

China's Digital Silk Road: Integration into National IT Infrastructure and Wider Implications for Western Defence Industries

Meia Nouwens

Indonesia – by Alexander Neill, AN Consulting

Republic of Korea – by Alexander Neill, AN Consulting

United Arab Emirates – by Camille Lons and Nawafel Shehab, IISS

Israel – by Camille Lons and Nawafel Shehab, IISS

Poland – By Scott Malcomson, Strategic Insight Group

February 2021

Contents

Executive summary	4
Introduction	6
Context of the Digital Silk Road and security-related concerns	7
Five country case studies	14
Key findings and potential implications for Western defence industries and government	47
Notes	52

Index of maps and figures

Figure 1: Digital Silk Road project categories and types 8

Map 1: Indonesia 14

Map 2: Republic of Korea 20

Map 3: United Arab Emirates 27

Map 4: Israel 34

Map 5: Poland 41

Executive summary

The geopolitical dispute between the United States and China is taking place on the fault line of global telecommunications infrastructure and digital technologies. As this competition grows, so too does the likelihood of a potential bifurcation in the global information and security technological ecosystems, split between US-allied liberal democracies on the one side and countries dependent on Chinese-based information and communications technology (ICT) on the other. The impact of this competition reaches beyond telecommunications companies and those involved in their supply chains. Indeed, second and third order of magnitude implications exist for the security and defence sectors. While this competition unfolds, the Chinese Government's Digital Silk Road (DSR) continues apace and leverages the strengths of Chinese public- and private-sector giants to further integrate Chinese technologies and standards into the digital ecosystems of the least-developed, emerging and developed economies alike.

The existing literature on the security and defence implications of the integration of Chinese ICT into national digital ecosystems is primarily concerned with the potential threats posed to intelligence and defence cooperation. However, the implication of China's global digital investments for US and other Western defence industries is an understudied subject that deserves greater attention.

To provide greater clarity to Western defence industries on these issues, this project has sought to answer four forward-looking questions. Firstly, what risks does the possibility of a bifurcated global digital ecosystem pose for the national and industrial security of key Asian, European and Middle Eastern states and economies? Secondly, to what extent does the integration of Chinese information technology and digital

infrastructure create challenges for alliance intelligence and defence cooperation? Thirdly, what level of integration should be considered significant and how might security-cooperation efforts (e.g. Western arms exports) be affected? Lastly, can security risks to companies doing business abroad be mitigated when the integration of Chinese digital technology into national digital ecosystems is already high?

This report has aimed to address this gap in current analysis by outlining the potential risks posed by China's global digital and technological investments to defence industries. It follows with an analysis of the extent of Chinese DSR activity in five case-study countries across Asia, the Middle East and Europe that are of high security and defence importance to the US: Indonesia, the Republic of Korea (ROK), Israel, the United Arab Emirates (UAE) and Poland. In doing so, the report aims to provide greater insight into government decision-making and lessons learned for Western defence industries.

Countries still hedging against possibility of complete bifurcation of the global digital ecosystem

The US has argued that the integration of Chinese technology in national digital ecosystems will have significant consequences for national security and defence cooperation with the US, including defence-industrial cooperation. However, with the exception of Israel, this report found that in all case-study countries Chinese ICT investment was prevalent across almost all sectors of the national ICT ecosystems, from physical infrastructure to service provision and 'over the top' platforms. Based on this evidence, indications are that all the case-study countries are to a certain extent still hedging against the possibility of a fully bifurcated global digital ecosystem.

The report also found that although all five case-study countries were recipients of largely the same diversity and scale of Chinese technological investments, government responses to the US campaign to further restrict Chinese technologies in national ecosystems were diverse. Predictably, governments struggled to find a balance between commercial and security interests. However, even in countries where governments were dependent on the US as their only security guarantor, this struggle was not any more decisive regarding security concerns. Also of note was the lack of governmental and public debate in some countries as part of decision-making processes about accepting Chinese tech investments.

Challenges for alliance intelligence and defence cooperation?

Despite the varied and, in some instances, deep integration of Chinese ICT investments in national ICT ecosystems, this did not seem to have an impact on the defence and intelligence cooperation between the US and the countries studied. In some cases, the security relationship with the US played a stronger role in governmental decision-making than in others. However, the decision to exclude or limit the integration of Chinese technology by any of the governments analysed was based purely on the hypothetical consequences of not doing so for defence and intelligence cooperation with the US and allies. It could be possible that there are examples of this, but the evidence is classified and thus outside the scope of this paper, which is based on open-source intelligence research.

What level of integration should be considered significant?

This report argues that it is difficult to examine in full the extent of the integration of Chinese ICT technologies throughout the national ICT ecosystems of each case-study country examined. Doing so is well beyond the remit of this report and requires further detailed examination. However, it is interesting to note that in all case studies, decisions made by national governments seemed to largely centre around discussions of Huawei 5G networks and other physical infrastructure. Debates also largely focused on whether to accept top-level Chinese physical infrastructure and did not, for example, seem to delve into debates around whether to rely on imports of copper wire from China, or whether to permit Chinese investment in local start-up industries. It could be concluded from this research that it is difficult for national-level governments to precisely determine what level of integration of Chinese ICT technologies should be considered significant.

Can security risks to companies doing business abroad be mitigated?

An important conclusion for defence industries is that efforts by national governments to mitigate security risks were found lacking in the majority of cases studied. Furthermore, central government decision-making appeared not to take into account the reality of national investment landscapes at lower levels of government. Moreover, Chinese tech companies in all case studies were also quick to adapt to new measures imposed by central governments that would otherwise restrict their business in-country.

