units enforce the Competition Ordinance, the Fair Trading Sections of the Trade Descriptions Ordinance, and the Unsolicited Electronic Messages Ordinance.[70] The Communications Authority releases regular statements that guide the development of the telecommunications and broadband industries, and codes of practice and guidelines for the industries.[71] OFCA releases reports on service outages and technical developments, as well as "consultancy reports" on specific technical questions.[72] OFCA manages relationships with service providers, approving licenses, reviewing complaints, and responding to enquiries.[73]

3.3 INTERNET INFORMATION LIAISON GROUP

The Internet Infrastructure Liaison Group (IILG, 互聯網基建聯絡小組) was established by the Office of the Government Chief Information Officer (OGCIO) in 2005.[74] It is the only cooperative framework that organizes all Internet infrastructure stakeholders in Hong Kong. The IILG "mechanism" is intended to respond to "major events," "incident outbreaks," or natural disasters,[75] and the group holds roundtable meetings to coordinate

risk mitigation strategies. The IILG framework could be coopted for national security incidents that are construed as "emergencies," serving as the collaborative mechanism for any rapid crackdowns taken on by various organs simultaneously.

All government units that operate with relation to Internet infrastructure are members of this group, which is chaired by the Deputy Government Chief Information Officer. The official members are:[76]

- Office of the Government Chief Information Officer (OGCIO)
- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)
- Hong Kong Internet Exchange (HKIX)
- Hong Kong Internet Registration Corporation Limited (HKIRC)
- Hong Kong Internet Service Providers Association (HKISPA)
- Hong Kong Police Force (HKPF)
- Office of the Communications Authority (OFCA)

The group's stakeholders, which include official IILG members and major Internet service providers, cooperate to achieve the following:[77]

- "share first-hand information;
- facilitate the formulation of rapid and coordinated response;
- align actions and media response if appropriate; and
- plan on contingency measures"

IILG's "terms of reference" are:[78]

- "To provide a forum of exchange on issues concerning the smooth operation including stability, security, availability and resilience of the Internet Infrastructure of Hong Kong;
- To facilitate the stakeholders to formulate rapid and coordinated response in case of major incident outbreaks that will affect the smooth operation of the Internet infrastructure of Hong Kong; and
- To promote IT management best practices, experience and knowledge sharing and mutual assistance among members of the Liaison Group on protection of the Internet infrastructure of Hong Kong."

In the last two years, the IILG has addressed issues like DDoS attacks, DNS security, community testing programs (pandemic-related), vigilance against cyberattacks, DNS hijacking, and even highly specific projects, like "Protections against Vulnerability in Microsoft Windows Remote Desktop Services," and "Removal of the Old Key Signing Key (KSK-2010) of DNSSEC Root Zone."[79]

3.4 HONG KONG SECURITY BUREAU

The Hong Kong Security Bureau (香港特別行政區政府的保安局) serves as the HKSAR's superordinate body for managing law enforcement, immigrations and customs control, and emergency services.[80] Since the passing of the Hong Kong National Security Law, the Hong Kong Security Bureau (保安局) has been charged with coordinating various law enforcement agencies to enforce the legislation. These include the Hong Kong Police Force (香港警務處), Hong Kong Customs Enforcement (香港海關), the Hong Kong Immigration Department (入境事務處), prisons and correctional services (懲教署), the Fire Services Department, and the Government Flying Service (政府飛行服務隊).[81] Members of the aforementioned services are also cleared to be deputized to the Security Bureau in order to act as "special police" (特務警察) in order to augment the manpower of the HK security forces and deal with emergency situations.[82]

3.4.1 HONG KONG POLICE FORCE

Among the myriad institutions the Hong Kong Security Bureau coordinates that undertake national security work, the Hong Kong Police Force (香港警務處, HKPF) undertakes the lion's share of activities pertaining to surveilling and prosecuting subversive online activity. The HKPF operates several specialized departments under the auspices of the commissioner of police.[83] Within the HKPF's organizational structure, three departments maintain portfolios related to monitoring online activity. These are the "B Department," which handles Crime and Security, the "D Department," which handles management services, and the "NS Department," which is responsible for enforcement of the Hong Kong National Security Law.

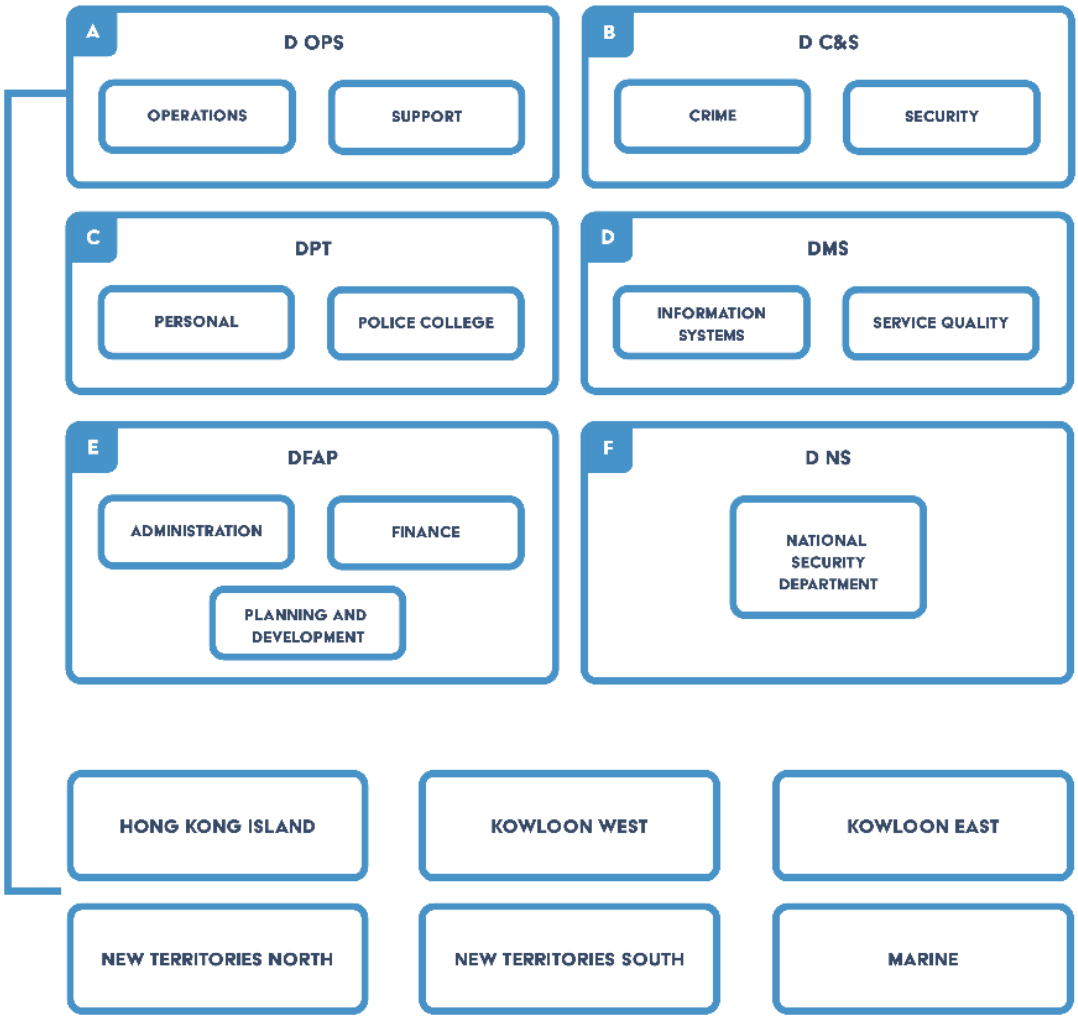

FIGURE 1: ORGANIZATIONAL STRUCTURE OF THE HKPF[84]

3.4.1.1 'B' DEPARTMENT (CRIME AND SECURITY)

HKPF's 'B' or "Crime and Security Department" (乙部門 (刑事及保安處)) is the Force's main organ for undertaking criminal investigations. The Department operates several sub-bureaus charged with combatting illicit activities including commercial malfeasance, narcotics trafficking, and anti-racketeering.

B Department's main instrument for surveilling and investigating computer crime is its Cyber Security and Technology Crime Bureau (網絡安全及科技罪案調查科, CSTCB).[85] The institution was originally known as the Technology Crime Division of the Commercial Crime Bureau (TCD CCB) before being upgraded to full Bureau status in 2015. CSTCB is charged primarily with "maintaining the cyber security of Hong Kong and preventing and detecting computer crimes."[86] Its mission set includes:

1) Enhancing public awareness of computer and cyber security as well as the risks and liabilities associated with the Internet and social media through a multi-agency approach.
2) Enhancing cooperation with other law enforcing agencies and stakeholders to target technology crime.
3) Strengthening coordination and sharing of expertise in handling and investigating technology crime.
4) Enhancing investigative and intelligence gathering capabilities for tackling technology crime. [87]

In addition to these functions, the CSTCB also operates the Collaboration Team of the Cybersecurity Division (網絡安全組協作隊, CoI CSD), which is "responsible for the formulation and implementation of crime prevention programs and raising the awareness of technology crime prevention techniques amongst the general public."[88]

According to its website, one of the core functions of CSTCB is "proactively liaising with major Internet Service Providers" within the HKSAR.[89] This suggests that CSTCB is tasked with requisitioning information from ISPs relevant to criminal investigations and may be how the HKPF transmits requests to restrict access to proscribed websites. However, the exact nature of these liaison relationships is unclear, and there is little publicly available information detailing their function. To wit, in a 2017 session of Hong Kong's Legislative Council, officials observed that the HKPF does not maintain records of the number of cases where ISPs rejected requests for information on users, nor does it keep a statistical record of the number of cases where the Force had to apply for search warrants to obtain information from ISPs.[90] That same session featured testimony that noted that information that can potentially be requisitioned from ISPs is often restricted by the regions that the providers are located in, as well as internal policies regarding retention of information.[91]

3.4.1.2 'D' DEPARTMENT (MANAGEMENT SERVICES)

HKPF's 'D' or "Management Services" Department (丁部門 (監管處)) plays a major role in maintaining technical infrastructure used for network surveillance as well as other miscellaneous administrative functions.[92] The Department maintains a Communications Branch, which is responsible for maintaining HKPF telecommunications hardware and software such as radios, telephones, and other electronic equipment, as well as an IT Branch, which is tasked with maintaining HKPF network and information systems. [93] Additionally, in 2019 the Department established an Innovation and Solution Lab (創新方案實驗室) which is tasked with undertaking research and development of digital technologies used to "streamline and refine police work."[94] The Lab also conducts technical and market research aimed at enhancing the Force's ability to utilize new technologies.[95]

3.4.1.3 NATIONAL SECURITY (NS) DEPARTMENT

The HKPF's National Security or NS Department (國家安全處) was formed in 2020 in the wake of the promulgation of the Hong Kong National Security Law.[96] It is tasked with conducting investigations into violations of the law as well as undertaking operations to ensure enforcement. The NS Department defines its primary areas of responsibility as follows:

1) Collecting and analyzing intelligence and information concerning national security.
2) Planning, coordinating, and enforcing measures and operations for safeguarding national security.
3) Investigating offenses endangering national security.
4) Conducting counter-interference investigations and national security review activities.
5) Carrying out tasks for safeguarding national security assigned by the Committee for Safeguarding National Security of the Hong Kong SAR.
6) Performing other duties and functions necessary for enforcement of the National Security Law.[97]

Under the provisions of the Hong Kong National Security Law, the NS Department is empowered to conduct electronic surveillance of persons suspected of activities that jeopardize national security.[98] It also has the authority to enlist the help of ISPs in undertaking investigations and can issue takedown notices for websites and platforms which host objectionable content.[99] Notably, the Department only needs the approval of the Hong Kong Chief Executive to exercise these powers, rather than a court order.[100] In the year since its establishment, the NS Department has made a number of high-profile arrests for violations of the Hong Kong National Security Law, with charges ranging from "colluding with hostile foreign forces" to posting objectionable material on social media.[101] [102] [103] Arrests for social media activity appear to be relatively uncommon, at least in comparison to the number of arrests for activities that occur in real life rather than in cyberspace. However, it is unclear if this is because social media surveillance is not a HKPF priority, or if the implementation of the Hong Kong National Security Law had a "chilling effect" on Internet discourse. Widespread anecdotal evidence supports the latter hypothesis, with many denizens of Hong Kong scrubbing their public social media feeds in the wake of the Hong Kong National Security Law's implementation.[104]

In addition to its role as a prosecutorial and enforcement body, the NS Department is likely carrying out much of the work behind Hong Kong's nascent forays into Internet censorship. Since 2020, there have been several instances in which the HKPF has asked ISPs to take down material deemed to be in violation of the Hong Kong National Security Law.[105] Most of these takedown requests appear to have been for websites that are perceived as explicitly encouraging secession, such as sites maintained by pro-democracy advocacy groups in Hong Kong, or are associated with political activity in Taiwan (e.g., the website of the Democratic Progressive Party).[106] It remains to be seen

whether these censorship efforts will remain small-scale and targeted, or if this merely presaged a wider effort by Beijing to exert control over Internet content in the HKSAR.

3.4.2 COORDINATION EFFORTS BETWEEN HKPF AND PRC SECURITY ORGANS

The degree to which Hong Kong security forces coordinate with their mainland counterparts remains unknown. Currently, there is no public information detailing collaboration between the HKPF and PRC security forces, and Hong Kong security officials have refused to comment on the degree to which the HKPF will coordinate with its mainland counterparts.[107] However, both of the PRC's premier security services, the Ministry of State Security (MSS) and PRC Ministry of Public Security (MPS) have issued statements pledging to "direct and support" efforts by HKPF to investigate and prosecute crimes that violate Hong Kong's National Security Law.[108]

3.5 INTERNET REGULATORY AUTHORITIES

The HKSAR oversees a suite of organizations tasked with preventing and mitigating cybercrime and network intrusions outside the police force. These entities maintain mission portfolios that are ostensibly apolitical and focus mainly on tasks such as cyber incident response. Nevertheless, this network security apparatus has been instrumentalized in achieving policy ends in several instances. Hence, the following should not be conceptualized as a "comprehensive Internet censorship apparatus," but rather as a "tool kit" of institutions that the Hong Kong government may selectively use to disrupt activity deemed to be seditious.

3.5.1 GOVERNMENT INFORMATION SECURITY RESPONSE OFFICE (GIRO)

The Hong Kong Government Information Security Incident Response Office (GIRO) is a government-wide institution that acts as a main authority for coordinating cybersecurity incident response tasks. Its core membership is comprised of representatives from the Office of the Government Chief Information Officer, the Hong Kong Security Bureau, and the Hong Kong Police Force.[109] GIRO also provisionally employs staff members from Information Security Incident Response Teams (ISIRT), who are invited to assist the Office's operations when necessary, depending on the nature of the incident in question.[110] Its core functions include:

- Maintaining a central inventory and overseeing the handling of all information security incidents involving the Hong Kong government.
- Preparing periodic statistical reports on cybersecurity incidents involving the Hong Kong government
- Acting as a central office to coordinate responses to simultaneous attacks on government information systems.
- Enabling information exchanges among departmental ISIRTs.
- Forming and coordinating a "special task force" in the event of a cybersecurity incident that affects "multiple [bureaus and departments] and/or the overall operation and stability of the Government as a whole."[111]

To carry out these functions, GIRO acts as the central contact point for ISIRT branches across the Hong Kong government and as the central coordinating body for whole-of-government responses to major incidents.[112] In keeping with this role, it frequently coordinates with both GovCERT.HK and HKPF's Cyber Security and Technology Crime bureau when necessary.[113]

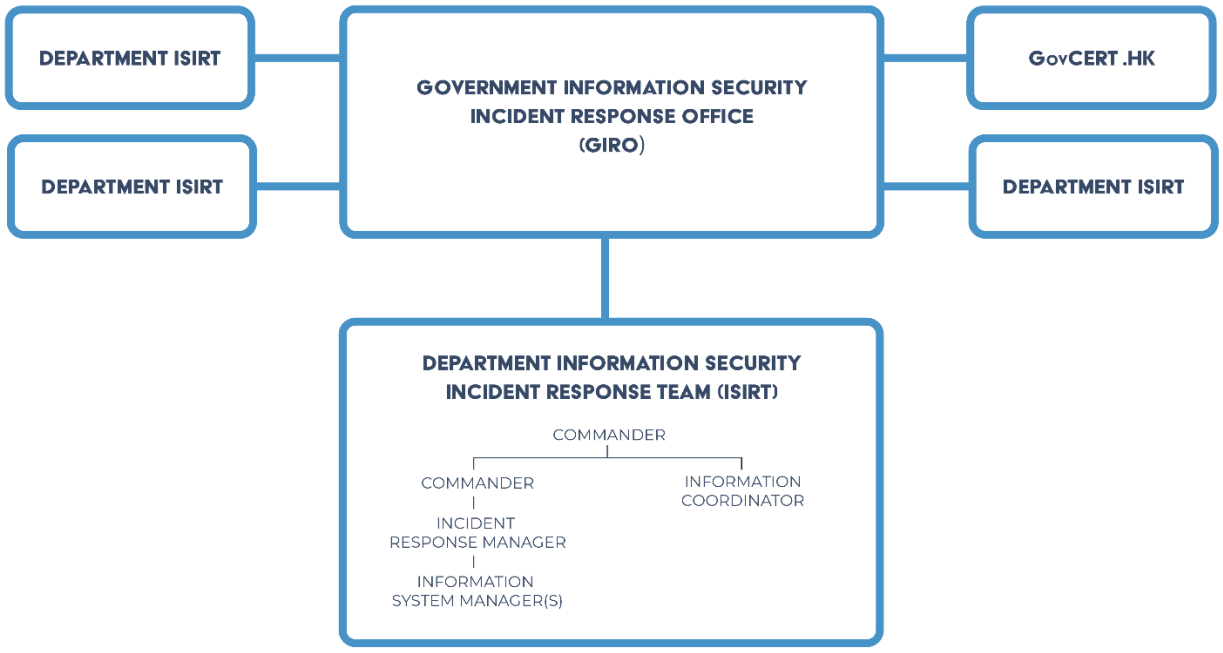

FIGURE 2: OUTLINE OF THE GIRO ORGANIZATIONAL STRUCTURE[114]

3.5.2 GOVERNMENT COMPUTER EMERGENCY RESPONSE TEAM HONG KONG (GOVCERT.HK)

Government Computer Emergency Response Team Hong Kong (政府電腦保安事故協調中心), or GovCERT.HK, is a cybersecurity emergency response team tasked with addressing incidents affecting the HKSAR government,[115] and is therefore likely a major stakeholder in restricting or circumscribing Internet freedom in Hong Kong. GovCERT.HK was established in April 2015 and acts as a government-wide coordinating body for IT administrators and departmental incident response teams.[116] Its main areas of responsibility include:

- Acting as a "bridge" between HKCERT and other incident response teams within government.
- Coordinating and advising government departments in directing responses to information security incidents.
- Disseminating threat intelligence security alerts, advisories, and other relevant information.
- Promoting security awareness within the general public.

- Collaborating with the wider CERT community and industry stakeholders to share information related to security threats. [117]

3.5.3 HONG KONG COMPUTER EMERGENCY RESPONSE TEAM (HKCERT)

The Hong Kong Computer Emergency Response Team (香港電腦保安事故協調中心) or HKCERT serves as the main cybersecurity incident response center within the Hong Kong SAR.[118] The CERT is managed by the Hong Kong Productivity Council (香港生產力促進局).[119] Its mission set includes responsibilities such as:

- Facilitating the dissemination of public information related to cybersecurity.
- Providing advice on taking active measures to prevent security threats.
- Promoting information security awareness. [120]

In order to achieve these goals, HKCERT routinely collaborates with organs within the Hong Kong government such as HKPF and the Office of the Government Chief Information Officer to promote campaigns such as the annual "Build a Secure Cyberspace" (共建安全網絡) program, which is designed to raise general public awareness about cybersecurity issues.[121]

In addition to working with local stakeholders to safeguard cybersecurity, HKCERT maintains a close working relationship with the PRC's National Computer Network Emergency Response Technical Team/Coordination Center (国家互联网应急中心), or CNCERT/CC. A notable instance of coordination between the two organizations occurred during the 2014 "Occupy Central" protests, when both entities worked closely together to combat hacktivist activity connected to the "OpHongKong" campaign. According to a report issued by CAC the two entities exchanged intelligence on websites that attackers intended to target, and jointly coordinated policy to mitigate damage done to the targeted websites.[122] The report concluded by emphasizing the importance of close bilateral cooperation in "preventing social incidents brought about by large-scale network attacks" (避免因大量网络攻击而引发社会事件).[123] In addition to coordinating on incident response work, CNCERT/CC and HKCERT collaborate in publishing materials such as the "Hong Kong Google Play Store App Security Risk Report" and routinely participate in local security conferences.[124]

3.5.4 OFFICE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA

The Hong Kong Office of the Privacy Commissioner for Personal Data (香港個人資料私隱專員公署, PCPD) is an independent regulatory body tasked with overseeing implementation of Hong Kong's Personal Data Privacy Ordinance (個人資料（私隱）條例, PDPO).[125] According to the Office's official website, its core mission entails "ensuring the protection of individual privacy" through "promoting a culture of protecting and respecting personal data."[126] Ostensibly, the Office's charter suggests that it acts as a bulwark against administrative and surveillance overreach by law enforcement. However, this role appears to have been at least partly obviated by the 2020 NSL, which supersedes

the PDPO in instances where the two conflict.[127] Indeed, within the past year, the Office appears to have been deputized in the effort to combat "secessionist activity" within Hong Kong. For example, in October of 2021 the Office announced that it would serve as the main enforcement body for the Personal Data (Privacy) Amendment Ordinance 2021, colloquially known as the "anti-doxxing" ordinance. [1282] According to the enacted legislation, the Office would be tasked with carrying out "criminal investigations and prosecutions for doxxing and related offenses." The ordinance is widely regarded as a response to the 2019 anti-extradition protests, which saw repeated instances of pro-democracy activists exposing the personal information of HKPF officers.[129] Critics have charged that the law is written to be intentionally vague, providing government prosecutors with a far-reaching legal cudgel that could be used to silence dissent.[130]

[2] "Doxxing" is an Internet slang term which refers to unauthorized targeted release of personal data through public forums such as social media platforms or forums with intent to cause harm.

4.0 HONG KONG'S INTERNET INFRASTRUCTURE

The sections below survey major components of Hong Kong's Internet infrastructure, including its Internet service providers, major data centers, Internet exchange points, autonomous system numbers, and submarine cable landing stations allocated to the city. The sequence in which these components are covered in the discussion below reflects a very general depiction of how these components interact with a typical Internet user and with each other. The depiction of these relationships in the diagram below is not a comprehensive description of events and paths mapping Internet traffic, which can vary significantly depending on network infrastructure and how users employ it. Instead, the diagram below is a rough representation of where these infrastructure components are situated relative to Internet users.

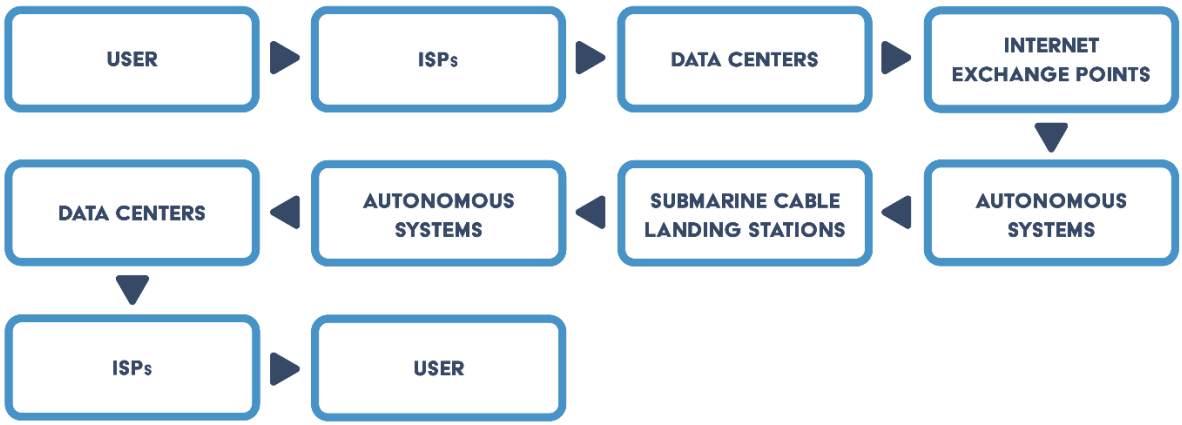

FIGURE 3: REPRESENTATION OF MAJOR INTERNET INFRASTRUCTURE COMPONENTS

4.1 HONG KONG INTERNET SERVICE PROVIDERS

The Hong Kong Communications Authority (CA) divides Internet service providers (ISPs) into four main classes, defined by the types of services they provide and the strength of the licensing requirements.[131] In the Hong Kong legislative context, ISPs provide any sort of Internet or communications services, and are not all network service providers (as in the U.S. context). The first three "classes" of licensees are Service-Based Operators (SBOs). SBOs who provide Class 1 or Class 2 services are "local voice telephony" providers, and are differentiated by whether they provide all services of conventional telephone carriers, and fulfill all license conditions of carrier licenses (Class 1 has stricter requirements, while Class 2 has minimal requirements for consumer protection only).[132] Class 1 and Class 2 SBOs assign Hong Kong telephone numbers, and allow customers to make and receive calls with other Hong Kong numbers.[133] Hong Kong has six currently registered Class 1 or Class 2 SBOs.[134]

Class 3 SBOs provide services using circuits leased from fixed telecommunications network services licensees, fixed carrier licensees, or unified carrier licensees (Class 3 licensees are not permitted to establish or maintain their own circuits).[135] These services include external telecommunications (communication to places outside of Hong Kong),

value-added services for telephone communications, mobile virtual networks, radio relay, teleconferencing, private payphones, security and alarms, and aircraft mobile communications services.[136] Class 3 SBO licensees are dependent on the physical infrastructure of other licensees to provide their services, and are the most common type of SBO licensee in Hong Kong. There are 248 currently licensed Class 3 SBOs.[137]

The fourth type of ISP license, which most closely resembles the U.S. conception of that term, is the Unified Carrier License (UCL). UCLs are the only type of carrier license that permit the provision of fixed, mobile, or combined services.[138] Companies that possess UCLs establish and maintain telecommunications networks and facilities that are available to the public and can apply to provide mobile virtual network services as well.[139] There are currently 27 licensed UCLs in Hong Kong.[140]

While most Internet governance laws in Hong Kong treat ISPs as a unified category, the burden of enforcing government network policies, like blocking websites, falls on UCL companies. Since Class 3 SBOs depend on UCL companies for their physical infrastructure, censorship or regulatory actions taken at the UCL level will affect the SBOs. This analysis focuses almost exclusively on UCL companies, hereinafter referred to as UCLs, given that they, as the network providers, are the entities who can enforce government censorship or surveillance.

4.1.1 HONG KONG'S UNIFIED CARRIER LICENSEES

Loosely, Hong Kong's 27 UCLs can be divided into three categories of ownership: government-owned, foreign/private, and domestic/private. While ownership categories do not fully account for a UCL's relationship with governmental authorities—for example, some have larger physical infrastructure investments in Hong Kong, and are thus more bound to the Hong Kong market and related governing rules—their relationships to the government can largely be summaries in these three categories.

Ten of the UCLs described above are fully or partially owned by the Chinese government—either the mainland government or the Hong Kong authorities. China Mobile, a partially government-owned telecommunications company and the largest mobile phone provider in the world, operates two licensed UCLs in Hong Kong: China Mobile Hong Kong (CMHK) and China Mobile International (CMI).[141] CMI provides the physical infrastructure to connect overseas, owning two cable landing stations that land some of Hong Kong's newest and most-used cable systems.[142] CMI also has a new submarine cable that connects Hong Kong to Hainan, which has been viewed as integral to China's "Belt and Road Initiative" (BRI).[143] CMHK is a significant investor in Hong Kong's broadband and fiber services, working to expand broadband infrastructure to remote villages and providing broadband services to Hong Kong consumers.[144] CMHK also has one of the most extensive 5G networks in Hong Kong and was rated the fastest 5G provider in the region.[145]

State-owned telecom giants China Unicom and China Telecom both operate in Hong Kong as well, along with ComNet Telecom (HK), which is owned by the state-run CITIC Group Corporation (中国中信集团有限公司).[146] None of these three are licensed as mobile or fixed-line providers in the region, unlike China Mobile. These state-owned companies have varying levels of infrastructural investment in Hong Kong. China Telecom was the first Chinese state-owned Internet provider to partner with a local Hong Kong fixed network provider to connect the mainland and Hong Kong networks in 2000, when they partnered with HGC to create a "Guangzhou-Shenzhen-Hong Kong SDH Ring."[147] China Telecom also owns one of Hong Kong's largest carrier and cloud neutral data centers, in cooperation with Daily-Tech and Global Switch. The data center is in the TKO Industrial Estate, by three of Hong Kong's cable landing stations.[148] However, the company did not open its first brick-and-mortar store in Hong Kong until 2018.[149] China Unicom and ComNet are provide largely value-added Internet services in the region and are less active than China Telecom.[150]

The Chinese government through the State-owned Assets Supervision and Administration Commission (SASAC) also owns a partial share of PCCW, Hong Kong's primary fixed-line carrier, since SASAC-controlled China Netcom (now China Unicom) acquired a 20 percent share of PCCW in 2005.[151] This ownership shift has changed how PCCW functions in the market. The same year that China Unicom purchased shares, PCCW and China Netcom announced a "strategic alliance" to develop business in the mainland.[152] China Netcom began exerting its shareholder power over PCCW when the chairman, Richard Li, tried to sell his controlling share to foreign companies (both an Australian and a U.S. company offered $7 billion). China Netcom intervened and refused to allow the sale on nationalist grounds.[153] China Unicom's current stake in PCCW has dropped to 18.4 percent, but the state-backed entity maintains its hold on the company, including through personnel: Mai Yanzhou, a senior vice president at China Unicom, serves as a non-executive director of PCCW.[154]

PCCW, which is itself a UCL, controls two other UCLs in Hong Kong. The first is Hong Kong Telecom (HKT), which it acquired in 2000. Hong Kong Telecom, like PCCW, has long had a state-owned telecommunications firm as its second largest stakeholder. In 1990, CITIC was HKT's second-largest stakeholder, and in 1998, China Telecom took over as HKT's second-largest stakeholder.[155] A year after PCCW acquired HKT, it joined in a 50-50 partnership with the Australian UCL Telstra to create a new UCL called Reach, which was founded to offer IP backbone services.[156]

Along with the eight UCLs with ties to the mainland government, there are two small UCLs which are owned by the Hong Kong government. The first of these, Towngas Telecommunications Fixed Network Ltd., is owned by the Hong Kong government and China Gas Company Ltd., which was previously a public utilities company and is now 42 percent controlled owned by private shareholders and 49 percent by the public.[157] The second, TraxComm Limited, is owned by a state transit organization, the MTR Corporation.[158]

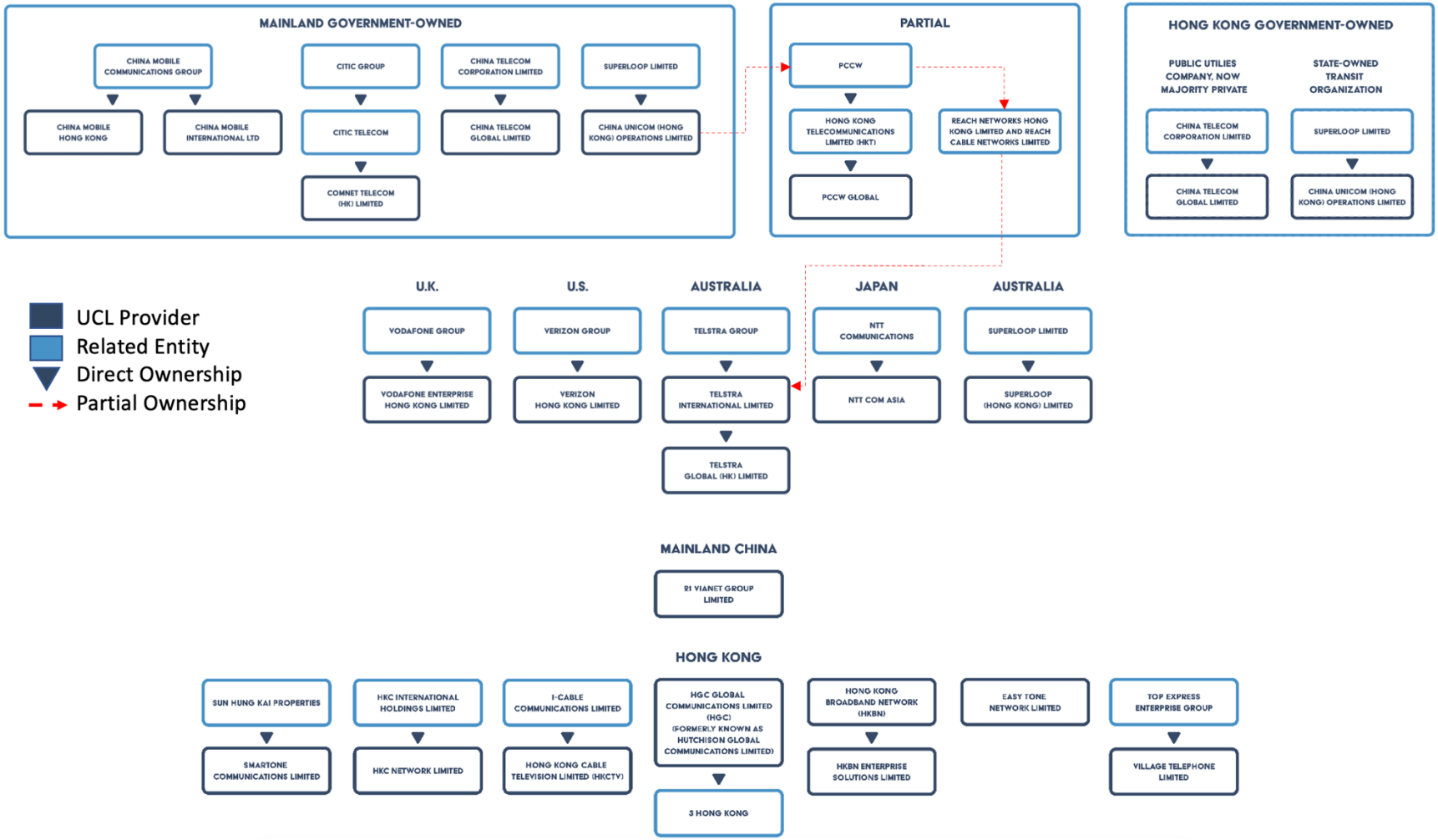

FIGURE 4: MAJOR HONG KONG INTERNET SERVICE PROVIDERS

4.1.2 FIXED NETWORK AND MOBILE NETWORK PROVIDERS

Hong Kong has seven major licensed fixed network providers: CMHK, HKBN, HKCTV, HGC, PCCW-HKT, SmarTone, and HKBN Enterprise Solutions.[159] Of these main fixed providers, CMHK and PCCW-HKT are state-owned and partially state-owned respectively, and either already cooperate or are highly likely to work with the government to restrict Internet freedoms. Information on Hong Kong's fixed network providers, including several minor ones, is included in Table 1 below.

In 2018, the Hong Kong government launched an initiative to expand its fiber-optic infrastructure into rural villages.[160] The government selected two licensed fixed fiber providers, CMHK and PCCW, to lead the official efforts to expand Hong Kong's fiber broadband network. CMHK and PCCW won three government contracts each from the Office of the Communications Authority in June 2020 to expand fiber-optic infrastructure into villages across Hong Kong.[161] Before that point, the Hong Kong authorities assessed that the largest fixed fiber-optic network providers in villages were HKC Network Ltd. and Village Telephone Ltd., neither of which is licensed as a fixed network provider.[162]

This discrepancy between licensure and actual services rendered indicates that OFCA does not necessarily enforce its categorizations for class licensees, to such a point that other government bodies can contract companies to supply services they are not licensed to provide. In the case of fixed networks, villages were consistently contracting Top Express (the parent company of Village Telephone) to build fixed optical networks, even though the company is not a licensed fixed network operator. According to meeting minutes from the Kwai Tsing District Council, this trend is longstanding and common knowledge; OFCA representatives were present at the meeting, with no comment on Top Express' lack of licensure. [163]

Hong Kong has four mobile network operators: CMHK, HKT, Hutchison Telephone Company ("3"), and SmarTone.[164] Of these four, one (CMHK) is wholly owned by the Chinese government and is already cooperating with authorities to restrict Internet freedom, while HKT is partially Chinese-owned and is highly likely to assist government efforts. The remaining two (Hutchison and SmarTone) are moderately likely to cooperate with government restrictions on Internet freedom based on their respective business operational footprints. There are also 24 mobile virtual network operators that do not have their own physical infrastructure but operate virtualized mobile networks on leased infrastructure.[165] Information on Hong Kong's mobile network operators is included in Table 2 below.

With the exception of Australian-owned Superloop and U.S.-owned Equinix (which runs data centers), all of Hong Kong's major fixed and mobile network providers with physical infrastructure are owned by Hong Kong or Chinese entities. All other foreign-owned providers do not have physical infrastructure in the city. Information on providers with no physical infrastructure in Hong Kong is included in Table 3 below.

TABLE 2: MAJOR HONG KONG FIXED LINE UCLS

Name	Country of Origin	Type of company	Services provided	Likelihood of cooperation with the Chinese government
China Mobile Hong Kong	China	State-owned (China)	Mobile network provider Fixed network provider	***Already cooperates*** with the Chinese government. Parent company China Mobile is a state-owned enterprise that cooperates on censorship and surveillance within mainland China.[166]
PCCW *and* Hong Kong Telecommunications Ltd	Hong Kong	Partially state-owned (China) and private (Hong Kong)	Mobile network provider Fixed network provider Submarine cable provider	***Highly likely*** to cooperate with the Chinese government. Partial owner of PCCW China Unicom is a state-owned enterprise that cooperates on censorship and surveillance within mainland China.[167] China Unicom has already exercised power over who can buy PCCW shares.[168] Mai Yanzhou, a senior vice president at China Unicom, serves as a non-Executive Director of PCCW.[169] PCCW is the parent company of HKT.[170]
Towngas Telecommunications Fixed Network Ltd.	Hong Kong *and* China	State-owned (Hong Kong)	Fixed network provider (minor)	***Highly likely*** to cooperate with the Chinese government. Towngas operates a significant portion of its business in mainland China, and thus has experience cooperating with the mainland government on Internet restrictions.[171] Towngas is dependent on the mainland market.[172] It is also majority controlled by the Hong Kong government.[173]
TraxComm	Hong Kong	State-owned (Hong Kong)	Fixed network provider (minor)	***Highly likely*** to cooperate with the Chinese government. Traxcomm is owned by a Hong Kong state-owned metro-rail company, meaning it is fully responsive to the government.[174]
SmarTone Communications Ltd.	Hong Kong	Private	Fixed network provider Mobile provider	***Moderately likely*** to cooperate with the Chinese government. SmarTone is part of the Sun Hung Kai Properties portfolio, which is the largest property development company in Hong Kong.[175] SmarTone only operates in Hong Kong and Macau; failure to comply would hurt its performance in all of its markets and would likely have negative consequences for its parent company.
HKC Network Ltd	Hong Kong	Private	Fixed network provider (minor) [176]	***Moderately likely*** to cooperate with the Chinese government. HKC only operates in Hong Kong, so failure to comply would hurt its performance in all of its markets.[177] HKC cannot afford not to comply.

Hong Kong Cable Television Ltd. (HKCTV)	Hong Kong	Private	Fixed network provider	***Moderately likely*** to cooperate with the Chinese government. HKCTV only operates in Hong Kong, so failure to comply would hurt its performance in all of its markets.[178] HKCTV cannot afford not to comply.
HGC Global Communications Ltd.	Hong Kong	Private	Fixed network provider	***Moderately likely*** to cooperate with the Chinese government. HGC Global Communications is now owned by a Western investment company, lessening its likelihood of cooperating with the Chinese government.[179] However, its ownership of five cross-border cables into mainland China (including one constructed after the company was sold) indicate that it already cooperates with the mainland government on Internet regulations.[180]
Hong Kong Broadband Network (HKBN) *and* HKBN Solutions Ltd.	Hong Kong	Private	Fixed network provider	***Moderately likely*** to cooperate with the Chinese government. HKBN only operates in Hong Kong, so failure to comply would hurt its performance in all its markets. HKBN also provides about 80% of fixed line services in Hong Kong, meaning that any government regulations would only be effective if HKBN complies.[181] HKBN's private ownership status, however, implies less risk of compliance.
Easy Tone Network Ltd.	Hong Kong	Private	Building to building fixed-line network provider	***Moderately likely*** to cooperate with the Chinese government. Easy Tone is the newest UCL, and its entire business model centers on its infrastructure investment in Hong Kong. [182] Easy Tone's private ownership status, however, implies less risk of compliance.
Village Telephone Ltd.	Hong Kong	Private	Fixed network provider (minor)	***Moderately likely*** to cooperate with the Chinese government. Village Telephone is part of the Top Express Enterprise Group, which operates in Hong Kong, Macau, and China. [183] The company is also a contractor for Chinese communications behemoth Huawei.[184] Top Express has won Chinese government contracts on the mainland.[185] Village Telephone and its parent company cannot afford not to comply.
Superloop (Hong Kong) Ltd.	Australia	Private	Building to building fixed-line network provider	***Moderately unlikely*** to cooperate with the Chinese government. While Superloop's Hong Kong infrastructure investment makes up a high proportion of its total resources, its business model depends on foreign companies, like banks, trusting the system's security.[186] Most of its clients are likely to encrypt or protect traffic.