Introduction

The geopolitical dispute between the US and China is taking place on the fault line of global telecommunications infrastructure and digital technologies. As this competition grows, so too does the likelihood of a potential bifurcation in the global information and security technological ecosystems, split between US-allied liberal democracies on the one side and countries dependent on Chinese-based information and communications technology (ICT) on the other. The impact of this competition reaches beyond telecommunications companies and those involved in their supply chains, and implications exist for the security and defence sectors. While this competition unfolds, the Chinese Government's DSR continues apace and leverages the strengths of Chinese public and private sector entities to further integrate Chinese technologies and standards into the digital ecosystems of the least developed, emerging, and developed economies alike.

This project looks specifically at the implications of the DSR for Western defence industry, and seeks to answer three forward-looking questions through in-depth thematic research on the Digital Silk Road and five national case studies from Europe, the Middle East and the Asia-Pacific. Firstly, what risks does the possibility of a bifurcated global digital ecosystem pose for the national and industrial security of key Asian, European, and Middle Eastern states and economies? Secondly, to what extent does the integration of Chinese information technology and digital infrastructure create challenges for alliance intelligence and defence cooperation, and what level of integration should be considered significant and how might security cooperation efforts (e.g. Western arms exports) be affected? Lastly, can security risks to companies doing business abroad be mitigated when the integration of Chinese digital technology into national digital ecosystems is high?

1. Context of the Digital Silk Road and security-related concerns











In 2013, the Chinese government launched its Belt and Road Initiative (BRI) – a grand plan to connect China with the rest of Asia, and further west with Africa and Europe, through a variety of road, railway, port and other traditional infrastructure projects as well as trade and transport corridors. Though the project initially consisted of the 21st Century Maritime Silk Road and the Silk Road Economic Belt, the plan has since then diversified to include further sub-strands. In addition to an ‘Aerial Silk Road’ and a ‘Polar Silk Road’, the Chinese government has also launched a digital sub-strand of the BRI – namely, the Digital Silk Road. Elements of today’s DSR were first mentioned in 2015 in ‘Visions and Actions on Jointly Building Silk Road Economic Belt and 21st Century Maritime Silk Road’, which laid the foundation of the BRI and mentioned an ‘Information Silk Road’ that included the joint construction of ‘cross-border optical cables and other communications trunk line networks, [and] improve international communications connectivity’.¹ The DSR gained further attention as a formal concept in its own right in 2015 at the World Internet Conference in Wuzhen, and in 2017 at the Belt and Road Forum for International Cooperation, where the DSR gained further political support. There, President Xi Jinping emphasised the importance of digital connectivity and information sharing, and he proposed to ‘pursue innovation-driven development, to intensify cooperation in frontier technological areas such as digital economy, artificial intelligence, nanotechnology and quantum computing, and to advance the development of big data, cloud computing and smart cities so as to turn them into a digital silk road of the 21st Century’.² Since 2017, the DSR has gained top-level attention in official Chinese government speeches, potentially signalling its increasing importance as a foreign-policy priority. At the 2019 Second Belt and Road Forum, Xi again urged BRI countries to

keep up with the trend of the Fourth Industrial Revolution, jointly seize opportunities created by digital, networked, and smart development, explore new technologies and new forms and models of business, foster new growth drivers and explore new development pathways, and build the digital Silk Road and the Silk Road of innovation.³

Though officially touted as part of the BRI, the DSR is a unique ambition that acts more as a parallel effort than a sub-strand of the Chinese government’s BRI. The DSR differs in characteristic from the BRI in scope, types of projects included, and the relationship between key stakeholders and the Chinese government. This would suggest that the DSR is in fact a larger initiative in its own right, and that its future development might also be less dependent on the future of the BRI writ large.

While the BRI operates largely through the signing of bilateral agreements between China and recipient governments (largely at the national, but also at the sub-national level as seen in Victoria, Australia), according to the YiDaiYiLu.gov.cn (the Chinese government’s website dedicated to the BRI), 140 countries have joined the Belt and Road Initiative – though only 133 have officially signed a memorandum of understanding (MOU). Although the DSR also operates according to the signing of MOUs, its scope reaches far beyond official bilateral agreements of DSR cooperation. By 2020 at least 16 countries had signed DSR MOUs with China, however, IISS China Connects shows that DSR-related projects have been carried out or planned in 137 countries worldwide. There is thus no definitive overlap between where China operates the BRI and DSR officially through MOUs.

Figure 1: Digital Silk Road project categories and types

Over-the-top Platforms		E-Commerce
		E-Governance
		Financial Technology (FinTech)
Services		Smart City
		Security Information System
		Data Centre
Infrastructure		Fibre Optic Cables
		Telecom
		5G Network
		Satellite Tracking Ground Stations

Source: IISS China Connects: From coal to code, 2020

The key areas of investment in the DSR span hard infrastructure, digital economic platforms, financial technology and security-related services and platforms (see Figure 1).

The first category includes investments in national telecommunications networks from pre-5G to 5G (and presumably next-generation networks in the years ahead), submarine and overland cable networks, as well as satellite ground tracking stations to assist with the roll-out of China's BeiDou satellite navigation and communication system. The DSR also includes the global roll-out of Chinese technology services, particularly in the areas of smart cities, security information systems (such as Huawei's Safe City projects) and data centres, both brick-and-mortar and cloud-based. Safe- and smart-city projects are promoted as improving the efficiency and safety of urban localities, while data centres aim to support the roll-out of services and over-the-top platforms by reducing latency for users. Examples of over-the-top platforms that participate in the DSR include e-commerce, financial technology and e-governance platforms. These categories overlap with more traditional BRI infrastructure projects at times. When they do overlap, they are included as part of a larger BRI investment project, for example to serve

connectivity purposes at BRI-linked ports or along railways, or to provide security and surveillance systems at BRI infrastructure locations. However, DSR investments are often stand-alone projects.

Aside from the difference in the type of projects invested in, the key stakeholders in the DSR also differ from those of the BRI. The BRI is driven by the Chinese government, and projects receive significant funding from China's state-backed financial institutions such as the Export-Import Bank of China, China Development Bank (CDB) and China's four state-owned commercial banks (the Bank of China, China Construction Bank, Industrial and Commercial Bank of China and Agricultural Bank of China). While these banks also fund some DSR projects, this is limited mainly to funding the roll-out of physical ICT infrastructure and less apparent in investments by China's internet companies in the services and platform sectors.

Furthermore, in contrast to the DSR, as of October 2018 Chinese state-owned enterprises (SOEs) contracted roughly 50% of BRI projects by number and over 70% according to project value.⁴ As argued by Zhang and Yin, by participating in the BRI, SOEs represent the Chinese state – explained through concepts such as *yijing cuzheng* (以经促政, use economics to promote politics) and *zhengjing jiehe* (政经结合, combine politics and economics). However, commercial and economic rationales also play a role in addition to political interests. Through the BRI, SOEs expand their reach to new global markets through a second *zou chu qu* (走出去, going out) strategy, thereby accessing resources and raw materials for China's economy. SOEs also leverage the BRI to redirect excess industrial capacity out of China. By accessing new markets, and doing so with government support, SOEs also hope to increase their global competitiveness. The economic and commercial rationale of the BRI's prioritised SOE orientation is like that of stakeholders in the DSR. However, the main stakeholders in the DSR are private-sector companies that are leading within China, and increasingly globally, in strategic digital industries. Furthermore, while state-backed lending and financing of DSR projects is mainly seen in projects led by SOEs, for example ZTE in the roll-out of ICT infrastructure, most projects do not seem to have the same level of government-backed financing.⁵

The importance of China's private sector to the DSR and DSR-related activities cannot be overstated. Indeed, the centrality of China's private sector to the DSR initiative raises the question of the relationship between the Chinese state, the Chinese Communist Party and Chinese private-sector companies. As a project that is less defined by the Chinese state than the BRI (no 'Vision' document has been published for the DSR), and as one that is led by the private sector rather than state-owned enterprises, it is assumed that the DSR is less likely to be controlled by the Chinese government. Nevertheless, this has not dampened concerns over the potential leverage that the Chinese government may have over China's tech sector. This concern has been particularly strong in the United States and like-minded liberal democracies, especially following the updated National Intelligence Law of China in 2018. Article 7 of this law legally obliges Chinese citizens, organisations and organs to comply with national intelligence work; while Article 14 grants national intelligence agencies authority to insist on this support. To what extent Chinese private-sector companies and the individuals that work for them are in fact leveraged to this end is difficult to determine through open-source research. Some existing research has already been published that shows the link between private-sector tech services and the Chinese government's ability to leverage data collected through services for state security purposes.⁶

Text box 1: National Intelligence Law of the People's Republic of China, 2017

中华人民共和国国家情报法

Article 7

All organisations, and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of. The State protects individuals and organisations that support, assist, and cooperate with national intelligence efforts.

Article 14

National intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation.

Source: National People's Congress of the People's Republic of China, 2017⁷

1.1 Geopolitical competition in the twenty-first century

China is still a relative newcomer on the global silicon highways targeted by the DSR. Corporations from the US and allied countries still dominate global markets, with 42 of the top 50 telecoms and tech companies compared with China's eight. US and other Western corporations dominate the undersea cable system and still outperform Chinese corporations in exploitation of space for telecommunications. China's Digital Silk Road policy, less than a decade old, seeks to penetrate countries where the European empires have dominated telecommunications since the beginning of the telegraph and where national elites established since independence have come to see control of their own independent telecommunications sector as a source of national pride, some political power and often illegal enrichment. The telecommunications infrastructure existing in all countries for the 70 years prior to 2010 were dominated by leading Western corporations or powerful domestic corporations. And with the exception of the US, all national ICT ecosystems in the world are the result of the integration of foreign technology and companies across the technology ladder, spanning physical infrastructure, software provision, content production and service delivery. In physical infrastructure alone, the ecosystem has many separate sectors of commercial activity: landline, mobile, broadband, fibre-optic cables (land-based and undersea), copper cables, industrial control systems, data storage centres, data processing (large mainframe computers), consumer electronics (handsets, laptops, phones), satellite earth stations, and national phone and communications networks.

Nevertheless, geopolitical competition in the twenty-first century has centred on technological dominance, and from the US perspective in particular, the extent to which Chinese tech companies are integrated into national ICT ecosystems around the world. The Digital Silk Road and other national efforts that aim to transform China into a high-tech superpower – the Made in China 2025 Strategy, AI National Development Plan, China Standards 2035, and others – signal the shift that Chinese strategy has undergone in the past decade. While initially aiming to raise the technological prowess of Chinese domestic industry, China's strategy is

‘increasingly about shaping the global ICT environment in ways favourable to its own interests, making use of its status as the global manufacturing hub for ICT products, and its growing economic and political reach’.⁸

Huawei’s central role in debates around technological competition is not new. While the US has been a leader in voicing concerns about, and acting against, Huawei, it is not alone. Since 2018, the governments of Australia, the United Kingdom and Japan have all banned Huawei from taking part in their national 5G network roll-outs due to security concerns – though in the case of the UK, this decision came belatedly and was instead taken on the basis that following a US export ban on critical components Huawei could no longer guarantee the quality of its future equipment supplies.

1.2 Implications for defence

Though definitive evidence of any ‘backdoors’ in Huawei’s 5G equipment is yet to publicly emerge, the security concerns regarding utilising Chinese technology go beyond China’s ability to access or control national infrastructure through the roll-out of Chinese-built and -owned network infrastructure. Nor should the case of Huawei and 5G be the sole focus of security-related concerns. Indeed, the vast scope of the integration of Chinese technologies through the Digital Silk Road means that 5G networks should be viewed as just one component of a whole. The issue of potential backdoors in network infrastructure is thus but one security-related concern for governments when deciding where to allow or limit the integration of Chinese technology into national critical infrastructures. The concern over Huawei’s 5G networks, however, has also served as an incentive for governments to understand in greater detail to what extent Chinese digital technology is already integrated into their national digital ecosystems.