TABLE 3: HONG KONG MOBILE NETWORK UCLS

Name	Country of Origin	Type of company	Services provided	Likelihood of cooperation with the Chinese government
China Mobile Hong Kong	China	State-owned (China)	Mobile network provider Fixed network provider	***Already cooperates*** with the Chinese government. Parent company China Mobile is a state-owned enterprise that cooperates on censorship and surveillance within mainland China.[187]
PCCW *and* Hong Kong Telecommunications Ltd	Hong Kong	Partially state-owned (China) and private (Hong Kong)	Mobile network provider Fixed network provider Submarine cable provider	***Highly likely*** to cooperate with the Chinese government. Partial owner of PCCW China Unicom is a state-owned enterprise that cooperates on censorship and surveillance within mainland China.[188] China Unicom has already exercised power over who can buy PCCW shares.[189] Mai Yanzhou, a senior vice president at China Unicom, serves as a non-executive director of PCCW.[190] PCCW is the parent company of HKT.[191]
SmarTone Communications Ltd.	Hong Kong	Private	Fixed network provider Mobile provider	***Moderately likely*** to cooperate with the Chinese government. SmarTone is part of the Sun Hung Kai Properties portfolio, which is the largest property development company in Hong Kong.[192] SmarTone only operates in Hong Kong and Macau; failure to comply would hurt its performance in all of its markets and would likely have negative consequences for its parent company.
Hutchison Telecommunications	Hong Kong	Private	Mobile network provider	***Moderately likely*** to cooperate with the Chinese government. Hutchison Telecommunications and its mobile phone service, "3," have been involved in cross-border communications projects, indicating that the company is willing to cooperate with Chinese network regulations.[193]

TABLE 4: MAJOR HONG KONG UCLS WITH NO PHYSICAL INFRASTRUCTURE

Name	Country of Origin	Type of company	Services provided	Likelihood of cooperation with the Chinese government
ComNet Telecom (HK) Ltd.	China	State-owned (China)	No physical network infrastructure	***Already cooperates*** with the Chinese government. Parent company CITIC is a state-owned enterprise that cooperates on censorship and surveillance within mainland China.[194]
China Unicom (Hong Kong) Operations Ltd.	China	State-owned (China)	No physical network infrastructure	***Already cooperates*** with the Chinese government. Parent company China Unicom is a state-owned enterprise that cooperates on censorship and surveillance within mainland China.[195]
Vodafone Enterprise Hong Kong Ltd.	U.K.	Private	No physical network infrastructure	***Unlikely*** to cooperate with the Chinese government. Vodafone's footprint in China is small, with no physical infrastructure and no established cooperation with Chinese state-owned enterprises.[196] Vodafone has little incentive to cooperate.
Verizon Hong Kong Ltd.	U.S.	Private	No physical network infrastructure	***Unlikely*** to cooperate with the Chinese government. Verizon's footprint in China is small, with no physical infrastructure and no established cooperation with Chinese state-owned companies.[197] Verizon has little incentive to cooperate, and significant disincentive through pressure from its main markets in the West.
Equinix Hong Kong Ltd.	U.S.	Private	No physical network infrastructure (*see data center infrastructure below*)	***Moderately unlikely*** to cooperate with the Chinese government. Equinix has significant infrastructure investment in Hong Kong's data centers but could face reputational damage for cooperating that would affect its standing in other global markets.[198] Equinix does not have a significant footprint in mainland China.
21 ViaNet Group Ltd.	China	Private	No physical network infrastructure	***Moderately likely*** to cooperate with the Chinese government. 21 ViaNet cooperates with Chinese government requirements for its mainland data centers and would likely do the same in Hong Kong. It currently does not operate in Hong Kong.[199]

4.2 DATA CENTERS

Hong Kong prides itself on being a prime location for data centers, due to its pro-business environment, proximity to mainland China, robust infrastructure, and data protection laws.[200] Hong Kong's Office of the Government Chief Information Officer (OGCIO) established the "Data Center Facilitation Unit" as a helpdesk to assist companies in setting up data centers in Hong Kong.[201] The OGCIO advertised Hong Kong as a prime location for free information flow, saying in a 2021 pamphlet pushing data center providers to come to Hong Kong that "Hong Kong enjoys free flow of information. There is no law or administrative arrangement allowing the Government to interfere with data centre operations or exercise content censorship."[202]

Since the passage of the Hong Kong National Security Law, the demand for data center locations has continued to grow, and the market is expected to see massive investments and a 30 percent growth in the next five years.[203] Sites have been in high demand; in July of 2020, China Mobile won a new data center site, overbidding for the land to such an extent that they outbid the next bidder by almost 56 percent.[204]

Hong Kong has more than 50 co-location data centers, but several players in the market are especially notable, with the largest and most numerous facilities.[205] SUNeVision and PCCW dominated the market in 2020, while the top 10 data center providers together made up more than 80 percent of the market.[206] Along with the companies mentioned below, the UCLs China Mobile, HKBN, and Telstra all own data centers in Hong Kong, as do international companies AT&T and HSBC.[207]

TABLE 5: SUMMARY OF DATA CENTERS IN HONG KONG

Name	Country of Origin	Locations	Likelihood of Cooperation
Global Switch Hong Kong	U.K. (registered)	18 Chun Yat Street, Tseung Kwan O Industrial Estate, Hong Kong	***Moderately likely*** to cooperate with the Chinese government. A subsidiary of Chinese steel firm Jiangsu Shagang purchased the controlling share of Global Switch in 2016 and subsequently bought an additional 24% in 2019. [208] In 2020, the company's ownership was transferred under Jiangsu Shagang. [209] The board is almost entirely run by Jiangsu Shagang Group directors, many of whom have served in state-owned enterprises.[210] The company's new Chinese ownership links make it likely to cooperate with the government.
iAdvantage (SUNeVision)	Hong Kong	• MEGA Plus: 299 Wan Po Road, Tseung Kwan O, New Territories • MEGA-i: 399 Chai Wan Road, Chai Wan, Hong Kong • MEGA Two: 8-12 Wong Chuk Yeung Street, Fo Tan, Shatin, New Territories • ONE: Standard Chartered Tower, Millennium City 1, 388 Kwun Tong Road, Kwun Tong, Kowloon • JUMBO: 145-159 Yeung Uk Road, Tsuen Wan, New Territories[211]	***Moderately likely*** to cooperate with the Chinese government. iAdvantage is the brand name used for the data centers owned by SUNeVision Holdings, which is in turn controlled by Sun Hung Kai Properties Ltd.[212] Sun Hung Kai Properties owns SmarTone, one of the largest UCLs in Hong Kong.[213] As mentioned above, Sun Hung Kai Properties, which operates predominantly in Hong Kong, cannot afford not to comply with the government.
Equinix	U.S.	• HK1: 17/F Global Gateway, 168 Yeung Uk Road, Tsuen Wan, N.T., Hong Kong[214] • HK2: 17/F Kerry Warehouse, 3 Shing Yiu Street, Kwai Chung, N.T., Hong Kong[215] • HK3: 6/F, 1 Wang Wo Tsai Street, Tsuen Wan, N.T., Hong Kong[216] • HK4: 13-14/F Ever Gain Building No. 3, 22 On Sum Street, Siu Lek Yuen, Shatin, Hong Kong[217] • HK5: Tower 2, No. 299 Wan Po Road, Tseung Kwan O, Hong Kong[218]	***Moderately unlikely*** to cooperate with the Chinese government. Equinix's main infrastructural investment in Hong Kong is five data centers in Hong Kong that also serve as "business Internet exchanges" (IBXs).[219] Equinix was founded in Silicon Valley and its shareholders are largely U.S. investment companies.[220] Equinix has a significant infrastructure investment in Hong Kong's data centers but could face reputational damage for cooperating that would affect its standing in other global markets. Equinix does not have a significant footprint in mainland China.
Telehouse (KDDI) and HKCOLO	Japan and Hong Kong	• Telehouse Hong Kong CCC: 2 Chun Yat St, Tseung Kwan O Industrial Estate, Hong Kong	***Moderately likely*** to cooperate with the Chinese government. Telehouse and HKCOLO formed a joint venture in 2011 under the name HKCOLO.net, combining

		• HKCOLO Sino Favour Center SFC: Sino Favour Centre, 1 On Yip Street, Chai Wan, Hong Kong	their resources in a 50-50 split to jointly control two Hong Kong data centers, the "Cloud Computing Complex" and the "Carrier Colocation Center."[221] Telehouse also has data centers in Shanghai and Beijing, partnering with Chinese data center companies for legal co-location in China, and so already complies with Chinese regulations.[222] HKCOLO is a Hong Kong-based company and cannot afford to risk its market in Hong Kong.[223]
DigitalBridge	Hong Kong	• MCX 5 (Sheung Wan): West Exchange Tower, 322 Des Voeux Road Central, Sheung Wan, Hong Kong • MCX 6 (Cyberport): Cyberport 2, 100 Cyberport Road, Hong Kong • MCX 9 (Fanling): On Ting Industrial Center, Lot No.62, 3 On Chuen Street, Fanling, New Territories • MCX10 (Kwai Chung): Cargo Consolidation Complex, No.43 Container Port Road, Kwai Chung, New Territories • MCX7 (Fotan): Sun Hung Kai Logistic Center, 8 Wong Chuk Yeung Road, Fo Tan, New Territories[224]	***Moderately unlikely*** to cooperate with the Chinese government. DigitalBridge now owns five data centers in Hong Kong, after it purchased PCCW's Asia data center business in July of 2021.[225] DigitalBridge is a re-formed version of the Florida-based real estate company, Colony Capital.[226] This represents a transfer of ownership from a Chinese company to a U.S. company. Colony Capital had to be re-formed to improve its image after its founder was arrested, indicating that it is likely trying to protect its new image.[227]
CITIC	China (state-owned)	• CITIC Telecom Tower: 25/F CITIC Telecom Tower, 93 Kwai Fuk Road, Kwai Chung, Hong Kong[228] • CITIC ALC: 111 Lee Nam Road,Ap Lei Chau, Hong Kong (5th Floor, DCH Motor Service Building)[229]	***Already cooperates*** with the Chinese government. CITIC is a Chinese state-owned enterprise. It owns two major Hong Kong data centers under the brand "DataHOUSE." The DataHOUSE centers are cloud-based and connected to SmartCLOUD Cloud Service Centers and CITIC's other data centers—including those in China.[230] The CITIC Telecom Tower hosts the main backup for the HKIX, likely a government target of interest.[231]

4.3 INTERNET EXCHANGE POINTS

Hong Kong, like many regions, uses Internet exchange points (IXPs) to route intra-Hong Kong traffic, providing the physical infrastructure for network service providers and content providers to exchange traffic.[232] IXPs work like a large Layer 2 LAN, with numerous Ethernet switches physically interconnected. Network service providers and content providers join IXPs for secure, cheaper, and faster connections to other providers.[233]

Hong Kong has at least six IXPs, but the dominant one is the Hong Kong Internet Exchange (HKIX).[234]

TABLE 6: SUMMARY OF IXPS IN HONG KONG

Name	Owner's country of origin	Owner(s)	Location(s)	Likelihood of Cooperation
Hong Kong Internet Exchange (HKIX)	Hong Kong	Chinese University of Hong Kong (CUHK)	*Main sites:* - HKIX1 and HKIX1b are located at the Sha Tin campus of CUHK, within 2km of each other.[235] - HKIX1c, which is on an independent power grid separate from HKIX1 and HKIX1b, was just finished in August of 2021. Its location is not public.[236] *Satellite sites*:[237] - HKIX2 (Co-operated by CITIC, a Chinese state-owned enterprise): CITIC Telecom Tower, 93 Kwai Fuk Rd, Kwai Chung, Hong Kong - HKIX3 (Co-operated by SUNeVision Holdings Limited, Hong Kong's largest data center provider): Sun Hung Kai Logistics Centre (Shatin), 8 Wong Chuk Yeung Street, Fo Tan Sha Tin, Hong Kong - HKIX3b (Co-operated by SUNeVision Holdings Limited): 399 Chai Wan Rd, Chai Wan, Hong Kong - HKIX4 (Co-operated by NTT Com Asia Limited, a Japanese UCL): 6 Chun Kwong St, Tseung Kwan O Industrial Estate, Hong Kong - HKIX5 (Co-operated by KDDI Hong Kong Limited, a data center provider): 2 Chun Yat Street, Tseung Kwan O Industrial Estate, Hong Kong	***Moderately likely*** to cooperate with the Chinese government. CUHK has eventually cooperated with other government national security orders like closing its unions.[238] Satellite locations are almost all likely to comply, particularly state-owned telecom giant CITIC.
AMS-IX	Germany and Hong Kong	AMS and HCG (Hong Kong Communications Group)	Infrastructure is housed at HCG's data center: Sino Favour Centre, 1 On Yip St, Chai Wan, Hong Kong[239]	***Moderately unlikely*** to comply with the Chinese government. AMS is unlikely to cooperate with the Chinese government, given that it depends more on its other markets than its Hong Kong market. However, HCG, which owns Sino Favour, would be likely to give the government access to the location. This may cause AMS to withdraw.

Equinix-HK	U.S.	Equinix	- HK1: 17/F Global Gateway, 168 Yeung Uk Road, Tsuen Wan, N.T., Hong Kong[240] - HK2: 17/F Kerry Warehouse, 3 Shing Yiu Street, Kwai Chung, N.T., Hong Kong[241] - HK3: 6/F, 1 Wang Wo Tsai Street, Tsuen Wan, N.T., Hong Kong[242] - HK4: 13-14/F Ever Gain Building No. 3, 22 On Sum Street, Siu Lek Yuen, Shatin, Hong Kong[243] - HK5: Tower 2, No. 299 Wan Po Road, Tseung Kwan O, Hong Kong[244]	***Moderately unlikely*** to cooperate with the Chinese government. Equinix's main infrastructure investment in Hong Kong is five data centers in Hong Kong that also serve as "business Internet exchanges" (IBXs).[245] Equinix was founded in Silicon Valley and its shareholders are largely U.S. investment companies.[246] Equinix has a significant infrastructure investment in Hong Kong's data centers but could face reputational damage for cooperating that would affect its standing in other global markets. Equinix does not have a significant footprint in mainland China.
BBIX-HK	Japan	BBIX (at data centers owned by Equinix and Mega-i)	- Co-hosted with Mega-i: iAdvantage MEGA-I, 399 Chai Wan Road, Chai Wan, Hong Kong[247] - Co-hosted with Equinix: HK1: 17/F Global Gateway, 168 Yeung Uk Road, Tsuen Wan, N.T., Hong Kong[248]	***Moderately unlikely*** to cooperate with the Chinese government. BBIX is a Japanese company, and the bulk of its data centers are in Japan, Europe, and North America. It has no footprint in mainland China. The reputational damage would outweigh losing the Hong Kong market.[249]
ACME-IX	Hong Kong	ACME Communications	- 22/F, China Online Centre, 333 Lockhart Road, Wan Chai, Hong Kong[250] - Sino Favour Centre, 1 On Yip St, Chai Wan, Hong Kong[251] - 22/F Corporation Park, 11 On Lai Street, Shatin, Hong Kong[252] - China: ACME Universal Communications, 5/F, GDC Building, 9 Gaoxin Central Avenue 3rd, Nanshan District, Shenzhen, China[253] *(ACME has four points of presence (PoP) for its network, all of which connect to other IXPs and ISPs. ACME is a licensed ISP in China and is one of the only IXPs to have a PoP in China.[254])*	***Already cooperating*** with the Chinese government. ACME-IX is licensed as an ISP in China as well as Hong Kong and operates an IX location in Shenzhen.[255] ACME's main selling point is its access to the Chinese market, meaning it will work hard to protect a good relationship with the Chinese government.

Megaport	Australia	Megaport	Megaport does not operate its own Internet exchange in Hong Kong. Instead, it has “Megaport enabled locations” at 18 partner facilities, including those owned by Equinix, NTT, HKT, Global Switch, One Asia, and iAdvantage.[256]	***Unlikely*** to cooperate with the Chinese government. Megaport does not have its own infrastructural investment in Hong Kong. Megaport does not depend on its Hong Kong market.

4.4 AUTONOMOUS SYSTEM NUMBERS IN HONG KONG

Autonomous System Numbers (ASNs) are globally unique identifiers that correspond with a group of IP address prefixes, which are run by a single network operator. They maintain a clearly defined routing policy.[257] There are 1,020 ASNs assigned to Hong Kong, representing a variety of entities including universities, ISPs, data centers, and government organizations.[258] These autonomous systems have varying numbers of IP addresses and routes.[259] For each of Hong Kong's UCLs, the assigned ASNs are below.

TABLE 7: ASNS ASSIGNED TO HONG KONG

Name of ISP	ASNs
Hong Kong Telecommunications (HKT) Limited and PCCW *(shared ownership structure has led to shared Ases)*	AS4515 AS4760 AS9263 AS9444 AS9925 (Powerbase Data Center) AS17984 AS55940 AS135146 (PCCW Business Internet Access) AS135621 (PCCW Business Internet Access) AS137046 (PCCW Business Internet Access) AS9237
Reach Networks Hong Kong Limited and Reach Cable Networks Limited	AS17500
China Telecom Global Limited	AS63527 AS64079 AS135386
Vodafone Enterprise Hong Kong Limited	None.
HKBN Enterprise Solutions Limited	AS2706 AS9269 AS9381 AS10103 AS58441 AS133849 AS136501
HGC Global Communications Limited and Hutchison Communications *(previous name)*	AS9304 AS10032 AS18116 AS45590 AS63521 AS133160 AS140551 AS10116 AS10118 AS10232 AS17794 AS45562 AS131280

Telstra International HK Limited and Telstra International Limited	AS4637 AS9225 AS9581 AS9740 AS17500 AS17744
Verizon Hong Kong Limited	None.
NTT Com Asia Limited	AS9293
China Mobile International Limited	AS9231 AS58807 AS136750 AS137872
21 ViaNet Group Limited	None.
Equinix Hong Kong Limited	AS55852 AS134533
Hong Kong Cable Television Limited	AS9513 AS9908
SmarTone Communications Limited	AS9474 AS17924
Towngas Telecommunications Fixed Network Limited	AS9899 AS10098 AS10132
Superloop (Hong Kong) Limited	None.
China Unicom (Hong Kong) Operations Limited	AS10099 AS132101
Village Telephone Limited	None.
Easy Tone Network Limited	None.
ComNet Telecom (HK) Limited	AS7705 AS17814
TraxComm Limited	None.
HKC Network Limited	None.

4.5 SUBMARINE CABLE LANDING STATIONS

Internet traffic enters Hong Kong at eight submarine cable landing stations (CLS). Hong Kong's CLSs are all located on the southeast coastline, in three main areas: (1) Tong Fuk, which is on Lantau Island's southern coast; (2) the southern part of Hong Kong island, at Deep Water Bay, Chung Hom Kok, and cape D'Aguilar; and (3) Tseung Kwan O, on the southeastern part of the New Territories.[260] Each CLS is owned by one of Hong Kong's UCL operators, though some provide co-location services to other UCLs that land their cable systems in the same CLS.[261]

China Mobile International owns two of the CLSs, which cumulatively land five cable systems. All of these cable systems connect only to Asia; the proposed Hong Kong–America cable, which was owned by China Telecom Global and planned to land at Chum Hom Hok CLS, was withdrawn for application in the United States. China Mobile obtained the Chung Hom Hok CLS by purchasing the station's owner, GB21, which was previously a subsidiary of Singtel.[262] China Telecom Global has co-location at the Chung Hom Hok CLS, where it lands its SJC and ADC cables (see table below).[263]

Four of the CLSs are owned by a combination of PCCW, which is partially owned by China Unicom, and its subsidiaries. PCCW and HKT own the Cape D'Aguilar Cable Landing Station, which was the first CLS in Hong Kong.[264] This CLS was touted as part of China's "One Belt, One Road" initiative (now rebranded as the BRI) when it was used to land the AAE-1 cable, indicating that the mainland views the site as part of its infrastructure and global agenda.[265] Both of the landing sites on Landau (Lantau) Island (the Landau CLS and the Tong Fuk CLS) are owned by Reach, which is 50 percent owned by PCCW.[266] The Deep Water CLS is owned jointly by Reach and PCCW Global (a subsidiary of HKT).[267]

There are only two CLSs run by companies that are not owned (in whole or part) by the Chinese government: the Tseung Kwan O NTT and Telstra CLSs. These two CLSs each have only one cable system.[268] The Asia Submarine-cable Express (ASE) was built by Japanese telecom company NTT, which manages its landing station.[269] This is the only cable system that has no connection to a Chinese-government linked CLS in Hong Kong. Telstra has a landing station for the East Asia Crossing – City-to-City cable system, but this cable system also goes through the Chung Hom Hok CLS that is owned by China Mobile.[270]

TABLE 8: MAJOR HONG KONG UCLS PROVIDING SUBMARINE CABLES

Name	Country of Origin	Type of company	Likelihood of cooperation with the Chinese government
China Mobile International Ltd.	China	State-owned (China)	***Already cooperates*** with the Chinese government. Parent company China Mobile is a state-owned enterprise that cooperates on censorship and surveillance within mainland China.[271]
PCCW *and* Hong Kong Telecommunications Ltd	Hong Kong	Partially state-owned (China) and private (Hong Kong)	***Highly likely*** to cooperate with the Chinese government. (See Table 1)
China Telecom Global Ltd.	China	State-owned (China)	***Already cooperates*** with the Chinese government. Parent company China Telecom is a state-owned enterprise that cooperates on censorship and surveillance within mainland China.[272]
Reach Networks Hong Kong Ltd. *and* Reach Cable Networks Ltd.	Hong Kong	Partially state-owned (China) and private	***Moderately likely*** to cooperate with the Chinese government. Reach is a 50-50 joint venture between partially state-owned company PCCW and Australian telco Telstra. The PCCW connection to CITIC may be used to pressure Reach to cooperate.
Telstra International Ltd. *and* Telstra Global (HK) Ltd.	Australia	Private	***Moderately unlikely*** to cooperate with the Chinese government. Telstra has a moderate infrastructural investment in Hong Kong, even after leaving the mobile phone market in 2013.[273] Telstra bought PacNet in 2015 and now controls its submarine cable and data center resources.[274]
NTT Com Asia	Japan	State-owned (Japan)	***Moderately unlikely*** to cooperate with the Chinese government. NTT has a moderate infrastructural investment in Hong Kong through its ASE cable and CLS, as well as a data center, but does not maintain its own physical network infrastructure in Hong Kong.[275] NTT has little incentive to cooperate with the Chinese government.

TABLE 9: SUMMARY OF CABLE LANDING STATIONS IN HONG KONG

Station Name (Station Owner)	Owner's country of origin	Submarine Cable Systems	Address and Owner	Likelihood of Cooperation *(See Table 2)*
Tseung Kwan O (TKO) Cable Landing Station (China Mobile International) *(also known as CMI TKO CLS)*	China (state-owned)	• Asia-Pacific Gateway (APG)	6 Chun Kwong Street, Tseung Kwan O Industrial Estate, Hong Kong[276]	***Already Cooperates***
Tseung Kwan O (TKO) Cable Landing Station (NTT)	Japan	• Asia Submarine-cable Express (ASE)	6 Chun Kwong Street, Tseung Kwan O Industrial Estate, Hong Kong[277]	***Moderately Unlikely***
Tseung Kwan O (TKO) Cable Landing Station (Telstra) *(Also called Pacnet landing station. Telstra bought Pacnet in 2015.)*[278]	Australia	• East Asia Crossing- City-to-city (EAC-C2C) *(EAC and C2C were merged under Pacnet in 2007)*[279]	12 Chun Kwong Street, Tseung Kwan O Industrial Estate, Hong Kong[280]	***Moderately Unlikely***
Lantau Cable Landing Station (Reach)	Hong Kong	• Asia-America Gateway (AAG) • Asia-Pacific Cable Network (APCN) • Asia-Pacific Cable Network 2 (APCN-2) • FLAG Europe Asia (FEA)	Tong Fuk, South Lantau Coast, HKSAR[281]	***Moderately Likely***
Tong Fuk Cable Landing Station (Reach)	Hong Kong	• Flag North Asian Loop/Reach North Asian Loop (FNAL/RNAL)[282]	Tong Fuk, South Lantau Coast, HKSAR[283] (Lantau CLS and Tong Fuk CLS are about 200m apart.)[284]	***Moderately Likely***
Cape D'Aguilar Cable Landing Station (HKT/PCCW Global)	Hong Kong	• Asia-Africa-Europe 1 (AAE-1) • Hong Kong-Taiwan 2 (Hon-Tai 2) • Asia-Pacific Cable (APC)[285]	Cape D'Aguilar Road, Shek O, HK[286]	***Highly Likely***
Chung Hom Kok Cable Landing Station (GB21, a subsidiary of China Mobile International)	China (state-owned)	• Asia Direct Cable (ADC) *operational 2022* • City-to-city (C2C) • South-East Asia Japan Cable System (SJC) • South-East Asia Japan Cable System 2 (SJC2) *operational 2022*	Rural Building Lot 1154, Teleport, Chung Hom Kok[287]	***Already Cooperates***
Deep Water Bay Cable Landing Station (Reach/PCCW Global)	Hong Kong	• Sea-Me-We 3 (SMW3) • TGN-Intra Asia Cable System (TGN-IA) • Thailand-Vietnam-Hong Kong (TVH)	Deep Water Bay on the central island of Hong Kong[288]	***Moderately to Highly Likely***

4.6 CONNECTIONS TO MAINLAND CHINA

The Chinese government has stressed increasing interconnectedness between Hong Kong, Macao, and the mainland as a matter of strategic economic policy. This is one of the main goals of the Greater Bay Area cooperation framework that ties Guangdong to Hong Kong and Macao.[289] Through this framework, the government has supported building new optical cables from Hong Kong to the mainland.[290] Beyond this, UCLs have been constructing physical links between Hong Kong and China over the last twenty years, led largely by Chinese state-owned enterprises.

China Mobile currently maintains five cross-border transmission channels between Hong Kong and Guangdong.[291] The most recent is a cross-border optic cable on the Hong Kong–Zhuhai–Macao Bridge.[292] The four other routes come from Wenjindu, Luohu, Futian, and the Western Way.[293]

China Mobile also connects Hong Kong to Hainan. China Mobile's Hainan Wenchang–Hong Kong submarine optical cable system was completed on June 30, 2021. Hainan has been identified as a key point in the BRI and a future hub for the informatization of BRI construction. The Hong Kong submarine cable is Hainan's first connection to the global Internet and a key step in turning the city into an international trade hub.[294]

China Telecom and Hutchison Global Crossing (now HGC Global Communications) maintained one of the first cross-border Internet traffic systems. They operated a Synchronous Digital Hierarchy (SDH) ring connecting China Telecom's cables in Guangzhou and Shenzhen to Hutchison's fiber optic infrastructure in Hong Kong, starting in 2000.[295] In 2018, China Telecom signed another deal with HGC, this time to create a carrier-to-carrier interconnection on the Hong Kong–Zhuai–Macau bridge.[296] China Telecom finished its first large-scale optical cable from Hong Kong to Guangdong in December of 2020. The cable stretches from Hong Kong's Sha Tian (specifically, from Fo Tan), across the Shenzhen Bay Bridge to Shenzhen's Binhai.[297] China Telecom also has direct connections from Hong Kong to Dongguan, Guangzhou, and Shenzhen on its premium Greater Bay Area network.[298]

HGC Global Communications has five fiber-optic cable connections to mainland China. They were the first company to provide cross-border telecom services through the Hong Kong-Shenzhen Western corridor in 2008, with other cables starting in Lok Ma Chau, Man Kam To and Lo Wu.[299] This, along with the new carrier-to-carrier connection with China Telecom, makes HGC the Hong Kong carrier with the most connections to the mainland.[300]

5.0 MECHANISMS FOR RESTRICTING OR REGULATING INTERNET FREEDOM

This report has described the grounds for why the Chinese government is likely to continue to tighten restrictions on online behavior within Hong Kong, focusing on preventing civic unrest, and established that the Hong Kong government has laid the regulatory groundwork to increase surveillance and censorship of Hong Kong's Internet. These contexts, however, do not necessarily predict *how* a crackdown will be implemented. The section below lays out various actions that authorities could take to restrict Internet freedom in Hong Kong and their effects. This examination of possible tactics is based on a combined understanding of Hong Kong's current Internet infrastructure and regulatory framework paired with a discussion of established Internet control methods used within mainland China's "Great Firewall" (防火长城) or its broader "domestic Internet" (内地网络).

5.1 A NOTE ON PRC INTERNET RESTRICTIONS

Censorship methods used within mainland China have been well documented over the last two decades in both theoretical and technical literature. The censorship apparatus in China is built into the Internet infrastructure at every level. Three state-owned entities—China Mobile, China Telecom, and China Unicom—have a monopoly on Internet service provision and enact the government's filtering, surveillance, and throttling requirements.[301] These service providers conduct filtration at the limited number of international gateways that connect China's intranet to the global Internet by wiretapping all connections and using Deep Packet Inspection (DPI) to check content for banned keywords.[302] They also censor content at any autonomous systems (ASes) that peer with foreign ISPs, even in provincial ASes, with different Chinese ISPs placing their main censorship tools at different levels.[303] The connections deemed illegal are then blocked through three main methods: IP address blocking (which the designers of the Great Firewall explicitly address in a publicly released paper), DNS injection, and TCP resets.[304] These tactics are described in depth in several existing reports, including those by Cisco's ThousandEyes and ACM Queue's Daniel Anderson.[305]

Known circumvention methods have been selectively blocked in mainland China, but dedicated Chinese Internet users are still able to access foreign content through VPNs. As HTTPS gained popularity, China's DPI tools were unable to inspect content for banned terms; in response, HTTPS connections are killed "at random," leading to a significant degradation in service.[306] Unlicensed VPNs are banned in China and most foreign VPNs have been removed from China's Apple and Android App stores,[307] but users who download the tools abroad are often able to use them to access content, albeit with lower service quality.[308] VPN usage is discussed in depth in section 5.7.2.

This incomplete censorship of China's Internet is likely a policy matter rather than a result of technical limitations. Molly Roberts addressed China's "permeable censorship" in her 2018 book CENSORED*: Distraction and Diversion Inside China's Great Firewall*, making

the argument that the Chinese government has crafted a censorship regime that uses "friction" methods like quality-of-service reductions and throttling to dissuade less invested Internet users from inadvertently or casually seeking destabilizing content, while still allowing some circumvention methods to stand. This allows highly dedicated and already informed users (often a part of the intellectual elite) to eventually access the content, preventing the total blackout of information that could spur this group to focus on taking down the entire censorship system.[309]

This report does not cover the existing scholarship on China's Internet censorship methods, which is ably described in the literature referenced above. Instead, it addresses types of Internet freedom restrictions unique to Hong Kong—tactics that would fit with Hong Kong's developed and privatized Internet environment, highly online society, and current political conditions. In instances where tactics may overlap with Chinese methods, this report refers to literature describing in detail how China restricts content, which can be consulted for information on existing domestic censorship.

5.2 METHODOLOGY AND KEY CONSIDERATIONS

This report assesses a variety of methods of restricting Internet freedom by grading each method on feasibility, cost, effectiveness, political concordance, and implementation speed. We rate each of these criteria as high, medium, or low, based upon available qualitative research and assessment. In all instances, a grade of "high" suggests that the given method may by more likely to be adopted, while "low" grades suggest they may be less likely to be adopted in the immediate future.

For the purposes of this report, we regard feasibility as a description of the theoretical ease of deployment based on the maturity of legal and technical frameworks required for implementation. Legal pathways and justifications for Internet restrictions include laws, codes, or policy documents detailing why and when restrictions may be enforced, while technical frameworks refer to replicable processes and procedures for instituting technical Internet restrictions. Highly mature frameworks for restricting Internet freedom are enduring and already in use in Hong Kong, while mature frameworks are complete and may be in force in mainland China but have not yet been introduced in the city or have only recently been implemented in Hong Kong. At the opposite end of the spectrum, immature frameworks are still under development and have not been introduced in either the mainland or Hong Kong.

A second critical factor that impacts the likelihood of deploying Internet restrictions is affordability, which can be manifested in actual government outlays and abstract costs. Actual government outlays include amounts spent on the research, development, and deployment of technical infrastructure, as well as associated "support" costs of staffing, court cases, and other enabling elements. Abstract costs are knock-on costs resulting from Internet restrictions, including those passed on to businesses like higher utility rates or slower Internet speeds, as well as opportunity costs like a firm's decision to avoid doing business in Hong Kong thanks to Internet restrictions. We capture these abstract costs

as “business friendliness” and “business opportunity,” respectively. Because a detailed survey of budgetary documents and business lost due to Internet restrictions is beyond the scope of this report, and because abstract costs are exceptionally difficult to measure precisely, this report assesses high, medium, and low affordability subjectively.

Effectiveness is a third important factor in determining the likelihood of adopting a given Internet restriction. For this report, effectiveness is defined as a measure’s ability to defeat or degrade unwanted behavior while still allowing permissible behavior, as well as the ability to deter unwanted behavior. Highly effective measures demonstrate both abilities, while measures with medium effectiveness demonstrate one and those with low effectiveness fail to demonstrate either.

Implementation speed, while not necessarily a direct determinant of likelihood of adoption, is nevertheless an important fourth factor in determining which measure to adopt. Though timelines are widely variable and difficult to predict precisely, given past and ongoing timeframes for action, we consider “high” implementation speed to be any period shorter than 6 months, “medium” implementation speed to be 6-12 months, and “low” implementation speed to be any period greater than 12 months.

Finally, conformity with trends in the political environment may also have an impact on whether a certain measure is adopted to restrict Internet freedom in Hong Kong. The political divergence of a measure reflects consistency with existing policy stances or the political leanings of the Hong Kong government. Measures with “high” political concordance are either already in effect or have been explicitly championed by Hong Kong authorities. Measures with “medium” concordance may either be under consideration by members of the government or indirectly referenced by authorities, while “low” concordance would suggest that the measure is not explicitly part of the Hong Kong political discourse.

TABLE 10: ASSESSMENT OF MECHANISMS FOR RESTRICTING INTERNET FREEDOM IN HONG KONG

	Legal Pressure	Real Name Registration	Data Localization	Control over IXPs
Feasibility	High	Medium	Low	Medium
Affordability	High	Medium	Low	Medium
Effectiveness	Medium	Medium	Medium	High
Implementation Speed	High	Low	Low	High
Political Concordance	High	Medium	Low	Medium

This methodological approach helps summarize a complex range of factors that the Hong Kong government could be considering ahead of any action to suppress Internet freedom. This report, however, does not rely upon quantitative judgments of any kind to arrive at conclusions about possible Internet restriction methods, as this type of research and

analysis remain outside its scope. As a result, these grades should be understood as subjective assessments by analysts based on all available information. For clarity of language, the variables are coded only as “high,” “low,” and “medium” to provide some sense of comparison for prioritization. At the end of the summaries of each of the four methods is a section on “timeline and indications,” which is intended to facilitate the transition from analysis and observation to practice.

The following sections describe these mechanisms and their development and employment in Hong Kong, assessing their advantages, disadvantages, and prospects for future rollout in Hong Kong proper.

5.3 LEGAL PRESSURE

Hong Kong government authorities have already demonstrated a willingness to use legal pressure and threats of fines to force individuals, companies, and ISPs to assist in restricting Internet freedom. Several legal mechanisms for doing so are codified in the Implementation Guidelines for Article 43 of the National Security Law (NSL), which stipulate several legal mechanisms used to enforce an Internet crackdown in Hong Kong.

Legal Pressure	
Feasibility	**High**
- Maturity of legal framework	High; *Hong Kong has already introduced its own framework under the National Security Law and the Personal Data Protection Ordinance*
- Maturity of technical framework	High; *Government does not need technical resources, and private companies have demonstrated their ability to remove or block content.*
Affordability	**High**
- Affordability of R&D and Deployment	High; *already past this stage, no longer relevant.*
- Affordability of support	High; *no new manpower required, while legal enforcement is relatively inexpensive*
- Business Friendliness	Medium; *no new tools or staff needed for businesses. The only cost is reputational should businesses comply, or fines for non-compliance (which have not yet been enforced).*
- Business Opportunity	High; *businesses have not left after the NSL passage, and Internet environment has continued to grow despite new restrictions.*
Effectiveness	**Medium**
- Ability to defeat/degrade unwanted behavior	Low; *foreign companies and encrypted messaging platforms unlikely to comply, so users dedicated to finding workarounds will persevere.*
- Ability to deter unwanted behavior	High; *the cost for individuals and companies to host and post unwanted content has increased, such that entities with lower interest in unwanted behavior will comply or voluntarily censor.*
Implementation Speed	**High; *already in the implementation stage.***
Political Concordance	**High; *already enacted, now represents the political status quo.***

5.3.1 METHODS

The most prominent of the legal measures in the Hong Kong NSL empower police officers to require service providers to surveil hosted content and censor or de-anonymize that content when necessary. These methods are described briefly below.

5.3.1.1 REQUIRING SERVICE PROVIDERS TO CENSOR CONTENT

One method of restricting content is laid out in detail in the NSL's Article 43 Section 4, which states that: [310]

"A police officer may, in accordance with Schedule 4, exercise the power to remove messages endangering national security, and require a platform service provider, a hosting service provider and a network service provider to provide assistance."

The implementation guidelines for this law specify a hierarchy of actions a "designated officer" (a Hong Kong police officer at or above the rank of Assistant Commissioner of Police) is permitted to take to remove content from a platform. This "order of intervention" allows an officer to first require an individual to remove a message they have posted to a platform, then require that a "platform service provider" take "disabling action" upon the message. In this context, "disabling action" refers to the censorship of the message – either by removing the content from the platform or by restricting all access to the message, which could include restricting access to an entire platform. [311]

Should action against the posting individual prove insufficient, the takedown request can be escalated further to require a "hosting service provider" or a "network service provider" to take disabling action.[312] In essence, the order of intervention begins with the entity most intimately connected to the message, and expands outward, moving from (1) the person who posted the message, to (2) the platform service provider, (3) the hosting service for the platform, and (4) the network service provider for the hosting service, as depicted in the diagram below.

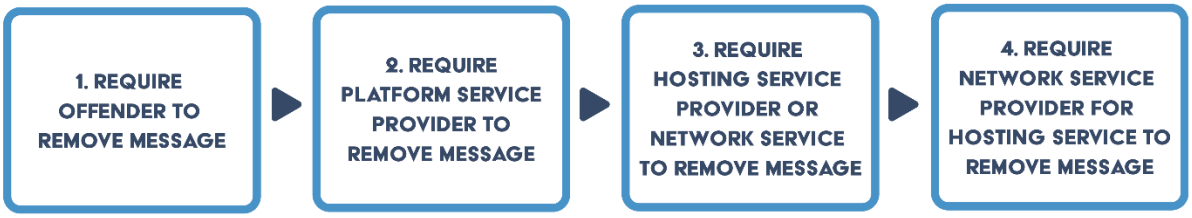

FIGURE 5: SUMMARY OF NSL ORDER OF INTERVENTION AGAINST MESSAGES ENDANGERING NATIONAL SECURITY

A new amendment to Hong Kong's Personal Data Privacy Ordinance (PDPO) may provide a second avenue for requiring content removal, focused specifically on "doxxing" content.[313] The new regulations will require service providers to take down doxxing-related content using official takedown notices, with increased penalties for noncompliance.[314] With doxxing interpreted broadly, there are fears that any act of information sharing that includes authorities could be criminalized. For example, a 2019

injunction aimed at protecting police from doxxing was so vaguely worded that it could include all identifiable pictures taken of a police officer, suggesting that new doxxing laws might in effect criminalize reporting on policing.[315] The law may have other sweeping implications, including the legal basis to criminally charge and imprison local employees of any platform that refuses to remove content deemed "doxxing" (like Facebook, Google, and Twitter), and possible outright bans on websites that host doxxing content.[316]

5.3.1.2 REQUIRING SERVICE PROVIDERS TO DECRYPT OR IDENTIFY

Beyond the removal of content, Section 4 of the NSL also allows police to force service providers to decrypt messages or provide user identification data if they believe that the messages may provide evidence of national security threats.[317] The law is tailored to permit compelled disclosure of the identity of the person who published the message on a platform only, rather than other associated individuals.[318] The efficacy of this law is questionable, given that the platforms who host the content are often foreign – targets include large U.S. technology companies. The law can be enforced if there is reasonable ground for suspecting that "a service provider has in its possession, custody or control an identification record for the message, or may provide decryption assistance in respect of the message."[319]

5.3.1.3 ENTITIES TARGETED BY LEGAL PRESSURE

According to the NSL, the first entity that a police officer should approach to remove illegal online content is the posting individual. However, while the NSL does specify individuals as an entity that must comply with national security related censorship, they are unlikely to be a main target of police pressure. The overall trend in enforcing content removal suggests that the police rarely use NSL mechanisms to compel individuals to remove messages, likely because the most incendiary public-facing websites and posts that remain after the initial wave of self-censorship are posted by individuals who will not voluntarily comply, while private messages and efforts to organize are more likely to be seized as evidence in prosecuting posters rather than removed altogether. More discussion on using enforcing the NSL on individuals can be found in section 5.3.

Platform service providers are more likely targets of the NSL, for two kinds of government pressure: content removal and data disclosure. Although the NSL provides a legal framework for both sorts of pressure, enforcement appears to have been largely focused on data disclosure rather than content removal. There is no indication that the government has leveraged the NSL to ask platform providers to remove content, but they have previously requested that content be removed from social media platforms available in Hong Kong, including Douyin (TikTok's Chinese equivalent), LinkedIn, and Facebook.[320] There have been no public reports of such censorship in Hong Kong since the passage of the NSL.

According to current information, the passage of the NSL has resulted in *limiting* the degree to which U.S.-based technology platforms have complied with data disclosure

requests, despite the passage of rules requiring compliance in decryption and identification. Between July 2019 and July 2020, before the passage of the NSL, the Hong Kong government made 1,399 requests for user data from Apple, Google, Facebook, and Twitter. According to company transparency reports, hundreds of these requests were granted.[321] Granting these requests often included identifying devices and accounts, and providing IP addresses, transactional information, and email addresses.[322] After the passage of the NSL, however, the companies – with the exception of Apple – publicly announced that they would be "pausing" data requests from the Hong Kong authorities and routing them through official, legal channels like the Mutual Legal Assistance Treaty with the United States.[323] Transparency reports indicate that Google, Facebook, Microsoft and Twitter have not complied with any requests from Hong Kong since announcing a "pause."[324] Available data indicates that the number of requests made by the Hong Kong authorities for data from U.S.-based platforms have dropped significantly since June of 2020, perhaps because of their stated stances on not responding to such requests.[325]

Hosting service providers have also been pressured to remove content several times since the passage of the NSL, especially during the leadup to the 2021 Tiananmen Square vigils on June 4. In early June 2021, a Hong Kong activist site called the "2021 Hong Kong Charter," was temporarily taken down by its hosting service provider, the Israeli company Wix.[326] Wix disabled the content after receiving a letter from the Hong Kong Police Force requiring the company to "take disabling action on electronic message(s) on an electronic platform" within 72 hours. The letter, as published by activist and site owner Nathan Law on Twitter, names section 7(4)(b) of Schedule 4 to the Implementation Rules for Article 43 of the NSL, referring to Wix as the "hosting service provider."[327] It states that the website in question "constitutes an offense endangering national security" through inciting secession and subversion as defined by undermining "national unification."[328] Finally, the letter notes that failure to comply with the letter by disabling the content will lead to prosecution, with penalties of a $100,000 fine and six-month imprisonment.[329] Wix originally complied with the letter, then reversed its decision. The site was disabled prior to a June 4 Tiananmen Square vigil and was restored on June 3 after public pressure caused the company to reevaluate.[330] Wix apologized for the action, said the removal was an accident, and promised to review its process for screening takedown requests.[331]

At the same time, U.S.-based hosting company Wordpress removed a similar pro-democracy website, the Hong Kong Liberation Coalition, saying only that it violated Wordpress's terms of service, and the website would be suspended permanently. The company did not provide any explanation for the suspension other than a "violation of terms." Service has not been resumed.[332]

Aside from hosting service providers, pressure from authorities on network service providers (also referred to as ISPs) to block websites is perhaps of greatest concern to outside observers. While ISP-level bans are less complete than a removal of content,

which will (usually) make it unavailable in any region, they represent the ability to block numerous websites without compliance from individual platform or hosting service providers. This is the closest approximation of the Chinese Great Firewall system to date – while those connecting from abroad, including VPN users, can still access content, domestic users will experience site restrictions.

The Hong Kong government first (publicly) exercised its power to ban a website at the ISP level in January of 2021, when it required ISPs to block a high-profile protest website called HKChronicles.[333] All tested service providers – including China Mobile Hong Kong, HKBN, PCCW, Hutchison Telecommunications, and SmarTone – failed to connect to the website, though observers noted that they failed in different ways.[334] At least one ISP, China Mobile, intervened at the DNS level through reconfiguring its firewall environment, a move called a "drop action."[335] Others altered the user's IP address to prevent connection.[336] A professor at CUHK predicted that the discrepancies were likely due to a lack of coordination, given that this was the first ban order.[337]

In the months following this first ban, Hong Kong's government quietly exercised temporary bans on other sites, largely those with ties to Taiwan. On February 13, 2021, it was confirmed that the Taiwan Transitional Justice Commission website had become inaccessible within Hong Kong, with SmarTone, HKBN, HKT, 3, and China Mobile Hong Kong all blocking connections to the site using HTTP blocks.[338] From April 24-27, the Presbyterian Church in Taiwan and Democratic Progressive Party websites were blocked in Hong Kong, which led to an apparent spillover into some foreign servers; tests indicate that TCP/IP based blocking was used.[339] The Presbyterian Church in Taiwan was reported to be communicating with Hong Kong protestors and providing financial aid, and was accused of seditious and destabilizing activity by a government-backed news site.[340] The Recruitment Center of National Armed Forces in Taiwan website was also blocked starting on April 24, and was not unblocked when the prior two sites were made available again.[341] Notably, on June 18, the Hong Kong Charter 2021 website was blocked by some Hong Kong ISPs. This website had previously been removed, and then restored, by Wix.[342]

The key predictor of whether service providers will comply with government orders is not the type of service they provide, but the comparative strength of the company's foreign or domestic interests. The common denominator for the platform service providers that stated that they would not comply with data requests under the NSL is that these platforms are already banned in mainland China, so the reputational cost of compliance for them would be higher than any potential cost of losing access to the Chinese market.[343] In contrast, Hong Kong's ISPs are almost all domestically based, and are highly invested in the Hong Kong market. For them, the cost of losing access to the Hong Kong market would be greater than the reputational cost of complying with the government. The likelihood of compliance is not related to service provider type, but to the relative pressures of foreign observers and the local authorities.

5.3.2 ADVANTAGES

Tightening restrictions on Internet behavior by pressuring companies into cooperating is likely to be the first step in Internet restrictions in Hong Kong. There are three main reasons that this tactic is practical and preferable: no technological investment is necessary, authorities can experiment with and gradually increase restrictions, and it is less threatening to businesses than infrastructural alternatives.

First, pressuring Internet service providers to comply with censorship and data requirements avoids the challenges of imposing an infrastructure-based censorship and surveillance system on an existing cyberspace ecosystem. While the passage of the NSL caused many outside observers to comment that the "Great Firewall" China has built into its mainland Internet ecosystem is "descending" on Hong Kong, the actual model of censorship that China uses is deeply intertwined in the Internet backbone (网络骨干网) infrastructure.[344] China's Internet has developed in tandem with its censorship methods, relying on a small number of choke points for traffic entering or exiting the country and cooperation from government-controlled ISPs in filtering traffic at border and backbone ASes.[345] Imposing these same technological restrictions on Hong Kong after decades of unchecked Internet development and decentralization would be time consuming and technologically challenging; it would require more than simply mimicking the restriction tools used on the mainland.

Second, relying on legal compliance by service providers has allowed the Hong Kong police force to test the limits of ISP and platform compliance, measure the international response to website restrictions, and experiment with methods of blocking websites out gradual Internet restrictions. After the passage of the NSL, a public backlash from Western technology companies and announcements that they would no longer comply with data requests from the Hong Kong government led to a recalibration of the ways that Hong Kong works with foreign technology companies and platforms.[346] Across the board, these technology companies noted in semi-annual transparency reports that Hong Kong's government reduced the volume of data requests, in some cases from hundreds within six months to zero, likely in acknowledgement of the companies' changed policies.[347] However, while foreign companies took a stance in noncompliance, local ISPs appeared to comply with government censorship requirements in multiple instances.[348]

Hong Kong has implemented content restrictions gradually since the passage of the NSL in 2020, waiting more than six months to use ISPs to block a website, and almost a year before sending the first reported message takedown request to a foreign hosting service.[349] This initial gradual rollout allowed for a wave of self-censorship, as groups disbanded and voluntarily removed content without requiring governmental intervention.[350] In each instance, Hong Kong was also able to measure the international response to steps taken before further escalating or tightening. Trends reflect that the first enforcement of a power under the NSL – the ISP blocking of a website, or the hosting service disabling of content – received significant media attention, while subsequent instances were underreported, or noted mostly in regional publications. By gradually

tightening restrictions, Hong Kong's authorities have managed to avoid prolonged international scrutiny.

A gradual roll-out also allowed Hong Kong's ISPs to experiment with different methods of website blocking. Tests run by using website blocking probe OONI, or based on observations of error pages, revealed that pages were blocked with a mix of IP address filtering, DNS tampering, and TCP/IP blocking.[351]

Third, Hong Kong's reliance on cooperation from ISPs has thus far kept major technology companies from leaving the city – either by moving data outside of the country or ceasing service to the region.[352] There have been some exceptions like Canada-based VPN company TunnelBear, which has removed its Hong Kong servers.[353] Other companies may reevaluate their status as laws tighten. As Hong Kong moves towards changing its privacy rules under new anti-doxxing amendments, technology companies like Facebook, Twitter, and Google have again threatened to quit the region, saying it would put their local staff in danger.[354]

By and large, however, no major moves have been taken to move data centers, servers, or key personnel abroad. By avoiding physical takeover of key infrastructure to date, Hong Kong's authorities have apparently managed to keep their policies sufficiently palatable to foreign technology companies.

5.3.3 DISADVANTAGES

While the legal pressure approach to governing Internet behavior has benefits, it has drawbacks that undermine its reach and scalability. Service providers have already demonstrated varying levels of compliance with Hong Kong police orders, and have not yet faced prosecution, indicating that Hong Kong's authorities lack the leverage to enforce the NSL on foreign companies – particularly those like U.S. social media platforms that do not operate in the mainland and are not dependent on Chinese markets. International audiences have exerted counter-pressure on foreign companies and increased their scrutiny of companies' behavior in Hong Kong, making it harder for them to quietly comply.[355] As a result, service provider compliance has been incomplete and subject to reversals, hindering Hong Kong's ability to censor. Depending on companies to comply on a case-by-case basis may prove a risk that the authorities are not willing to take.

Even complete blocks on websites or removal of content have proven weak compared to the mainland's "Great Firewall" system. Hong Kong's website blocks have appeared to use either IP blocking or DNS injection tactics – both relatively "lightweight" solutions with known workarounds.[356] In IP blocking, a router will identify a blacklisted destination IP address and inject routing information into the BGP that hijacks traffic to the banned site, breaking the two-way communication necessary for a connection to be established.[357] IP blocking can be easily evaded by using a proxy or moving to a new IP address.[358] DNS injection is a tactic of identifying sensitive queries to a DNS, and injecting a faked DNS response with a spoofed IP address that will reach the user faster than the real response,

thus blocking their connection to the banned site.[359] When DNS tampering occurs, it is sometimes possible to directly access a site through its IP address, to use an alternative DNS server, or to access the same content through a different (unblocked) domain name.[360] China's "Great Firewall" uses not only IP blocking and DNS injection, but also relies on Deep Packet Inspection (DPI) to identify banned keywords or content.[361] This tactic is much harder to evade, and filters out a great deal more content.

Without using DPI, the current method of restricting content is not only easy to evade, but also challenging to scale. IP blocking and DNS tampering both require a complete list of sites to block and require manual censorship to identify when sites have moved to new domains or switched IP addresses. This method can work to block a limited number of sites who are not actively trying to evade censorship but will not be able to completely block a large, dynamic list of sites.

5.3.4 PROSPECTS

Going forward, observers can expect to see more sites blocked, more completely, for longer amounts of time. Hong Kong Chronicles, the first site blocked by ISPs, was incompletely blocked from the start; regular web probe tests run on the site by OONI indicate that the site could be reached some proportion of the time even in the earliest days of the ban.[362] Between January 1 and January 25, 2021, only about half of tested ASes blocked Hong Kong Chronicles.[363] Among those that did not block Hong Kong Chronicles were ASes from HKBN, China Mobile, and Hutchison—ISPs that did block at least some traffic to Hong Kong Chronicles during that time period.[364]

ASes that blocked Hong Kong Chronicles between January 1 and January 25 included:[365]

AS	AS Owner	Block Type	Block Ended
AS10118	Hutchison Telecommunications[366]	TCP-IP	01/25
AS4760	PCCW[367]	TCP-IP	01/16
AS17924	SmarTone[368]	DNS	Block remained in place through 03/24
AS4515	Hong Kong Telecommunications (HKT)[369]	TCP-IP	
AS9908	Hong Kong Cable Telecommunications (HKCT)[370]	TCP-IP (in January), DNS on 03-17	Block remained in place, as DNS, through 03-17

ASes that did not block Hong Kong Chronicles between January 1 and January 25 included the following:

AS	AS Owner
AS9269	HKBN[371]
AS38819	CSL[372]
AS9304	HGC Global Communications[373] (Hutchison)
AS133752	Leaseweb Asia Pacific[374]
AS4641	HKIX[375]
AS9231	China Mobile Hong Kong[376]

The sites that are most likely to be blocked appear to be those with ties to the protest movement and Taiwan, particularly those that are taking direct action in supporting independence, secession, or expatriation agendas. For example, the Presbyterian Church of Taiwan was blocked because it was said to be funding secession in cooperation with a Hong Kong-based pro-secession figure.[377]

Beyond more comprehensive, longer lasting website blocks, there are still avenues for Beijing to tighten Internet control through cooperation with U.S. service providers. Apple, in particular, has acted in concordance with the Hong Kong government in the past: it removed content from the App store that showed "pro-police" and "pro-protest" restaurants and businesses, and removed an app with protest maps, both in apparent capitulation to the Hong Kong authorities.[378] Apple has already made VPNs unavailable in mainland China's App store.[379]

It is also possible that in tightening its restrictions, foreign companies will move their offices and key personnel outside of the region, hurting Hong Kong's economy and reducing the authorities' ability to exert pressure. Foreign technology companies reportedly started looking at backup plans for Asia-Pacific locations after the passage of the NSL in 2020, and publicly threatened to quit Hong Kong in 2021 over the proposed anti-doxxing law, primarily due to concerns that local staff could be held criminally responsible for the platform's refusal to comply with content removal requests.[380] China may use a workaround that India has recently imposed on Internet companies: mandating the presence of a compliance officer within the country for all Internet service providers.[381] This individual could serve as leverage for the Chinese government, and a target for criminal charges should foreign companies refuse to comply.

5.3.5 TIMELINE AND INDICATORS

There are two categories of indicators to watch for to measure how legal pressure is being used to stifle Internet freedom in Hong Kong: increasing instances of the existing tactics, and escalation into new forms of pressure. As established above, the Hong Kong authorities are already using legal pressure to curb Hong Kong's Internet freedom, so outside observers should not focus on *whether* authorities are using legal pressure, but *to what extent* they are using this tactic. The focus should be on identifying escalation, either in volume or in the type of tactic authorities use to pressure companies to comply.

Many of the indicators of whether this censorship method is being used more frequently are readily apparent; they will likely mark a continuation of current trends, with increasing rates of behaviors that are already being observed. One relevant metric for increasing legal pressure is the request rate for companies to release data to the Hong Kong authorities. For numerous American technology and communications companies, this data is disclosed in regular transparency reports.[382] Tracking Apple's transparency reports may be particularly telling, because Apple is one of the only companies that releases transparency reports to operate on the mainland and has been the most hesitant to commit to noncompliance with NSL requests.[383] An increase in government data requests from Hong Kong would be a clear sign of escalation. However, most of these companies release transparency reports for a given period months, or even years, after the relevant timeframe, meaning that this metric may be too delayed to serve as a useful gauge.[384]

Another sign of an increased volume of legal requests to take down content is higher rates of unexplained website removals. Websites that are taken down by the hosting provider will be unavailable globally, likely without any explanation for their removal. Hosting companies like Wix and Wordpress that have previously removed sites in cooperation with the Hong Kong authorities, are likely to be issued a letter that explicitly states that "pursuant to Article 63(3) of the National Security Law, the relevant institutions, organisations and individuals who assist with the handling of a case shall keep confidential any information pertaining to the case."[385] This was the case for the removal letter sent to Wix by the Hong Kong police.[386] One of the most effective ways to track website removals is with tools like OONI, which crowd-sources a list of sensitive websites (including Hong Kong specific websites), and runs regular "probes" through various ASes in Hong Kong and around the world to check if the website is still accessible.[387] These tests will reveal if the website is removed globally (taken down by either the site owner, either in self-censorship or in response to a police request, or by a hosting service provider), or locally (indicating ISP censorship).

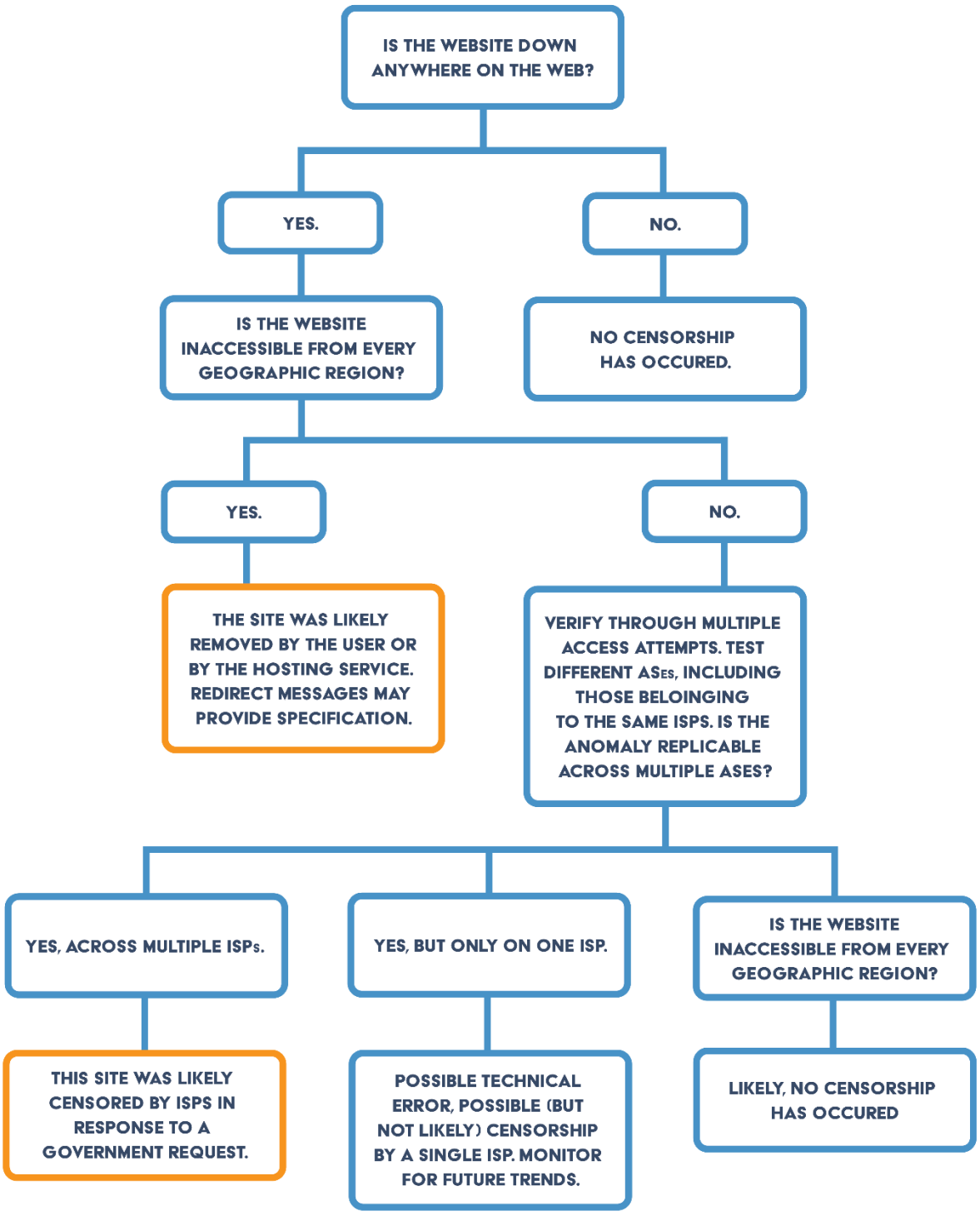

FIGURE 6: FLOWCHART FOR INVESTIGATING WEBSITE BLOCKAGES

In contrast to the above instances of legal pressure, which have already been observed in Hong Kong to some extent, there are some types of indicators that observers can track to look for escalating forms of legal pressure—signs that the authorities are using legal pressure in more coordinated or comprehensive ways.

Timing of website blockage

In the previous instances of ISP-level website blocks, sites have been removed for short periods of time (usually, less than a month), before they become at least partially accessible again. In the case of Hong Kong Chronicles, the first site to be blocked on an ISP level, the site was inaccessible from all tested ISPs for periods of time ranging from several days, to almost two months.[388] By April and May, no ASes were blocking the site.[389] More permanent website bans would represent an escalation of legal pressure.

On another timing note, several police requests for hosting services to take down content were correlated with political timelines; two website takedown requests just predated the Tiananmen anniversary in early June.[390] A likely sign of further escalation is targeted website removals or blocks at politically relevant anniversaries, intended to stifle discourse and minimize mobilization. This scaling up of crackdowns in anticipation of anniversaries is a common tactic in mainland Internet censorship and could logically be incorporated into Hong Kong's toolkit.[391]

Coordinated and comprehensive blocks

Previous instances of ISP-level website blocks have taken effect on different days, lasted for different lengths of time, and used different methods. In some cases, a few ASes belonging to an ISP blocked a site, while others did not.[392] One observer hypothesized that the difference in blocking methods could be attributed to a lack of ISP cooperation, indicating that government officials had ordered a block without specifying a method or timeframe.[393] Coordinated blocks, then, that use the same method, for the same time frame, would indicate increasing government oversight. It would signal a transition from an experimental phase, where ISPs are given relatively free reign to interpret government directions, to close oversight and strict implementation guidelines.

Legal or retaliatory action taken against non-compliant entities

While the NSL lays out consequences for entities that do not comply with governmental takedown orders, no legal action has been taken thus far against entities other than individuals who do not comply.[394] Should the police choose to fine a company (a provision under the NSL), arrest local employees (allowed by the new anti-doxxing provision of the PDPO), or ban a platform for failing to comply, this would mark a clear escalation of legal pressure. Even a single instance of enforcement would send a clear message that the government has the intention and means to enforce a rule that will hurt its business environment, a stance that the authorities have yet to fully adopt.

Official legal actions are not the only way for the government to make its displeasure with a noncompliant company apparent. Officials can also take retaliatory action on the

mainland to exert further pressure on a targeted entity. The government's ability to crack down on a company's presence in the mainland is thought to be the key factor in Apple's historic compliance with Hong Kong police requests for data or App store takedowns.[395] Watching for action taken against telecommunications or Internet companies in mainland China may reveal threats or retaliation for a company's behavior in Hong Kong.

Timeline for escalation

In contrast to some of the other methods discussed here, legal pressure is a tactic with its regulatory framework already in place and active. Any of the above steps could be taken without any other warning and could be implemented immediately. Implementation of the NSL has so far come in waves; individuals were arrested and charged in groups, with all relevant individuals targeted simultaneously. [396] Legal enforcement of the NSL on Internet companies would likely take a similar shape: a coordinated enforcement against several relevant entities simultaneously.

The only caveat to this timeline estimate is that website bans through ISPs would likely be limited in scale compared to lists on the mainland – while mainland providers block banned content along with certain domains and web addresses, ISPs in Hong Kong are not asked to perform in-house content filtration under the NSL, and thus would be required only to block a given list of sites. As discussed in the disadvantages section, there are known workarounds to this method. [397] For content blocking measures that are more advanced than manually entering a set list of IP addresses or domain names to ban, which would be easily implemented by ISPs, scaling a content blocking system would be time consuming. That type of content moderation is beyond what we expect to fall under this category.

5.4 REAL-NAME REGISTRATION

While mainland China's "Great Firewall" focuses on *censoring* content to assert control over information availability in cyberspace, the Hong Kong government has thus far largely prioritized *monitoring* online content, and using it to detain, threaten, or incarcerate individuals seen as undermining national security. The Hong Kong government's goals for regulating Internet behavior center on curbing "anti-government" or "pro-secession" mobilization. To that end, de-anonymizing all online behavior has the potential to stifle free expression and allows the police to identify, detain, and incarcerate those who persist in various forms of activism.

Hong Kong's government has already begun to institute real-name verification for some aspects of Internet usage and may expand real-name registration to cover broader aspects of the cyber ecosystem in the short term. In the long term, technological developments like IPv6 uptake rates may de-anonymize even more online behavior.

Real-Name Registration	
Feasibility	**Medium**
- Maturity of legal framework	Medium; *Hong Kong has passed one real-name registration law, and can incorporate mainland China's rules in the future.*
- Maturity of technical framework	Medium; *Hong Kong government requires no technology. Companies must build real-name registration database and increase staffing to enforce new rules.*
Affordability	**Medium**
- Affordability of R&D and deployment	Medium; *Government must develop legislation, negotiate with stakeholders, and enforce new rules.*
- Affordability of support	High; *Maintenance only requires enforcement and inspection staffing.*
- Business friendliness	Medium; *Businesses must develop real-name registration databases and increase staffing.*
- Business opportunity	Medium; *Businesses may find implementation and reputational costs for compliance too great to operate in the region.*
Effectiveness	**Medium**
- Ability to defeat/degrade unwanted behavior	Medium; *Workarounds for real-name registration still exist through VPNs, foreign platforms, and foreign SIM cards.*
- Ability to deter unwanted behavior	High; *Finding a workaround is costly and requires significant investment, and*

	perceptions of surveillance lead to high self-censorship.
Implementation Speed	Low; *Long legislative process and implementation period.*
Political Concordance	Medium; *Real-name registration of SIM cards is already a part of the political environment, but no other regulations are in drafting yet.*

5.4.1 METHODS

The ability of a real-name registration regime to successfully regulate Internet freedom in Hong Kong is dependent on multiple levels of de-anonymization and the self-censorship that results. De-anonymizing online behavior reduces undesirable content in two ways: it increases self-censorship of online content, while allowing police to criminally charge and even incarcerate individuals who refuse to self-censor. This tactic has long proved effective in mainland China, where real-name registration rules for various platforms stifled political and social discourse for more than a decade.[398]

The effect of real-name registration on individuals' removal of illegal content is already apparent in Hong Kong after the passage of the NSL. Real-name registration is a precondition for implementing the NSL's power to force individuals to self-censor or face legal consequences - this provision cannot be enforced without identifying the user who posted illegal content. Under the NSL, individuals can be required to remove messages within a certain timeframe if they either constitute or are likely to cause a national security threat. Real-name registration on all social media platforms or SIM cards would allow the government to trace content to users.

The public's response to the passage of the NSL shows how real-name registration can stifle Internet freedom on many levels simultaneously, triggering self-censorship, seizure of devices known to be linked to illegal content, and heightened surveillance of associated individuals. After the passage of the NSL, many individuals admitted to deleting political messages, changing profile pictures, and removing all evidence of support for the pro-democracy movement.[399] For others, deleting information on protests was seen as a way of protecting others within the movement; Joshua Wong, a democracy advocate currently incarcerated under the NSL, discussed deleting records of meetings in case phones were seized.[400] After the passage of the NSL, more than 3,700 phones were seized over the span of five months, and content was accessed, indicating that some changes to content could have been attributed to police rather than individual compliance with the NSL.[401]

Identifying a singular method that was used to remove illegal content – police seizure of devices, activation of the NSL's powers over individuals, or simply self-censorship - is challenging because these tactics tend to coincide.[402] One case highlights the difficulty in identifying which mechanism leads individuals to remove content. In June of 2021, the Facebook page of democracy activist Agnes Chow, who was released from prison earlier

that month, was disabled.[403] It is unclear whether police forced her to take it down under an NSL notice, or whether she self-censored in the wake of her incarceration. However, the resulting censorship nonetheless demonstrates the power of real-name registration in restricting Internet freedom.

While Hong Kong is still in the early stages of linking online content to verified identities, this tactic has long proved effective in mainland China, where real-name registration rules for various platforms stifled political and social discourse for more than a decade.[404] Mainland China can serve as an example of how real-name registration can be scaled into a fully identified Internet ecosystem that represses free speech through policing and self-censorship.

Mainland China has steadily implemented a variety of real-name registration rules over more than a decade, all designed to ensure that every step of a user's behavior in cyberspace was identifiable, from accessing the Internet to sharing content. These measures began with platform-level real name login requirements in 2009, and were quickly followed by Weibo account real-name registration verification in 2011 and Internet access real-name registration rules for telecommunications providers and mobile phones in 2013.[405] By 2017, these efforts had culminated in a more rigorous and comprehensive set of regulations requiring real-name registration for Internet forums, comment threads, and online groups,[406] as well as for account registration on any sites or services.[407] Much of the legal burden for enforcement of these rules was placed upon network and website operators.[408] By implementing a real-name requirement on many levels and relying on a set number of state-backed telecommunications providers to gatekeep all access to the Internet, China was able to reduce circumvention options relatively quickly.[409]

While Hong Kong has yet to adopt real-name registration at anything remotely approaching the scale with which it is employed in China, Hong Kong authorities are beginning to implement real-name registration in various realms related to Internet freedom, especially for mobile phone SIM cards and digital wallets as described below.

5.4.1.1 REAL-NAME REGISTRATION FOR SIM CARDS

Hong Kong is already beginning real-name registration for mobile SIM cards purchased from local telecom operators. It was announced in January 2021 that all individuals purchasing new SIM cards in China would have to submit identification paperwork to their telecom operator before service is provided.[410] The law specifically targets pre-paid SIM cards (PPS), since SIM service plan (SSP) cards already require personal details to be activated for regular billing.[411] Currently, PPS cards can be purchased from most convenience stores and require no identifying details, which the government argues makes them easy to use for criminal activity.[412] Hong Kong's Under Secretary for Security states that 70% of local crimes involving SIM cards used PPS cards, and 90% of telephone deception cases on local SIM cards used anonymous cards.[413] Currently, 56% of total mobile cards in Hong Kong are unregistered PPS cards, and users own an average of three SIM cards.[414]

The new regulations will require that all PPS cards be registered to a verified individual or business by February 23, 2023. Operators must implement their customer registration storage system by March 1, 2022, while all PPS cards must be registered to users by the following year.[415] There will also be a per-person cap on PPS cards, with 10 per individual, and 25 per corporation.[416] The time frame and PPS card cap restrictions were both loosened after public consultation.

Real-name registration regulations specifically allow law enforcement authorities (LEAs) to obtain registration details for a SIM card without a warrant "if the nature of the crime is serious or urgent."[417] The original drafting of the law made no mention of the NSL, focusing instead on fraud and other crimes.[418] However, the Deputy Director of the Hong Kong and Macao Affairs Office, Deng Zhonghua, linked the registration system to other policies aimed at protecting national security in a speech marking the one-year anniversary of the NSL's passage.[419] The regulation was put in the same category as the oath of allegiance requirement for civil servants and new education curriculum rules.[420]

5.4.1.2 REAL-NAME REGISTRATION FOR DIGITAL WALLETS

The Hong Kong Monetary Authority introduced real-name registration for all Hong Kong digital wallets in July 2021, limiting the functionality of wallets that did not link to their real names.[421] Real-name registration for digital wallets came with privileges in 2021, such as the ability to test out a new digital RMB wallet, which was only available to those with real-name registered digital wallets.[422]

5.4.2 ADVANTAGES

Real-name registration is a likely tactic to restrict Internet freedom in Hong Kong because the framework for these regulations has already been established in the mainland, it requires no technical investment from the government, and it relies on pressuring the same entities who are already involved in censoring websites under Hong Kong's National Security Law. Perhaps most importantly, real-name registration directly supports a Hong Kong law enforcement priority in regulating Internet behavior: identifying and criminally charging individuals who undermine Chinese government authority.

First, mainland China's experience with real-name registration means that minimal regulatory effort or policy experimentation would be required to effect real-name registration laws in Hong Kong. China's first efforts at real-name registration were ineffective, both because technology companies had little incentive to comply, and retroactively registering existing users was challenging.[423] The 2017 strengthening of real-name registration rules by the CAC was far more effective as it placed the penalties for non-compliance on service providers.[424] On a regulatory level, China has already experimented with methods of increasing cooperation and compliance. Hong Kong authorities can be expected to learn lessons from the Chinese experience and could directly import this Internet surveillance framework to the city with minimal changes to technical or legal infrastructure.

Second, like the censorship and takedown requirements mandated under the NSL, real-name registration would require no technical investment on the part of the government, instead pushing any substantive implementation costs to service providers who bear the brunt of liability for enforcement. The system relies on compliance from service providers, who are held legally accountable for incomplete or inaccurate registrations.[425] By shifting the implementation burden onto service providers, government authorities escape the technical and financial burden of creating a real-name verification infrastructure.[426]

Third, Hong Kong authorities could rely upon established relationships with mobile carriers and ISPs to execute real-name registration. Over the last year, the Hong Kong police has used the NSL several times to require cooperation from ISPs, demonstrating that the government has sufficient leverage over these network providers to require cooperation on real-name registration.[427] Additionally, several of these companies operate in mainland China, indicating that they have experience implementing identity verification, and are willing to cooperate with the regulation. (The largest mobile provider in Hong Kong is China Mobile, a state-controlled carrier that operates on the mainland).

Last but certainly not least, real-name registration supports the identification and arrest of violators, which appears to comport with Hong Kong's current security priorities. Since the passage of the NSL in June 2020, the law has been repeatedly and predominantly used to identify individuals posting "illegal" messages online. The police have placed their focus on arresting and charging violators of the NSL, rather than on using the other powers of the NSL, like censoring online messages. Overall, the Hong Kong police have arrested 117 people suspected of violating the NSL in the first year since its passage.[428] Many of these individuals were specifically arrested for their online messages. In June 2020, four students were arrested for advocating for Hong Kong independence online.[429] In August of that year, four more students were arrested for advocating for terrorism online, in connection to the University of Hong Kong student union.[430] In July 2021, two men were arrested for online calls for boycotts and threats against a Hong Kong broadcasting company.[431] Compared to arrest rates, the Hong Kong police appears to be using its censorship through takedown request powers rarely, with less than ten websites known to be targeted and even temporarily suspended within the last year.[432]

5.4.3 DISADVANTAGES

While real-name registration is comparatively efficient and requires little technical or policy investment on the part of government authorities, it is not a perfect solution for implementing controls on Internet freedom. Real-name registration may be rendered less effective when foreign platforms refuse to comply, service providers lose customers, and if international SIM cards remain unregulated.

Foreign platforms are unlikely to comply with China's real-name registration policies in the current climate, particularly as many companies have recently taken stances on non-cooperation with Chinese government identification and data request policies.[433] The

language of Article 4 of the NSL, requiring service providers to comply with data requests from the authorities, specifically states that authorities may demand identification records or decryption assistance if "there is reasonable ground for suspecting that…. a service provider has in its possession, custody or control an identification record for the message, or may provide decryption assistance in respect of the message."[434] Foreign companies, like VPN providers, have thus far intentionally avoided making and storing such identification records.[435] Other companies, like Google, have historically refused to comply with government real-name registration requirements: in 2009, Google refused to comply with South Korea's real name registration system, choosing to disable content upload and comments rather than verify user identities.[436] Although platforms like Facebook and Google have maintained their own real-name registration requirements for several years as a matter of company policy,[437] they are currently unlikely to either share this information with governments or to strengthen these policies in line with new laws in Hong Kong.[438]

Beyond the possible refusal of foreign companies to comply with real-name registration, such a regime would also be hindered by costs imposed on the Internet service providers that would have to bear the actual cost of enforcing the rules. The costs for Internet service providers to implement identity verification is high, particularly for platforms with large, existing user bases.[439] These costs were a major obstacle in enforcing real-name verification in mainland China before 2017.[440] Combined with the possible loss of customers who do not want to comply with real-name registration could disincentivize cooperation with a real-name registration regime in Hong Kong, the cost of enforcing real-name verification on an organizational level could prove unfavorable for the ISPs actually carrying out the policy.[441]

Finally, existing real-name registration policies may be rendered less effective by failure or inability to cover all known circumvention methods. One known circumvention method for real-name registration in Hong Kong is to use international SIM cards with roaming; under the new SIM card registration rules, international SIM cards are exempt from registration.[442] Circumvention methods for real-name registration are challenging, however, especially because providers are incentivized to verify identity documents carefully, or face punishment.[443] The rules for real-name registration usually include producing official identity documents, meaning that circumvention is challenging at best.[444]

5.4.4 PROSPECTS

To the extent that real-name registration efforts in Hong Kong parallel the regime in China, such efforts to de-anonymize Internet services can be expected to expand. The future of real-name registration, both in Hong Kong and in mainland China, is likely to center on IPv6, a new Internet protocol system with enough unique IP addresses that each device in the world could be individually identified.[445] While IPv6 provides numerous benefits, China's push for IPv6 deployment can be at least partially linked to the ability to identify the machine behind every piece of traffic on the Internet.[446]

Chinese lawmakers and security experts have pointed to IPv6 as a target for massive, device-level real-name registration, and have been planning for IPv6 adoption for the last two decades, starting with rudimentary research between 2003 and 2010.[447] The government is considering creating a system where unique IP addresses are assigned to individuals, which would allow Internet behavior to be tracked in a way that is inconceivable with the IPv4 system.[448] Articles have been published in Chinese-language sources on IPv6 real-name registration dating back almost a decade.[449] This sentiment was made explicit by Wang Jianmin, the chair of computer science and technology at Tsinghua University: "With IPv6, we would know where every piece of data is from, which machine it was sent from, and who received it."[450]

Others have expounded on the potential of IPv6 to enable real-name registration across the Internet. Wu Hequan, who served as chairman of the Internet Society of China, explained that China planned to make IP generation "regular and followable" by creating a set of IP address allocation rules where IP addresses would be as traceable as "telephone and mobile numbers."[451] He has confirmed this plan in several interviews, saying "The traceability of IPv6 can also support online applications to established real name authentication systems."[452] In an interview with *The Paper* in 2017, Wu said that "At present, our IP addresses are dynamically distributed, and it is impossible to realize one-to-one correspondence between addresses and computers, or addresses and people. But in the IPv6 era, with enough addresses, each person can have an address, and we can realize the real-name system, with improved network security management capabilities."[453] Specifically, Wu said that IP addresses would be allocated like phone number area codes, with region, operator, and age of user specified by the number.[454]

While its capabilities are still being developed, the Chinese IPv6 registration system is based on combining separate sets of information: user data, IP usage reports, and IP address assignment. The IPv6 address allocation system will assign devices their own unique IP addresses which will then be associated with a user. IP usage reports will allow the government to "Monitor the IP usage of frequent users of broadband access services, cooperate with the upper-level application management system to find out that the IP address has not been reported for use, and find IP addresses whose actual usage is inconsistent with reported usage."[455] Usage reports will monitor IP address usage "abnormalities" in daily reports.[456] This system will allow for information lookup and management for all users based on IP address, which will be associated with verified, real identities.[457] This information record will include the user's ID, real name, their ID document type, their ID number, their state, city, village, address, zip code, telephone number, mobile number, and email.[458] For foreigners, it will also include an immigration number, and for businesses, their business registration information.[459] Every piece of information transmitted from an IP address can be tracked to a single device and its associated user in the most complete method of real-name registration to date.

The IP real-name registration system being developed in mainland China could plausibly be implemented in Hong Kong as its IPv6 deployment rate continues to grow. Hong

Kong's transition to IPv6 has been less publicized than mainland China's, but its rate of IPv6 deployment is similar.[460] More than 63% of web content in Hong Kong is accessible via IPv6, and more than 80% of Hong Kong's transit ASes are IPv6 enabled.[461] China's rate of IPv6 enabled transit ASes is slightly higher than Hong Kong's, while its IPv6 content rate is less than 30%.[462] Hong Kong's rate of IPv6 uptake is more linear – and steeper – than mainland China's, indicating that it will be continue rapidly transitioning towards IPv6, though there is no evidence that Hong Kong is pushing to become a single-stack network.[463]

5.4.5 TIMELINE AND INDICATORS

There are two ways that authorities can escalate real-name registration in Hong Kong: take advantage of the new laws they have passed that implement real name registration in Hong Kong, and create new laws that de-anonymize other forms of online behavior. According to the phases laid out by the real-name registration regulation for SIM cards, this type of Internet restriction will, by its nature, slowly escalate in level of control between March of 2022 and February of 2023. The SIM card real name registration rule will not be fully implemented until February 2023. [464] This does not mean that SIM card registration data will not be available until this date – instead, by March of 2022, telecommunications providers are required to upgrade their SIM card registration platform to meet the standards specified in the Guidelines on Implementation of Real-name Registration for SIM Cards.[465] Starting in March of 2022, all new SIM cards will be registered with users' identifying information in a standardized database format that will allow for easy police access. [466]

Indicators that SIM card real-name registration is being used to monitor Internet behavior will be hard to track publicly, since the most likely use for this information is covert law enforcement and surveillance efforts. The Hong Kong police has been able to track SIM cards for users with registered plans for a number of years, but does not publicize the use of SIM cards as part of its law enforcement techniques.