Ongoing debates and analysis that have already been published about security concerns are focused on issues of data privacy for the individual consumer, the security of national critical infrastructure for government, the ability to safeguard and securely share national intelligence, as well as the consideration of the implications for militaries operating in future battlefields where the 5G infrastructure might rely on Chinese technology.⁹ However, the implications of the DSR for Western

defence industries have not yet received similar attention in current literature. Indeed, the US government has on numerous occasions warned allied and partner countries that ‘reliance on Chinese 5G vendors could render our partners’ critical systems vulnerable to disruption, manipulation and espionage. It could also jeopardise our intelligence and communication-sharing capabilities, and by extension it could jeopardise our alliances.’¹⁰ This warning also applied to partner-country militaries, as then-US secretary of state Mike Pompeo warned in 2019 that ‘if [Huawei] equipment is co-located where we have important American systems, it makes it more difficult for us to partner alongside them’.¹¹

The overarching concern is one of standards and future competition. The ability of militaries to communicate, engage and operate through faster streams of data will allow them to keep up with changing environments. The US Department of Defense (DoD) has stated that ‘5G ecosystems of technology can equally revolutionize DoD operations, networks, and information processes’.¹² As it argues, 5G networks could allow the DoD to combine its currently fragmented networks into a single network and improve situational awareness and decision-making, while also allowing for the deployment of new technologies such as hypersonic weapons and hypersonic defences, as well as a potentially strengthening nuclear command, control and communications (NC3). 5G could vastly improve daily tasks such as logistics and maintenance, and improve the efficiency of work across the US military. Who has the leading edge and the greatest roll-out of this technology could determine which standards 5G networks and networked platforms operate on. The competition with China over technologies like 5G and others in the DSR’s remit is as much about security as it is about market access, maintaining competitiveness and future innovation capabilities. US and other Western defence industries will thus need to factor the ability to remain networked, and to what standards, into their research and development (R&D) and production of systems and platforms.

But the question of protecting future competitiveness and innovation is not just about 5G. Concern is also based on the ability of China to leverage its DSR investments to access large quantities of data. Even if it is assumed that the risk posed by Chinese technologies

to intelligence security is low, the ability to harness big data should be of concern to defence industries as it has relevance to future competitiveness in machine learning and artificial intelligence (AI). By some accounts, such as that of Oxford Insight's Government AI Readiness Index, China still ranks far behind the world's AI superpowers. While the US ranks first in their annual list of AI government readiness, China ranks surprisingly low, at 19th place out of 172 countries studied, despite its ambitions to challenge the US for AI supremacy. The authors acknowledge that the national score for China does not account for, and might therefore underestimate, the strengths of regional hubs in China such as Beijing and Shanghai.¹³ Nevertheless, if it is assumed that data sent through servers could be routed through Beijing, and that data could thus be accessed, then China's ability to harness large quantities of domestic data as well as foreign data could potentially be beneficial to its ability to train AI and machine-learning algorithms on an increasingly diversified data set. This of course is not just a privacy or competition concern limited to Chinese companies, but it is also a security concern for Western companies directing traffic through Chinese servers. For example, in 2020 Zoom faced criticism for mistakenly routing some user data through Chinese servers, including a report by Citizen Lab that meeting encryption keys may have been routed through China in one of their test exercises.¹⁴

Just as there is concern in the civilian realm about the supposed risk to information security, the DoD is concerned about the risk to military information security and intelligence sharing. In its 2020 annual evaluation of the health of the US defence industry the National Defense Industrial Association (NDIA) reported that overall industrial security scored six points lower in 2019 than in the previous year. The primary factor that caused the decrease in industrial security was an increase in the threats to information security for defence companies and contractors. The report highlighted that while intellectual-property (IP) rights are foundational to profitability for information-intensive and high-tech industries and companies, 'threats to intellectual property rights have proliferated'. However, the total number of FBI-investigated cases of IP rights violations has remained unchanged from 2017. Cyber vulnerabilities

of individual companies as well as the erosion of industrial cyber security is, however, argued to be worsening and 'the growing number of cyberattacks suggests that it is only a matter of time before new vulnerabilities become new attack vectors'.¹⁵ This has as much to do with cyber security at home for defence companies and contractors as it does with the ability of these companies to ensure cyber security and IP rights abroad. To what extent defence-industry markets in foreign countries can guarantee the same safeguards and business environment also applies to the ability of defence companies to trust the foreign networks they operate on, as well as the ability of subcontractors along the entire supply chain abroad to maintain cyber security standards.

The extent of the integration of the DSR at multiple levels of a country's digital ecosystem should be of concern, not only to ensure IP protection and cyber security at multiple layers of the cyber environment in which a Western defence prime operates, but also to understand what the future restrictions might be on Western defence companies' military exports abroad. With weapons and platforms increasingly interconnected with networks, the extent to which a potential market economy is integrated with Chinese technology may in the future determine whether Western companies receive export licences for sensitive technologies and products. The US has in the past year already increased its export controls on dual-use and critical components for trade with China, and the US defence industry does not export weapons or platforms to China. However, it is unknown if in the future such restrictions will also extend to third countries that are particularly integrated into the DSR. Currently, the US continues to export to, and operate militarily in, allied and partner countries – even those with significant existing Chinese digital investments. According to China Connect data, Germany, for instance, hosts 38 DSR-related projects, including 5G trials, pre-5G telecoms networks, data centres, e-commerce and fintech investments, security and smart-city-related services. The question is whether Germany's decision whether to integrate Huawei technology into the national 5G infrastructure will ultimately be the deciding factor if the US government decides to restrict intelligence, defence and defence-industrial ties.