If the Hong Kong authorities choose to extend real-name registration rules beyond SIM cards, the speed of the rollout will be limited by the regulatory process. For context, the real-name registration rules for SIM cards were proposed for public consultation in January of 2021, approved in June of 2021, with implementation guidelines taking effect in September.[467] The full implementation of the law was scheduled to take 18 months. [468] Other real-name registration guidelines will likely take less time to implement – the time frame of the SIM card regulation was expanded under public pressure due to the scope of the project, but less comprehensive regulations may see less pushback.[469] Another factor that may speed up the passage of regulation is that many of the platforms the government may seek to regulate – like social media or messaging platforms, as in mainland China – have experience implementing real-name verification systems, either in other territories (like mainland China) or for their internal use (like Google and Facebook). [470] Translating existing laws and databases into a new territory would be less

time consuming than building these systems from scratch, meaning that the government could draw up a tighter timeline.

5.5 DATA LOCALIZATION

Mainland China uses data localization laws to exercise control over personal and industry data, a tactic that allows the government physical access to sensitive information. This type of restriction not only allows the government to access and use large amounts of possibly sensitive data, but also grants them leverage over service providers, forcing them to comply with censorship and surveillance directives. Data localization rules, like the ones already in place in mainland China, would force many technology companies operating in Hong Kong to either cooperate with the NSL, or leave Hong Kong altogether.

Data Localization	
Feasibility	Low
- Maturity of legal framework	Medium; *Mainland China has a legal framework, but Hong Kong does not.*
- Maturity of technical framework	Low; *Lacking necessary technical infrastructure.*
Affordability	Low
- Affordability of R&D and deployment	Low; *The government must invest in building data centers and designing legal frameworks.*
- Affordability of support	Medium; *Staffing and legal enforcement is costly.*
- Business friendliness	Low; *Data localization makes storage more expensive and requires infrastructural investment.*
- Business opportunity	Medium; *Data localization is a deterrent to operating in the region, but has not caused companies to leave mainland China.*
Effectiveness	Medium
- Ability to defeat/degrade unwanted behavior	Medium; *Government can access data for surveillance but is unlikely to alter and censor content.*
- Ability to deter unwanted behavior	Medium; *Unlike other options, data localization will have little effect on user behavior.*
Implementation Speed	Low; *The legislative process and expanding technological infrastructure will take years.*
Political Concordance	Low; *Officials have specifically said they support cross-border data transfer.*

5.5.1 METHODS

Mainland China enforces data localization through an assortment of different rules within the Cybersecurity Law (CSL) and its implementing guidelines, as well as sector-specific rules. That could allow China to access large amounts of user data that can be used to

identify disruptive or dissenting behavior, access and copy data under "national security" pretexts (often for the purpose of building a criminal case against a dissenter), force data into their own jurisdiction, enforce censorship rules, and undermine encryption.[471]

The most explicit and sweeping rule on data localization is Article 37 of China's Cybersecurity Law (网络安全法), which states: "Personal information and important data collected and produced by critical information infrastructure operators during operations in the territory of the People's Republic of China shall be stored within the territory."[472]

Critical information infrastructure is defined in Article 31 of the CSL as pertaining to "public communication and information services, energy, transportation, water conservation, finance, public services, online government, and more."[473] The phrasing used here of "personal information and important data" (个人信息和重要数据) allows for broad interpretation of the data localization law.[474]

Other bureaus have implemented supporting data localization rules, focused on sectors like credit information, financial data, transportation apps, and public health statistics.[475] Each of these laws tends to define "important information" (theoretically subject to data localization laws) differently. A new automotive sector draft law, for example, went into detail on the types of information deemed "critical" after a Tsinghua professor commented that Tesla's autonomous vehicles could gather on-the-ground information about China and its environment, and share it with the U.S. government.[476] The draft law includes as important data:

> *"data on the flow of people and vehicles in important sensitive areas…surveying and mapping data higher than the accuracy of the publicly released maps of the state; operating data on the car electric charging network; data like vehicle types and automotive flow on the road; external audio and video data including faces, voices, license plates, etc.; and other data that may affect national security and public interests, as specified by the State Cyberspace Administration and the relevant departments of the State Council."*[477]

In 2021, China passed the Data Security Law (数据安全法), which tightened the rules on storing and processing data within the country. The law defined a new category for data of interest, "core country data," which includes "data related to national security, the lifeline of the national economy, important daily life, and major public interests."[478] More notably, the language of Article 31 expanded the powers of the Cybersecurity Law to extend to all "important outbound data" collected or produced by critical information infrastructure operators within the PRC, meaning that foreign companies who produce and process data in China for export are subject to the same outbound scrutiny, storage rules, and government oversight as local producers.[479] Article 46 lays out fines, with possible penalties like loss of license, for companies who "provide important data abroad" without going through the proper channels.[480]

Most relevant for surveillance and censorship data are the localization rules for personal information, as defined under the recent Personal Information Protection Law (个人信息保护法).[481] This law asserts jurisdiction over personal data processed within China, or data gathered from individuals within China that will either be used to provide services to or analyze individuals within China.[482] Any data that is individually identifiable will fall under this category.[483] Article 40 expands data localization laws to specifically apply to personal data of a certain scale, saying:

"Critical information infrastructure operators and personal information processing entities who process personal information in the volume specified by the state cyberspace administration shall store the personal information collected and produced in the territory of the People's Republic of China within the territory."[484]

This law, and a tapestry of other regulations, effectively enforces data localization of personal information for all companies operating in China.

There are multiple ways that government authorities can take advantage of data localization laws to restrict Internet freedom. The first and perhaps most relevant to Hong Kong is the forcing of data into China's jurisdiction. The question of national jurisdiction over online information, and increasingly, over application or platform gathered data, traces back at least a decade. China, Russia, and other non-Western aligned countries expressed concerns about national sovereignty over online data at the U.N. in 2011, pointing to U.S. dominance over Internet infrastructure, and proposing an international "Code of Conduct for Information Security."[485] After the passage of the European General Data Protection Regulation, Chinese scholars explored whether that regulation was effective in governing personal data and protecting its cross-border flow, particularly as it concerned cloud storage and foreign companies. [486] In the end, Chinese scholars largely found data protection laws did not provide governments with sufficient control over data due to jurisdictional challenges, and advocated strongly for data localization as a method of excluding foreign access to Chinese data.[487] One Chinese legal scholar presented an article advocating for a "China Model" of data governance, that would use data localization as a "defensive measure" to promote the "expansion of jurisdiction and network sovereignty."[488] Data localization is frequently tied to broader conceptions of network sovereignty. By establishing a clear jurisdiction over the data, China can enforce its own laws – including censorship, surveillance, and national security laws – on any data collected or stored locally.[489]

A second way that the government can use data localization to restrict Internet freedom is using physical infrastructure as leverage to force companies to comply with censorship and surveillance requirements. This measure is clearly tied to questions of sovereignty and jurisdiction, as companies weigh the costs of regulatory compliance.[490] In the case of the Hong Kong NSL, for example, the government can request information that they know or suspect a service provider can produce. If the data is locally stored, companies are less able to either deny the existence of the data or direct authorities to diplomatic

law enforcement information sharing channels. Specifically, this would prevent companies like Google from pointing law enforcement authorities to the Mutual Legal Assistance Treaty as their only option for obtaining data, as it would no longer be considered an export.[491] More than clarifying jurisdictional control, however, localizing data lessens the technical burden of accessing critical information, and assures China that the sought data is available.[492] Forcing companies to establish physical infrastructure in the region will require greater cooperation, as the data center may serve as a leverage point – companies cannot quickly exit the region to avoid harsher regulations, and their resources employees on the ground could be endangered should they refuse to comply.[493]

Finally, data localization provides the obvious benefit of allowing authorities to physically access data for surveillance or censorship. This is the greatest risk, as pointed out by the American Chamber of Commerce in China after the passage of the Cybersecurity Law, which wrote that "there is little to prevent security authorities from interpreting the law as providing expansive access to private information, trade secrets, intellectual property, or internal business communications."[494] The government, in the name of enforcing data protection rules like the new Multi-Level Protection Scheme (MLPS 2.0) introduced under the Cybersecurity Law, has relatively unchecked rights to enter and inspect local data centers, and demand invasive amounts of information regarding data storage methods.[495] Under the Data Security Law, the state maintains the right to access data for national security reasons.[496] The Data Security Law states that it will require data processing entities to:

> *"comply with other laws and regulations (like the National Security Law); to favor economic and social development in line with the CCP's social morality and ethics; to enhance risk inspection and reporting to regulatory authorities in case of security incidents; to conduct periodic risk assessments; to report the categories, amount, collection, storage, processing, usage of important data, along with security risks and countermeasures; to request data source notification, to review identities of parties, and to keep records by agents of data transactions; to require organizations and individuals to cooperate during evidence collection by police and national security authorities; and to report to Chinese regulatory authorities upon request by regulatory authorities abroad."*[497]

Perhaps most importantly, data centers in China are all fully or partially owned by Chinese companies or government entities, often with equipment that has built in surveillance "backdoors" or other vulnerabilities, giving the government physical—if not unencrypted—access to any data stored in a Chinese data center.[498] These data centers are required by law to secretly comply with government or intelligence data requests.[499]

5.5.2 ADVANTAGES

Data localization is a viable means of restricting Internet freedom in Hong Kong largely because it is an increasingly global trend, adopted and promoted by democratic counties like Germany and France, as well as China and Russia, as a means of protecting privacy and avoiding foreign surveillance.[500] Many Western and Chinese scholars frame the data

localization trend as a response to abuse of user data by American companies like Facebook and Google, or the revelation that the U.S. conducts massive, global surveillance of telecommunications systems, leading to mistrust of U.S.-based storage options, and a preference for domestic Internet infrastructure.[501] Data localization measures range in their restrictiveness, the processes for transferring data across borders, and their impact on privacy.[502] However, the language of data localization encompasses the entire range of localization rules, meaning that observers often place the GDPR and Chinese and Russian localization rules in the same category, despite the different implications for localization rules depending on type of governance.[503]

China's data localization laws are framed largely as a means of protecting citizens or the state from Western surveillance and data gathering, rather than as a tool of censorship or surveillance. The key pieces of data localization legislation– in the 2017 Cybersecurity Law, the 2021 Data Security Law, and the 2021 Personal Information Protection Law – categorize data localization as a tool of either export control or privacy legislation.[504] These laws fit within international norms for privacy laws, with marked similarities to the GDPR (for privacy protection), the U.S. National Security and Personal Data Protection Act of 2019, and even CFIUS rules for exporting critical sector-specific data.[505] By drafting laws that use the same language and rationale as Western regulations, China frames their efforts as mainstream privacy protections or security precautions, despite their much broader interpretations of critical infrastructure and stricter localization requirements.
A second advantage of data localization for Hong Kong authorities looking for a means of controlling Internet freedom is that it mitigates the technical challenges of accessing a large amount of data. One of the most cited objections to data localization is that it actually undermines its stated goal: instead of protecting privacy, centralizing data storage makes it easier to target and obtain data, while a single vulnerability could affect enormous amounts of information.[506] This works to the advantage of actors who want to conduct surveillance over data, because centralized storage lessens the technical challenges of locating and accessing relevant data.[507] China has existing regulations and systems that allow them largely unfettered access to data stored in local data centers, so forcing all "important information" and personal data into local storage would facilitate governmental access to all relevant data.[508]

5.5.3 DISADVANTAGES

Data localization laws are seen as anti-competitive or expensive for the private sector, with data restrictions undermining the activities of multi-national technology companies in ways that could severely impact Hong Kong's economy. For instance, American technology companies protested India's data localization laws in 2019, saying that they hurt entrants to the marketplace and prevented foreign companies from operating normally in the country.[509] Forced data localization imposes costs on companies by reducing access to a critical resource, increasing storage costs, slowing service, and reducing trade incentives. Financial firms have estimated that localization laws increase the cost of data storage by between 30 and 60%.[510] For smaller businesses, this cost can be higher; India's data localization laws were expected to raise the cost for startups by up

to 60%.[511] The costs for data localization are higher in regions that are more hot and humid, or have less reliable electricity (an obstacle that China avoids by locating many of its data centers in the northwest and southwest, where temperatures are lower and power sources are plentiful and cheap).[512]

China is well aware of the costs of data localization to companies, because many Chinese companies have been punished for violating these rules – and other data privacy rules – abroad.[513] TikTok and Mobike have both been investigated for GDPR violations by various national legislatures, and TikTok has been required to pay settlements in the U.S. for failing to comply with U.S. data collection laws.[514] Stricter data regulations have caused some Chinese companies to stop operating in affected regions; for example, Xiaomi temporarily suspended selling its Yeelight brand in the E.U. until it could meet GDPR standards.[515]

Data localization laws are famously expensive for the government as well, with multiple overseas think tanks estimating that China's 2017 rules would cost the country as much as 1.1% of their GDP through reduced domestic investment and exports.[516] Another study found that, on average, countries stand to lose about 1.7% of their GDP by forcing localization, because digital connectivity is positively linked with trade services.[517] Data localization also impacts consumer welfare, leading to higher prices when demand outpaces supply. China has more to lose than most countries on this front, with an estimated $61.6-63.8 billion reduction in welfare resulting from data localization.[518] This number averages out to an estimated 13% reduction in the average worker's salary as a cost of data localization.[519]

Beyond cost, data localization has commonly served as a rallying point for foreign technology enterprises, who view the move as a threat to commercial success and a risk for human rights violations.[520] India's draft law on data localization caused numerous companies to protest, writing letters to the Indian government recommending against the move, and suggesting that it might limit their ability to operate in the region.[521] In some cases, companies have refused to comply altogether with data localization laws, accepting legal consequences rather than storing their data in areas controlled by authoritarian governments; in May of 2021, Google, Twitter, and Facebook all chose to pay fines in Russia for failing to locally store data, rather than comply.[522] Over the past year, these technology companies have already indicated a willingness to leave Hong Kong, threatening to depart over doxxing rules that would leave their employees vulnerable to incarceration should their platforms choose not to comply with the Hong Kong government's takedown orders.[523] Forced data localization would likely serve as a tipping point for companies who have publicly staked their reputations on not sharing user data with the Chinese government—they could refuse to comply, facing penalties up to leaving the region altogether.

5.5.4 PROSPECTS

Forced data localization is a possible, but not yet probable, method for China to increase surveillance and censorship in Hong Kong. While China has increased its data protection laws over the last year, Hong Kong has made no moves to change the rules for data storage and processing. Hong Kong governs personal data storage and collection under the Personal Data Privacy Ordinance (PDPO).[524] Article 33 of the PDPO is the only law that restricts cross-border flow to any extent, but its provisions are broad enough to permit almost any data transfer.[525] This rule has been in place since 1996 but has never been brought into operation, though in 2014, the government released "Guidance on Personal Data Protection in Cross-border Data Transfer" in preparation for its implementation.[526] This guidance included the creation of a "whitelist" of countries with acceptably strict data protection laws.[527]

Hong Kong has no explicit data localization rules under the PDPO, meaning that data flowing in or out of Hong Kong is not restricted, largely for economic reasons. Prior to the passage of the NSL, data localization was largely seen as a protective measure *against* Chinese law enforcement, restricting the flow of data into China from Hong Kong.[528] In 2020, the Privacy Commissioner for Personal Data (PCPD) of Hong Kong responded to a media request for information on Hong Kong's data localization, specifically concerning user data for Zoom and TikTok, saying that:

> *"The PDPO does not provide for express extra-territorial application if a data user does not exercise control over the collection, holding, processing or use of the personal data in or from Hong Kong… We have no conclusive information demonstrating that data localization would help secure data collection/storage when using Zoom or TikTok. Suffice to say that free flow of information is a unique and irreplaceable attribute to Hong Kong being an international trade, finance and commercial centre."*[529]

In 2020, Hong Kong's Securities and Futures Commission (SFC) issued a new circular to licensed corporations on the use of external electronic data storage providers (EDSPs) that marks perhaps the closest approximation of data localization currently present in Hong Kong's regulatory environment. The circular, which was scheduled to go into effect on June 30, 2020 but was pushed to December 30 of the same year in response to implementation challenges during the COVID-19 pandemic, places restrictions on the types of EDSPs that licensed corporations can use if they solely store their regulatory records electronically.[530] Specifically, licensed corporations must use EDSPs that (1) are incorporated in Hong Kong, or registered in Hong Kong under the Companies Ordinance, and store data in a Hong Kong data center, or (2) are not located in Hong Kong, but provide assistance and regulatory records as requested by the SFC.[531] The rules require that data center providers (based in Hong Kong) or overseas cloud providers guarantee to provide information on demand to the SFC without notifying their client.[532] The rules, which one expert called "data localization by the back door,"[533] were publicly opposed by the U.S. and Singapore in a joint statement that condemned "generally applicable data localization requirements as long as financial regulators have access to data needed for

regulatory and supervisory purposes."[534] The localization rules are intended to help with enforcement of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, according to the circular.[535] Money laundering is a common charge that coincides with NSL charges, according to arrest and court records, indicating that this unfettered and secret access to corporate records could be used to crack down on protest or crowd mobilization financing.[536] This type of access is demonstrably common in Hong Kong law enforcement; the SFC used search warrants 14 times between April and December 2019 alone.[537]

However, while this regulation does mandate easier access to corporate data, it does not constitute strict "data localization," in that it allows for firms to store data in foreign electronic data centers as long as records can be requested by the SFC.[538] Indeed, the circular explicitly affirms that data can be stored with overseas cloud vendors – and solely overseas vendors – a question that was unclear before the circular was issued, because there was no explicit guidance on storing records solely online.[539] Additionally, multiple stakeholders in Hong Kong's business environment are negotiating with the SFC to loosen the new regulations.[540] The outcome of these negotiations may give some insight into the relative priority given to regulatory power and business interests in Hong Kong when it comes to data localization.

The financial costs of implementing in Hong Kong the same comprehensive, forced data localization as in mainland China are likely too high for the government to use this type of restriction. In 2019, the government issued a statement confirming that Hong Kong's financial success relies on its free flow of data.[541] Moreover, China relies on Hong Kong as a middle ground for data security, as both an international data hub and a secure location for mainland Chinese data.

A national emphasis on increasing the interconnectedness of the "Guangdong-Hong Kong-Macao Greater Bay Area," (粤港澳湾区) especially in terms of technology and innovation, will require China and Hong Kong to find a middle ground on data storage and processing.[542] The growth of the region, which was established by the central government as a "Pilot Demonstration Zone of Socialism with Chinese Characteristics" (中国特色社会主义先行示范区), depends on the construction of an integrated data center system with a "convergence node" in southern China.[543] This project will necessitate the transfer of data between mainland China and Hong Kong.

One recent article on the construction of this data center argued that Hong Kong's status would allow for greater "flexibility" of data transfer out of China.[544] The authors argue that Hong Kong is the perfect region for policy experimentation in data localization and cross-border flow, where it could serve as a "middle ground," white-listed by China for data-flow if reciprocal measures are met, with some moderate increase in data protection rules.[545] The authors' personal data protection measures allow for the establishment of some "reciprocal" regions or countries – including Hong Kong - with whom China will allow for relatively free data flow.[546]

Other scholars proposed similar, middle-ground solutions for different data protection laws in Hong Kong and the mainland, largely focused on making Hong Kong a data hub for the mainland. In a 2019 article from the Beijing Data Science Research Center, the authors recommended driving Hong Kong's compliance with China's data security laws, but not necessarily implementing the same strict rules in Hong Kong.[547] The article also recommended finding ways for the mainland to "seize the right to speak and dominate the data circulation in the Guangdong-Hong Kong-Macao Greater Bay Area."[548]

5.5.5 TIMELINE AND INDICATORS

Hong Kong adopting forced data localization would require a significant, multi-step transition away from the region's current policy trajectory. Before any legal change, Hong Kong authorities would have to clearly signal a change in their stance on data localization; the current Personal Data Privacy Commissioner has made explicit statements on the importance of the "free flow of information" in Hong Kong's economy. [549] In the absence of a shift in public statements, a significant personnel change (either for the role of Personal Data Privacy Commissioner or in the Communications Authority) could lead to a change in policy.

Data protection rules would need to be materially changed to force localization in Hong Kong, but that change could happen either through legislative revision of the PDPO, or through judicial or bureau-level re-interpretation of the existing clauses regarding overseas data transfers. The Hong Kong Legislative Council is likely to make some rules regarding overseas data transfer in the coming year, though there is no indication that this will include a pivot away from the current free flow of data priority to forced data localization. According to law firm DLA Piper, which has tracked proposed changes to the PDPO over the last several years, proposals to amend the PDPO to cover overseas data transfers have been "passing through the Legislative Council for the last couple of years."[550] That this topic was not included in the 2020 revisions to the PDPO, the first since 2012, was notable.[551] According to minutes from a January 2020 panel meeting on proposed revisions to the PDPO, several Legislative Council members asked the PCPD and Constitutional and Mainland Affairs Committee, who advised the amendments to the PDPO, why transfer of personal data outside of Hong Kong was not covered in the amendments, and the PCPD "indicated that it is currently working on designing guidelines on transfer for release later in 2020 and will consider Article 33 thereafter," [552] (Article 33 of the PDPO restricts transfer of Hong Kong data outside of the region unless certain conditions are met, but has never been activated). No action was taken in 2020, but with the proposed amendments from 2020 finally taking effect in late 2021, the PCPD may now pivot to address overseas data transfer.

Given the length of time taken to pass the previous amendments to the PDPO, which included largely politically unobjectionable content, with the exception of the "anti-doxxing" action, any amendment to change the way that limits data transfer and storage can be expected to take a significant length of time to pass. Implementation of any rule would

take even longer; given that the compliance period for the SFC rule for storing regulatory records, which clarified existing guidelines rather than actually changing the status quo, was extended to almost a year,[553] any rules mandating data localization or changed data transfer protocols would inevitably have a lengthy implementation period.

Data localization rules, once passed, would likely be followed by implementation guidelines from either or both of the PCPD and the OFCA. This was the case for rules on SIM card real-name registration, which was first mandated by the Legislative Council, and then implemented by the Communications Authority. [554] These rules would include deadlines for compliance and phases for implementation, as well as penalties for noncompliance.

Infrastructural requirements would also slow the implementation timeline for data localization laws. Hong Kong is already facing a shortage of space in data centers, with an estimated 86% of space in data centers under construction already pre-committed, leaving little room for growth.[555] Data centers take an average of three years to construct, meaning that space will stay limited in the short term, even if immediate action is taken to expand data centers.[556] It appears that the government is indeed planning a massive infrastructural expansion; Hong Kong is planning to allocate 5.2 million square feet of space to the data center market in the next four years.[557]

Government-sponsored data center expansion initiatives should not necessarily be interpreted as an indicator that Hong Kong is developing the infrastructure to force data localization; while infrastructure is a prerequisite to forced data localization, data storage availability is an economic necessity regardless of regulatory changes, and is a lucrative market for Hong Kong. Instead, indicators of possible forced localization would include attempts to increase regulation of data centers, particularly foreign data centers, in a way that erodes their privacy and security. This could include forcing foreign data centers to partner with local companies in order to operate in Hong Kong, similar to mainland rules which allow only investors based in the mainland, Hong Kong, and Macao to obtain data center licenses.[558] It could also appear as state-owned companies overbidding to the extent that they crowd foreign data center operators out of the market; in 2020, China Mobile overbid for a new data center site, offering 56% more than the next nearest bidder and crowding out local competitors, indicating that this strategy is a possible option.[559] Any changes in data center regulations – either in law or in practice – should be carefully monitored, as they could serve as indicators for upcoming regulatory changes.

Data localization laws, if implemented, will invariably have effects on other Internet control methods in Hong Kong. Primarily, data localization will affect the amount of leverage that the Hong Kong authorities have over companies operating in the region, making it harder for companies to refuse to comply with data requests. Data localization, through requiring physical infrastructure, requires companies to fully invest in their presence in the region, making it harder for them to leave if Internet regulations become more stringent; by requiring an increased physical presence in Hong Kong, authorities are raising the costs

of noncompliance. Relocating data between data centers is estimated to cost $10,000 per rack, with about $120,000 total on average.[560] With limited rack space in Hong Kong currently, forced data localization will increase demand while supply lags, increasing the cost of data storage in the region.[561] Higher data storage costs will mean that companies who commit to staying in Hong Kong will invest significantly more in the local market, with physical property that is challenging and costly to move, which will skew their cost-benefit analysis of complying with Hong Kong government data requests. If there are forced to choose between complying and relocating, they will be more likely to comply, because the cost of relocating has grown as the extent of investment in the region has increased.

Data localization will increase the efficacy of legal pressure by raising the costs of relocating, but will also decrease the need to rely on companies to access information, by providing an alternative way for authorities to get the desired data if companies do not comply: they can access the data themselves. Apple's compromises to maintain access to the Chinese market serve as a strong example of the consequences of data localization. After the passage of China's data localization laws in 2017, Apple was forced to store all Chinese customer data in Chinese data centers – which are, by Chinese law, at least partially owned by Chinese companies.[562] This led to negotiations between Apple and the Chinese government about encryption practices; while data stored in Apple's China data centers was encrypted, the storage location of the encryption keys was a main point in discussions between the two parties. Apple eventually agreed to store the keys in China, meaning that while the data is encrypted, the government has access to all encryption keys.[563] The NSL implementation guidelines explicitly prioritize access to both data and decryption keys, indicating that any data localization actions taken in Hong Kong would likely similarly prioritize local storage of decryption keys.[564]

The authorities are equally likely to use physical access to data centers as a workaround for legal pressure. In mainland China, Apple found a compromise that allowed the government to access the data without asking the company for permission, thus evading U.S. government rules barring cooperation with Chinese government data requests. By jointly owning all Chinese customer data with Guizhou-Cloud Big Data, or GCBD, Apple has created a system where the government can request data from the Chinese co-owner of the data, without involving Apple directly. Apple then does not have to actively comply with or reject a data request. GCBD is the operator of the physical data centers, while Apple employees only work with the site remotely, meaning that the Chinese company has eventual say over who physically accesses the data.[565] This type of workaround, where the government goes through a data center operator, co-owner, or otherwise compliant Chinese company to access the physical data of foreign companies (with their implicit knowledge that this type of access is occurring) is likely to become more popular if data storage rules in Hong Kong are tightened. It allows companies to evade the counter-pressure from Western consumers or observers for actively complying with the Chinese government (pressure that caused companies like Wix to walk back their compliance), while satisfying authorities' requests for data. [566]

Data localization will likely have little effect on whether authorities choose to implement real-name registration, or physically access IXPs - though it's worth noting that IXPs are hosted in data centers, so both accessing IXPs and localizing data would require the government to build relationships with data center providers in order to physically access the sites, and both methods might be preceded by tightened restrictions on the types of companies that are allowed to operate data centers. The only insight that data localization would provide into whether the other two methods are more likely is that data localization in Hong Kong's current economic climate would represent a stark divergence from current policy, and a willingness to sacrifice the business environment for national security concerns. While data localization may not appear to be the most extreme measure, compared to censoring websites or installing filters on Internet exchanges, it would be the most onerous for businesses operating in the region, and is highly public. If Hong Kong's leaders are willing to take this step, they are signaling that they are willing to alienate businesses by taking any manner of more extreme Internet restrictions.

5.6 CONTROL OVER INTERNET EXCHANGE POINTS

Internet Exchange Points, or IXPs, are targeted for surveillance and monitoring purposes by governments around the world. In 2016, the largest IXP in the world, DE-CIX, famously sued German surveillance agency BND over "excessive" surveillance powers.[567] DE-CIX claimed that the surveillance of traffic moving through its exchange point was comprehensive and untargeted, beyond the scope permitted under German national security law.[568] Other governments have cited national security reasons for increasing oversight over IXPs: in Cameroon, quasi-governmental organizations and NGOs jointly oversee IXPs, while acknowledging that "Beside the improved Internet speed to end users and the passive revenue generation to ISPs, an IXP is also of national security importance. They process and sometimes collect customers [*sic*] telecommunication and personal identifiable information since all Internet traffic in that city or region transits through the IXP."[569]

Foreign scholars have long hypothesized that China uses its IXPs as part of the country's comprehensive censorship apparatus, and the methods used in the mainland could be imported to Hong Kong. The Chinese government is able to conduct censorship at the "backbone" level, using its control over the physical infrastructure of the Internet to monitor and censor traffic at various choke points—usually, points at which the Chinese Internet connects to the international Internet. [570] China's state-backed Internet providers—called Internet Access Providers, or IAPs—peer at three IXPs that connect to the global Internet.[571] Scholars have hypothesized that these IXPs, which act as choke points to the global Internet, serve as a main location for China's Internet filtering,[572] a model that could be applied to surveil and restrict Hong Kong's Internet traffic.

Control Over IXPs	
Feasibility	**Medium**
- Maturity of legal framework	Low; *No legal framework in place in Hong Kong or mainland China, though the government might not pass laws before acting.*
- Maturity of technical framework	Medium; *Mainland China controls IXPs, but there is no evidence that the authorities already control IXPs in Hong Kong.*
Affordability	**Medium**
- Affordability of R&D and deployment	Medium; *Harnessing technological tools and enforcement authorities requires significant investment.*
- Affordability of support	Medium; *IXP monitoring will require technological resources and personnel.*
- Business friendliness	High; *Unlikely to significantly slow down Internet traffic, since China's censorship*

	method does not significantly slow traffic compared to "on-path" systems.
- Business opportunity	Medium; *If IXP surveillance is discovered, public pressure could cause businesses to pull out.*
Effectiveness	High
- Ability to defeat/degrade unwanted behavior	High; *Like China's GFW, could filter most unwanted connections, except those masked by a VPN.*
- Ability to deter unwanted behavior	Low; *Unlikely that the authorities would advertise their control over an IXP, so it wouldn't affect consumer behavior.*
Implementation Speed	High; *Could take little to no time to physically take over an IXP, if they cooperate.*
Political Concordance	Medium; *No statements made one way or the other.*

5.6.1 METHODS

Some evidence suggests that surveillance or censorship activities at the IXP level could be very difficult to detect, especially as China and Hong Kong move to IPv6 infrastructure. This opacity would make it difficult to precisely identify means of surveillance or censorship beyond descriptions of physical control over IXPs. For instance, China's use of filtering within routers has been studied more comprehensively than its filtering within IXPs, not because routers are necessarily thought to do the bulk of the filtering, but because trace-routes do not show hops within IXPs.[573] Trace-routes, the most common method of tracking Internet traffic, are usually measuring using IPv4, while China's Internet backbone is implemented in IPv6.[574] "Hops" between different providers using an IXP will be viewed as "single hops"—a switch between two ISPs, with no intermediary—because they happen within an "IPv6 tunnel," which cannot be picked up by the IPv4 measuring tool.[575]

China's IXP strategy may be shifting, opening possible opportunities for authorities to control IXPs and monitor traffic passing through them. In 2016, the Ministry of Industry and Information Technology (MIIT) listed broadband expansion of international Internet entrances and exits as a national priority, and proposed the exploration of a new form of IXPs as part of that project.[576] China is now investing in pilot launches of the "New Type Internet Exchange Centers" (新型网络交换中心), which will be faster, more efficient, and more reliable than the older IXPs, speeding up network traffic domestically and internationally.[577] The new IXPs are aimed at improving interconnectivity, but also at aggregating data within the IXPs, indicating that these access points will be used to collect information on Internet activity on both the aggregate and individual levels.[578] New Internet Exchange Centers have been launched in Hangzhou, Shenzhen, and Ningxia.[579]

Internet exchange points can also be used as crucial leverage to convince ISPs to comply with state law. For instance, recently passed Russian laws stipulate that IXPs will be required to disconnect ISPs that refuse to install the Deep Packet Inspection (DPI) monitoring and censoring tools provided by the Russian government, thereby severely impairing or even severing their access to other ISPs (and therefore their ability to "peer," share traffic, and reliably connect users to the Internet).[580] All local ISPs will be required to use local, government-sanctioned IXPs, meaning that these IXPs could act as comprehensive "on-off switches" for ISP traffic.[581]

The Hong Kong Internet Exchange (HKIX) is Hong Kong's largest IXP, and likely the most vulnerable to government control. The point was established in 1995, and is based at the Chinese University of Hong Kong (CUHK).[582] HKIX connects different networks in Hong Kong and mainly operates to exchange intra-Hong Kong traffic.[583] HKIX serves more than 200 private and government organizations, including overseas companies like Google, Facebook, and Yahoo, as well as local fixed-line telecommunications and mobile broadband service providers.[584] The IXP also connects the CUHK campus network to Chinese mainland and foreign research institutions, including the Chinese Science and Technology Network, which falls under the Chinese Academy of Sciences.[585] HKIX is estimated to transmit about 80% of Hong Kong's Internet traffic, and 99% of intra-Hong Kong messages.[586] HKIX serves as a valuable choke-point for Hong Kong's Internet, transmitting most of the region's internal traffic as well as information of significant research and commercial importance.[587]

The HKIX remains a likely target for a government crackdown. Charles Mok, the president of Hong Kong's Internet Society, a former legislator, and a leading technology entrepreneur, talked to Taiwan reporters about the effects of the government taking over the HKIX.[588] Mok noted that HKIX has five different locations, two of which are at CUHK campuses.[589] To fully control or shut down HKIX, the government would have to access all of its satellite locations.[590] In November of 2019, the Hong Kong police sieged CUHK, which observers in the technology and information security spaces hypothesized was part of an attempt to take over HKIX.[591]

5.6.2 ADVANTAGES

Controlling IXPs gives security forces access to internal traffic at scale. The police priority in Hong Kong has thus far been inspecting internal traffic, using online behavior to identify and arrest violators of the Hong Kong NSL. This focus on internal traffic, rather than stopping in-bound international traffic (as is the case in mainland China) would make the HKIX a strong target: an estimated 80-99% of internal traffic moves through the HKIX.[592] When asked about the effects of taking the HKIX offline, Internet entrepreneur Charles Mok said that the greatest effect would be on the speed of intra-Hong Kong traffic, which would have to be routed either out of the country or to other IXPs.[593] If police are able to access the HKIX, they would be able to surveil most internal communications within the region for law enforcement purposes.

Taking over an IXP would allow for easier censorship. One of China's censorship methods, DNS blocking, depends on being the first machine to respond to a DNS query, and sending back a "spoofed" reply that prevents the server from connecting with the end user.[594] The police would be able to install Deep Packet Inspection (DPI) devices at the IXP, which would identify sensitive queries and respond with faked replies before the real response can be routed back to the end-user. Focusing on gateway routers or exchange points can remove the need to tamper with each ISP's individual server.[595] Studies on DNS-based attacks, including DNS spoofing, indicate that targeting DNS attacks at IXPs can lead to an amplification of the threat; in Hong Kong, this would mean that taking over an IXP would amplify the censorship beyond the traffic that flows directly through the exchange point.[596]

Controlling IXPs may be the only technical censorship method used in China's "Great Firewall" that can be relatively easily implemented in Hong Kong, as Hong Kong authorities could readily avail themselves of Chinese experience. While Hong Kong has numerous ISPs, including many foreign-owned companies that may be less likely to comply with government censorship and filtering requests, the city has a very limited number of IXPs – and the HKIX is so dominant in the sector that the police would have a fairly comprehensive ability to surveil internal traffic by only controlling the HKIX.[597] China is currently implementing censorship methods in the IXP space, which means that its IXP-based monitoring and censorship technology will be up-to-date enough to install in Hong Kong's facilities.[598] Perhaps more notably, China has demonstrated the ability to design, construct, and launch a full Internet exchange center in less than three years, suggesting a familiarity with the technology that could be easily applied to minor technological tweaks to HKIX or other IXPs in Hong Kong.[599]

5.6.3 DISADVANTAGES

There are some ways to increase the security and privacy of traffic coming through an IXP without outright refusing to comply with the government. Changes can be made on the IXP level and can protect its members without requiring them to change their operating procedure. For example, in order for peering agreements to work in large-scale IXPs, the IXP must gather and often share the import and export policies of each of the members, which is often confidential information.[600] IXPs can implement Secure Multi-party Computation (SMPC), or trusted execution environments (TEEs), among other fixes, to allow companies to keep their import and export policies private while still sharing the crucial information necessary to peer.[601] Users can also use secure their traffic using VPNs, which will keep traffic private even through IXPs.[602]

Internet restriction at the IXP level can also be weakened when foreign companies refuse to cooperate. Hong Kong's IXP providers vary significantly in terms of ties to the Chinese government, and some of them are unlikely to quietly cooperate with government surveillance. Some companies, like ACME-IX and Equinix, also have locations in China, and thus have experience cooperating with the Chinese government, and have likely been asked to share data in the past.[603] AMS-IX and Megaport are both foreign-based

companies with no mainland China locations.[604] These companies may be less likely to cooperate with the Chinese government, particularly because to do so publicly would damage their reputations globally, and Hong Kong is not their largest market.

Finally, implementing IXP filtering at HKIX could be logistically challenging slowing Internet performance and attracting significant negative attention. Physical takeover of the locations may not be challenging, because CUHK is likely to cooperate with government requests, but may still draw attention. Since 2014, HKIX has had two "Core Sites," HKIX1 and HKIX1b, that are less than 2 km apart and are physically connected.[605] HKIX added a third core location, HKIX1c, in August of 2021.[606] There are four additional satellite locations, each in locations owned by private companies (notably, all Hong Kong-owned companies, rather than foreign owned).[607] In order to fully control and filter HKIX traffic, authorities would have to take over all seven sites. While the proximity of the core locations would make physical takeover easier, the satellite sites would be more challenging to access, requiring authorities to either cooperate with or coerce both the HKIX management team and four different private companies. Given that CUHK has hosted significant protests in the past, a visible police presence at HKIX core locations would likely be noticed and reported on social media.

On a technical, rather than physical, level, filtering the volume of traffic that flows through HKIX would be challenging. The police would have to implement tools powerful enough to filter most of Hong Kong's internal traffic without significantly affecting traffic speeds. If traffic speeds are too greatly affected, HKIX participants will likely find other locations to peer, and other IXPs will become more popular. Thus, authorities will have to find monitoring and filtering methods that do not noticeably affect traffic speeds, without excessive experimentation – implementing them without suspending HKIX service.

5.6.4 PROSPECTS

There are at least five other IXPs in Hong Kong[608] with varying degrees of vulnerability to government control and surveillance measures. The largest is the HKIX, which has seen a 35% increase in traffic since the beginning of the Covid-19 epidemic.[609] HKIX is the most likely target for government control, due to its quasi-governmental status (as a university-owned entity), as well as its dominance in the sector. However, other IXP owners have established relationships with the mainland, which may make them more susceptible to requests or data demands by the mainland government. These others include:

- AMS-IX Hong Kong, which is owned by an Amsterdam-based company. In 2012, AMS-IX opened its Hong Kong IXP, in cooperation with HCG (Hong Kong Communications Group).[610] AMS does not have a mainland China location.[611]
- ACME-IX is owned by a Hong Kong company with no other locations. ACME has a China ISP License and is the only ISP in Hong Kong permitted to provide Access PoP to mainland China.[612] ACME-IX has close China ties, including recognition from MIIT.[613]

- Equinix-HK is owned by a Silicon Valley-based company, with 220 total IXPs.[614] Equinix has a China location but does not provide IXP services in China.[615]
- BBIX-HK has two IXP locations in Hong Kong, based at data centers owned by Equinix and Mega-i.[616] It does not have a China location.[617]
- Megaport has locations in Hong Kong but was founded by an Australian company.[618] Megaport has more than 390 locations worldwide.[619]

5.6.5 TIMELINE AND INDICATORS

While all three of the other tactics for restricting Internet freedom involve some type of regulatory action, necessitating a degree of public-facing action, governmental control of IXPs would likely happen without legal proceedings. It is possible that the Legislative Council could pass a regulation authorizing a new set of surveillance powers, to include explicit permission to access IXP facilities, but the more likely outcome is that the Hong Kong NSL could be broadly construed to allow for monitoring and censorship at IXPs. IXPs could be construed as "service providers" (though not licensed as such) and tasked with removing content or providing data under the same provisions that are used to pressure ISPs.