1.3 Government responses

In response to US concerns about civilian and military data security in any system in which Chinese technology is involved, the US government under president Donald Trump undertook a swift national campaign to block the export of US core technologies, as well as other foreign components based on US design, to China (or any other country that the US deems a security threat). The Trump administration further expanded its 'entity list' of companies to which US companies are prohibited from exporting products or technology in absence of an export licence. Some telecommunications companies, like Huawei and Xiaomi, are alleged to have connections with the Chinese military.¹⁶

The US defence industry, aware of the challenges these new rules pose to their businesses, has been watching these policy developments closely. Not all are supportive, and some industry associations have been critical of the short timelines they must meet when making significant alterations to their supply chains. In mid-2020, the leaders of the NDIA and the Professional Services Council (PSC) called for a further postponement of the enactment of regulations that would prohibit government contracting with companies whose supply chains contain products from five Chinese companies (including Huawei). PSC President and CEO David Berteau has argued that these new regulations 'could affect nearly every contractor and subcontractor across the entire federal government' and that 'compliance with a complex rule, one with consequences that reach beyond prime contractors, could be confusing, complicated and technically challenging'.¹⁷

The US has not only taken these measures at home but has also spent significant effort over the past two years to lobby the governments of partner and allied countries to adopt similar messages. In 2019, then-secretary of state Pompeo took the idea of creating an alliance of 'Clean Networks' around the world, lobbying central governments in Europe and elsewhere to join the US push to ban Huawei and other Chinese technologies in their national digital ecosystems. Clean Network elements include carriers, applications, app stores, cloud, paths and undersea cables. However, not all US allies and partners have signed up to the Clean Network Initiative or signed MOUs with the US on 5G

security. Though then-US under secretary of state Keith Krach declared in 2020 that NATO was now 'in sync' on 5G, 11 NATO members still have not officially signed an MOU with the US on 5G security or officially signed onto the Clean Network Initiative. Furthermore, six NATO members do not have any investment-screening mechanism in place and do not yet have any plans to establish one. The potential for continued Chinese technological investment in these countries with which the US shares a defence alliance thus remains a reality.

A potential contributing factor to national decision-making regarding the acceptance of Chinese technologies could be that the motivation behind criticism from the US is not always clear. While in some cases clear connections are drawn between a Chinese enterprise and a Chinese military end-use, thus presumably presenting a cause for US government concern over the end-use of some American technological exports, at other times commercial interests also factor in US decision-making. According to the *Financial Times*, the US DoD and State Department had pushed to include China's three largest internet companies (Alibaba, Tencent and Baidu) in its latest rounds of blacklisting. However, according to the report, 'Steven Mnuchin, the Treasury Secretary, prevailed in an internal battle, arguing it would harm US investors'.¹⁸ US criticism of its allies and partner countries, particularly in Europe, for choosing commercial interest over security concerns when weighing whether to accept Chinese tech investments at times risks seeming disingenuous. Countries like Hungary, who import gas and electricity from Russia and cooperate with China on economic relations, brush off US concerns over China. Hungary's Minister of Foreign Affairs and Trade Péter Szijjártó stated in 2019 that 'when it comes to cooperation with Russia or cooperation with the People's Republic of China, that does not harm us being reliable as a NATO ally'.¹⁹

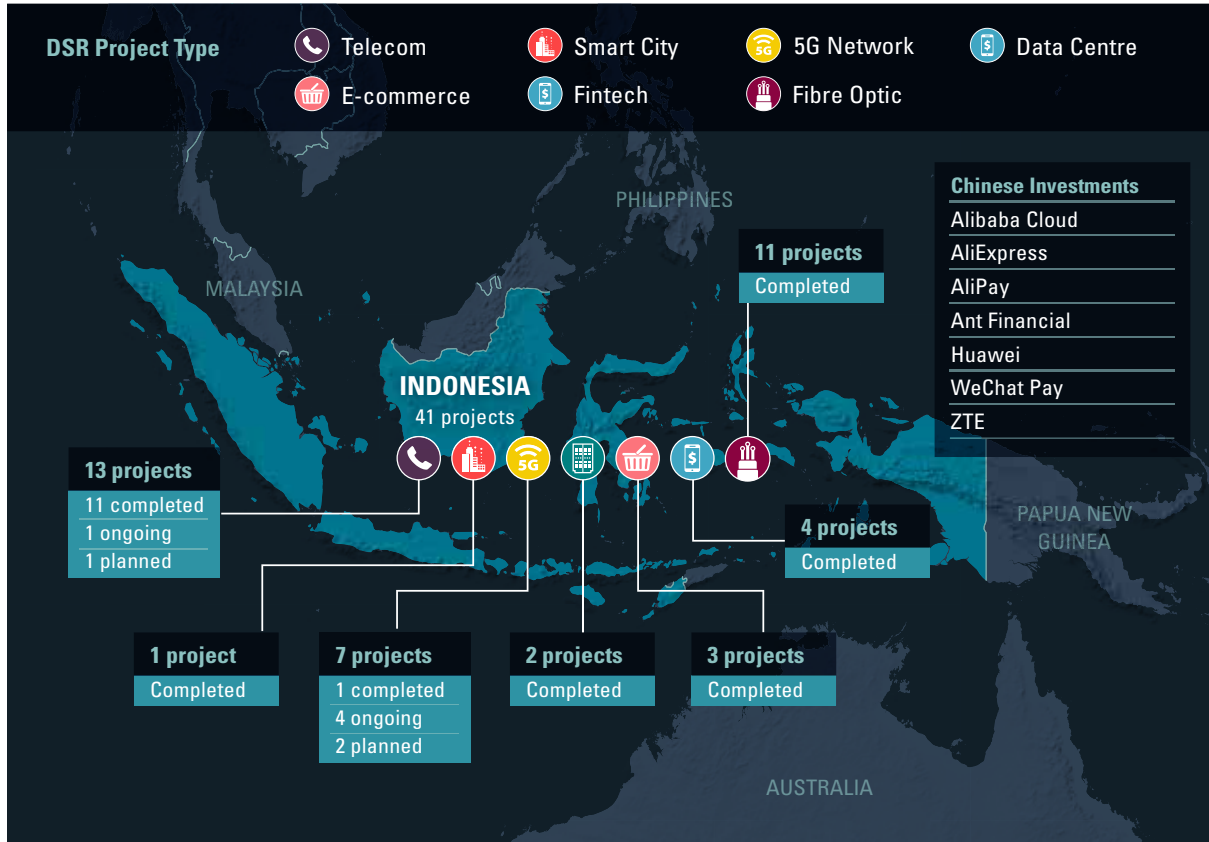
Not all countries agree with the US on the risks of integrating Chinese technology into their national critical infrastructure. But understanding these decision-making processes, as well as the key factors that determine the final decision, is important for US and other Western defence companies. Defence industry should consider the current level of Chinese technology integrated into national ICT infrastructure, as well