HKIX occupies a unique position as an IXP, in that it is technically owned by a private company but operates in many ways as a quasi-governmental unit or a type of public work. HKIX is owned by Hong Kong Internet eXchange Limited, a wholly owned subsidiary of the CUHK Foundation, and is operated by the Information Technology Services Center (ITSC) of CUHK.[620] CUHK falls under government oversight as a public university, with its charter coming directing from the Legislative Council of Hong Kong.[621] The University has taken strong stances against protests in the past; in November of 2020, it "promptly reported" a student protest to the Hong Kong police, calling the protestors a "small minority" who had tricked students as part of a "sinister political plot," while supporting the national security agency in investigating cases and "dealing with them according to law."[622] CUHK's cooperation with the police on national security matters like protests indicates that HKIX, under its control, would likely cooperate with the government on national security grounds.

HKIX is not only owned by a public university overseen by the government, but also takes on quasi-governmental functions of its own. HKIX was deemed "critical Internet infrastructure" as early as 2010, according to presentations made by the organization at that time.[623] It is a member of the Internet Infrastructure Liaison Group (IILG), which is made up almost exclusively of government organs (including the HKPF, the OFCA, and the OGCIO), and it is part of the Hong Kong government's emergency response system.[624] In government-designated crisis situations, HKIX acts in coordination with the police and other agencies, indicating that it could be controlled for national security purposes.

HKIX's annual "planned works" and upcoming projects could give indicators on whether it will be used for Internet control purposes. These efforts are usually disclosed in publicly

available presentations. HKIX updates its infrastructure and services frequently,[625] but changes in filtering methods, security systems, or data storage should be monitored for possible dual purposes. This could indicate that the infrastructure for monitoring or filtration is being established. For example, one of HKIX's projects for 2021 was implementing a "security operations center (SOC)."[626] No further details were provided on what a SOC entails.

Another HKIX 2021 project involved the network filtering system.[627] Network filtering at IXPs based on IP addresses is used to weed out "bad actors" or misconfigurations and ensure that IXP participants are sending legitimate routes.[628] HKIX supports Resource Public Key Infrastructure (RPKI), which can prove that an IP address is associated with a specific owner. This system requires participants to opt in to IP address filtering.[629] In theory, HKIX could expand its list of "bad actors" to include IP addresses provided by the government.

Another key warning sign is significant traffic slowdowns. This would likely indicate that part of the HKIX system (one of its core sites) is being taken offline. HKIX does perform regular maintenance at its sites, which could lead to slowdowns.[630] However, a significant, prolonged maintenance episode should be investigated, since some forms of maintenance may involve installing and testing new hardware in HKIX locations. A slowdown without a warning should, similarly, raise red flags, as a possible sign that traffic is being filtered or routing protocol has otherwise been significantly altered.

5.7 ADDITIONAL METHODS FOR CONSIDERATION

While the four methods of restricting Internet freedom discussed above are the most comprehensive and likely steps that China could take in Hong Kong, there are some alternative or supplemental tactics that could infringe on Hong Kong's Internet environment. These additional methods are discussed below.

5.7.1 VIRTUALIZED MIDDLEBOXES AS A CENSORSHIP TACTIC

As telecommunications technology rapidly evolves, new developments that can improve network functionality can be challenging to implement thanks to proprietary technology and specific hardware features. To avoid overreliance on hardware specifications and the accompanying slowdowns, network researchers from around the world have increasingly pushed for the virtualization of network functions (or VNFs, virtual network functions).[631] Network Function Virtualization (NFV) separates network functions from physical hardware, using software-based networking components—the VNFs—that can be moved, instantiated, or updated without changing the existing hardware.[632] The goal of NFV is to move beyond the physical hardware necessary to comprise a network—the message router, CDN, session border controller, DPI, Firewall, and more—to base networks on only the hardware of servers, storage, and switches, which will then run virtual versions of network components.[633]

The transition from hardware-based censorship to software-based censorship has required significant research investment within China. China's censorship system appears to currently rely on hardware - specifically, the use of IDSes and DPIs at IXPs, on the "Internet backbone," and on edge routers.[634] The transition to NFV requires ways to virtualize DPIs and other "middleboxes"—intermediary devices that perform functions other than moving traffic from host to destination, like inspecting, filtering, or altering traffic.[635]

Inspecting and filtering traffic in a virtualized network has been an area of significant research for Chinese Internet scholars, including Fang Binxing, the "Father of the Great Firewall."[636] Fang Binxing has worked on incorporating middleboxes into virtualized networks, describing the creation a traffic filtering system that mimics the way that Deep Packet Inspection currently works on China's Internet. China's filtering system relies on an "on-path" system rather than "in-path barriers;" filtering routers send copies of traffic to out-of-band inspection devices, while allowing the packets to continue directly to the user. The copies are then inspected, and the content is compared to a government keyword and URL blacklist. If the inspection technology finds blacklisted content, the router will inject forged TCP resets, severing the connection and blocking the user from reconnecting to the same IP address.[637] Fang Binxing's proposed virtualized network system replicates the out-of-band inspection and subsequent TCP reset, making explicit that the government-sponsored research on proposed middleboxes is intended to virtualize existing censorship systems.[638] Other researchers have published on the same topic, including from elite research institutions like Tsinghua University.[639]

Fang Binxing's new lab, the Pengcheng Internet Laboratory, specializes in NFV censorship and content inspection tools, among other areas.[640] The lab was founded by the Shenzhen city government to meet national innovation needs, and represents an experiment with a new kind of state-backed laboratory.[641] In a presentation at the 8th National Internet and Information Security Defense Summit (XDef, 第八届全国网络与信息安全防护峰会), the Pengcheng Lab presented their new "Cyber Range," which could be used to test out new technologies against various cyber attacks. This included tools for testing virtualized content inspection engines based on DPIs.[642] The Pengcheng lab designs its own virtualized content inspection systems, complete with the out-of-band filtering system.[643] This research focus, coming out of a state-backed lab, indicates a national interest in virtualized censorship tools.

Some network providers have been promoting a more national-level transition to virtualized networks. China Mobile helped co-author the first white paper on NFV in 2014, and has been making significant strides towards automatic launching and dynamically updating NFVs since then.[644] The company has also been experimenting with national virtualized networks, including the "Novonet Experient Network," which was built in 2016 and includes four provinces and seven data centers.[645] The company used this project to recommend how the network could be scaled on a national level.[646] Similarly, H3C, a Chinese digital infrastructure company, published a lengthy article on how the national Internet might integrate NFV into the "Internet backbone."[647] The combination of governmental, academic, and industry interest in moving towards NFV indicates that this shift is attracting significant interest.

Virtualized networks have also come to Hong Kong, meaning that virtual middleboxes (including DPI with TCP resets) could be integrated without a hardware investment. China Mobile Hong Kong transitioned to a fully virtualized, cloud-based network in 2018, with the help of Huawei.[648] PCCW is implementing "next generation data centers" that use NFV in Hong Kong.[649] HKT is, like CMHK, working with Huawei to transition to cloud-based networks with NFV.[650] This push towards NFV in Hong Kong could make installing middleboxes that censor or surveil content as simple as a software update, rather than a hardware installation.

5.7.2 TECHNICAL BLOCKING OF CIRCUMVENTION TOOLS

Virtual Private Networks (VPNs) are a plausible target of government crackdowns in Hong Kong, as the main censorship and surveillance evasion tactic. VPNs encrypt traffic and allow users to mask their online behavior through a "tunnel" to a shared IP address associated with the VPN provider, from which they can access the Internet. This allows users from Hong Kong to experience the Internet as if they were in another region, and access sites that are banned in their own region but accessible abroad. It also de-individuates traffic, mixing the queries of different VPN users together so that anyone monitoring the connection would not be able to tell what user requested the content.[651] By allowing users to both anonymize their online behavior and evade censorship, VPNs

negate the two major priorities laid out under the implementation guidelines of the Hong Kong NSL.[652]

The mainland government has already experimented with a variety of ways to ban, criminalize, and block VPN usage within its own Internet environment, and these steps could be taken in Hong Kong as well. Unlicensed VPN usage is illegal in China; users must register VPNs through the government, usually for business purposes. The January 2017 MIIT Notice on Cleaning Up and Regulating the Internet Access Service Market (工业和信息化部关于清理规范互联网网络接入服务市场的通知), forbade the use of "dedicated lines (including virtual private networks/VPN) or other information channels must not be created or hired on one's own to conduct cross-border business activities."[653] This launched an effort that lasted until March 2018 to crack down on VPN usage and other methods of accessing the foreign Internet through private channels (often referred to as 翻墙软件, or "wall-scaling software").[654] Following the passage of this VPN law, MIIT allegedly sent notices to China's three main ISPs (China Unicom, China Telecom, and China Mobile) requiring them to start blocking private users from accessing the Internet through VPN technology by February 2018 (MIIT has denied sending this order).[655] ISPs apparently responded by sending notices to clients, alerting them that they would need to assist in the Internet "clean up" process under an order from the Ministry of Public Security. The quoted Ministry of Public Security order called for local network security detachments to "carry out a clean-up, deletion, and removal of circumvention software," focusing on specific sites and circumvention tools "developed by hostile foreign forces" including Freegate, Ultra, Lantern, Psiphon, and Squidproxy.[656] These orders were mirrored at local levels; the Chongqing government started levying fines of up to $2,210 on unlicensed VPN users.[657] In several cases, this law was enforced against private users seeking to access foreign content for personal reasons, causing backlash from the public.[658]

There are two main ways to enforce VPN bans: removing VPN apps from Chinese app stores and blocking connections that use recognizable encryption protocols. Apple and Android have removed VPN apps from their virtual stores in China in line with requests from the Chinese government.[659] This means that VPN users must have downloaded the applications when abroad, when using another VPN, or through other more involved workarounds. This is the main way that the government prohibits users from accessing VPN technologies. For those with existing connections, there are several ways that ISPs can block or degrade service. They can recognize specific encryption protocols that are commonly used by VPNs, like LT2P and PPTP, and sever all connections using that protocol. This method is called "port blocking." However, sophisticated VPNs can randomize and change which ports they use, evading this blocking method.[660] Many ISPs, as well as some websites, like Netflix, will also compare queries to a list of known VPN IP addresses, and forbid connections from those users, effectively blacklisting VPN IP addresses.[661] This method is fairly simple for ISPs to implement, but can be evaded by rotating which IP address is used to access the Internet.[662] While this is a known workaround, it can be challenging for service providers to implement depending on their

resources or infrastructure design. If the traffic is not obfuscated, monitors can use deep packet inspection to examine the payload, identifying the traffic as coming through a VPN.[663] None of these methods individually is effective in blocking all VPN use, since users can rotate ports, VPN providers, IP addresses, and tunneling methods. However, they cumulatively decrease the quality of service, which can be effective in creation "friction" and deterring users who are less committed to accessing the content.[664]

Implementing these same types of VPN restrictions in Hong Kong is less likely to be effective and would likely have higher costs to the business environment. The rate of VPN usage in Hong Kong is higher than it is in mainland China – and it increased seven-fold in the leadup to the Hong Kong NSL.[665] Removing VPNs from the Apple and Android App stores, which is the easiest method of blocking access to the circumvention tools, is less effective when most users who are interested in protecting their traffic likely have already downloaded the tools. The high number of foreign businesses in the region, as well as foreigners living in Hong Kong, means that blocking VPNs will undermine economic activity. Connecting to the outside Internet is necessary for Hong Kong's status as an international economic hub. In a cost-benefit analysis, the cost to business of banning VPNs is likely to outweigh the possible gains of implementing a semi-permeable VPN ban. The types of Internet users that Hong Kong authorities are aiming to surveil or censor are likely the users who have already downloaded VPNs – a relatively low-effort tool compared to the use of unregistered, burner SIM-cards, a common practice among activists.[666] In the long term, banning VPNs may reduce the amount of foreign influence in Hong Kong (a high priority for the government, as evidenced by the clauses on registering foreign influence in the Hong Kong NSL[667] and the rates of Hong Kong NSL-linked arrests tied to foreign collusion[668]), but will be unlikely to provide a law-enforcement benefit by effectively surveilling or censoring in the short term.

The other avenue worth considering in terms of VPN usage is the possibility that the Chinese government will coopt existing VPN providers, using data gathered by the circumvention tool providers to surveil users. The U.S. Department of Homeland Security has been tracking foreign governments' interest in using VPN tools to spy on Internet traffic for several years, and has noted that these tools "have the potential to be vulnerable to surveillance and other threats."[669] Should users download VPNs from adversary nations, warned former U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) director Christopher Krebs, foreign exploitation of the data is "somewhat or highly likely," and would likely include "contacts, user history, geolocation, photographs, and any other accesses granted by the user to the application."[670] In June of 2021, an investigation of the most popular free VPN apps found that 59% of the apps (17) have ties to China, indicating that many of these tools likely collect data on users.[671] These free VPNs may not be the most attractive tools for users in Hong Kong, because Chinese-owned free VPNs are not usually capable of "jumping" the Great Firewall and thus are less popular choices for China-based users.[672] While there are free VPNs that are not linked to the Chinese government, users may not be able

to differentiate between the options. It is worth considering whether Chinese authorities may coopt VPNs, rather than simply blocking them, to restrict internet freedom.

6.0 WORKS CITED

[1] Peng Bo 彭波 and Zhang Quan 张权. The Formation and Evolution of China's Internet Governance Model (1994-2019) 中国互联网治理模式的形成与嬗变 (1994-2019). Jiemian Xinwen 界面新闻. January 29, 2021. https://www.jiemian.com/article/5498649.html
[2] Ibid.
[3] Zhang Ping 张平. Discussion on the Problems of Internet Law 互联网法律规制的若干问题探讨. Intellectual Property 知识产权. no. 8 (August 1, 2012).
[4] Peng and Zhang, The Formation and Evolution of China's Internet Governance Model (1994-2019) 中国互联网治理模式的形成与嬗变 (1994-2019).
[4] Ibid.
[5] Xie, Yong-jiang 谢永江 and Jiang Shu-li 姜淑丽. Analysis of the Situation and Problem on the Legislation of Cyberspace in China 我国网络立法现状与问题分析. Chinese Journal of Network and Information Security 网络与信息安全学报. 1, no. 1 (December 1, 2015).
[6] Peng and Zhang, The Formation and Evolution of China's Internet Governance Model (1994-2019) 中国互联网治理模式的形成与嬗变 (1994-2019).
[7] Kong Xiangwen 孔祥稳. Reflections on the Public Law Regulatory Structure of Information Content on Internet Platforms 网络平台信息内容规制结构的公法反思. China University of Political Science and Law, School of Law-Base Government (中国政法大学法治政府研究院). November 12, 2020. http://fzzfyjy.cupl.edu.cn/info/1037/12445.htm.
[8] Beijing Morning Post 北京晨报. Office of the Central Cyberspace Affairs Commission Rectifies the Chaos of Posts, Must not Violate the "Nine Forbidden" Content Categories and "Seven Bottom Lines" 网信办整治跟帖乱象 不得违反"九不准""七条底线". June 23, 2016. http://www.xinhuanet.com/zgjx/2016-06/23/c_135459215.htm
[9] Chinalawinfo Database 北大法律英文网. Provisions on Ecological Governance of Network Information Content Provisions on Ecological Governance of Network Information Content 网络信息内容生态治理规定. December 15, 2019. http://www.lawinfochina.com/display.aspx?id=bec3b28d770ecf9ebdfb&lib=law&EncodingName=gb2312.
[10] Beijing Morning Post 北京晨报. Office of the Central Cyberspace Affairs Commission Rectifies the Chaos of Posts, Must not Violate the "Nine Forbidden" Content Categories and "Seven Bottom Lines" 网信办整治跟帖乱象 不得违反"九不准""七条底线".
[11] Chinalawinfo Database 北大法律英文网. Provisions on Ecological Governance of Network Information Content Provisions on Ecological Governance of Network Information Content 网络信息内容生态治理规定. http://www.lawinfochina.com/display.aspx?id=bec3b28d770ecf9ebdfb&lib=law&EncodingName=gb2312.
[12] Beijing Morning Post 北京晨报. Office of the Central Cyberspace Affairs Commission Rectifies the Chaos of Posts, Must not Violate the "Nine Forbidden" Content Categories and "Seven Bottom Lines" 网信办整治跟帖乱象 不得违反"九不准""七条底线". June 23, 2016. http://www.xinhuanet.com/zgjx/2016-06/23/c_135459215.htm
[13] Chinalawinfo Database 北大法律英文网. Provisions on Ecological Governance of Network Information Content Provisions on Ecological Governance of Network Information Content 网络信息内容生态治理规定. December 15, 2019. http://www.lawinfochina.com/display.aspx?id=bec3b28d770ecf9ebdfb&lib=law&EncodingName=gb2312.
[14] Office of the Central Cyberspace Affairs Commission 中共中央网络安全和信息化委员会办公室. Improving Comprehensive Internet Governance Capability with Innovative Ideas 以创新理念提高网络综合治理能力. March 11, 2020. http://www.cac.gov.cn/2020-03/11/c_1585473200114875.htm.
[15] Peng and Zhang. The Formation and Evolution of China's Internet Governance Model.
[16] Tao, Peng 陶鹏. The Theoretical Dimension and Significant of Xi Jinping's "Internet Thinking" 习近平"互联网思维"的理论维度及意义指向. Observation and Ponderation 观察与思考. 0, no. 2 (February 1, 2017).

[17] Zheng Ying-qin 郑英琴. Trends, Causes, and Effect of the Confluence of "Hong Kong Pro-Independence" and "Taiwan Pro-Independence" "港独"与 "台独"合流的动向、原因及影响. Modern Taiwan Studies 现代台湾研究. no. 4 (April 1, 2018).
[18] Zheng Xiang-hong 曾向红 and Zhang Jun-su 张峻溯. [Internal and External Linkage: The 2019 Hong Kong Riot in a New Wave of Global Protest] 内外联动： 新一轮全球抗议浪潮中的 2019 年香港暴乱. *Journal of United Front Science* 统一战线学研究. 4, no. 3 (May 21, 2020).
[19] China National Radio (央广网). [One Word of Xi of the Day] The Internet Is Not a Territory of Outlaws 【每日一习话】互联网不是法外之地. February 24, 2021. http://news.cnr.cn/dj/20210224/t20210224_525419954.shtml.
[20] HKSAR Gazette. Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region. July 6, 2020. https://www.info.gov.hk/gia/general/202007/06/P2020070600784.htm; McGregor, Grady. Fortune. How Hong Kong's New Security Law is Already Throttling Its Open Internet. July 7, 2020. https://fortune.com/2020/07/07/hong-kong-law-Internet-freedom/.
[21] Lam, Carrie 林鄭月娥. HKSAR Information Services Department. A Letter to from Chief Executive to All Hong Kong Citizens 行政長官致全港市民的信. May 29, 2020. https://www.isd.gov.hk/nationalsecurity/chi/pdf/Letter.pdf.
[22] Now News (Now 新聞). Lam: We will Strengthen Supervision and Management of Schools, Media, the Internet, and Other Issues Related to National Security 林鄭：未來會加強監管學校媒體和網絡涉國安事宜的處理. April 15, 2021. https://news.now.com/home/local/player?newsId=431126.
[23] Lam, Carrie (林鄭月娥). The Chief Executive's 2021 Policy Address, Supplement II: Upholding and Improving the "One Country, Two Systems" Practice. October 6. 2021. https://www.policyaddress.gov.hk/2021/eng/pdf/supplement_2.pdf.
[24] Rao, Geping. Hong Kong Journal. Two Views of Hong Kong's Basic Law: From Beijing, "One Country" Must Dominate the Two Systems. January 1, 2006. https://carnegieendowment.org/hkjournal/PDF/2006_spring/rao.pdf.
[25] Ibid.
[26] HKSAR Basic Law. Chapter 3: Fundamental Rights and Duties of the Residents. Last accessed October 11, 2021. k/en/basiclaw/chapter3.html.
[27] Legislative Council 香港立法會. A Companion to the History, Rules and Practices of the Legislative Council of the Hong Kong Special Administrative Region Part I: An Introduction to the Legislative Council, Its History, Organisation and Procedure. Chapter 1: An Overview of the Development of Practices and Procedures in the Hong Kong Legislature. Last accessed October 11, 2021. https://www.legco.gov.hk/general/english/procedur/companion/chapter_1/chapter_1.html
[28] The Law Reform Commission of Hong Kong. Civil Liability for Invasion of Privacy. December 1, 2004. https://www.hkreform.gov.hk/en/docs/rprivacy-e.pdf.
[29] "Personal Data (Privacy) Ordinance," (promulgated by the Hong Kong Legislative Council, Aug. 1, 1996), Hong Kong e-Legislation, https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y.
[30] 通訊事務管理局條例（第 616 章）, (promulgated by the Legislative Council of Hong Kong, Apr. 1, 2012), Cap. 616, https://www.elegislation.gov.hk/hk/cap616!en-sc?INDEX_CS=N.
[31] Hong Kong Official Portal. Five Questions from the Legislative Council: Protect Hong Kong Residents' Freedom of Speech and Communications Privacy. 立法會五題：保護香港居民的通訊自由和通訊秘密. July 3, 2013. https://www.info.gov.hk/gia/general/201307/03/P201307030379.htm.
[32] 中华人民共和国香港特别行政区维护国家安全法, (promulgated by the Standing Committee of the National People's Conference of the PRC, Jun. 30, 2020), 新华网, http://www.npc.gov.cn/npc/c30834/202007/3ae94fae8aec4468868b32f8cf8e02ad.shtml.
[33] Hong Kong Legislative Council 香港立法會. Apply National Laws in Hong Kong. December 30, 2015. https://www.legco.gov.hk/research-publications/english/essentials-1516ise07-applying-national-laws-in-hong-kong.htm.
[34] Hong Kong Legislative Council. Apply National Laws in Hong Kong.
[35] Congressional Research Service. China's National Security Law for Hong Kong: Issues for Congress. August 3, 2020. https://sgp.fas.org/crs/row/R46473.pdf.

[36] Wong, Lydia and Kellogg, Thomas E. Georgetown Center for Asian Law. Hong Kong's National Security Law: A Human Rights and Rule of Law Analysis. February 1, 2021. https://www.law.georgetown.edu/law-asia/wp-content/uploads/sites/31/2021/02/GT-HK-Report-Accessible.pdf.
[37] Rudolf, Moritz. German Institute for International and Security Affairs. The Hong Kong National Security Law: A Harbinger of China's Emerging International Legal Discourse Power. November 26, 2020. https://www.swp-berlin.org/10.18449/2020C56/
[38] National Security (Legislative Provisions), (gazette by the Hong Kong Legislative Council, Feb. 14, 2003, lapsed Jul. 22, 2004), C007-e01, https://www.legco.gov.hk/yr02-03/english/bills/c007-e.pdf.
[39] Rudolf. The Hong Kong National Security Law.
[40] Lam, Paul Ting-kwok (林定國). HKSAR Education Bureau: National Security Education Knowledge Enrichment Seminar Series. Fallacy of Hong Kong National Security Law 對香港國安法的謬誤. Last accessed October 11, 2021. https://www.edb.gov.hk/attachment/tc/curriculum-development/kla/pshe/national-security-education/National_Security_Education_Knowledge_Enrichment_Seminar_Series/Knowing_more_about_the_Law_Continental_Law_Common_Law_and_National_Security_Law.pdf.
[41] Lam, Paul Ting-kwok. Fallacy of Hong Kong National Security Law.
[42] InMedia HK 獨立媒體(香港). Hong Kong Police Made Thousands of Personal Data Requests with no Judicial Oversight 警務處再踞榜首 索取最多網民資料. February 28, 2014. https://inmediahk.org/2014/02/28/hong-kong-police-made-thousands-of-personal-data-requests-with-no-judicial-oversight/.
[43] Hong Kong Police Force. Commissioner's Operational Priorities 2020. Modified on October 1. 2021. https://www.police.gov.hk/ppp_en/01_about_us/cop2020.html.
[44] Rtnk 香港電台. Chief Executive: Social Media and Internet Lack of Supervision 特首：社交媒體及網絡缺乏監管. July 6, 2021. https://news.rthk.hk/rthk/ch/component/k2/1599505-20210706.htm.
[45] Now News (Now 新聞). Chris Tang: Hong Kong Plans for Cybersecurity Law, Regulating Internet Providers' Responsibility and Management 鄧炳強：擬訂網絡安全法　規定基礎設施營運者的防範管理責任. October 7, 2021. https://news.now.com/home/local/player?newsId=452354.
[46] Now News (Now 新聞). Raymond Siu: Be Aware Violence Goes Underground; Worsen Police-Citizen Relationship Is Due to Fake News 蕭澤頤：提防暴力地下化　警民關係差源自假新聞. October 10, 2021. https://news.now.com/home/local/player?newsId=452717.
[47] OffBeat 警聲. CSTCB Sticks with Technology Development to Catch Behind-the-Scenes of Internet Crimes 網罪科緊貼科技發展 揪出網絡罪案幕後黑手. Issue 1165. August 5-18, 2020. https://www.police.gov.hk/offbeat_ebook/1165/Offbeat_1165_compress.pdf.
[48] Reuters. Hong Kong Security Chief Claimed Interception Communications Ordinance Covers All Instant Message, Paralleled with National Security Law. January 14, 2021. https://cn.reuters.com/article/hk-security-instant-messengers-0115-idCNKBS29K0GQ.
[49] Radio France International (法廣 RFI). John Lee Admits Hong Kong Authority Has Another Mechanism to Intercept Communications If National Security Involved. January 16, 2021. https://www.rfi.fr/cn/政治/20210116-李家超承认倘涉及国安法港府有另一机制截取通讯.
[50] "香港特別行政區維護國家安全委員會舉行首次會議（附圖）," 香港特別行政区政府新闻公报, Jul. 6, 2020, https://www.info.gov.hk/gia/general/202007/06/P2020070600527.htm.
[51] 中华人民共和国香港特别行政区维护国家安全法, (promulgated by the Standing Committee of the National People's Conference of the PRC, Jun. 30, 2020), 新华网, http://www.npc.gov.cn/npc/c30834/202007/3ae94fae8aec4468868b32f8cf8e02ad.shtml.
[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Ibid.
[57] 中華人民共和國香港特別行政區基本法附件二香港特別行政區立法會的產生辦法和表決程序, (promulgated by the Chairman of the People's Republic of China, Mar. 30, 2021), 人民網－人民日報, http://cpc.people.com.cn/BIG5/n1/2021/0331/c64387-32065680.html.

[58] “香港特別行政區維護國家安全委員會舉行首次會議（附圖）,” 香港特别行政区政府新闻公报, Jul. 6, 2020, https://www.info.gov.hk/gia/general/202007/06/P2020070600527.htm.
[59] “香港特別行政區維護國家安全委員會舉行首次會議（附圖）,” 香港特别行政区政府新闻公报, Jul. 6, 2020, https://www.info.gov.hk/gia/general/202007/06/P2020070600527.htm; “駱惠寧,” 百度百科, accessed Oct. 13, 2021, https://baike.baidu.hk/item/%E9%A7%B1%E6%83%A0%E5%AF%A7/3511667.
[60] Telecommunications (Registration of SIM Cards) Regulation, (promulgated under the Hong Kong Legislative Council, Jun. 1, 2021), CCIB/SD 605-15/1, https://www.cedb.gov.hk/ccib/en/legco-business/document/LegCo%20Brief%20SIM_EN.pdf.
[61] Ibid.
[62] “Online Licenses Application,” OFCA, accessed Oct. 13, 2021, https://www.ofca.gov.hk/en/electronic_services/licence/index.html.
[63] 通訊事務管理局條例（第 616 章）,(promulgated by the Legislative Council of Hong Kong, Apr. 1, 2012), Cap. 616, https://www.elegislation.gov.hk/hk/cap616!en-sc?INDEX_CS=N.
[64] Ibid.
[65] “角色及職能,” OFCA, accessed Oct. 13, 2021, https://www.ofca.gov.hk/tc/about_us/roles_and_functions/index.html.
[66] Ibid.
[67] Office of the Communications Authority, “通訊事務管理局辦公室 二零二零至二一年度主要工作和計劃,” (Hong Kong: 2020), https://www.ofca.gov.hk/filemanager/ofca/tc/content_92/majortasks_20-21_c.pdf.
[68] Ibid.
[69] “Legislation,” Communications Authority, accessed Oct. 13, 2021, https://www.coms-auth.hk/en/policies_regulations/legislation/index.html.
[70] Ibid.
[71] “Regulation & Enforcement,” Communications Authority, accessed Oct. 13, 2021, https://www.coms-auth.hk/en/policies_regulations/index.html.
[72] “Consultancy Reports,” OFCA, accessed Oct. 13, 2021, https://www.ofca.gov.hk/en/industry_focus/pub_report/consultancy/index.html.
[73] “e-Applications/ Services,” OFCA, accessed Oct. 13, 2021, https://www.ofca.gov.hk/en/electronic_services/index.html.
[74] “Collaboration with Stakeholders,” Office of the Government Chief Information Officer, accessed Oct. 27, 2021, https://www.ogcio.gov.hk/en/our_work/information_cyber_security/collaboration/.
[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] “保安局-保安局全力落實《香港國安法》- 國家安全　全民有責,” 中华人民共和国香港特别行政区政府保安局, Aug. 1, 2021, https://www.sb.gov.hk/chi/nsl/nsed.html.
[81] Ibid.
[82] Ibid.
[83] “Organization Structure: Organization Chart of HKPF,” Hong Kong Police Force, accessed Oct. 14, 2021, https://www.police.gov.hk/ppp_en/01_about_us/os_chart.html.
[84] Ibid.
[85] Ibid.
[86] “'B' Department (Crime & Security),” Hong Kong Police Force, accessed Oct. 7, 2021, https://www.police.gov.hk/ppp_en/01_about_us/os_cs.html.
[87] “Cyber Security and Technology Crime Bureau (CSTCB),” Hong Kong Police Force, accessed Oct. 7, 2021, https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/tcd.html.
[88] Ibid.
[89] “網絡安全組協作隊提供的服務,” 香港警務處網, accessed Oct. 14, 2021, https://www.police.gov.hk/ppp_tc/04_crime_matters/tcd/tcd_services.html.
[90] Minutes of the 41st meeting of the Finance Committee of the Legislative Council, May 19, 2017, https://www.legco.gov.hk/yr16-17/english/fc/fc/minutes/fc20170519.pdf.
[91] Ibid.

[92] "丁部門(監管處) ," 香港警務處網, accessed Oct. 14, 2021, https://www.police.gov.hk/ppp_tc/01_about_us/os_ms.html.
[93] Ibid.
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Christy Leung, "Hong Kong police to launch national security hotline for public to help specialist officers enforce Beijing-imposed law," South China Morning Post, Oct. 28, 2020, https://www.scmp.com/news/hong-kong/law-and-crime/article/3107489/hong-kong-police-launch-national-security-hotline.
[99] Ibid.
[100] Ibid.
[101] 莊芷游, 梁思行, "學生動源四名前成員被上門拘捕 涉違國安法 警方深夜記者會實錄," Initium Media, Jul. 29, 2020, https://theinitium.com/article/20200730-whatsnew-student-localism-arrested-national-security-law/.
[102] "警務處國家安全處根據《香港國安法》展開執法行動," 香港特別行政区新闻公报, Jul. 21, 2021, https://www.info.gov.hk/gia/general/202107/21/P2021072100376.htm.
[103] "港警国安处拘捕壹传媒五高层 壹传媒停牌," Zaobao, Jun. 17, 2021, https://www.zaobao.com.sg/realtime/china/story20210617-1157187.
[104] Shibani Mahtani and Eva Dou, "China's security law sends chill through Hong Kong, 23 years after handover," Washington Post, Jun. 30, 2020, https://www.washingtonpost.com/world/asia_pacific/hong-kong-national-security-law-ends-freedom-democracy-china/2020/06/30/c37e5a4a-ba8b-11ea-97c1-6cf116ffe26c_story.html.
[105] "港版國安法｜香港寬頻事隔 6 日改口 首認按《國安法》封「香港編年史」網站," 苹果新闻, Jan. 15, 2021, https://web.archive.org/web/20210128033931/https://hk.appledaily.com/local/20210114/MTWLC2Y2GRDPHMMRRMWPFTYSKE/.
[106] Rhoda Kwan, "In a first under security law, Hong Kong police order telecom firms to block anti-gov't doxing website – report," Hong Kong Free Press, Jan, 11, 2021, https://hongkongfp.com/2021/01/11/in-a-first-under-security-law-hong-kong-police-order-telecoms-firms-to-block-anti-govt-doxing-website/; "港府疑再封網　民進黨官網、國軍募兵網站無法瀏覽," 苹果新闻, Apr. 25, 2021, https://web.archive.org/web/20210429013008/https://tw.appledaily.com/international/20210425/XLB3JBWX7NBVTDK3ZCSJGSACJ4/.
[107] Gary Cheung and Christy Leung, "Hong Kong police unit dedicated to enforcing new national security law already in the works, minister reveals to Post," South China Morning Post, Jun. 10, 2020, https://www.scmp.com/news/hong-kong/law-and-crime/article/3088261/hong-kong-police-unit-dedicated-enforcing-new-national.
[108] 岳弘彬, "国家安全部：香港国安法依法治港 坚决贯彻党中央重大决策部署," 人民网, Jul. 5, 2020, http://politics.people.com.cn/n1/2020/0705/c1001-31771607.html; Jun Mai, "China Ministry of Public Security backs Hong Kong police in rolling out national security law," South China Morning Post, Jul. 5, 2020, https://www.scmp.com/news/china/politics/article/3091900/china-ministry-public-security-backs-hong-kong-police-rolling.
[109] Office of the Government Chief Information Officer, *Practice Guide for Information Security Incident Handling [ISPG-SM02] Version 1.1*, (Hong Kong: Office of the Government Chief Information Officer for the Government of the Hong Kong Special Administrative Region, 2017), accessed Oct. 14, 2021, https://www.govcert.gov.hk/doc/ispg-sm02_en.pdf.
[110] Ibid.
[111] Ibid.
[112] Ibid.
[113] Ibid.
[114] Ibid.
[115] "政府電腦保安事故協調中心 (GovCERT.HK)," GovCert, accessed Oct. 14, 2021, https://www.govcert.gov.hk/tc/about.html.
[116] Ibid.

[117] "政府電腦保安事故協調中心 (GovCERT.HK)," GovCert, accessed Oct. 14, 2021, https://www.govcert.gov.hk/tc/about.html; Office of the Government Chief Information Officer, *Practice Guide for Information Security Incident Handling [ISPG-SM02] Version 1.1*, (Hong Kong: Office of the Government Chief Information Officer for the Government of the Hong Kong Special Administrative Region, 2017), accessed Oct. 14, 2021, https://www.govcert.gov.hk/doc/ispg-sm02_en.pdf.
[118] "使命," 香港電腦保安事故協調中心, accessed Oct. 14, 2021, https://www.hkcert.org/tc/about-us/mission.
[119] Ibid.
[120] Ibid.
[121] "「共建安全網絡」資訊保安推廣活動," 香港金融管理局, accessed Oct. 14, 2021, https://www.hkma.gov.hk/chi/smart-consumers/public-education-events/build-a-secure-cyberspace-promotional-campaign/.
[122] 国家计算机网络应急技术处理协调中心, *2014 中国互联网网络安全报告* (北京： 人民邮电出版社，2014), accessed Oct. 14, 2021, http://www.cac.gov.cn/files/pdf/wlaq/Annual%20Report/2014AnnualReport1.pdf.
[123] Ibid.
[124] Hong Kong Computer Emergency Response Team Coordination Centre, *Annual Report 2016* (Hong Kong: Hong Kong Productivity Council, 2016), accessed Oct. 14, 2021, https://www.hkcert.org/f/press_center/246401/3a692971-8158-4213-b38c-ba46f841ed9f-DLFE-10901.pdf.
[125] "個人資料私隱專員歡迎辭," Office of the Privacy Commissioner for Personal Data, accessed Oct. 14, 2021, https://www.pcpd.org.hk/tc_chi/about_pcpd/commissioner/commissioner.html.
[126] "Ibid.
[127] Kathleen Magramo, "Veteran government lawyer appointed to lead Hong Kong's privacy watchdog amid concerns over national security law, doxxing incidents," South China Morning Post, Jul. 24, 2020, https://www.scmp.com/news/hong-kong/politics/article/3094593/veteran-government-lawyer-tapped-lead-hong-kongs-privacy.
[128] Personal Data (Privacy) (Amendment) Ordinance 2021, (promulgated by the Hong Kong Legislative Council, Oct. 8, 2021), Ord. No. 32 of 202, A3363, https://www.gld.gov.hk/egazette/pdf/20212540/es12021254032.pdf.
[129] Pak Yiu, "Hong Kong legislature passes controversial anti-doxxing privacy bill," Reuters, Sep. 29, 2021, https://www.reuters.com/world/asia-pacific/hong-kong-legislature-passes-controversial-anti-doxxing-privacy-bill-2021-09-29/.
[130] Ibid.
[131] Guidelines for the Application for Services-Based Operator ("SBO") Licence, (promulgated by the Office of the Communications Authority of Hong Kong, June 1, 2012), GN-40/2012, https://www.coms-auth.hk/filemanager/common/licensing/SBO-Guideline.pdf.
[132] Ibid.
[133] Ibid.
[134] "List of Internet Service Providers," Office of the Communications Authority, accessed Oct. 7, 2021, https://www.ofca.gov.hk/en/news_info/data_statistics/Internet/list_of_Internet_service_providers/index.html.
[135] Guidelines for the Application for Services-Based Operator ("SBO") Licence, (promulgated by the Office of the Communications Authority of Hong Kong, June 1, 2012), GN-40/2012, https://www.coms-auth.hk/filemanager/common/licensing/SBO-Guideline.pdf.
[136] Ibid.
[137] "List of Internet Service Providers," Office of the Communications Authority, accessed Oct. 7, 2021, https://www.ofca.gov.hk/en/news_info/data_statistics/Internet/list_of_Internet_service_providers/index.html.
[138] Guidelines for Submission of Applications for Unified Carrier Licence, (promulgated by the Office of the Communications Authority of Hong Kong, Dec. 31, 2020, Issue 15), GN-12/2020, https://www.coms-auth.hk/filemanager/statement/en/upload/544/gn122020.pdf.
[139] Ibid.

[140] "List of Internet Service Providers," Office of the Communications Authority, accessed Oct. 7, 2021, https://www.ofca.gov.hk/en/news_info/data_statistics/Internet/list_of_Internet_service_providers/index.html.
[141] "About China Mobile Hong Kong Company Limited," China Mobile Hong Kong, accessed Oct. 7, 2021, https://eshop.hk.chinamobile.com/en/about_us/corporate_overview/index.html; List of Internet Service Providers," Office of the Communications Authority, accessed Oct. 7, 2021, https://www.ofca.gov.hk/en/news_info/data_statistics/Internet/list_of_Internet_service_providers/index.html.
[142] "Cable Landing Stations in HK," Submarine Cable Networks, accessed Oct. 7, 2021, https://www.submarinenetworks.com/stations/asia/hongkong.
[143] "China Mobile's Hainan-Hong Kong submarine optical cable system is fully integrated," Hugewealth Finance, Jun. 30, 2021, https://www.hugewealthfinance.com/2021/china-mobiles-hainan-hong-kong-submarine-optical-cable-system-is-fully-integrated.
[144] "Home Broadband," China Mobile Hong Kong, accessed Oct. 8, 2021, https://eshop.hk.chinamobile.com/en/broadband/home.html.
[145] "China Mobile Hong Kong Triumphs As Hong Kong's Fastest 5G Network," Taiwan News, Apr. 1, 2021, https://www.taiwannews.com.tw/en/news/4166296.
[146] List of Internet Service Providers," Office of the Communications Authority, accessed Oct. 7, 2021, https://www.ofca.gov.hk/en/news_info/data_statistics/Internet/list_of_Internet_service_providers/index.html; "ComNet," CITIC Telecom International, accessed Oct. 7, 2021, https://www.citictel.com/subsidiary/%E4%BF%A1%E9%80%9A%E9%9B%BB%E8%A9%B1-comnet/.
[147] "Hutchison Global Crossing and China Telecom announce inauguration of Guangzhou-Shenzhen-Hong Kong SDH Ring: First new fixed network provider in Hong Kong to link up mainland network," CK Hutchison Holdings Limited, Oct. 12, 2000, https://www.ckh.com.hk/en/media/press_each.php?id=319.
[148] "Global Switch launches state-of-the-art HK$5bn Hong Kong data centre services with China Telecom Global and Daily-Tech," Global Switch, Dec. 13, 2017, https://www.globalswitch.com/about-us/news/13-12-17-global-switch-launches-state-of-the-art-hk-5bn-hong-kong-data-centre-services-with-china-telecom-global-and-daily-tech/.
[149] "Global Business," CTExcel, accessed Oct. 8, 2021, https://www.ctexcel.com/global/globalBusiness-en.html.
[150] "Mobile Services," ComNet, accessed Oct. 8, 2021, https://www.comnet-telecom.com.hk/en/mobile-plan/; "Fixed Network Operators and Mobile Network Operators," Office of the Communications Authority, accessed Oct. 8, 2021, https://www.ofca.gov.hk/en/consumer_focus/operators_information/telecommunications_services_providers/index.html; "Home," ComNet, accessed Oct. 8, 2021, https://www.comnet-telecom.com.hk/en.
[151] Xiaofei Li, *China's Outward Foreign Investment: A Political Perspective*, University Press of America, 2010, https://books.google.nl/books?id=xVK8edumB2AC&pg=PA97&lpg=PA97&dq=pccw+sasac&source=bl&ots=9Q_dVPg9Ff&sig=ACfU3U2tby5n725hJUaxxFignqJYDtPGag&hl=en&sa=X&ved=2ahUKEwj6pt7b-7jzAhXZwQIHHaCxBYcQ6AF6BAgREAM.
[152] "Milestones," HKT, accessed Oct. 7, 2021, https://www.hkt.com/about-hkt/company-profile/milestones/index.page?sectionId=2&locale=en.
[153] Xiaofei Li, *China's Outward Foreign Investment: A Political Perspective*, University Press of America, 2010.
[154] "Bio: Mai Yanzhou," China Unicom, accessed Oct. 7, 2021, https://www.chinaunicom.com.hk/en/about/bio.php?from=directors&id=maiyanzhou.
[155] "Milestones," HKT, accessed Oct. 7, 2021, https://www.hkt.com/about-hkt/company-profile/milestones/index.page?sectionId=2&locale=en.
[156] Ibid.
[157] "What Kind of Shareholders Own the Hong Kong and China Gas Company Limited (HKG:3)?" Simply Wall St, Apr. 14, 2021, https://simplywall.st/stocks/hk/utilities/hkg-3/hong-kong-and-china-gas-shares/news/what-kind-of-shareholders-own-the-hong-kong-and-china-gas-co-1.
[158] "Business Overview," MTR, accessed Oct. 7, 2021, https://www.mtr.com.hk/en/corporate/overview/profile_index.html; "About TraxComm," TraxComm, accessed Oct. 7, 2021, https://www.traxcomm.hk/about_us/mission/.