as the decision-making of governments in existing and potential export markets, in order to fully understand the potential risk to future business and competitiveness. The following section will investigate these questions through in-depth case studies of five existing and potential markets for the Western defence industry. The five case studies seek to cover markets across the Asia-Pacific, Middle East and Europe: Indonesia, the Republic of Korea, the United Arab Emirates, Israel and Poland. Poland, the ROK and Israel represent established markets and countries with which the US has military alliances. Companies like Lockheed Martin have conducted business with the ROK for over 30 years. Poland represents a key market for companies like Lockheed Martin, which has been a strategic partner for Poland's national and NATO defence needs

for over 20 years, directly employs 1,700 people at its PZL Mielec facility and sustains more than 5,000 jobs through more than 470 suppliers.²⁰ Middle Eastern markets continue to be important business markets for large defence primes, such as Lockheed Martin. For example, Lockheed Martin has conducted business with the UAE for over 40 years and is a key weapons supplier to Israel. Lockheed Martin also works with Israeli subcontractors, such as Israel Aerospace Industries (IAI) for a production line of skins for the F-35 wings.²¹ Indonesia represents a growing market for Western defence primes with ongoing modernisation efforts, and the US is an important trading partner for Indonesia. However, China's technological investment in these markets poses new challenges to companies seeking to understand the investment and security landscape.

2. Five country case studies

2.1 Indonesia



Map 1: Chinese digital investments in Indonesia, IISS China Connects, 2020

Indonesian President Joko Widodo is at the helm of an ambitious national digital initiative – to transform Indonesia into the largest digital economy in Southeast Asia. Indonesia is the world’s fourth most populous country, and it is also a young population, with a third of that population under 15 years of age. Urbanisation is expected to increase to about 65% of the population by 2025 and internet use is rising sharply. However, nearly 40% of the population does not have access to the internet.²² The huge number of islands comprising Indonesia’s archipelago and massive disparities in wealth and development across the country have created ‘two Indonesias’: about 180 million Indonesians in the remote east and interior, lacking access to education

and infrastructure, contrasted with another 80 million urban Indonesians, primarily in Java and the west of the country, with access to Indonesia’s rapidly advancing digital networks. In addressing Indonesia’s enormous challenges and opportunities, Chinese ICT investment has been present every step of the way.

Market opportunity

Indonesia occupies the biggest share of ASEAN’s ICT market, amounting in 2019 to US\$20.9 billion. Indonesia’s ICT sector offers huge market opportunities with an internet penetration of 64.4% of the total population of 272.1 million; and Indonesia’s digital economy is forecast to grow to US\$133bn annually by 2025. Some

96% of Indonesia's internet users between the ages of 16 to 64 own a mobile phone. In 2019, Indonesia's digital economy was US\$40bn,²³ growing annually around 50% since 2015, and forecast to reach US\$133bn by 2025, around 45% of the total for ASEAN. There are big gaps in the demand for supply of ICT talent, with 278 IT workers per one million people, compared to 1,159 per million in India and 1,834 per million in Malaysia. This amounts to a projected shortage by 2030 of nine million ICT workers.²⁴ Through the establishment of 1,000 start-ups driven by high-tech innovation and several national programmes, including the 100 Smart City Movement, Go Digital Vision 2020 and e-smart IKM, the government of Indonesia aims to support smaller enterprises and start-ups as Indonesia catches up with some of its more hyper-connected neighbours in ASEAN. Indonesia's Ministry of Communication and Information (MCI) has increased its budget allocation to IDR 421bn (US\$29.8m)²⁵ for ICT infrastructure development and digital human resources. In May 2020, Indonesia boasted over 2,000 ICT start-up companies and five unicorns (a privately held start-up company valued at over US\$1bn) driven by a selection of incubator programmes and venture-capital projects.

Chinese investment

Indonesia is an enormously lucrative market for Chinese investment. Chinese companies are targeting the development of Indonesia's cloud, the Internet of Things (IoT) and Software as a Service (SaaS) solutions, and the hardware and devices enabling them. Chinese investors are playing a big role in new technologies and analytics facilitating data-centre management. In 2016, imports of ICT devices and parts into Indonesia amounted to US\$6.3bn in value, with goods coming primarily from China. China has heavily invested in Indonesia's unicorns, and Chinese internet giants including Tencent, Alibaba, and JD.com have played a major role in the explosive success of companies like Gojek, Tokopedia, Traveloka and Bukalapak. Google and Singapore's Temasek reported in 2018 that Indonesian internet users spend four hours daily using mobile internet, putting Indonesia in the global top ten of internet users and making it the largest and fastest-growing user base in Southeast Asia.