[159] "Fixed Network Operators and Mobile Network Operators," Office of the Communications Authority, accessed Oct. 8, 2021, https://www.ofca.gov.hk/en/consumer_focus/operators_information/telecommunications_services_providers/index.html.
[160] Minutes of the 2nd Meeting of the Planning and District Facilities Management Committee (2018) of Kwai Tsing District Council, Apr. 17, 2018, accessed Oct. 8, 2021, https://www.districtcouncils.gov.hk/kwt/doc/2016_2019/en/committee_meetings_minutes/DFMC/2nd_2018_minutes_en.pdf.
[161] "Fiber optic to shine in fixed broadband in Hong Kong," Telecomlead, Mar. 24, 2021, https://www.telecomlead.com/broadband/fiber-optic-to-shine-in-fixed-broadband-in-hong-kong-99329.
[162] Minutes of the 2nd Meeting of the Planning and District Facilities Management Committee (2018) of Kwai Tsing District Council, Apr. 17, 2018, accessed Oct. 8, 2021, https://www.districtcouncils.gov.hk/kwt/doc/2016_2019/en/committee_meetings_minutes/DFMC/2nd_2018_minutes_en.pdf.
[163] Minutes of the 2nd Meeting of the Planning and District Facilities Management Committee (2018) of Kwai Tsing District Council, Apr. 17, 2018, accessed Oct. 8, 2021, https://www.districtcouncils.gov.hk/kwt/doc/2016_2019/en/committee_meetings_minutes/DFMC/2nd_2018_minutes_en.pdf.
[164] "Fixed Network Operators and Mobile Network Operators," Office of the Communications Authority, accessed Oct. 8, 2021, https://www.ofca.gov.hk/en/consumer_focus/operators_information/telecommunications_services_providers/index.html.
[165] "Services-Based Operator (SBO) Licences Enquiry," Office of the Communications Authority, accessed Oct. 8, 2021, https://app1.coms-auth.hk/apps/telecom_lic/content/sbo_lic_list.asp?mobservice=Y.
[166] United States Senate Committee on Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*, (Washington, D.C.: 2020), https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.
[167] Xiaofei Li, *China's Outward Foreign Investment: A Political Perspective*, University Press of America, 2010, https://books.google.nl/books?id=xVK8edumB2AC&pg=PA97&lpg=PA97&dq=pccw+sasac&source=bl&ots=9Q_dVPg9Ff&sig=ACfU3U2tby5n725hJUaxxFignqJYDtPGag&hl=en&sa=X&ved=2ahUKEwj6pt7b-7jzAhXZwQIHHaCxBYcQ6AF6BAgREAM.
[168] Ibid.
[169] "Bio: Mai Yanzhou," China Unicom, accessed Oct. 7, 2021, https://www.chinaunicom.com.hk/en/about/bio.php?from=directors&id=maiyanzhou.
[170] "Milestones," HKT, accessed Oct. 7, 2021, https://www.hkt.com/about-hkt/company-profile/milestones/index.page?sectionId=2&locale=en.
[171] "Connectivity," Towngas Telecom, accessed Oct. 8, 2021, https://www.towngastelecom.com/business-scope/connectivity/.
[172] Ibid.
[173] "About Us," Towngas Telecom, accessed Oct. 13, 2021, https://www.towngastelecom.com/about-us/introduction/.
[174] "About TraxComm," Traxcomm, accessed Oct. 8, 2021, https://www.traxcomm.hk/about_us/mission/.
[175] "Who are the Kwok brothers?" BBC News, Apr. 18, 2012, https://www.bbc.co.uk/news/business-17752115.
[176] Minutes of the 2nd Meeting of the Planning and District Facilities Management Committee (2018) of Kwai Tsing District Council, Apr. 17, 2018, accessed Oct. 8, 2021, https://www.districtcouncils.gov.hk/kwt/doc/2016_2019/en/committee_meetings_minutes/DFMC/2nd_2018_minutes_en.pdf.
[177] HKC International Holdings Ltd, *Annual Report 2021*, (Hong Kong: HKC International Holdings Ltd, 2021), https://hkc.com.hk/wp-includes/annualreport/e0248_210717_ar.pdf.
[178] "Home," i-Mobile, accessed Oct. 8, 2021, https://www.i-mobile.com.hk/tc/; "HomeLine Service," Cable TV HK, accessed Oct. 8, 2021, http://www.cabletv.com.hk/en/homeline.php.

[179] Karen Yeung, "Hutchison Telecom sells fixed-line network business for US$1.9b," South China Morning Post, Jul. 30, 2017, https://www.scmp.com/business/companies/article/2104676/hutchison-telecom-sells-fixed-line-business-us19b.
[180] "Company Profile," HGC Global Communications, accessed Oct. 8, 2021, https://www.hgc.com.hk/about-hgc/about-us/company-profile.
[181] "Milestones," HKBN, accessed Oct. 8, 2021, https://www.hkbn.net/new/en/about-us--our-company--milestones.shtml.
[182] "Easy Tone Network Limited: Southeast Asia Focus Telecommunication Services Provider," Easy Tone, accessed Oct. 8, 2021, http://www.easytone.net/wp-content/uploads/2021/01/Easy-Tone-Brochure-V4.3.pdf.
[183] "China & Overseas Project," Top Express Enterprise Group, accessed Oct. 8, 2021, http://www.topexpress.com/Projects/Overseas.html.
[184] "History & Milestones," Top Express Enterprise Group, accessed Oct. 12, 2021, http://www.topexpress.com/About-Us/History-Milestones.html.
[185] "China & Overseas Project," Top Express Enterprise Group, accessed Oct. 8, 2021, http://www.topexpress.com/Projects/Overseas.html.
[186] "Hong Kong Network," Superloop, accessed Oct. 8, 2021, https://www.superloop.com/our-network/hong-kong.html.
[187] United States Senate Committee on Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*, (Washington, D.C.: 2020), https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.
[188] Xiaofei Li, *China's Outward Foreign Investment: A Political Perspective*, University Press of America, 2010, https://books.google.nl/books?id=xVK8edumB2AC&pg=PA97&lpg=PA97&dq=pccw+sasac&source=bl&ots=9Q_dVPg9Ff&sig=ACfU3U2tby5n725hJUaxxFignqJYDtPGag&hl=en&sa=X&ved=2ahUKEwj6pt7b-7jzAhXZwQIHHaCxBYcQ6AF6BAgREAM.
[189] Xiaofei Li, *China's Outward Foreign Investment: A Political Perspective*, University Press of America, 2010, https://books.google.nl/books?id=xVK8edumB2AC&pg=PA97&lpg=PA97&dq=pccw+sasac&source=bl&ots=9Q_dVPg9Ff&sig=ACfU3U2tby5n725hJUaxxFignqJYDtPGag&hl=en&sa=X&ved=2ahUKEwj6pt7b-7jzAhXZwQIHHaCxBYcQ6AF6BAgREAM.
[190] "Bio: Mai Yanzhou," China Unicom, accessed Oct. 7, 2021, https://www.chinaunicom.com.hk/en/about/bio.php?from=directors&id=maiyanzhou.
[191] "Milestones," HKT, accessed Oct. 7, 2021, https://www.hkt.com/about-hkt/company-profile/milestones/index.page?sectionId=2&locale=en.
[192] "Who are the Kwok brothers?" BBC News, Apr. 18, 2012, https://www.bbc.co.uk/news/business-17752115.
[193] "About," Three Hong Kong, accessed Oct. 8, 2021, https://web.three.com.hk/about3hk/about/index-en.html.
[194] Jonathan Shieber, "China is reportedly using US satellite technologies to bolster its surveillance capabilities," Tech Crunch, Apr. 23, 2019, https://techcrunch.com/2019/04/23/china-is-reportedly-using-us-satellite-technologies-to-bolster-its-surveillance-capabilities/?guccounter=1; "Corporate Profile," CITIC Limited, accessed Oct. 13, 2021, https://www.citic.com/en/aboutus/.
[195] United States Senate Committee on Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*, (Washington, D.C.: 2020), https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.
[196] "Vodafone Business in Asia-Pacific," Vodafone, accessed Oct. 8, 2021, https://www.vodafone.com/business/why-vodafone/our-global-network/asia-pacific; "物联网,"Vodafone, accessed Oct. 8, 2021, https://www.vodafone.com/business/zh-cn.
[197] "U.S. Securities and Exchanges Commission Fork 10-K: Verizon Communications Inc," Verizon, 2020, https://www.verizon.com/about/sites/default/files/2020-Annual-Report-on-Form-10-K.PDF; "Verizon Hong Kong Limited," Office of the Government Chief Information Officer, accessed Oct. 8, 2021, https://www.ogcio.gov.hk/sc/our_work/business/business_window/doc/Verizon.pdf.

[198] "Why Choose Hong Kong Data Centers?" Equinix, accessed Oct. 8, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers; "IX Service," BBIX, accessed Sep. 27, 2021, https://www.bbix.net/en/service/ix/.
[199] "Consumer Alert on the Cessation of 21 Vianet," Office of the Communications Authority, Oct. 8, 2019, https://www.ofca.gov.hk/en/consumer_focus/guide/general/consumer_alert_on_the_service_cessation_of_21viane/index.html; "U.S. Securities and Exchange Commission Form 20-F: 21 ViaNet," 21 ViaNet Groups, 2020, https://21vianetgroupinc.gcs-web.com/static-files/396f9f63-8e53-4cc8-8548-94526c389720.
[200] "Hong Kong – The Prime Location for Data Centres," Office of the Government Chief Information Officer, Hong Kong Special Administrative Region, Jan. 2021, https://www.datacentre.gov.hk/en/downloads/HK%20as%20DC%20prime%20location.pdf.
[201] "Data Centre Facilitation Unit," Developing Data Centers in Hong Kong, accessed Oct. 12, 2021, https://www.datacentre.gov.hk/en/home.html#dcfu.
[202] "Hong Kong – The Prime Location for Data Centres," Office of the Government Chief Information Officer, Hong Kong Special Administrative Region, Jan. 2021.
[203] "Hong Kong Data Center Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021-2026)," Mordor Intelligence, accessed Oct. 12, 2021, https://www.mordorintelligence.com/industry-reports/hong-kong-data-center-market.
[204] "Tender awarded for site in Sha Tin," the Government of the Hong Kong Special Administrative Region, Jul. 8, 2020, https://www.info.gov.hk/gia/general/202007/08/P2020070800751.htm; Diana Li, "China Mobile Outbid Local Tycoons by 56% for Hong Kong Data Centre Site," Mingtiandi, Aug. 10, 2020, https://www.mingtiandi.com/real-estate/projects-real-estate/china-mobile-overbids-for-hong-kong-data-centre-site/.
[205] "Hong Kong Data Center Market," Baxtel, accessed Oct. 11, 2021, https://baxtel.com/data-center/hong-kong; "Colocation Hong Kong," Data Center Map, accessed Oct. 11, 2021, https://www.datacentermap.com/hong-kong/hong-kong/.
[206] Cheryl Heng, "Hong Kong's data centre providers eye regional expansion to meet surging demand as coronavirus drives Internet use," South China Morning Post, Sep. 5, 2021, https://www.scmp.com/business/companies/article/3147529/hong-kongs-data-centre-providers-eye-regional-expansion-meet.
[207] "Hong Kong Data Center Market," Baxtel, accessed Oct. 11, 2021, https://baxtel.com/data-center/hong-kong.
[208] "沙钢集团收购 Global Switch 24%股权," Global Switch, accessed Oct. 11, 2021, https://www.globalswitch.cn/about-us/news/27-08-2019-24-stake-in-global-switch-acquired-by-shagang-group/.
[209] "Report: Global Switch is on sale for $11bn," Data Center Dynamics, Jan. 6, 2021, https://www.datacenterdynamics.com/en/news/report-global-switch-sale-11bn/.
[210] "董事会简介," Global Switch, accessed Oct. 11, 2021, https://www.globalswitch.cn/about-us/board-members/.
[211] "Locations," iAdvantage, accessed Oct. 11, 2021, https://www.iadvantage.net/index.php/locations.
[212] "Company," iAdvantage, accessed Oct. 11, 2021, https://www.iadvantage.net/index.php/company.
[213] "Telecommunications," Sun Hung Kai Properties, accessed Oct. 11, 2021, https://www.shkp.com/en-US/our-business/non-property-portfolio-businesses/telecommunications.
[214] "HK1," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk1.
[215] "HK2," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk2.
[216] "HK3," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk3.
[217] "HK4," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk4.
[218] "HK5," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk5.
[219] "Hong Kong Metro: At-a-Glance," Equinix, 2020, https://www.equinix.nl/content/dam/eqxcorp/en_us/documents/resources/data-sheets/ds_hong_kong_china_metro_international_business_exchange_en_oct2020.pdf.

[220] "Global Executive Leadership," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/about/leadership; "Equinix Inc.," CNN Business, accessed Oct. 11, 2021, https://money.cnn.com/quote/shareholders/shareholders.html?symb=EQIX&subView=institutional.
[221] "HKCOLO: The Neutral Colocation Provider Bridging Asia Pacific," HKCOLO, accessed Oct. 12, 2021, https://www.hkcolo.com/hkc_website/site_flash/location.html; "About Us," Telehouse HK, accessed Oct. 12, 2021, https://telehouse.com.hk/en/about-us/.
[222] "Asia Data Centers," Telehouse, accessed Oct. 11, 2021, https://www.telehouse.com/global-data-centers/asia/.
[223] "Trailblazing: Hong Kong Data Center Operator HKCOLO.NET Welcomes HKIX," HKCOLO, 2017, https://www.hkcolo.com/news/press-release1.html.
[224] "PCCW Solutions," Data Center Map, accessed Oct. 11, 2021, https://www.datacentermap.com/company/pccw-solutions_datacenters.html.
[225] "PCCW sells data center business to DigitalBridge for $750m," Data Center Dynamics, Jul. 26, 2021, https://www.datacenterdynamics.com/en/news/pccw-sells-data-center-business-to-digitalbridge-for-750m/.
[226] "Colony Capital Announces Rebrand as DigitalBridge," BusinessWire, Jun. 8, 2021, https://www.businesswire.com/news/home/20210608005723/en/Colony-Capital-Announces-Rebrand-as-DigitalBridge.
[227] "Colony Capital Announces Rebrand as DigitalBridge," BusinessWire, Jun. 8, 2021, https://www.businesswire.com/news/home/20210608005723/en/Colony-Capital-Announces-Rebrand-as-DigitalBridge.
[228] "Data Centre," CITIC, 2017, https://www.citictel.com/wp-content/uploads/2017/05/CTT-Data-Centre-leaflet-2017.pdf.
[229] "CITIC Telecom CPC," Baxtel, accessed Oct. 12, 2021, https://baxtel.com/data-center/citic-telecom-cpc.
[230] "Products & Services," CITIC, accessed Oct. 12, 2021, https://www.citictel-cpc.com/EN/NL/Pages/product-services/asia-pacific-data-center.
[231] "Data Centre," CITIC, 2017, https://www.citictel.com/wp-content/uploads/2017/05/CTT-Data-Centre-leaflet-2017.pdf.
[232] "What is an Internet Exchange Point?" ThousandEyes, accessed Oct. 8, 2021, https://www.thousandeyes.com/learning/techtorials/Internet-exchange-point.
[233] Ibid.
[234] "Your Interconnection Platform in Hong Kong," AMS IX Hong Kong, accessed Sep. 27, 2021, https://www.ams-ix.net/hk; "Internet Exchange Services," ACME HK, accessed Sep. 27, 2021, https://www.acmehk.net/solutions/connectivity/Internet-exchange-services/; "Equinix Internet Exchange," Equinix, accessed Sep. 27, 2021, https://www.equinix.se/interconnection-services/Internet-exchange; "IX Service," BBIX, accessed Sep. 27, 2021, https://www.bbix.net/en/service/ix/; "Internet Exchange," Megaport, accessed Sep. 27, 2021, https://www.megaport.com/services/Internet-exchange/.
[235] "TraxComm Networks and Services," TraxComm, accessed Oct. 11, 2021, https://www.traxcomm.hk/network_service/coverage/; Chee-Hoo Cheng, "HKIX General," (presentation, APRICOT 2014, 2014), accessed Sep. 27, 2021, http://www.hkix.net/hkix/Presentation/APRICOT2014.pdf.
[236] "News/Announcements," HKIX, Aug. 10, 2021, http://www.hkix.net/.
[237] "Satellite Sites," HKIX, accessed Oct. 11, 2021, http://www.hkix.net/hkix/satellite-sites.htm.
[238] Tony Cheung, "National security law: Chinese University of Hong Kong's student union becomes latest opposition-leaning group to disband under pressure," South China Morning Post, Oct. 7, 2021, https://www.scmp.com/news/hong-kong/politics/article/3151478/national-security-law-chinese-university-hong-kongs-student.
[239] "AMS-IX Colocation," AMS-IX, accessed Oct. 11, 2021, https://www.ams-ix.net/hk/colocations.
[240] "HK1," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk1.
[241] "HK2," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk2.
[242] "HK3," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk3.

[243] "HK4," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk4.
[244] "HK5," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk5.
[245] "Hong Kong Metro: At-a-Glance," Equinix, 2020, https://www.equinix.nl/content/dam/eqxcorp/en_us/documents/resources/data-sheets/ds_hong_kong_china_metro_international_business_exchange_en_oct2020.pdf.
[246] "Global Executive Leadership," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/about/leadership; "Equinix Inc.," CNN Business, accessed Oct. 11, 2021, https://money.cnn.com/quote/shareholders/shareholders.html?symb=EQIX&subView=institutional.
[247] "BBIX Hong Kong," Inflect, accessed Oct. 11, 2021, https://inflect.com/ix/bbix-hong-kong#top.
[248] "HK1," Equinix, accessed Oct. 11, 2021, https://www.equinix.com/data-centers/asia-pacific-colocation/hong-kong-colocation/hong-kong-data-centers/hk1.
[249] "Company Info," BBIX, accessed Oct. 12, 2021, https://www.bbix.net/en/company/.
[250] "ACME Universal Communications," Data Center Map, accessed Oct. 11, 2021, https://www.datacentermap.com/company/acme-universal-communications.html.
[251] "Internet Exchange," ACME, accessed Oct. 11, 2021, https://www.acmehk.net/solutions/connectivity/Internet-exchange-services/.
[252] "ACME Universal Communications," Data Center Map, accessed Oct. 11, 2021, https://www.datacentermap.com/company/acme-universal-communications_datacenters.html.
[253] Ibid.
[254] "Internet Exchange," ACME, accessed Oct. 11, 2021, https://www.acmehk.net/solutions/connectivity/Internet-exchange-services/.
[255] "ACME Universal Communications," Data Center Map, accessed Oct. 11, 2021, https://www.datacentermap.com/company/acme-universal-communications_datacenters.html.
[256] "Megaport Enabled Locations," Megaport, accessed Oct. 11, 2021, https://www.megaport.com/megaport-enabled-locations/.
[257] "Autonomous System Number (ASN) from AFRINIC," AFRINIC, accessed Oct. 12, 2021, https://afrinic.net/asn.
[258] "1020 AS Numbers (ASN) are allocated to Hong Kong," IP Geolocation, accessed Oct. 12, 2021, https://ipgeolocation.io/browse/asn/countries/HK.
[259] Ibid.
[260] "Cable Landing Stations in HK," Submarine Cable Networks, accessed Oct. 7, 2021, https://www.submarinenetworks.com/stations/asia/hongkong.
[261] "Chung Hom Kok Cable Landing Station," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/chung-hom-kok.
[262] Ibid.
[263] Ibid.
[264] "Cape D'Aguilar Cable Landing Station," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/cape-daguilar.
[265] Jason McGee-Abe, "PCCW Global lands AAE-1 cable system in Hong Kong," Capacity, Jul. 13, 2017, https://www.capacitymedia.com/articles/3732928/pccw-global-lands-aae-1-cable-system-in-hong-kong.
[266] "Cable Landing Stations in HK," Submarine Cable Networks, accessed Oct. 7, 2021, https://www.submarinenetworks.com/stations/asia/hongkong.
[267] "Deep Water Bay Cable Landing Station," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/deep-water-bay.
[268] "Tseung Kwan O (TKO) Cable Landing Station (Telstra)," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/tseung-kwan-o; Winston Qiu, "Tseung Kwan O (TKO) Cable Landing Station (NTT)," Submarine Cable Networks, Feb. 15, 2020, https://www.submarinenetworks.com/en/stations/asia/hongkong/tko-cls-ntt.
[269] "ASE," Submarine Cable Networks, accessed Oct. 7, 2021, https://www.submarinenetworks.com/systems/intra-asia/ase.
[270] "EAC-C2C," Fiber Atlantic, accessed Oct. 7, 2021, http://www.fiberatlantic.com/system/5yLDB.
[271] United States Senate Committee on Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned*

Carriers, (Washington, D.C.: 2020), https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.
[272] United States Senate Committee on Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*, (Washington, D.C.: 2020), https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.
[273] Pat MacGrath, "Telstra to sell stake Hong Kong-based mobile phone business CSL to HKT Limited for $2 billion," Dec. 20, 2013, https://www.abc.net.au/news/2013-12-20/telstra-to-sell-hong-kong-mobile-business/5169156.
[274] Paul Mah, "Why Telstra is paying $700m for Pacnet," Data Center Dynamics, Jan. 12, 2015, https://www.datacenterdynamics.com/en/analysis/why-telstra-is-paying-700m-for-pacnet/.
[275] "ASE," Submarine Cable Networks, accessed Oct. 7, 2021, https://www.submarinenetworks.com/systems/intra-asia/ase.
[276] Winston Qiu, "Tseung Kwan O (TKO) Cable Landing Station (CMI)," Submarine Cable Networks, Feb. 15, 2020, https://www.submarinenetworks.com/en/stations/asia/hongkong/tko-cls-cmi.
[277] Ibid.
[278] Paul Mah, "Why Telstra is paying $700m for Pacnet," Data Center Dynamics, Jan. 12, 2015, https://www.datacenterdynamics.com/en/analysis/why-telstra-is-paying-700m-for-pacnet/.
[279] "EAC-C2C," Submarine Cable Networks, accessed Oct. 7, 2021, https://www.submarinenetworks.com/en/systems/intra-asia/eac-c2c.
[280] "Tseung Kwan O (TKO) Cable Landing Station (Telstra)," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/tseung-kwan-o.
[281] Reach, *Asia-America Gateway (AAG) Cable Network, South Lantau: Project Profile*, (Hong Kong: Reach, Oct. 2007), accessed Oct. 7, 2021, https://www.epd.gov.hk/eia/register/profile/latest/dir160/dir160.pdf.
[282] "Tong Fuk Cable Landing Station," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/tong-fuk.
[283] Reach: *Asia-America Gateway (AAG) Cable Network, South Lantau: Project Profile*, (Hong Kong: Reach, Oct. 2007), accessed Oct. 7, 2021, https://www.epd.gov.hk/eia/register/profile/latest/dir160/dir160.pdf.
[284] "Tong Fuk Cable Landing Station," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/tong-fuk.
[285] "Cape D'Aguilar Cable Landing Station," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/cape-daguilar.
[286] "Members Portfolios Property Registers," 香港物業管理公司協會有限公司, May 28, 2019, https://hkapmc.org.hk/wp-content/uploads/2018/04/PCPD-Facilities-PR.pdf.
[287] "Chung Hom Kok Cable Landing Station," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/chung-hom-kok.
[288] "Deep Water Bay Cable Landing Station," Submarine Cable Networks, May 17, 2011, https://www.submarinenetworks.com/en/stations/asia/hongkong/deep-water-bay.
[289] Constitutional and Mainland Affairs Bureau, *Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area* (Hong Kong: Constitutional and Mainland Affairs Bureau, Feb. 18, 2019), https://www.bayarea.gov.hk/filemanager/en/share/pdf/Outline_Development_Plan.pdf.
[290] China Mobile International Ltd, "China Mobile opens first cross-border optical cable on Hong Kong-Zhuhai-Macao Bridge, helps facilitate development of the Guangdong-Hong Kong-Macao Greater Bay Area," PR Newswire, Apr. 11, 2018, https://en.prnasia.com/releases/apac/china-mobile-opens-first-cross-border-optical-cable-on-hong-kong-zhuhai-macao-bridge-helps-facilitate-development-of-the-guangdong-hong-kong-macao-greater-bay-area-207279.shtml.
[291] Ibid.
[292] Ibid.
[293] 王德清, "中国移动率先打通港珠澳大桥跨境光缆 助力粤港澳大湾区腾飞," CWW, Apr. 12, 2018, http://www.cww.net.cn/article?id=430187.
[294] "China Mobile's Hainan-Hong Kong submarine optical cable system is fully integrated," Hugewealth Finance, Jun. 30, 2021, https://www.hugewealthfinance.com/2021/china-mobiles-hainan-hong-kong-submarine-optical-cable-system-is-fully-integrated.

[295] "Hutchison Global Crossing and China Telecom announce inauguration of Guangzhou-Shenzhen-Hong Kong SDH Ring," CK Hutchison Holdings, Oct. 12, 2000, https://www.ckh.com.hk/en/media/press_each.php?id=319.
[296] "HGC and China Telecom cooperate for the first carrier-to-carrier Interconnection at Hong Kong-Zhuhai- Macau Bridge," HGC Global Communications, May 8, 2018, https://www.hgc.com.hk/press-releases/hgc-and-china-telecom-cooperate-for-the-first-carrier-to-carrier-interconnection-at-hong-kong-zhuhai-macau-bridge.
[297] 朱文凤，" 重磅！中国电信国际在香港建成首条通信管道光缆！" CWW, Jan. 22, 2021, http://www.cww.net.cn/article?id=482217.
[298] "Network Capabilities," China Unicom, accessed Oct. 12, 2021, https://network.chinaunicomglobal.com/#/premium-network/premium-network.
[299] "HGC and China Telecom cooperate for the first carrier-to-carrier Interconnection at Hong Kong-Zhuhai- Macau Bridge," HGC Global Communications, May 8, 2018, https://www.hgc.com.hk/press-releases/hgc-and-china-telecom-cooperate-for-the-first-carrier-to-carrier-interconnection-at-hong-kong-zhuhai-macau-bridge.
[300] Ibid.
[301] Henry Hu, "The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration," *China Quarterly* 207 (2011), https://www.cambridge.org/core/journals/china-quarterly/article/abs/political-economy-of-governing-isps-in-china-perspectives-of-net-neutrality-and-vertical-integration/678FA3FEDDF28AE8B096CE9FC743B6F5.
[302] Daniel Anderson, "SplInternet: Behind the Great Firewall of China," *ACM Queue* 10, no. 11 (2012), https://queue.acm.org/detail.cfm?id=2405036.
[303] Young Xu, "Deconstructing the Great Firewall of China," ThousandEyes, Mar. 8, 2016, https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.
[304] Daniel Anderson, "SplInternet: Behind the Great Firewall of China," *ACM Queue* 10, no. 11 (2012), https://queue.acm.org/detail.cfm?id=2405036; Young Xu, "Deconstructing the Great Firewall of China," ThousandEyes, Mar. 8, 2016, https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.
[305] Ibid.
[306] Ibid.
[307] Jon Russell, "China's mobile operators are reportedly being told to ban all use of VPNs," Tech Crunch, Jul. 20, 2017, https://techcrunch.com/2017/07/10/china-vpn-ban/?guccounter=1.
[308] Michael Gargiulo, "Which Countries Block VPNs, and Why?" VPN.com, Apr. 7, 2021, https://www.vpn.com/guide/which-countries-block-vpn/.
[309] Molly Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*, (Princeton, NJ: Princeton University Press, 2018).
[310] Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (promulgated by the Hong Kong Chief Executive, Jun. 7, 2020), L.N. 139 of 2020, https://www.gld.gov.hk/egazette/pdf/20202449e/es220202449139.pdf.
[311] Ibid.
[312] Ibid.
[313] "美媒：香港拟修法惩罚"人肉搜索"脸谱网推特私下发函扬言退出香港," 人民网资讯, July 6, 2021, https://baijiahao.baidu.com/s?id=1704512654322451776&wfr=spider&for=pc; Mary Hui and Jane Li, "Why Hong Kong's proposed doxxing law alarms Google and Facebook," Quartz, July 21, 2021, https://qz.com/2036212/why-hong-kongs-doxxing-law-alarms-google-facebook-twitter/.
[314] Personal Data (Privacy) (Amendment) Bill 2021 (promulgated by the Hong Kong Leg. Co., July 13, 2021), CMAB/CR/7/22/45, https://www.legco.gov.hk/yr20-21/english/brief/cmabcr72245_20210714-e.pdf.
[315] "美媒：香港拟修法惩罚"人肉搜索"脸谱网推特私下发函扬言退出香港," 人民网资讯, July 6, 2021, https://baijiahao.baidu.com/s?id=1704512654322451776&wfr=spider&for=pc
[316] "美媒：香港拟修法惩罚"人肉搜索"脸谱网推特私下发函扬言退出香港," 人民网资讯, July 6, 2021, https://baijiahao.baidu.com/s?id=1704512654322451776&wfr=spider&for=pc; "香港拟修订私隐条例惩治人肉搜索，网络平台或担刑事责任," 南方都市报, July 8, 2021, https://www.163.com/dy/article/GEBPV4A305129QAF.html.
[317] Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (promulgated by the Hong Kong Chief

Executive, Jun. 7, 2020), L.N. 139 of 2020, https://www.gld.gov.hk/egazette/pdf/20202449e/es220202449139.pdf.
[318] Ibid.
[319] Ibid.
[320] Will Feuer, "Zuckerberg blasts Facebook rival TikTok for censorship in China, and he might be right ," CNBC, Oct. 17, 2019, https://www.cnbc.com/2019/10/17/facebook-ceo-zuckerberg-calls-out-tiktok-censorship-in-china.html; "China 'censors Hong Kong protest posts on social media,'" BBC, Sep. 29, 2014, https://www.bbc.com/news/world-asia-china-29411270; Charles Riley, "LinkedIn draws fire for China censorship," CNN Business, Jun. 4, 2014, https://money.cnn.com/2014/06/04/technology/linkedin-china-censorship/index.html.
[321] Selina Cheng, "Hong Kong gov't made 1,400 requests for user data from Apple, Google, Facebook and Twitter in year before security law," Hong Kong Free Press, May 8, 2021, https://hongkongfp.com/2021/05/08/hong-kong-govt-made-1400-requests-for-user-data-from-apple-google-facebook-and-twitter-in-year-before-security-law/.
[322] Ibid.
[323] "脸书、谷歌、推特也"跟风"：暂停处理港府索取用户数据的要求," 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc; 暂停处理港府索取用户数据的要求," 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc; Ellen Nakashima, Shibani Mahtani, and Rachel Lerman, "Google ends direct cooperation with Hong Kong authorities on data requests," Washington Post, Aug. 14, 2020, https://www.washingtonpost.com/world/asia_pacific/google-hong-kong-national-security-law-data-requests/2020/08/14/c492b9e2-ddce-11ea-b4f1-25b762cdbbf4_story.html.
[324] "Government and Non-Government Information Requests," Twitter Transparency, July 14, 2021, https://transparency.twitter.com/en/reports/information-requests.html#2020-jul-dec; "Government Requests for User Data," Facebook Transparency Center, accessed Sept 24, 2021, https://transparency.fb.com/data/government-data-requests/; "Government requests to remove content" Google Transparency Report, accessed Sept 24, 2021, https://transparencyreport.google.com/government-removals/overview?hl=en; "Law Enforcement Requests Report," Microsoft Corporate Social Responsibility, accessed Sep. 24, 2021, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-reportintel.
[325] Ibid.
[326] Nathan Law, Twitter Post, Jun. 3, 2021, 6:03 a.m., https://twitter.com/nathanlawkc/status/1400392731189514243/photo/1; "[香港約章 2021」網站復活　網站供應商就錯誤刪網致歉　港警曾去信供應商要求下架," 立场新闻, Jun. 3, 2021, https://www.thestandnews.com/politics/%E9%A6%99%E6%B8%AF%E7%B4%84%E7%AB%A0-2021-%E7%B6%B2%E7%AB%99%E8%A2%AB%E5%B0%81-%E7%BE%85%E5%86%A0%E8%81%B0-%E8%AD%A6%E6%96%B9%E5%90%91%E7%B6%B2%E7%AB%99%E4%BE%9B%E6%87%89%E5%95%86%E7%99%BC%E4%BF%A1%E8%A6%81%E6%B1%82%E4%B8%8B%E6%9E%B6-%E6%8C%87%E5%85%A7%E5%AE%B9%E6%88%96%E9%81%95%E5%9C%8B%E5%AE%89%E6%B3%95.
[327] Nathan Law, Twitter Post, Jun. 3, 2021, 6:03 a.m., https://twitter.com/nathanlawkc/status/1400392731189514243/photo/2.
[328] Nathan Law, Twitter Post, Jun. 3, 2021, 6:03 a.m., https://twitter.com/nathanlawkc/status/1400392731189514243/photo/3.
[329] Nathan Law, Twitter Post, Jun. 3, 2021, 6:03 a.m., https://twitter.com/nathanlawkc/status/1400392731189514243/photo/4.
[330] Nathan Law, Twitter Post, Jun. 3, 2021, 9:13 a.m., https://twitter.com/nathanlawkc/status/1400440427422044161.
[331] Paul Mozur, "In Hong Kong, Short-Lived Censorship Hints at a Deeper Standoff," New York Times, Jun. 3, 2021, https://www.nytimes.com/2021/06/03/technology/hong-kong-Internet-censorship.html.
[332] "管过界? 港警要求以色列公司下架网站," DW.com, April 6, 2021, https://www.dw.com/zh/%E7%AE%A1%E8%BF%87%E7%95%8C-%E6%B8%AF%E8%AD%A6%E8%A6%81%E6%B1%82%E4%BB%A5%E8%89%B2%E5%88%97%E5%85%AC%E5%8F%B8%E4%B8%8B%E6%9E%B6%E7%BD%91%E7%AB%99/a-57775066.

[333] 艾米, "'香港编年史'成为《国安法》下首个被封的香港网站," RFI, Jan. 14, 2021, https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20210114-%E9%A6%99%E6%B8%AF%E7%BC%96%E5%B9%B4%E5%8F%B2-%E6%88%90%E4%B8%BA-%E5%9B%BD%E5%AE%89%E6%B3%95-%E4%B8%8B%E9%A6%96%E4%B8%AA%E8%A2%AB%E5%B0%81%E7%9A%84%E9%A6%99%E6%B8%AF%E7%BD%91%E7%AB%99.

[334] Paul Mozur and Aaron Krolik, "A Hong Kong Website Gets Blocked, Raising Censorship Fears," New York Times, Jan. 9, 2021, https://www.nytimes.com/2021/01/09/technology/hong-kong-website-blocked.html; Cannix Yau and Christie Yeung, "Hong Kong police use national security law for first time to block access to website recording anti-government protests, officers' details," South China Morning Post, Jan. 9, 2021, https://www.scmp.com/news/hong-kong/law-and-crime/article/3117072/hong-kong-police-use-national-security-law-block; 林偉聰, "警疑封編年史新 IP 株連數百網站 IT 人批損香港營商環境," 苹果新闻, Jan. 12, 2021, https://web.archive.org/web/20210112165525/https://hk.appledaily.com/local/20210112/LL2N7DQUONA7ZHJYUJOOMJPNDM/; "【國安封網】中大學者：封網手法不一　或無明確指示　憂引入大陸「防火長城," 立场新闻，Jan. 14, 2021, https://www.thestandnews.com/politics/%E5%9C%8B%E5%AE%89%E5%B0%81%E7%B6%B2-%E4%B8%AD%E5%A4%A7%E5%AD%B8%E8%80%85-%E5%B0%81%E7%B6%B2%E6%89%8B%E6%B3%95%E4%B8%8D%E4%B8%80-%E6%88%96%E7%84%A1%E6%98%8E%E7%A2%BA%E6%8C%87%E7%A4%BA-%E6%86%82%E5%BC%95%E5%85%A5%E5%A4%A7%E9%99%B8-%E9%98%B2%E7%81%AB%E9%95%B7%E5%9F%8E.

[335] Ibid.

[336] 【國安封網】中大學者：封網手法不一　或無明確指示　憂引入大陸「防火長城," 立场新闻，Jan. 14, 2021, https://www.thestandnews.com/politics/%E5%9C%8B%E5%AE%89%E5%B0%81%E7%B6%B2-%E4%B8%AD%E5%A4%A7%E5%AD%B8%E8%80%85-%E5%B0%81%E7%B6%B2%E6%89%8B%E6%B3%95%E4%B8%8D%E4%B8%80-%E6%88%96%E7%84%A1%E6%98%8E%E7%A2%BA%E6%8C%87%E7%A4%BA-%E6%86%82%E5%BC%95%E5%85%A5%E5%A4%A7%E9%99%B8-%E9%98%B2%E7%81%AB%E9%95%B7%E5%9F%8E.

[337] Ibid.

[338] "台灣促進轉型正義委員會網站疑被禁 須用 VPN 經德、美登入," 苹果新闻, Feb. 13, 2021, https://web.archive.org/web/20210505132759/https://hk.appledaily.com/local/20210213/NJFC2CV2GRAEDBMN2HFCB752JE/.

[339] "【封網疑團】香港可重新登入台灣民進黨等兩網站　仍無法登入國軍招募網　保安局拒評," 立场新闻，Apr. 27, 2021, https://www.thestandnews.com/politics/%E5%B0%81%E7%B6%B2%E7%96%91%E5%9C%98-%E9%A6%99%E6%B8%AF%E5%8F%AF%E9%87%8D%E6%96%B0%E7%99%BB%E5%85%A5%E5%8F%B0%E7%81%A3%E6%B0%91%E9%80%B2%E9%BB%A8%E7%AD%89%E5%85%A9%E7%B6%B2%E7%AB%99-%E4%BB%8D%E7%84%A1%E6%B3%95%E7%99%BB%E5%85%A5%E5%9C%8B%E8%BB%8D%E6%8B%9B%E5%8B%9F%E7%B6%B2-%E4%BF%9D%E5%AE%89%E5%B1%80%E6%8B%92%E8%A9%95.

[340] "涉犯國安法　港封「台獨」教會網站," 文匯網, Apr. 4, 2021, https://www.wenweipo.com/a/202104/25/AP6084bc38e4b0476859b8404d.html.

[341] "【封網疑團】香港可重新登入台灣民進黨等兩網站　仍無法登入國軍招募網　保安局拒評," 立场新闻，Apr. 27, 2021, https://www.thestandnews.com/politics/%E5%B0%81%E7%B6%B2%E7%96%91%E5%9C%98-%E9%A6%99%E6%B8%AF%E5%8F%AF%E9%87%8D%E6%96%B0%E7%99%BB%E5%85%A5%E5%8F%B0%E7%81%A3%E6%B0%91%E9%80%B2%E9%BB%A8%E7%AD%89%E5%85%A9%E7%B6%B2%E7%AB%99-%E4%BB%8D%E7%84%A1%E6%B3%95%E7%99%BB%E5%85%A5%E5%9C%8B%E8%BB%8D%E6%8B%9B%E5%8B%9F%E7%B6%B2-%E4%BF%9D%E5%AE%89%E5%B1%80%E6%8B%92%E8%A9%95.

[342] 孔繁栩 and 鄭秋玲, "國安法一年｜「香港約章」網站再被禁　消息：港電訊商被勒令封網," 香港 01, Jun. 18, 2021,

https://web.archive.org/web/20210618123016/https://www.hk01.com/%E7%A4%BE%E6%9C%83%E6%96%B0%E8%81%9E/639845/%E5%9C%8B%E5%AE%89%E6%B3%95%E4%B8%80%E5%B9%B4-%E9%A6%99%E6%B8%AF%E7%B4%84%E7%AB%A0-%E7%B6%B2%E7%AB%99%E5%86%8D%E8%A2%AB%E7%A6%81-%E6%B6%88%E6%81%AF-%E6%B8%AF%E9%9B%BB%E8%A8%8A%E5%95%86%E8%A2%AB%E5%8B%92%E4%BB%A4%E5%B0%81%E7%B6%B2

[343] "脸书、谷歌、推特也"跟风":暂停处理港府索取用户数据的要求," 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc; 暂停处理港府索取用户数据的要求," 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc; Ellen Nakashima, Shibani Mahtani, and Rachel Lerman, "Google ends direct cooperation with Hong Kong authorities on data requests," Washington Post, Aug. 14, 2020, https://www.washingtonpost.com/world/asia_pacific/google-hong-kong-national-security-law-data-requests/2020/08/14/c492b9e2-ddce-11ea-b4f1-25b762cdbbf4_story.html.

[344] Lily Kuo, "China's Great Firewall descends on Hong Kong Internet users," Guardian, July 8, 2020, https://www.theguardian.com/world/2020/jul/08/china-great-firewall-descends-hong-kong-Internet-users; Tim Culpan, "Hong Kong Gets Its Great Firewall, One Brick at a Time," July 6, 2021, https://www.bloomberg.com/opinion/articles/2021-07-06/with-doxxing-law-hong-kong-gets-its-great-firewall-one-brick-at-a-time; Daniel Anderson, "SplInternet: Behind the Great Firewall of China," *ACM Queue* 10, no. 11 (2012), https://queue.acm.org/detail.cfm?id=2405036; Young Xu, "Deconstructing the Great Firewall of China," ThousandEyes, Mar. 8, 2016, https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.

[345] Young Xu, "Deconstructing the Great Firewall of China," ThousandEyes, Mar. 8, 2016, https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.

[346] "脸书、谷歌、推特也"跟风":暂停处理港府索取用户数据的要求," 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc.

[347] "Government and Non-Government Information Requests," Twitter Transparency, July 14, 2021, https://transparency.twitter.com/en/reports/information-requests.html#2020-jul-dec; "Government Requests for User Data," Facebook Transparency Center, accessed Sept 24, 2021, https://transparency.fb.com/data/government-data-requests/; "Government requests to remove content" Google Transparency Report, accessed Sept 24, 2021, https://transparencyreport.google.com/government-removals/overview?hl=en; "Law Enforcement Requests Report," Microsoft Corporate Social Responsibility, accessed Sep. 24, 2021, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-reportintel.

[348] Cannix Yau and Christie Yeung, "Hong Kong police use national security law for first time to block access to website recording anti-government protests, officers' details," South China Morning Post, Jan. 9, 2021, https://www.scmp.com/news/hong-kong/law-and-crime/article/3117072/hong-kong-police-use-national-security-law-block; 封網疑團】香港可重新登入台灣民進黨等兩網站　仍無法登入國軍招募網　保安局拒評," 立场新闻，Apr. 27, 2021, https://www.thestandnews.com/politics/%E5%B0%81%E7%B6%B2%E7%96%91%E5%9C%98-%E9%A6%99%E6%B8%AF%E5%8F%AF%E9%87%8D%E6%96%B0%E7%99%BB%E5%85%A5%E5%8F%B0%E7%81%A3%E6%B0%91%E9%80%B2%E9%BB%A8%E7%AD%89%E5%85%A9%E7%B6%B2%E7%AB%99-%E4%BB%8D%E7%84%A1%E6%B3%95%E7%99%BB%E5%85%A5%E5%9C%8B%E8%BB%8D%E6%8B%9B%E5%8B%9F%E7%B6%B2-%E4%BF%9D%E5%AE%89%E5%B1%80%E6%8B%92%E8%A9%95.

[349] 艾米, "'香港编年史'成为《国安法》下首个被封的香港网站," RFI, Jan. 14, 2021, https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20210114-%E9%A6%99%E6%B8%AF%E7%BC%96%E5%B9%B4%E5%8F%B2-%E6%88%90%E4%B8%BA-%E5%9B%BD%E5%AE%89%E6%B3%95-%E4%B8%8B%E9%A6%96%E4%B8%AA%E8%A2%AB%E5%B0%81%E7%9A%84%E9%A6%99%E6%B8%AF%E7%BD%91%E7%AB%99; Nathan Law, Twitter Post, Jun. 3, 2021, 6:03 a.m., https://twitter.com/nathanlawkc/status/1400392731189514243/photo/2.

[350] Kenji Kawase and Michelle Chan, "Hong Kongers erase digital footprints ahead of security laws," Nikkei Asia, Jun. 29, 2020, https://asia.nikkei.com/Politics/Hong-Kongers-erase-digital-footprints-ahead-of-security-laws; Jennifer Creery, "Hongkongers purge social media, delete accounts as Beijing passes national security law," Hong Kong Free Press, July 3, 2020, https://hongkongfp.com/2020/07/03/hongkongers-purge-social-media-delete-accounts-as-beijing-passes-

national-security-law/; Joshua Wong, “Using Technologies to Stand for Freedom in Hong Kong,” interview by Lindsay Lloyd, George W. Bush Presidential Center, October 13, 2020, https://www.bushcenter.org/publications/articles/2020/10/democracy-talks-using-technologies-to-stand-for-freedom-in-hong-kong.html#.

[351] “Ooni Explorer,” Open Observatory of Network Interference, accessed Sep. 24, 2021, https://explorer.ooni.org; 【國安封網】中大學者：封網手法不一　或無明確指示　憂引入大陸「防火長城,” 立场新闻，Jan. 14, 2021, https://www.thestandnews.com/politics/%E5%9C%8B%E5%AE%89%E5%B0%81%E7%B6%B2-%E4%B8%AD%E5%A4%A7%E5%AD%B8%E8%80%85-%E5%B0%81%E7%B6%B2%E6%89%8B%E6%B3%95%E4%B8%8D%E4%B8%80-%E6%88%96%E7%84%A1%E6%98%8E%E7%A2%BA%E6%8C%87%E7%A4%BA-%E6%86%82%E5%BC%95%E5%85%A5%E5%A4%A7%E9%99%B8-%E9%98%B2%E7%81%AB%E9%95%B7%E5%9F%8E; “港府疑再封網　民進黨官網、國軍募兵網站無法瀏覽,” 苹果新闻, Apr. 25, 2021, https://web.archive.org/web/20210429013008/https://tw.appledaily.com/international/20210425/XLB3JBWX7NBVTDK3ZCSJGSACJ4/.

[352] Lokman Tsui, “How tech companies should plan for Hong Kong’s precarious future,” Rest of World, accessed on Sep. 24, 2021, https://restofworld.org/2021/how-tech-companies-should-plan-for-hong-kongs-precarious-future/.

[353] Rita Liao, “VPN providers rethink Hong Kong servers after China’s security law,” Tech Crunch, July 15, 2021, https://techcrunch.com/2020/07/15/vpn-rethink-hong-kong-servers/.

[354] 美媒：香港拟修法惩罚“人肉搜索”脸谱网推特私下发函扬言退出香港,” 人民网资讯, July 6, 2021, https://baijiahao.baidu.com/s?id=1704512654322451776&wfr=spider&for=pc.

[355] Jon Fingas, “Google gave user data to Hong Kong officials despite moratorium promise,” Engadget, Sep. 11, 2021, https://www.engadget.com/google-gave-hong-kong-user-data-192728879.html.

[356] “Ooni Explorer,” Open Observatory of Network Interference, accessed Sep. 24, 2021, https://explorer.ooni.org;【國安封網】中大學者：封網手法不一　或無明確指示　憂引入大陸「防火長城,” 立场新闻，Jan. 14, 2021, https://www.thestandnews.com/politics/%E5%9C%8B%E5%AE%89%E5%B0%81%E7%B6%B2-%E4%B8%AD%E5%A4%A7%E5%AD%B8%E8%80%85-%E5%B0%81%E7%B6%B2%E6%89%8B%E6%B3%95%E4%B8%8D%E4%B8%80-%E6%88%96%E7%84%A1%E6%98%8E%E7%A2%BA%E6%8C%87%E7%A4%BA-%E6%86%82%E5%BC%95%E5%85%A5%E5%A4%A7%E9%99%B8-%E9%98%B2%E7%81%AB%E9%95%B7%E5%9F%8E; “港府疑再封網　民進黨官網、國軍募兵網站無法瀏覽,” 苹果新闻, Apr. 25, 2021, https://web.archive.org/web/20210429013008/https://tw.appledaily.com/international/20210425/XLB3JBWX7NBVTDK3ZCSJGSACJ4/.

[357] Daniel Anderson, “SplInternet: Behind the Great Firewall of China,” *ACM Queue* 10, no. 11 (2012), https://queue.acm.org/detail.cfm?id=2405036.

[358] Ibid.

[359] Ibid.

[360] Cormac Callanan, Hein Dries-Ziekenheiner, Alberto Escudero-Pascual, and Robert Guerra, “Leaping Over the Firewall: A Review of Censorship Circumvention Tools,” Freedom House, Mar., 2010, https://freedomhouse.org/sites/default/files/inline_images/Censorship.pdf.

[361] Young Xu, “Deconstructing the Great Firewall of China,” ThousandEyes, Mar. 8, 2016, https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.

[362] “Ooni Explorer,” Open Observatory of Network Interference, accessed Sep. 24, 2021, https://explorer.ooni.org.

[363] Ibid.

[364] 艾米, “‘香港编年史’成为《国安法》下首个被封的香港网站,” RFI, Jan. 14, 2021, https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20210114-%E9%A6%99%E6%B8%AF%E7%BC%96%E5%B9%B4%E5%8F%B2-%E6%88%90%E4%B8%BA-%E5%9B%BD%E5%AE%89%E6%B3%95-%E4%B8%8B%E9%A6%96%E4%B8%AA%E8%A2%AB%E5%B0%81%E7%9A%84%E9%A6%99%E6%B8%AF%E7%BD%91%E7%AB%99.

[365] “Ooni Explorer,” Open Observatory of Network Interference, accessed Sep. 24, 2021, https://explorer.ooni.org.

[366] “Hurricane Electric Internet Services,” Hurricane Electric, accessed on Sep. 24, 2021, https://bgp.he.net/AS10118.
[367] “PCCW IMS Limited,” DBIP, accessed on Sep. 24, 2021, https://db-ip.com/as4760-pccw-ims-limited.
[368] “AS17924 SmarTone Mobile Communications Ltd,” IPInfo.io, accessed on Sep. 24, 2021, https://ipinfo.io/AS17924.
[369] “Hurricane Electric Internet Services,” Hurricane Electric, accessed on Sep. 24, 2021, https://bgp.he.net/AS4515.
[370] “AS9908 Hong Kong Cable Television Limited,” BGP View, accessed on Sep. 24, 2021, https://bgpview.io/asn/9908.
[371] “Hurricane Electric Internet Services,” Hurricane Electric, accessed on Sep. 24, 2021, https://bgp.he.net/AS9269.
[372] “AS38819 CSL Limited,” DBIP, accessed on Sep. 24, 2021, https://db-ip.com/as38819-csl-limited
[373] “AS9304 HGC Global Communications Limited,” BGP View, accessed on Sep. 24, 2021, https://bgpview.io/asn/9304.
[374] “Hurricane Electric Internet Services,” Hurricane Electric, accessed on Sep. 24, 2021, https://bgp.he.net/AS133752.
[375] “Hurricane Electric Internet Services,” Hurricane Electric, accessed on Sep. 24, 2021, https://bgp.he.net/AS4641.
[376] “AS9231,” GBIR.net, accessed on Sep. 24, 2021, https://bgp.gibir.net.tr/as/9231.
[377] Huang Chunmei, “Taiwan Presbyterian Church Blocked by Hong Kong Pastor Huang Chunsheng Laments that Hong Kong has been ‘Inlandized,’” Radio Free Asia, April 26, 2021, https://www.bannedbook.org/en/bnews/ssgc/20210426/1534044.html.
[378] “苹果被指‘向北京折腰’库克称‘为保护用户,’” DW.com, Nov. 19, 2021, https://www.dw.com/zh/%E8%8B%B9%E6%9E%9C%E8%A2%AB%E6%8C%87%E5%90%91%E5%8C%97%E4%BA%AC%E6%8A%98%E8%85%B0-%E5%BA%93%E5%85%8B%E7%A7%B0%E4%B8%BA%E4%BF%9D%E6%8A%A4%E7%94%A8%E6%88%B7/a-50760376.
[379] “关于在中国苹果商店被审查的那 674 个软件,” GreatFire.org, Nov. 30, 2017, https://zh.greatfire.org/blog/2017/11%E6%9C%88/%E5%85%B3%E4%BA%8E%E5%9C%A8%E4%B8%AD%E5%9B%BD%E8%8B%B9%E6%9E%9C%E5%95%86%E5%BA%97%E8%A2%AB%E5%AE%A1%E6%9F%A5%E7%9A%84%E9%82%A3674%E4%B8%AA%E8%BD%AF%E4%BB%B6.
[380] 艾米, “‘香港编年史’成为《国安法》下首个被封的香港网站,” RFI, Jan. 14, 2021, https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20210114-%E9%A6%99%E6%B8%AF%E7%BC%96%E5%B9%B4%E5%8F%B2-%E6%88%90%E4%B8%BA-%E5%9B%BD%E5%AE%89%E6%B3%95-%E4%B8%8B%E9%A6%96%E4%B8%AA%E8%A2%AB%E5%B0%81%E7%9A%84%E9%A6%99%E6%B8%AF%E7%BD%91%E7%AB%99; ; Mary Hui and Jane Li, “Why Hong Kong’s proposed doxxing law alarms Google and Facebook,” Quartz, July 21, 2021, https://qz.com/2036212/why-hong-kongs-doxxing-law-alarms-google-facebook-twitter/; Selina Cheng, “Authorities may prosecute Hong Kong staff or ban overseas websites if they fail to remove doxxing content,” Hong Kong Free Press, May 18, 2021, https://hongkongfp.com/2021/05/18/authorities-may-prosecute-hong-kong-staff-or-ban-overseas-websites-if-they-fail-to-remove-doxxing-content/.
[381] Lokman Tsui, “How tech companies should plan for Hong Kong’s precarious future,” Rest of World, accessed on Sep. 24, 2021, https://restofworld.org/2021/how-tech-companies-should-plan-for-hong-kongs-precarious-future/.
[382] Government and Non-Government Information Requests,” Twitter Transparency, July 14, 2021, https://transparency.twitter.com/en/reports/information-requests.html#2020-jul-dec; “Government Requests for User Data,” Facebook Transparency Center, accessed Sept 24, 2021, https://transparency.fb.com/data/government-data-requests/; “Government requests to remove content” Google Transparency Report, accessed Sept 24, 2021, https://transparencyreport.google.com/government-removals/overview?hl=en; “Law Enforcement Requests Report,” Microsoft Corporate Social Responsibility, accessed Sep. 24, 2021, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-reportintel.
[383] “脸书、谷歌、推特也“跟风”：暂停处理港府索取用户数据的要求,” 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc; 暂停处理港府索取用户数据的要求,” 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc; Ellen Nakashima, Shibani

Mahtani, and Rachel Lerman, "Google ends direct cooperation with Hong Kong authorities on data requests," Washington Post, Aug. 14, 2020, https://www.washingtonpost.com/world/asia_pacific/google-hong-kong-national-security-law-data-requests/2020/08/14/c492b9e2-ddce-11ea-b4f1-25b762cdbbf4_story.html.
[384] Ibid.
[385] Nathan Law, Twitter Post, Jun. 3, 2021, 6:03 a.m., https://twitter.com/nathanlawkc/status/1400392731189514243/photo/4.
[386] Ibid.
[387] "OONI Tests," OONI, accessed Oct. 26, 2021, https://ooni.org/nettest/.
[388] "Ooni Explorer," Open Observatory of Network Interference, accessed Sep. 24, 2021, https://explorer.ooni.org.
[389] Ibid.
[390] Paul Mozur, "In Hong Kong, Short-Lived Censorship Hints at a Deeper Standoff," New York Times, Jun. 3, 2021, https://www.nytimes.com/2021/06/03/technology/hong-kong-Internet-censorship.html; Nathan Law, Twitter Post, Jun. 3, 2021, 9:13 a.m., https://twitter.com/nathanlawkc/status/1400440427422044161.
[391] Rebecca Davis, "China's Douban Platform Bans Popular Accounts as Censorship Is Raised for Tiananmen Square Anniversary," Variety, Jun. 3, 2021, https://variety.com/2021/digital/news/china-june-4-tiananmen-square-censorship-douban-1234988540/; Paul Mozur, "Twitter Takes Down Accounts of China Dissidents Ahead of Tiananmen Anniversary," The New York Times, Jun. 1, 2019, https://www.nytimes.com/2019/06/01/business/twitter-china-tiananmen.html; Kuang Keng Kuek Ser, "How China has censored words relating to the Tiananmen Square anniversary," The World, Jun. 4, 2016, https://www.pri.org/stories/2016-06-03/how-china-has-censored-words-relating-tiananmen-square-anniversary.
[392] 艾米, "'香港编年史'成为《国安法》下首个被封的香港网站," RFI, Jan. 14, 2021, https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20210114-%E9%A6%99%E6%B8%AF%E7%BC%96%E5%B9%B4%E5%8F%B2-%E6%88%90%E4%B8%BA-%E5%9B%BD%E5%AE%89%E6%B3%95-%E4%B8%8B%E9%A6%96%E4%B8%AA%E8%A2%AB%E5%B0%81%E7%9A%84%E9%A6%99%E6%B8%AF%E7%BD%91%E7%AB%99.
[393] Paul Mozur and Aaron Krolik, "A Hong Kong Website Gets Blocked, Raising Censorship Fears," New York Times, Jan. 9, 2021, https://www.nytimes.com/2021/01/09/technology/hong-kong-website-blocked.html.
[394] "Individuals Arrested under the Hong Kong National Security Law or by the National Security Department," China File, accessed Oct. 26, 2021, https://www.chinafile.com/individuals-arrested-under-hong-kong-national-security-law-or-national-security-department.
[395] Mary Hui, "Hong Kong's protest movement keeps getting stymied by Apple ties," Quartz, Jul. 14, 2020, https://qz.com/1879754/hong-kongs-protest-movement-stymied-by-apples-china-ties/.
[396] "Individuals Arrested under the Hong Kong National Security Law or by the National Security Department," China File, accessed Oct. 26, 2021, https://www.chinafile.com/individuals-arrested-under-hong-kong-national-security-law-or-national-security-department.
[397] "Ooni Explorer," Open Observatory of Network Interference, accessed Sep. 24, 2021, https://explorer.ooni.org;【國安封網】中大學者：封網手法不一　或無明確指示　憂引入大陸「防火長城," 立场新闻，Jan. 14, 2021, https://www.thestandnews.com/politics/%E5%9C%8B%E5%AE%89%E5%B0%81%E7%B6%B2-%E4%B8%AD%E5%A4%A7%E5%AD%B8%E8%80%85-%E5%B0%81%E7%B6%B2%E6%89%8B%E6%B3%95%E4%B8%8D%E4%B8%80-%E6%88%96%E7%84%A1%E6%98%8E%E7%A2%BA%E6%8C%87%E7%A4%BA-%E6%86%82%E5%BC%95%E5%85%A5%E5%A4%A7%E9%99%B8-%E9%98%B2%E7%81%AB%E9%95%B7%E5%9F%8E; "港府疑再封網　民進黨官網、國軍募兵網站無法瀏覽," 苹果新闻, Apr. 25, 2021, https://web.archive.org/web/20210429013008/https://tw.appledaily.com/international/20210425/XLB3JBWX7NBVTDK3ZCSJGSACJ4/.
[398] King-wa Fu, Chung-hong Chan, and Michael Chau, "Assessing Censorship on Microblogs in China," *IEEE Internet Computing* 17, No. 3, pp. 42-50 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265271; Min Jiang, "Managing the micro-self: the governmentality of real name registration policy in Chinese microblogosphere,"

Information, Communication & Society 19, No. 2 (2016), https://www.tandfonline.com/doi/abs/10.1080/1369118X.2015.1060723; Samm Sacks and Paul Triolo, "Shrinking Anonymity in Chinese Cyberspace," Lawfare, Sep. 25, 2017, https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.

[399] Kenji Kawase and Michelle Chan, "Hong Kongers erase digital footprints ahead of security laws," Nikkei Asia, Jun. 29, 2020, https://asia.nikkei.com/Politics/Hong-Kongers-erase-digital-footprints-ahead-of-security-laws.

[400] Joshua Wong, "Using Technologies to Stand for Freedom in Hong Kong," interview by Lindsay Lloyd, George W. Bush Presidential Center, October 13, 2020, https://www.bushcenter.org/publications/articles/2020/10/democracy-talks-using-technologies-to-stand-for-freedom-in-hong-kong.html#.

[401] 梁偉澄,"近 7000 人被捕 逾 3700 手機成證物 李家超稱示威者具組織性曾外地受訓," 晴报, Jan. 9, 2020, https://skypost.ulifestyle.com.hk/article/2536978/; Ng Kang-Chung, "Hong Kong police seized more than 3,700 mobile phones from protesters in space of five months and had devices broken into to read contents, security chief reveals," South China Morning Post, Jan. 8, 2020, https://www.scmp.com/news/hong-kong/law-and-crime/article/3045263/hong-kong-police-seized-more-3700-mobile-phones.

[402] Kenji Kawase and Michelle Chan, "Hong Kongers erase digital footprints ahead of security laws," Nikkei Asia, Jun. 29, 2020, https://asia.nikkei.com/Politics/Hong-Kongers-erase-digital-footprints-ahead-of-security-laws; Jennifer Creery, "Hongkongers purge social media, delete accounts as Beijing passes national security law," Hong Kong Free Press, Jul. 3, 2020, https://hongkongfp.com/2020/07/03/hongkongers-purge-social-media-delete-accounts-as-beijing-passes-national-security-law/; Joshua Wong, "Using Technologies to Stand for Freedom in Hong Kong," interview by Lindsay Lloyd, George W. Bush Presidential Center, October 13, 2020, https://www.bushcenter.org/publications/articles/2020/10/democracy-talks-using-technologies-to-stand-for-freedom-in-hong-kong.html#.

[403] "周庭 Facebook 專頁消失-未交代原因," 立场新闻, Jun. 28, 2021, https://www.thestandnews.com/politics/%E5%91%A8%E5%BA%AD-facebook-%E5%B0%88%E9%A0%81%E6%B6%88%E5%A4%B1-%E6%9C%AA%E4%BA%A4%E4%BB%A3%E5%8E%9F%E5%9B%A0.

[404] King-wa Fu, Chung-hong Chan, and Michael Chau, "Assessing Censorship on Microblogs in China," *IEEE Internet Computing* 17, No. 3, pp. 42-50 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265271; Min Jiang, "Managing the micro-self: the governmentality of real name registration policy in Chinese microblogosphere," *Information, Communication & Society* 19, No. 2 (2016), https://www.tandfonline.com/doi/abs/10.1080/1369118X.2015.1060723; Samm Sacks and Paul Triolo, "Shrinking Anonymity in Chinese Cyberspace," Lawfare, Sep. 25, 2017, https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.

[405] 北京市微博客发展管理若干规定, (promulgated by the Beijing Municipal Gov., Dec. 29, 2011), 110069/ZK-2019-001274, http://jxj.beijing.gov.cn/zwgk/zfxxgk/zfxxgkml/201911/t20191113_511218.html; Paul Bischoff, "A brief history of China's campaign to enforce real-name registration online," Tech in Asia, Feb. 5, 2015, https://www.techinasia.com/history-chinas-campaign-enforce-realname-registration-online; "新增电话用户实行实名制 非实名老用户可以补办," 北方网, Sep. 1, 2013, https://www.911monitor.com/system/2013/09/01/011273172.shtml; "中国明年 7 月前实施网络实名登记制度," BBC China, Mar. 23, 2013, https://www.bbc.com/zhongwen/simp/china/2013/03/130328_china_Internet_registration.

[406] Samm Sacks and Paul Triolo, "Shrinking Anonymity in Chinese Cyberspace," Lawfare, Sep. 25, 2017, https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.

[407] Ibid.

[408] Doggen Xu and Qiming Ge, "Rules of real name registration for Internet access in China: infrastructure for cyber security?" Forensic Research & Criminology International Journal 6, No. 1 (2018), http://medcraveonline.com/FRCIJ/FRCIJ-06-00183.pdf; 中华人民共和国网络安全法, (promulgated by the Office of the Central Cyberspace Affairs Commission, Nov. 7, 2016, effective Jun. 1, 2017), 新华社, http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm.

[409] Doggen Xu and Qiming Ge, "Rules of real name registration for Internet access in China: infrastructure for cyber security?" *Forensic Research & Criminology International Journal* 6, No. 1 (2018), http://medcraveonline.com/FRCIJ/FRCIJ-06-00183.pdf.
[410] "香港将展开电话卡实名制公众咨询," QQ, Jan. 29, 2021, https://new.qq.com/omn/20210129/20210129A08PBY00.html; "Public views sought on Real-name Registration Programme for SIM Cards," the Government of the Hong Kong Administrative Region Press Releases, Jan. 29, 2021, https://www.info.gov.hk/gia/general/202101/29/P2021012900421.htm.
[411] Telecommunications (Registration of SIM Cards) Regulation, (promulgated under the Hong Kong Legislative Council, Jun. 1, 2021), CCIB/SD 605-15/1, https://www.cedb.gov.hk/ccib/en/legco-business/document/LegCo%20Brief%20SIM_EN.pdf.
[412] "Public views sought on Real-name Registration Programme for SIM Cards," the Government of the Hong Kong Administrative Region Press Releases, Jan. 29, 2021, https://www.info.gov.hk/gia/general/202101/29/P2021012900421.htm.
[413] Ibid.
[414] Rhoda Kwan, "Hong Kong's pre-paid SIM card users must register under new law," Hong Kong Free Press, Jun. 1, 2021, https://hongkongfp.com/2021/06/02/hong-kongs-pre-paid-sim-card-users-must-register-under-new-law/.
[415] Ibid.
[416] Telecommunications (Registration of SIM Cards) Regulation, (promulgated under the Hong Kong Legislative Council, Jun. 1, 2021), CCIB/SD 605-15/1, https://www.cedb.gov.hk/ccib/en/legco-business/document/LegCo%20Brief%20SIM_EN.pdf.
[417] Rhoda Kwan, "Hong Kong's pre-paid SIM card users must register under new law," Hong Kong Free Press, Jun. 1, 2021, https://hongkongfp.com/2021/06/02/hong-kongs-pre-paid-sim-card-users-must-register-under-new-law/.
[418] Telecommunications (Registration of SIM Cards) Regulation, (promulgated under the Hong Kong Legislative Council, Jun. 1, 2021), CCIB/SD 605-15/1, https://www.cedb.gov.hk/ccib/en/legco-business/document/LegCo%20Brief%20SIM_EN.pdf.
[419] Rhoda Kwan, "Hong Kong's pre-paid SIM card users must register under new law," Hong Kong Free Press, Jun. 1, 2021, https://hongkongfp.com/2021/06/02/hong-kongs-pre-paid-sim-card-users-must-register-under-new-law/.
[420] Ibid.
[421] "香港金管局加强电子钱包身份认证标准 明年变相推实名制," 信报, Dec. 15, 2020, https://www.mpaypass.com.cn/news/202012/15092422.html.
[422] "深圳测试香港居民数字人民币跨境支付," 深圳特区报, Apr. 1, 2021, http://www.locpg.gov.cn/jsdt/2021-04/01/c_1211093914.htm.
[423] David Caragliano, "Why China's 'Real Name' Internet Policy Doesn't Work," The Atlantic, Mar. 26, 2013, https://www.theatlantic.com/china/archive/2013/03/why-chinas-real-name-Internet-policy-doesnt-work/274373/; Paul Bischoff, "A brief history of China's campaign to enforce real-name registration online," Tech in Asia, Feb. 5, 2015, https://www.techinasia.com/history-chinas-campaign-enforce-realname-registration-online.
[424] Paul Bischoff, "A brief history of China's campaign to enforce real-name registration online," Tech in Asia, Feb. 5, 2015, https://www.techinasia.com/history-chinas-campaign-enforce-realname-registration-online.
[425] "财 8 点：支付宝、财付通都被央行罚 3 万元，百度网盘也要实名了," 资讯频道, May 11, 2017, http://inews.ifeng.com/51075826/news.shtml?&back; Samm Sacks and Paul Triolo, "Shrinking Anonymity in Chinese Cyberspace," Lawfare, Sep. 25, 2017, https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.
[426] Jyh-An Li and Ching-Yi Liu, "Real-Name Registration Rules and the Fading Digital Anonymity in China," *Washington International Law Journal* 25, No. 1 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2719384; David Caragliano, "Why China's 'Real Name' Internet Policy Doesn't Work," The Atlantic, Mar. 26, 2013, https://www.theatlantic.com/china/archive/2013/03/why-chinas-real-name-Internet-policy-doesnt-work/274373/.
[427] Paul Mozur and Aaron Krolik, "A Hong Kong Website Gets Blocked, Raising Censorship Fears," New York Times, Jan. 9, 2021, https://www.nytimes.com/2021/01/09/technology/hong-kong-website-

blocked.html; 艾米, "'香港编年史'成为《国安法》下首个被封的香港网站," RFI, Jan. 14, 2021, https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20210114-%E9%A6%99%E6%B8%AF%E7%BC%96%E5%B9%B4%E5%8F%B2-%E6%88%90%E4%B8%BA-%E5%9B%BD%E5%AE%89%E6%B3%95-%E4%B8%8B%E9%A6%96%E4%B8%AA%E8%A2%AB%E5%B0%81%E7%9A%84%E9%A6%99%E6%B8%AF%E7%BD%91%E7%AB%99.

[428] "香港警方：共 117 人因涉嫌从事危害国家安全的活动被捕 ," 观察者网, July 1, 2021, https://www.sohu.com/a/475019085_115479.

[429] Alice Fung, "4 arrested under new Hong Kong security law for online posts," AP, July 30, 2020, https://apnews.com/article/technology-arrests-hong-kong-laws-5d193a73674780b3851ee02e6e3c0a4e.

[430] "Four Hong Kong students arrested for 'advocating terrorism,'" The Guardian, Aug. 18, 2020, https://www.theguardian.com/world/2021/aug/18/four-hong-kong-students-arrested-for-advocating-terrorism.

[431] Selina Cheng, "Two arrested over online calls for boycotts, threats against Hong Kong broadcaster TVB," Hong Kong Free Press, July 29, 2021, https://hongkongfp.com/2021/07/29/two-arrested-over-online-calls-for-boycotts-threats-against-hong-kong-broadcaster-tvb/.

[432] 艾米, "'香港编年史'成为《国安法》下首个被封的香港网站," RFI, Jan. 14, 2021, https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20210114-%E9%A6%99%E6%B8%AF%E7%BC%96%E5%B9%B4%E5%8F%B2-%E6%88%90%E4%B8%BA-%E5%9B%BD%E5%AE%89%E6%B3%95-%E4%B8%8B%E9%A6%96%E4%B8%AA%E8%A2%AB%E5%B0%81%E7%9A%84%E9%A6%99%E6%B8%AF%E7%BD%91%E7%AB%99; "管过界? 港警要求以色列公司下架网站," DW.com, April 6, 2021, https://www.dw.com/zh/%E7%AE%A1%E8%BF%87%E7%95%8C-%E6%B8%AF%E8%AD%A6%E8%A6%81%E6%B1%82%E4%BB%A5%E8%89%B2%E5%88%97%E5%85%AC%E5%8F%B8%E4%B8%8B%E6%9E%B6%E7%BD%91%E7%AB%99/a-57775066; Nathan Law, Twitter Post, Jun. 3, 2021, 6:03 a.m., https://twitter.com/nathanlawkc/status/1400392731189514243/photo/1; "【封網疑團】香港可重新登入台灣民進黨等兩網站　仍無法登入國軍招募網　保安局拒評," 立场新闻，Apr. 27, 2021, https://www.thestandnews.com/politics/%E5%B0%81%E7%B6%B2%E7%96%91%E5%9C%98-%E9%A6%99%E6%B8%AF%E5%8F%AF%E9%87%8D%E6%96%B0%E7%99%BB%E5%85%A5%E5%8F%B0%E7%81%A3%E6%B0%91%E9%80%B2%E9%BB%A8%E7%AD%89%E5%85%A9%E7%B6%B2%E7%AB%99-%E4%BB%8D%E7%84%A1%E6%B3%95%E7%99%BB%E5%85%A5%E5%9C%8B%E8%BB%8D%E6%8B%9B%E5%8B%9F%E7%B6%B2-%E4%BF%9D%E5%AE%89%E5%B1%80%E6%8B%92%E8%A9%95; "涉犯國安法　港封「台獨」教會網站," 文匯網, Apr. 4, 2021, https://www.wenweipo.com/a/202104/25/AP6084bc38e4b0476859b8404d.html.

[433] "脸书、谷歌、推特也"跟风"：暂停处理港府索取用户数据的要求," 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc.

[434] Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (promulgated by the Hong Kong Chief Executive, Jun. 7, 2020), L.N. 139 of 2020, https://www.gld.gov.hk/egazette/pdf/20202449e/es220202449139.pdf.

[435] Rita Liao, "VPN providers rethink Hong Kong servers after China's security law," Tech Crunch, July 15, 2021, https://techcrunch.com/2020/07/15/vpn-rethink-hong-kong-servers/.

[436] "Google refuses South Korean government's real-name system," Hankyoreh, Apr. 10, 2009, http://english.hani.co.kr/arti/english_edition/e_international/349076.html.

[437] Jyh-An Li and Ching-Yi Liu, "Real-Name Registration Rules and the Fading Digital Anonymity in China," Washington International Law Journal 25, No. 1 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2719384.

[438] Ibid.

[439] Ibid.

[440] Jyh-An Li and Ching-Yi Liu, "Real-Name Registration Rules and the Fading Digital Anonymity in China," Washington International Law Journal 25, No. 1 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2719384; David Caragliano, "Why China's 'Real Name' Internet Policy Doesn't Work," The Atlantic, Mar. 26, 2013, https://www.theatlantic.com/china/archive/2013/03/why-chinas-real-name-Internet-policy-doesnt-work/274373/.

[441] Jyh-An Li and Ching-Yi Liu, "Real-Name Registration Rules and the Fading Digital Anonymity in China," Washington International Law Journal 25, No. 1 (2016)
[442] "Hong Kong real name SIM card registration to roll out, but gov't says it won't regulate int'l roaming SIMs," Hong Kong Free Press, Aug. 31, 2021, https://hongkongfp.com/2021/08/31/hong-kong-real-name-sim-card-registration-to-roll-out-but-govt-says-it-wont-regulate-intl-roaming-sims/.
[443] "财 8 点：支付宝、财付通都被央行罚 3 万元，百度网盘也要实名了," 资讯频道, May 11, 2017, http://inews.ifeng.com/51075826/news.shtml?&back.
[444] Paul Bischoff, "A brief history of China's campaign to enforce real-name registration online," Tech in Asia, Feb. 5, 2015, https://www.techinasia.com/history-chinas-campaign-enforce-realname-registration-online.
[445] Valentin Bajrami, "What you need to know about IPv6," RedHat, Sep. 24, 2019, https://www.redhat.com/sysadmin/what-you-need-know-about-ipv6.
[446] John Xie, "China Embraces Bigger Internet with Virtually Unlimited IP Addresses," Voice of America, Aug. 12, 2020, https://www.voanews.com/east-asia-pacific/voa-news-china/china-embraces-bigger-Internet-virtually-unlimited-ip-addresses.
[447] David Dawson, "China Telecom's IPv6 efforts are beginning to show in the numbers," APNIC, Jan 12, 2021, https://blog.apnic.net/2021/01/12/china-telecoms-ipv6-efforts-are-beginning-to-show-in-the-numbers/.
[448] John Xie, "China Embraces Bigger Internet with Virtually Unlimited IP Addresses," Voice of America, Aug. 12, 2020, https://www.voanews.com/east-asia-pacific/voa-news-china/china-embraces-bigger-Internet-virtually-unlimited-ip-addresses.
[449] "IPv6 下的实名制，你们准备好了没?" *射频世界* (3), No. 53-54 (2012), http://qikan.cqvip.com/Qikan/Article/Detail?id=42375941.
[450] John Xie, "China Embraces Bigger Internet with Virtually Unlimited IP Addresses," Voice of America, Aug. 12, 2020, https://www.voanews.com/east-asia-pacific/voa-news-china/china-embraces-bigger-Internet-virtually-unlimited-ip-addresses.
[451] "IPv6 大看点：国内首个公共 DNS 正式发布！实现实名制，网民言论自由受限?" 开源中国, Dec. 2, 2017, https://mb.yidianzixun.com/article/0HpV5HNv?s=mb&appid=mibrowser.
[452] John Xie, "China Embraces Bigger Internet with Virtually Unlimited IP Addresses," Voice of America, Aug. 12, 2020, https://www.voanews.com/east-asia-pacific/voa-news-china/china-embraces-bigger-Internet-virtually-unlimited-ip-addresses.
[453] "IPv6 要大规模部署，一位院士说这有助于实名制," 北京酷睿奥思科技发展有限公司, Nov. 30, 2017, https://baijiahao.baidu.com/s?id=1585481547181038208&wfr=spider&for=pc.
[454] "IPv6 大看点：国内首个公共 DNS 正式发布！实现实名制，网民言论自由受限?" 开源中国, Dec. 2, 2017, https://mb.yidianzixun.com/article/0HpV5HNv?s=mb&appid=mibrowser.
[455] PRC Ministry of Industry and Informatization, "IPv6 Address Real Name Management – Interface Specifications for Access User Information Registration System (Draft for Approval) (YDT 3652-2020 IPv6 地址实名制管理 接入用户信息备案接口技术要求(报批稿))," PRC Communications Industry Standard (中华人民共和国通信行业标准).
[456] PRC Ministry of Industry and Informatization, "IPv6 Address Real Name Management – Interface Specifications for Access User Information Registration System (Draft for Approval) (YDT 3652-2020 IPv6 地址实名制管理 接入用户信息备案接口技术要求(报批稿))," PRC Communications Industry Standard (中华人民共和国通信行业标准).
[457] Ibid.
[458] Ibid.
[459] Ibid.
[460] "Statistics per Country: Hong Kong," Cisco 6Lab, accessed Sep. 24, 2021, https://6lab.cisco.com/stats/search.php.
[461] Ibid.
[462] Ibid.
[463] Ibid.
[464] Rhoda Kwan, "Hong Kong's pre-paid SIM card users must register under new law," Hong Kong Free Press, Jun. 1, 2021, https://hongkongfp.com/2021/06/02/hong-kongs-pre-paid-sim-card-users-must-register-under-new-law/.

[465] Guidelines on Implementation of Real-name Registration for SIM Cards, (promulgated by the Communications Authority of Hong Kong, effective Sept. 1, 2021), GN-15/2021, https://www.coms-auth.hk/filemanager/statement/en/upload/569/gn152021.pdf.
[466] Ibid.
[467] "Public views sought on Real-name Registration Programme for SIM Cards," The Government of the Hong Kong Special Administrative Region Press Releases, Jan. 29, 2021, https://www.info.gov.hk/gia/general/202101/29/P2021012900421.htm; "Government to enact new regulation to implement Real-name Registration Programme for SIM Cards," The Government of the Hong Kong Special Administrative Region Press Releases, Jun. 1, 2021, https://www.info.gov.hk/gia/general/202106/01/P2021060100607.htm; Guidelines on Implementation of Real-name Registration for SIM Cards, (promulgated by the Communications Authority of Hong Kong, effective Sept. 1, 2021), GN-15/2021, https://www.coms-auth.hk/filemanager/statement/en/upload/569/gn152021.pdf.
[468] Guidelines on Implementation of Real-name Registration for SIM Cards, (promulgated by the Communications Authority of Hong Kong, effective Sept. 1, 2021), GN-15/2021, https://www.coms-auth.hk/filemanager/statement/en/upload/569/gn152021.pdf.
[469] "Government to enact new regulation to implement Real-name Registration Programme for SIM Cards," The Government of the Hong Kong Special Administrative Region Press Releases, Jun. 1, 2021, https://www.info.gov.hk/gia/general/202106/01/P2021060100607.htm.
[470] Jyh-An Li and Ching-Yi Liu, "Real-Name Registration Rules and the Fading Digital Anonymity in China," Washington International Law Journal 25, No. 1 (2016).
[471] Adrian Shahbaz, Allie Funk, and Andrea Hackl, "User Privacy or Cyber Sovereignty?" Freedom House, 2020, https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty; Alexander Plaum, "The impact of forced data localisation on fundamental rights," Access Now, Jun. 4, 2014, https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/.
[472] 中华人民共和国网络安全法, (promulgated by the Office of the Central Cyberspace Affairs Commission, Nov. 7, 2016), 新华社, http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm.
[473] Ibid.
[474] Ibid.
[475] "China: Data localisation requirements," One Trust Data Guidance, July 2020, https://www.dataguidance.com/opinion/china-data-localisation-requirements.
[476] "数据安全法来了，数据储存本土化成大势所趋," 太平洋号, Jun. 16, 2016, https://hj.pcauto.com.cn/article/830850.
[477] "国家互联网信息办公室关于《汽车数据安全管理若干规定（征求意见稿）》公开征求意见的通知," 中华人民共和国中央人民政府, May 12, 2021, http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm.
[478] 中华人民共和国数据安全法, (promulgated by the Standing Committee of the National People's Congress on Jun. 10, 2021), 中国人大网, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.
[479] 中华人民共和国数据安全法, (promulgated by the Standing Committee of the National People's Congress on Jun. 10, 2021), 中国人大网, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.
[480] 中华人民共和国数据安全法, (promulgated by the Standing Committee of the National People's Congress on Jun. 10, 2021), 中国人大网, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.
[481] "国家互联网信息办公室关于《汽车数据安全管理若干规定（征求意见稿）》公开征求意见的通知," 中华人民共和国中央人民政府, May 12, 2021, http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm.
[482] Ibid.
[483] Ibid.
[484] Ibid.
[485] "中俄等国向联合国提交'信息安全国际行为准则,'" 中央政府门户网站, Sep. 13, 2011, http://www.gov.cn/jrzg/2011-09/13/content_1945825.htm.
[486] 王志安, "云计算和大数据时代的国家立法管辖权——数据本地化与数据全球化的大对抗?" *交大法学* 1, (2019), https://xueshu.baidu.com/usercenter/paper/show?paperid=1p7h0030yk0k02y0kq2d0xv0yd415254&site=x

ueshu_se; “十国/地区数据保护法十大合规要点对比 | #3 数据本地化存储要求,” 出海互联网法律观察, Sep. 19, 2021, https://www.shangyexinzhi.com/article/4199713.html; “警惕数据跨境流动监管的本地化依赖与管辖冲突 ,” 信息安全与通信保密 12 (2018), https://www.secrss.com/articles/7471.