Chinese investors are heavily involved in Indonesian app development and e-commerce. During a promotional event in Jakarta in February 2020, Huawei announced its intent to make 73 apps available in Indonesia²⁶ by the end of the first quarter, and to attract local app development through its Shining Start programme. Targeting mid- to high-end users, the apps offered banking and e-commerce services including Permata Bank, BCA Mobile, Link Aja and indigenous e-commerce platforms including Blibli, Tokopedia and Bukalapak. China's web-portal giants helped Indonesian internet companies raise US\$6bn between 2015 and 2018. Tokopedia, for example, secured US\$1.1bn in funding in 2018 with a significant proportion from Alibaba. More than 20 Chinese companies are members of the Southeast Asia Blockchain alliance, representing 40% of total membership.²⁷ Despite such enormous growth potential, Indonesia's ICT sector lacks homegrown talent and leadership, meaning that indigenous apps have taken second place to adapting Chinese apps for the local market. Chinese-designed apps have occasionally fallen foul of Indonesian authorities; for example, in July 2018, TikTok was temporarily banned in Indonesia for containing inappropriate content and blasphemy and only reinstated following pledges to deploy dedicated content screening. Censorship works both ways, with Chinese censorship allegedly extending into Indonesia's app market. According to media reports in 2020, Chinese tech company and TikTok owner ByteDance censored material critical of the Chinese government on newly acquired Indonesian news aggregator app Baca Berita (BaBe).

Two decades in Indonesia: The Huawei success story

In the space of 20 years, Huawei has grown to become deeply, if not inextricably, embedded in Indonesia's ICT ecosystem. The company's leadership enjoys a close relationship with key Indonesian government figures and has developed a good level of cultural literacy in Indonesia after its two-decade presence in the country. For example, Huawei has donated qurban (ritually sacrificed animals for the Islamic holiday Eid al-Adha) to the poor as part of Huawei's philanthropic programme, Huawei CARE.²⁸ In March 2020, Huawei Indonesia

came top of a list of most reputable companies helping to tackle COVID-19.²⁹ A Huawei representative revealed AI and cloud technology had been used to help tackle the outbreak under the TECH4ALL programme of social responsibility. Huawei has also joined forces with government agencies in using AI to prevent illegal logging in West Bali National Park. Leading the initiative is Coordinating Minister for Maritime Affairs and Investment Luhut Binsar Pandjaitan, who stated that by utilising Huawei technology to directly monitor voice data Indonesia can prevent illegal logging,³⁰ and he asked Huawei and all relevant ministries and agencies to harmonise systems and data. In a project dubbed 'Smart Forest Guardian', Huawei has joined forces with a cross-ministerial survey team from the Coordinating Ministry for Maritime Affairs and Investment, MCI, the National Cyber Encryption Agency (BSSN), the State Intelligence Agency (BIN) and the Ministry of Environment and Forestry.

Huawei has undergone a remarkable metamorphosis in Indonesia. Its early challenge was to address concerns over quality and to build trust amid stiff competition from Western providers. One way of doing that was to finance local ICT companies in the absence of any assistance from the Indonesian government. In 2010 the Industrial and Commercial Bank of China financed a US\$7.35m credit arrangement for Huawei's Indonesian clients, and in 2015, Indonesia's Huawei subsidiary, Huawei Tech Investment, received a US\$30m three-year structured trade finance package from Deutsche Bank to sell equipment to an unnamed Indonesian broadband company. Huawei proudly announced that a well-structured bridge financing solution offered lowered financing costs, enabling Huawei's plans to continue to expand business further in this market. Meanwhile, Deutsche Bank congratulated itself on an award-winning approach that spanned three jurisdictions: the sale transaction took place under Indonesian law, the credit cover insurance was achieved under Chinese law and the financing was structured under Singapore law. Although there appear to be few other examples of Western banks developing deals in support of Huawei's operations, Singapore seems to be an important hub for financing of such deals in Indonesia. Despite Indonesia's

openness to Huawei investment, Western banks have generally curtailed their activities since the introduction of US sanctions against Huawei.

In 2003, Huawei won contracts from two big cellular operators in Indonesia and, in 2010, its sales increased to US\$1bn. Huawei subsequently won several awards for innovation in its wireless equipment.³¹ From April 2012, Indonesia's second-largest mobile-telecommunications provider, XL Axiata, appointed Huawei to fully manage a national network for over seven years. In April 2016, Huawei hosted the inaugural Big Video Summit in Jakarta, highlighting Huawei's role in introducing ultra high definition (UHD) video in Indonesia. Then-CEO of Huawei Indonesia Sheng Kai described his pride in preparing Indonesia for the Ultra-Broadband (UBB) era, with its UBB 2020 strategy enhancing Indonesia's ICT maturity and broadband coverage in urban areas.³² Huawei's expanding footprint in Indonesia has at times generated acrimony with Indonesia's energetic trade-union movements. In 2013, union activists launched a campaign protesting alleged use of illegal foreign workers by the company.