[487] “十国/地区数据保护法十大合规要点对比 | #3 数据本地化存储要求,” 出海互联网法律观察, Sep. 19, 2021, https://www.shangyexinzhi.com/article/4199713.html; 邵怿, “论域外数据执法管辖权的单方扩张,” *社会科学* 10 (2020), https://www.cnki.com.cn/Article/CJFDTotal-SHKX202010012.htm.

[488] 邵怿, “论域外数据执法管辖权的单方扩张,” *社会科学* 10 (2020), https://www.cnki.com.cn/Article/CJFDTotal-SHKX202010012.htm.

[489] 邢奕琛, “刍议国际法中网络主权概念的合理性——以我国的数据保护政策为视角,” *兰州教育学院学报* 12 (2019), https://www.cnki.com.cn/Article/CJFDTotal-LZJY201912059.htm; “数据全球化与数据主权的对抗态势和中国应对——基于数据安全视角的分析,” 北京航空航天大学学报社科版 34, No. 3 (2021), https://bhxb.buaa.edu.cn/Jwk3_bhsk/CN/abstract/abstract10506.shtml.

[490] Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,” Information Technology & Innovation Foundation, July 19, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

[491] “脸书、谷歌、推特也“跟风”：暂停处理港府索取用户数据的要求,” 上海观察者信息技术有限公司官方帐号, July 7, 2020, https://baijiahao.baidu.com/s?id=1671529544046434404&wfr=spider&for=pc.

[492] Jonah Force Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders,” Lawfare Research Papers Series 2, No. 3 (2014), https://s3.documentcloud.org/documents/7276302/THE-GROWTH-OF-DATA-LOCALIZATION-POST-SNOWDEN.pdf.

[493] 美媒：香港拟修法惩罚“人肉搜索”脸谱网推特私下发函扬言退出香港,” 人民网资讯, July 6, 2021, https://baijiahao.baidu.com/s?id=1704512654322451776&wfr=spider&for=pc.

[494] Wei Chen, “Legal Update: China’s Cybersecurity Law,” American Chamber of Commerce in China, Dec. 6, 2016, https://www.amchamchina.org/legal-update-chinas-cybersecurity-law/.

[495] “网络安全等级保护制度为核心的网络安全合规管理制度,” Wolters Kluwer, accessed Sep. 27, 2021, https://lawv3.wkinfo.com.cn/topic/61000000924/4.HTML.

[496] 中华人民共和国数据安全法, (promulgated by the Standing Committee of the National People’s Congress on Jun. 10, 2021), 中国人大网, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

[497] Ibid.

[498] “Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People’s Republic of China,” U.S. Department of Homeland Security, Office of Strategy, Policy, and Plans, Office of Trade and Economic Security, 2020, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[499] Ibid.

[500] 史宇航, “OECD 数据本地化趋势及挑战报告：执行摘要,” 送法上网，Jan. 1, 2021, https://zhuanlan.zhihu.com/p/341167689.

[501] “TikTok 事件背后的“数据本地化”浪潮 中国企业如何应对？” 中国公司法务研究会, Oct. 16, 2020, https://www.sohu.com/a/425053704_744278; Jonah Force Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders,” Lawfare Research Papers Series 2, No. 3 (2014).

[502] 史宇航, “OECD 数据本地化趋势及挑战报告：执行摘要,” 送法上网，Jan. 1, 2021, https://zhuanlan.zhihu.com/p/341167689; “十国/地区数据保护法十大合规要点对比 | #3 数据本地化存储要求,” 出海互联网法律观察, Sep. 19, 2021, https://www.shangyexinzhi.com/article/4199713.html.

[503] “十国/地区数据保护法十大合规要点对比 | #3 数据本地化存储要求,” 出海互联网法律观察, Sep. 19, 2021, https://www.shangyexinzhi.com/article/4199713.html; Emily Wu, “Sovereignty and Data Localization,” The Belfer Center Cyber Project, July 2021, https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf; Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, Bert Verschelde, “The Costs of Data Localization: Friendly Fire on Economic Recovery,” *European Center for International Political Economy*, No. 3 (2014), https://aicasia.org/wp-content/uploads/2017/06/OCC32014__1.pdf.

[504] 中华人民共和国网络安全法, (promulgated by the Office of the Central Cyberspace Affairs Commission, Nov. 7, 2016, effective Jun. 1, 2017), 新华社, http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm; 中华人民共和国数据安全法, (promulgated by the Standing Committee of the National People's Congress on Jun. 10, 2021), 中国人大网, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml; 国家互联网信息办公室关于《汽车数据安全管理若干规定（征求意见稿）》公开征求意见的通知, (promulgated by the National Internet Information Office, May 12, 2021), 网信办网站, http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm.
[505] "十国/地区数据保护法十大合规要点对比 | #3 数据本地化存储要求," 出海互联网法律观察, Sep. 19, 2021, https://www.shangyexinzhi.com/article/4199713.html; "数据安全审查制度," 深圳数据合规律师 , accessed Sept 27, 2021, http://m.xtjtsgls.com/a/272.html; "《2019 美国国家安全与个人数据保护法案》全文翻译及评价," 出海互联网法律观察, Feb. 20, 2020, https://www.secrss.com/articles/17255.
[506] Erol Yayboke, Carolina G. Ramos, Lindsay R. Sheppard, "The Real National Security Concerns over Data Localization," CSIS, July 23, 2021, https://www.csis.org/analysis/real-national-security-concerns-over-data-localization; https://www.belfercenter.org/publication/sovereignty-and-data-localization; Wei Chen, "Legal Update: China's Cybersecurity Law," American Chamber of Commerce in China, Dec. 6, 2016, https://www.amchamchina.org/legal-update-chinas-cybersecurity-law/.
[507] Wei Chen, "Legal Update: China's Cybersecurity Law," American Chamber of Commerce in China, Dec. 6, 2016, https://www.amchamchina.org/legal-update-chinas-cybersecurity-law/; Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders," Lawfare Research Papers Series 2, No. 3 (2014), https://s3.documentcloud.org/documents/7276302/THE-GROWTH-OF-DATA-LOCALIZATION-POST-SNOWDEN.pdf.
[508] Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China," U.S. Department of Homeland Security, Office of Strategy, Policy, and Plans, Office of Trade and Economic Security, 2020, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf; Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders," Lawfare Research Papers Series 2, No. 3 (2014).
[509] "联合打击印度"数据本地化"，这次亚马逊、Facebook、微软站在了一起," 雷锋网, Aug. 19, 2018, https://baijiahao.baidu.com/s?id=1609209127019807922&wfr=spider&for=pc.
[510] Leviathan Security Group, *Quantifying the Cost of Forced Localization* (Seattle: Leviathan Security Group, 2015), accessed Sep. 27, 2021, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.
[511] "数据中心"本地化"渐成趋势,"总财，Sep. 21, 2020, https://baijiahao.baidu.com/s?id=1678401030115556141&wfr=spider&for=pc.
[512] Ibid.
[513] "TikTok 事件背后的"数据本地化"浪潮 中国企业如何应对？" 中国公司法务研究会, Oct. 16, 2020, https://www.sohu.com/a/425053704_744278.
[514] Ibid.
[515] Ibid.
[516] Cody Ankeny, "The Costs of Data Localization," Tech Wonk Blog, Information Technology Industry Council, Aug. 17, 2016, https://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization; Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, Bert Verschelde, "The Costs of Data Localization: Friendly Fire on Economic Recovery," *European Center for International Political Economy*, No. 3 (2014), https://aicasia.org/wp-content/uploads/2017/06/OCC32014__1.pdf.
[517] Conan French, Brad Carr, and Clay Lowery, *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy* (Institute of International Finance, 2020), accessed Sep. 27, 2021, https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf
[518] Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, Bert Verschelde, "The Costs of Data Localization: Friendly Fire on Economic Recovery," *European Center for International Political Economy*, No. 3 (2014), https://aicasia.org/wp-content/uploads/2017/06/OCC32014__1.pdf.
[519] Ibid.

[520] “联合打击印度“数据本地化”，这次亚马逊、Facebook、微软站在了一起,” 雷锋网, Aug. 19, 2018, https://baijiahao.baidu.com/s?id=1609209127019807922&wfr=spider&for=pc; Naomi Shiffman and Jochai Ben-Avie, “Data localization: bad for users, business, and security,” Open Policy and Advocacy, Mozilla, June 22, 2018, https://blog.mozilla.org/netpolicy/2018/06/22/data-localization-india/.
[521] Ibid.
[522] “Google, Twitter, and Facebook were fined for lack of data localization in Russia,” Crane I.P. Law Firm, May 7, 2021, https://craneip.com/rospatent-launched-the-pharmaceutical-register-of-patents-in-demo-version/.
[523] 美媒：香港拟修法惩罚“人肉搜索”脸谱网推特私下发函扬言退出香港,” 人民网资讯, July 6, 2021, https://baijiahao.baidu.com/s?id=1704512654322451776&wfr=spider&for=pc.
[524] “Personal Data (Privacy) Ordinance,” (promulgated by the Hong Kong Legislative Council, Aug. 1, 1996), Hong Kong e-Legislation, https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y.
[525] Ibid.
[526] “Guidance on Personal Data Protection in Cross-border Data Transfer,” (promulgated by the Office of the Privacy Commissioner for Personal Data, Hong Kong, Dec. 2014), Office of the Privacy Commissioner for Personal Data, https://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf.
[527] Ibid.
[528] “Response to Media Enquiry on Data Localisation,” Office of the Privacy Commissioner for Personal Data, Apr. 15, 2020, https://www.pcpd.org.hk/english/news_events/media_enquiry/enquiry_20200415.html.
[529] Ibid.
[530] Gabriela Kennedy, Karen Lee, and Cheryl Yip, “Hong Kong: Requirements On The Electronic Storage Of Data: Recent SFC Circular,” Mondaq, Jun. 30, 2020, https://www.mondaq.com/hongkong/securities/959892/requirements-on-the-electronic-storage-of-data-recent-sfc-circular.
[531] Circular to Licensed Corporations - Use of external electronic data storage, (promulgated by the Securities and Futures Commission of Hong Kong, published Oct. 31, 2019), accessed Oct. 27, 2021, https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59; “The SFC issues guidance on the use of external electronic data storage,” Norton Rose Fulbright, Dec. 2019, https://www.nortonrosefulbright.com/en/knowledge/publications/c5c19168/the-sfc-issues-guidance-on-the-use-of-external-electronic-data-storage.
[532] Alun John, “Hong Kong regulator considers easing strict data storage rules – sources,” Reuters, Mar. 11, 2021, https://www.reuters.com/article/hongkong-regulators-cloud/hong-kong-regulator-considers-easing-strict-data-storage-rules-sources-idUSL3N2AQ1XA.
[533] Ibid.
[534] Ibid.
[535] Circular to Licensed Corporations - Use of external electronic data storage, (promulgated by the Securities and Futures Commission of Hong Kong, published Oct. 31, 2019), accessed Oct. 27, 2021, https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59.
[536] “Individuals Arrested under the Hong Kong National Security Law or by the National Security Department,” China File, accessed Oct. 26, 2021, https://www.chinafile.com/individuals-arrested-under-hong-kong-national-security-law-or-national-security-department.
[537] Alun John, “Hong Kong regulator considers easing strict data storage rules – sources,” Reuters, Mar. 11, 2021, https://www.reuters.com/article/hongkong-regulators-cloud/hong-kong-regulator-considers-easing-strict-data-storage-rules-sources-idUSL3N2AQ1XA.
[538] Circular to Licensed Corporations - Use of external electronic data storage, (promulgated by the Securities and Futures Commission of Hong Kong, published Oct. 31, 2019), accessed Oct. 27, 2021, https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59.
[539] Ibid.
[540] Alun John, “Hong Kong regulator considers easing strict data storage rules – sources,” Reuters, Mar. 11, 2021, https://www.reuters.com/article/hongkong-regulators-cloud/hong-kong-regulator-considers-easing-strict-data-storage-rules-sources-idUSL3N2AQ1XA.

[541] "Response to Media Enquiry on Data Localisation," Office of the Privacy Commissioner for Personal Data, Apr. 15, 2020, https://www.pcpd.org.hk/english/news_events/media_enquiry/enquiry_20200415.html.
[542] "粤港澳大湾区大数据中心," 深圳国家高技术产业创新中心, May 20, 2021, http://fgw.sz.gov.cn/hiic/zlzx/zdptch/content/post_8650546.html.
[543] Ibid.
[544] 明宇, "閒話大灣區：大數據中心的挑戰與機遇 ," 香港經濟導報, July 15, 2019, www.jdonline.com.hk/index.php?m=wap&siteid=1m=wap&c=index&a=show&catid=86&typeid=28&id=44617.
[545] Ibid.
[546] Ibid.
[547] "粤港澳大湾区数据跨境合规流通研究 ," 京东数字科技研究院, Sept 11, 2019, https://www.secrss.com/articles/13625.
[548] Ibid.
[549] "Response to Media Enquiry on Data Localisation," Office of the Privacy Commissioner for Personal Data, Apr. 15, 2020, https://www.pcpd.org.hk/english/news_events/media_enquiry/enquiry_20200415.html.
[550] "Hong Kong: Important changes proposed to Hong Kong's data protection law," DLA Piper (blog), Feb. 28, 2020, https://blogs.dlapiper.com/privacymatters/hong-kong-important-changes-proposed-to-hong-kongs-data-protection-law/.
[551] Ibid.
[552] Gail E. Crawford, Fiona M. Maclean, Kieran Donovan, and Esther C. Franks, "Hong Kong Considers Sweeping Changes to Privacy Laws," *Latham & Watkins Client Alert Commentary*, no. 2580, Jan. 22, 2020, https://www.lw.com/thoughtLeadership/hong-kong-considers-sweeping-changes-to-privacy-laws.
[553] "The SFC issues guidance on the use of external electronic data storage," Norton Rose Fulbright, Dec. 2019, https://www.nortonrosefulbright.com/en/knowledge/publications/c5c19168/the-sfc-issues-guidance-on-the-use-of-external-electronic-data-storage.
[554] Rhoda Kwan, "Hong Kong's pre-paid SIM card users must register under new law," Hong Kong Free Press, Jun. 1, 2021, https://hongkongfp.com/2021/06/02/hong-kongs-pre-paid-sim-card-users-must-register-under-new-law/.
[555] "Hong Kong a desirable data center location despite political and pandemic troubles," Data Center News, Jun. 25, 2021, https://datacenternews.asia/story/hong-kong-a-desirable-data-center-location-despite-political-and-pandemic-troubles.
[556] Ibid.
[557] Hannah Jeong, "Demand for data centres is in a lull. The national security law has little to do with it," South China Morning Post, Sep. 14, 2021, https://www.scmp.com/business/article/3148648/demand-data-centres-lull-national-security-law-has-little-do-it.
[558] Yuxi Wei, "Chinese Data Localization Law: Comprehensive but Ambiguous," Henry M. Jackson School of International Studies, Feb. 7, 2018, https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.
[559] "Tender awarded for site in Sha Tin," the Government of the Hong Kong Special Administrative Region, Jul. 8, 2020, https://www.info.gov.hk/gia/general/202007/08/P2020070800751.htm; Diana Li, "China Mobile Outbid Local Tycoons by 56% for Hong Kong Data Centre Site," Mingtiandi, Aug. 10, 2020, https://www.mingtiandi.com/real-estate/projects-real-estate/china-mobile-overbids-for-hong-kong-data-centre-site/.
[560] "Best Practices for Data Center Relocation: Manage Expectations and Get It Right the First Time," Apposite Technologies, 2019, https://www.apposite-tech.com/wp-content/uploads/2019/02/Data-Center-Relocation-White-Paper.pdf.
[561] Previous studies showed that cloud storage costs increased between 10 and 52% in Europe under forced data localization regimes. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" *Information Technology & Innovation Foundation*, May 1, 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
[562] Yuxi Wei, "Chinese Data Localization Law: Comprehensive but Ambiguous," Henry M. Jackson School of International Studies, Feb. 7, 2018, https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/; Jack Nicas, Raymond Zhong and Daisuke Wakabayashi, "Censorship,

Surveillance and Profits: A Hard Bargain for Apple in China," The New York Times, May 17, 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.
[563] Jack Nicas, Raymond Zhong and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China," The New York Times, May 17, 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.
[564] Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (promulgated by the Hong Kong Chief Executive, Jun. 7, 2020), L.N. 139 of 2020, https://www.gld.gov.hk/egazette/pdf/20202449e/es220202449139.pdf.
[565] Jack Nicas, Raymond Zhong and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China," The New York Times, May 17, 2021.
[566] Nathan Law, Twitter Post, Jun. 3, 2021, 6:03 a.m., https://twitter.com/nathanlawkc/status/1400392731189514243/photo/1; "[香港約章 2021」網站復活　網站供應商就錯誤刪網致歉　港警曾去信供應商要求下架," 立场新闻, Jun. 3, 2021, https://www.thestandnews.com/politics/%E9%A6%99%E6%B8%AF%E7%B4%84%E7%AB%A0-2021-%E7%B6%B2%E7%AB%99%E8%A2%AB%E5%B0%81-%E7%BE%85%E5%86%A0%E8%81%B0-%E8%AD%A6%E6%96%B9%E5%90%91%E7%B6%B2%E7%AB%99%E4%BE%9B%E6%87%89%E5%95%86%E7%99%BC%E4%BF%A1%E8%A6%81%E6%B1%82%E4%B8%8B%E6%9E%B6-%E6%8C%87%E5%85%A7%E5%AE%B9%E6%88%96%E9%81%95%E5%9C%8B%E5%AE%89%E6%B3%95.
[567] "全球最大网络交换中心 DE ," 我酷网, Jul. 4, 2018, http://wosku.com/yl/bg/2018-06-04/482531.html.
[568] "全球最大网络交换中心 DE ," 我酷网, Jul. 4, 2018, http://wosku.com/yl/bg/2018-06-04/482531.html; Kieran McCarthy, "World's largest Internet exchange sues Germany over mass surveillance," The Register, Sep. 16, 2016. https://www.theregister.com/2016/09/16/ixp_sues_german_govt_surveillance/.
[569] Tomslin Samme-Nlar and Isaac Noumba, *An Analysis of the Decision to Authorize CAMIX to Manage the Yaounde and Douala IXPs* (Gefona, 2015), accessed Sep. 27, 2021, https://gefona.org/an-analysis-of-the-decision-to-authorize-camix-to-manage-the-yaounde-and-douala-ixps/.
[570] Xueyang Xu, Z. Morley Mao, and J. Alex Halderman "Internet Censorship in China: Where Does the Filtering Occur?" *Lecture Notes in Computer Science* 6579 (2011), https://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf.
[571] Jyh-An Li and Ching-Yi Liu, "Real-Name Registration Rules and the Fading Digital Anonymity in China," Washington International Law Journal 25, No. 1 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2719384.
[572] Philipp Winter and Stefan Lindskog, "The Great Firewall of China: How it Blocks Tor and Why it is Hard to Pinpoint," *Free and Open Communications on the Internet* (2012), https://www.diva-portal.org/smash/get/diva2:610844/FULLTEXT01.pdf; Nikhil Sonnad and Keith Collins, "How countries like China and Russia are able to control the Internet," Quartz, Oct. 15, 2016, https://qz.com/780675/how-do-Internet-censorship-and-surveillance-actually-work/; Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall, "Analyzing the Great Firewall of China Over Space and Time," Proceedings on Privacy Enhancing Technologies 1 (2015), https://censoredplanet.org/assets/Ensafi2015a.pdf.
[573] Philipp Winter and Stefan Lindskog, "The Great Firewall of China: How it Blocks Tor and Why it is Hard to Pinpoint," *Free and Open Communications on the Internet* (2012), https://www.diva-portal.org/smash/get/diva2:610844/FULLTEXT01.pdf.
[574] Ibid.
[575] Ibid.
[576] "国家新型互联网交换中心落户深圳前海，意味着什么？" 前海金融城邮报, Apr. 17, 2021, http://www.sznews.com/content/mb/2021-04/17/content_24138585.htm.
[577] "国家新型互联网交换中心落户深圳前海，意味着什么？" 前海金融城邮报, Apr. 17, 2021, http://www.sznews.com/content/mb/2021-04/17/content_24138585.htm.
[578] "新型互联网交换中心试点落地上海，探索更多互联创新业务," 新浪财经， Sep. 10, 2021, https://finance.sina.com.cn/china/gncj/2021-09-10/doc-iktzscyx3392976.shtml?cre=tianyi&mod=pcpager_tech&loc=17&r=0&rfunc=14&tj=cxvertical_pc_pager_spt&tr=164.
[579] "新型互联网交换中心试点落地上海，探索更多互联创新业务," 新浪财经， Sep. 10, 2021, https://finance.sina.com.cn/china/gncj/2021-09-10/doc-

iktzscyx3392976.shtml?cre=tianyi&mod=pcpager_tech&loc=17&r=0&rfunc=14&tj=cxvertical_pc_pager_spt&tr=164; "国家（中卫）新型互联网交换中心正式启用," 新华网, June 29, 2021, http://www.nx.xinhuanet.com/newscenter/2021-06/29/c_1127609759.htm.
[580] "Russia: New Law Expands Government Control Online," Human Rights Watch, Oct. 31, 2019, https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online.
[581] Charlotte Jee, "Russia Wants to Cut Itself Off from the Global Internet. Here's What That Really Means," MIT Technology Review, Mar. 21, 2019, https://www.technologyreview.com/2019/03/21/65940/russia-wants-to-cut-itself-off-from-the-global-Internet-heres-what-that-really-means/.
[582] "What is HKIX," Hong Kong Internet Exchange, accessed Sep. 27, 2021, http://www.hkix.net/hkix/whatishkix.htm.
[583] Ibid.
[584] Joshua But, Joyce Ng and Ernest Kao, "Internet exchange at Chinese University seen as target for hackers," South China Morning Post, Jun. 13, 2013, https://www.scmp.com/news/hong-kong/article/1259701/Internet-exchange-chinese-university-seen-target-hackers.
[585] Ibid.
[586] 羅正漢, "關於港警圍攻香港中文大學，控制 HKIX 將導致香港斷網的傳言，聽聽香港專業 IT 人員怎麼說," ITHome, Nov. 15, 2019, https://www.ithome.com.tw/news/134232; 喜马拉雅翻译组, "Why police attack CUHK? Hong Kong Internet Exchange is located on campus," GNews, Nov. 12, 2019, https://gnews.org/26276/.
[587] Ibid.
[588] 羅正漢, "關於港警圍攻香港中文大學，控制 HKIX 將導致香港斷網的傳言，聽聽香港專業 IT 人員怎麼說," ITHome, Nov. 15, 2019, https://www.ithome.com.tw/news/134232.
[589] Ibid.
[590] Ibid.
[591] "关于港警围攻香港中文大学，控制 HKIX 将导致香港断网的传言，听听香港专业 IT 人员怎么说," 报价宝, Nov. 17, 2019, https://www.baojiabao.com/bjbnews/zh201911171150462753.html.
[592] 羅正漢, "關於港警圍攻香港中文大學，控制 HKIX 將導致香港斷網的傳言，聽聽香港專業 IT 人員怎麼說," ITHome, Nov. 15, 2019, https://www.ithome.com.tw/news/134232; 喜马拉雅翻译组, "Why police attack CUHK? Hong Kong Internet Exchange is located on campus," GNews, Nov. 12, 2019, https://gnews.org/26276/.
[593] 羅正漢, "關於港警圍攻香港中文大學，控制 HKIX 將導致香港斷網的傳言，聽聽香港專業 IT 人員怎麼說," ITHome, Nov. 15, 2019, https://www.ithome.com.tw/news/134232; 喜马拉雅翻译组, "Why police attack CUHK? Hong Kong Internet Exchange is located on campus," GNews, Nov. 12, 2019, https://gnews.org/26276/.
[594] Daniel Anderson, "SplInternet: Behind the Great Firewall of China," *ACM Queue* 10, no. 11 (2012), https://queue.acm.org/detail.cfm?id=2405036.
[595] Ibid.
[596] Marcin Nawrocki, Mattijs Jonker, Thomas C. Schmidt, and Matthias Wählisch, "The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core," Arxiv, Sep. 2, 2021, https://arxiv.org/abs/2109.01104; Cédric Lévy-Bencheton, Louis Marinos, Rossella Mattioli, Thomas King, Christoph Dietze, Jan Stumpf, *Threat Landscape and Good Practice Guide for Internet Infrastructure*, (European Union Agency for Network and Information Security, 2015), accessed Sep. 27, 2021, https://www.enisa.europa.eu/publications/iitl/view/++widget++form.widgets.fullReport/@@download/Threat+Landscape+and+Good+Practice+Guide+for+Internet+Infrastructure.pdf; Justin Sherman, *The Politics of Internet Security: Private Industry and the Future of the Web* (Atlantic Council, 2020), accessed Sep. 27, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-politics-of-Internet-security-private-industry-and-the-future-of-the-web/,
[597] "Why police attack CUHK? Hong Kong Internet Exchange is located on campus," GNews, Nov. 12, 2019, https://gnews.org/26276/.
[598] "国家新型互联网交换中心落户深圳前海，意味着什么？" 前海金融城邮报, Apr. 17, 2021, http://www.sznews.com/content/mb/2021-04/17/content_24138585.htm.
[599] Ibid.
[600] Marco Chiesa, Daniel Demmler, Marco Canini, Michael Schapira, and Thomas

Schneider, “SIXPACK: Securing Internet eXchange Points Against Curious onlooKers,” *Proceedings of CoNEXT ’17* (2017), https://mcanini.github.io/papers/sixpack.conext17.pdf.
[601] Marco Chiesa, Daniel Demmler, Marco Canini, Michael Schapira, and Thomas Schneider, “SIXPACK: Securing Internet eXchange Points Against Curious onlooKers,”; Xiaohe Hum, Arpit Gupta, Nick Feamster, Aurojit Panda, and Scott Shenker, “Preserving Privacy at IXPs,” *APNet '18: Proceedings of the 2nd Asia-Pacific Workshop on Networking* (2018), https://dl.acm.org/doi/10.1145/3232565.3232575.
[602] “VPN security: How VPNs Help Secure Data and Control Access,” Cloudflare, accessed Sep. 27, 2021, https://www.cloudflare.com/learning/access-management/vpn-security/.
[603] “IX Service,” BBIX, accessed Sep. 27, 2021, https://www.bbix.net/en/service/ix/; “About,” Equinix, accessed Sep. 27, 2021, https://www.equinix.com/about.
[604] “About Megaport,” Megaport, accessed Sep. 27, 2021, https://www.megaport.com/about-megaport/; “About AMS IX,” AMS IX, accessed Sep. 27, 2021, https://www.ams-ix.net/hk/about-ams-ix.
[605] Chee-Hoo Cheng, “HKIX General,” (presentation, APRICOT 2014, 2014), accessed Sep. 27, 2021, http://www.hkix.net/hkix/Presentation/APRICOT2014.pdf.
[606] “Announcements,” Hong Kong Internet Exchange, Aug. 1, 2021, accessed Sep. 27, 2021, http://www.hkix.net/hkix/announce.htm.
[607] “Satellite Sites,” Hong Kong Internet Exchange, accessed Sep. 27, 2021, https://www.hkix.net/hkix/satellite-sites.htm.
[608] “Your Interconnection Platform in Hong Kong,” AMS IX Hong Kong, accessed Sep. 27, 2021, https://www.ams-ix.net/hk; “Internet Exchange Services,” ACME HK, accessed Sep. 27, 2021, https://www.acmehk.net/solutions/connectivity/Internet-exchange-services/; “Equinix Internet Exchange,” Equinix, accessed Sep. 27, 2021, https://www.equinix.se/interconnection-services/Internet-exchange; “IX Service,” BBIX, accessed Sep. 27, 2021, https://www.bbix.net/en/service/ix/; “Internet Exchange,” Megaport, accessed Sep. 27, 2021, https://www.megaport.com/services/Internet-exchange/.
[609] Katsuyasu Toyama, “The impacts of COVID-19 Pandemic on the IXPs in APAC Region,” (presentation, IX.br IX Forum, Dec. 2-4, 2020), https://forum.ix.br/files/apresentacao/arquivo/1025/20201204-ixbr-forum-katsuyasu-for-publish.pdf.
[610] “About AMS IX,” AMS IX, accessed Sep. 27, 2021, https://www.ams-ix.net/hk/about-ams-ix.
[611] “Home,” AMS IX, accessed Sep. 27, 2021, https://www.ams-ix.net/ams.
[612] “Internet Exchange Services,” ACME HK, accessed Sep. 27, 2021, https://www.acmehk.net/solutions/connectivity/Internet-exchange-services/.
[613] “Awards and Recognition,” ACME HK, accessed Sep. 27, 2021, https://www.acmehk.net/about-us/awards-recognition-2/
[614] “About,” Equinix, accessed Sep. 27, 2021, https://www.equinix.com/about.
[615] AMS IX HK, *Products and Services: Equinix Internet Exchange* (AMS IX HK, 2020), accessed Sep. 27, 2021, https://www.equinix.com/content/dam/eqxcorp/en_us/documents/resources/data-sheets/ds_equinix_Internet_exchange_en_oct2020.pdf.
[616] “IX Service,” BBIX, accessed Sep. 27, 2021, https://www.bbix.net/en/service/ix/.
[617] Ibid.
[618] “About Megaport,” Megaport, accessed Sep. 27, 2021, https://www.megaport.com/about-megaport/.
[619] Ibid.
[620] “What is HKIX,” HKIX, accessed Oct. 27, 2021, https://www.hkix.net/hkix/whatishkix.htm.
[621] “About CUHK,” The Chinese University of Hong Kong, accessed Oct. 27, 2021, https://web.archive.org/web/20130930141746/http://www.cuhk.edu.hk/english/aboutus/milestones/milestones.html.
[622] “Hong Kong National Security Police Raid Campus Over Slogans,” Radio Free Asia, Nov. 11, 2020, https://www.rfa.org/english/news/china/hongkong-campus-11202020133313.html.
[623] HKIX, “Hong Kong Internet Exchange,” (presentation, IET visit to HKIX, Jun. 26, 2010), accessed Oct. 27, 2021, https://www.hkix.net/hkix/Presentation/ietvisithkix20100626.pdf.
[624] “Collaboration with Stakeholders,” Office of the Government Chief Information Officer, accessed Oct. 27, 2021, https://www.ogcio.gov.hk/en/our_work/information_cyber_security/collaboration/.
[625] “News/ Announcements,” HKIX, accessed Oct. 27, 2021, https://www.hkix.net/.
[626] Ryan Ng, “HKIX Development and HKIX-R&E Updates at APAN 51,” (presentation, APAN 51, Feb. 1-5, 2021), accessed Oct. 27, 2021, https://www.hkix.net/hkix/Presentation/APAN51.pdf.

[627] Ryan Ng, "HKIX Development and HKIX-R&E Updates at APAN 51," (presentation, APAN 51, Feb. 1-5, 2021), accessed Oct. 27, 2021, https://www.hkix.net/hkix/Presentation/APAN51.pdf.
[628] "Route Policy," HKIX, accessed Oct. 27, 2021, http://www.hkix.net/hkix/filterupd.html.
[629] Ibid.
[630] "News/ Announcements," HKIX, accessed Oct. 27, 2021, https://www.hkix.net/.
[631] "Network Functions Virtualization – Introductory White Paper," (paper presented at SDN and OpenFlow World Congress, Darmstadt, Germany, Oct. 22-24, 2012).
[632] Ibid.
[633] Ibid.
[634] Xueyang Xu, Z. Morley Mao, and J. Alex Halderman "Internet Censorship in China: Where Does the Filtering Occur?" *Lecture Notes in Computer Science* 6579 (2011), https://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf; Young Xu, "Deconstructing the Great Firewall of China," ThousandEyes, Mar. 8, 2016, https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.
[635] Shan Huang, Félix Cuadrado, and Steve Uhlig, "Middleboxes in the Internet: A HTTP Perspective," 017 Network Traffic Measurement and Analysis Conference (TMA), 2017, pp. 1-9, https://ieeexplore.ieee.org/abstract/document/8002906/citations#citations.
[636] Chao Zheng, Qiuwen Lu, Qingyun Liu, Jia Li, and Binxing Fang, "A Flexible and Efficient Container-based NFV Platform for Middlebox Networking," *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, April 2018, https://dl.acm.org/doi/10.1145/3167132.3167240.
[637] Young Xu, "Deconstructing the Great Firewall of China," ThousandEyes, Mar. 8, 2016, https://www.thousandeyes.com/blog/deconstructing-great-firewall-china.
[638] Chao Zheng, Qiuwen Lu, Qingyun Liu, Jia Li, and Binxing Fang, "A Flexible and Efficient Container-based NFV Platform for Middlebox Networking," *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, April 2018, https://dl.acm.org/doi/10.1145/3167132.3167240.
[639] 王进文，张晓丽，李琦，吴平，江勇，"网络虚拟化技术研究进展," 计算机学报 42, No. 2, Feb, 2019, http://cjc.ict.ac.cn/online/onlinepaper/wjw-201912883153.pdf.
[640] 丁勇, "网络靶场结构与关键技术-鹏城实验室国家级网络靶场," (presented at the 第八届全国网络与信息安全防护峰会, Apr. 20, 2020), accessed Sep. 28, 2021.
[641] Ibid.
[642] Ibid.
[643] Ibid.
[644] "Network Functions Virtualization – Introductory White Paper," (paper presented at SDN and OpenFlow World Congress, Darmstadt, Germany, Oct. 22-24, 2012); "ZTE and China Mobile Complete Industry's first CloudOS and Commercial SDN System Decoupling Test in NFV Architecture," ZTE, Sep. 4, 2018, https://www.zte.com.cn/global/about/news/20180904.html;
[645] Fu Qiao, "Experience Sharing: the National Experiment Network for NFV Testing in China Mobile," (presentation, China Mobile, n.d.), accessed Sep. 28, 2021, https://wiki.lfnetworking.org/download/attachments/328197/Experience%20Sharing-China%20Mobile%20NovoNet%20Experiment%20Network.pdf?version=1&modificationDate=1522344418000&api=v2.
[646] Ibid.
[647] 陈鼎, "焦点：NFV 在运营商网络三大用武之地," H3C, Nov. 27, 2014, http://www.h3c.com/cn/d_201410/842424_30008_0.htm.
[648] "Huawei and China Mobile Hong Kong Win the 'Best Network Transformation Initiative' Award," Huawei, Nov. 7, 2018, https://www.huawei.com/en/news/2018/11/huawei-china-mobile-hongkong-awarded.
[649] "PCCW Global Plans Expansion to Deliver Enterprise, Edge Applications, NGV, and IOT Enablement to Customers," CPLANE.ai, May 11, 2017, https://cplaneai.com/pccw-global-plans-expansion-deliver-enterprise-edge-applications-nfv-iot-enablement-customers/.
[650] "Huawei OTF event: HKT's digital transformation strategy," Telecomlead, Sep. 18, 2017, https://www.telecomlead.com/telecom-equipment/huawei-otf-event-transforming-towards-digital-business-success-79334.
[651] Mark Smirniotis, "What Is a VPN and What Can (and Can't) It Do?," The New York Times, Mar. 3, 2021, https://www.nytimes.com/wirecutter/guides/what-is-a-vpn/.

[652] Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (promulgated by the Hong Kong Chief Executive, Jun. 7, 2020), L.N. 139 of 2020, https://www.gld.gov.hk/egazette/pdf/20202449e/es220202449139.pdf.
[653] 工业和信息化部关于清理规范互联网网络接入服务市场的通知, (promulgated by the Ministry of Industry and Information Technology, Jan. 17, 2017), 信息通信管理局, https://web.archive.org/web/20170131124315/http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html.
[654] "VPN Campaign Notice," China Law Translate, Jul. 20, 2017, https://www.chinalawtranslate.com/en/vpn-campaign-notice/.
[655] Echo Huang, "What You Need to Know about China's VPN Crackdown," Quartz, Jul. 12, 2017, https://qz.com/1026064/what-you-need-to-know-about-chinas-vpn-crackdown/.
[656] "VPN Campaign Notice," China Law Translate.
[657] 重庆市公安机关网络安全管理行政处罚裁量基准, (promulgated by the Chongqing Public Security Bureau, Jul. 27, 2016), https://web.archive.org/web/20180925224302/http://www.cq.gov.cn/publicinfo/web/views/Show!detail.action?sid=4186133.
[658] Gao Feng, "Fine For VPN Use Sparks Rare Backlash on Chinese Internet," Radio Free Asia, May 21, 2020, https://www.rfa.org/english/news/china/vpn-punishments-05212020103537.html; Masha Borak, "Man punished for using a VPN to scale China's Great Firewall and watch porn," South China Morning Post, Jul. 30, 2020, https://www.scmp.com/abacus/tech/article/3095201/man-punished-using-vpn-scale-chinas-great-firewall-and-watch-porn.
[659] Jon Russell, "China's mobile operators are reportedly being told to ban all use of VPNs," Tech Crunch, Jul. 20, 2017, https://techcrunch.com/2017/07/10/china-vpn-ban/?guccounter=1.
[660] Michael Gargiulo, "Which Countries Block VPNs, and Why?" VPN.com, Apr. 7, 2021, https://www.vpn.com/guide/which-countries-block-vpn/.
[661] Ibid.
[662] Ibid.
[663] Ibid.
[664] Molly Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*, (Princeton, NJ: Princeton University Press, 2018).
[665] Shelly Banjo, "VPN Downloads Surge in Response to Hong Kong Security Law," Bloomberg, May 21, 2020, https://www.bloomberg.com/news/articles/2020-05-22/vpn-downloads-surge-in-response-to-hong-kong-security-law.
[666] Shui-Yin Sharon Yam, "Hong Kong's SIM card registration plan aims to sow fear, distrust and self-censorship," Hong Kong Foreign Press, Feb. 5, 2021, https://hongkongfp.com/2021/02/05/hong-kongs-sim-card-registration-plan-aims-to-sow-fear-distrust-and-self-censorship/.
[667] Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (promulgated by the Hong Kong Chief Executive, Jun. 7, 2020), L.N. 139 of 2020, https://www.gld.gov.hk/egazette/pdf/20202449e/es220202449139.pdf.
[668] "Individuals Arrested under the Hong Kong National Security Law or by the National Security Department," China File, accessed Oct. 26, 2021, https://www.chinafile.com/individuals-arrested-under-hong-kong-national-security-law-or-national-security-department.
[669] Christopher Krebs to Ron Wyden, May 22, 2019, https://www.wyden.senate.gov/imo/media/doc/052819%20DHS%20Response%20to%20Wyden%20Letter%20RE%20Chinese%20Russian%20VPN.pdf.
[670] Ibid.
[671] Simon Migliano, "Free VPN Ownership Investigation," Top 10 VPN, Jun. 9, 2021, https://www.top10vpn.com/research/free-vpn-investigations/ownership/.
[672] Daniel Markusan, "What is the best VPN for China?" NordVPN, Oct. 23, 2021, https://nordvpn.com/blog/vpn-for-china/; Douglas Mabiria, "10 best VPNs for China to use in 2021 (the providers that actually work)," Privacy Savvy, Oct. 2, 2021, https://privacysavvy.com/vpn/best/china/.