Nurturing Indonesian ICT talent

Another key to Huawei's meteoric success in Indonesia was its commitment to redress the indigenous ICT talent gap. Huawei's then-country CEO Sheng Kai announced that in 2013 Huawei partnered with the MCI to develop a social-responsibility programme offering research and education in ICT. In 2015, the MCI signed an MOU with Huawei establishing an innovation centre designed to harness human resources in the sector. In March 2017, Huawei launched an ICT training programme with the endorsement of the Ministry of Communications and Information Technology (Kominfo) dubbed SmartGen for students from seven of Indonesia's top state campuses, allowing Indonesian students to undertake vocational training in Beijing and Huawei headquarters in Shenzhen. One year later, then-Kominfo minister Rudiantara presided over a SmartGen event with Huawei targeting 1,000 students of Indonesia's vocational schools to be involved in the programme activities. Huawei's ICT Academy launched the 'Learn ON' in June 2020 offering online ICT training at various leading universities.³³

Huawei is fully embedded in Indonesia's AI strategy supporting the Ministry of Research and Technology/ National Agency for Research and Innovation (Kemenristek-BRIN). As of October 2020 BPPT, Indonesia's Agency for the Assessment and Application of Technology, had signed an MOU with Huawei to develop Indonesia's digital ecosystem and to develop talent through knowledge transfer from Huawei. The agreement was in tune with BPPT's 'triple-helix' collaboration between academia, the government and industry towards Indonesia's digital economy 2035 goals and aspirations for developed-country status by 2045.³⁴ The focus, according to BPPT's head Hammam Riza, would be 5G technology, AI and the cloud. Describing the collaboration as the progenitor of Indonesia's efforts to become more competitive in the fourth industrial revolution, Research and Technology Minister Bambang Brodjonegoro proclaimed BPPT's collaboration with Huawei a symbol of open innovation, accelerating the development of a strong, innovation-based digital ecosystem in Indonesia. Huawei Indonesia CEO Jacky Chen described the venture as a token of trust.³⁵

Telkomsel and Huawei signed an MOU at the Mobile World Congress in Barcelona establishing the Joint Innovation Centre 5.0, offering digital services and talent development supporting Telkomsel goals for Digital Indonesia 2025. In July 2019, Huawei Indonesia was declared the winner of 'Best 5G Innovative Technology' by Indonesia's Selular Media Group. Huawei stated that the award was recognition of Huawei's sustainable investment in R&D and promotion of digitalisation in Indonesia.³⁶ On National Technology Awakening Day, 10 August, Huawei Indonesia in collaboration with the Indonesian Big Data & AI Association (ABDI) held a webinar on AI research and innovation development. The keynote speakers were Minister of Research and Technology Brodjonegoro and CEO of Huawei Indonesia Jacky Chen. Also at the event was the Head of the BPPT Hammam Riza, Director General of Higher Education of the Ministry of Education and Culture Professor Nizam, and Dr Rudi Rusdiah, Chair of ABDI.

Chinese hardware spanning the archipelago

Indonesia recently announced the completion of a historic digital-infrastructure project: the Palapa Ring.

Offering broadband and 4G access to some of the remotest islands and 500 regencies of the nation, the US\$1.5bn fibre-optic network comprises 35,000km of cable. Huawei constructed the middle portion of the project, including crucial nodes intersecting the entire network. Huawei Marine won the contract in 2009 with PT Telkom for the Mataram-Kupang submarine cable system (MKCS) connecting five islands in eastern Indonesia with Indonesia's central and western backbone cable networks. In September 2016, Huawei Marine Networks announced³⁷ that it has been selected to deploy SeaX-1, a marine cable system connecting Eastern Malaysia, Singapore and Indonesia's Batam Island. One month later, Huawei and PT.LEN Telekomunikasi Indonesia (LTI) signed an agreement to design and construct the middle portion of the Palapa Ring Project. The middle section of Palapa Ring connects Kalimantan, Sulawesi and North Maluku via a 1,600km submarine cable system. Huawei revealed this project to be the third domestic submarine cable provided to Indonesia since the MKCS and Bali Cable projects.

The US government, apparently in a counter-move to China's BRI, has joined forces with Indonesia to connect Southeast Asia directly to the US mainland with the world's longest fibre-optic telecommunications cable. The 16,000km cable will be completed within three years with support from the US International Development Finance Corporation (IDFC), which was formed in December 2019 to compete against the BRI. IDFC chief executive Adam Boehler met Indonesian President Widodo and pledged US\$5bn in development funds. Coordinating Minister for Maritime Affairs and Investment Luhut Panjaitan appears to be the point man in the venture, meeting several times with then-presidential advisor Jared Kushner for infrastructure-project discussions.

Established in 2014, FiberStar is a subsidiary of Indonesia's biggest conglomerate, the Salim Group, and is Indonesia's biggest carrier-neutral infrastructure provider, connecting 92 Indonesian cities across the islands of Sumatra, Java, Bali, Kalimantan and Sulawesi. Huawei signed an agreement with FiberStar to expand high-speed-fibre fixed network services and data centres across Indonesia. FiberStar also recently partnered with Huawei to build a 3,000km ring network linking

Jakarta and Surabaya, including marine and terrestrial cables. Huawei was also playing an important role providing data centres and ICT infrastructure upgrades in Indonesia's manufacturing sector, upgrading core data networks for one of Indonesia's biggest cement companies, Semen Indonesia, in May 2019. Huawei's CloudFabric Solution helped Semen Indonesia build a data-centre network including firewalls, load-balancers and disaster recovery (DR) and backup solutions. Telecoms carrier 3 Indonesia and Huawei collaborated to build Indonesia's first prefabricated modular data centre in Malang in East Java cutting construction times from three months to 40 days.

Impact of US sanctions

Indonesia's ICT leaders may be hedging on the outcome of the US presidential election and any policy changes in US approaches to Huawei. As international attention focusing on the security of Huawei's equipment continued to mount during 2019, Indonesia's then-minister of communications Rudiantara observed³⁸ that his ministry would be alert to such concerns but that due to Huawei's significance as a foreign provider of base-station technology, Indonesia could not be paranoid about curbing Huawei's wireless technology. Rudiantara's comments came as Indonesian state-controlled Telkom announced that it had agreed to a partnership with Huawei and that PT XL Axiata had renewed a five-year network-maintenance and equipment contract with Huawei. Telkom Indonesia's President Ririek Adriansyah revealed³⁹ in September 2019 that Huawei was still under consideration as a supplier for 5G and Telkom was waiting to see the outcome of US pressure on Huawei. Adriansyah considered Indonesia to be some years from launching 5G services. The company's smartphone penetration was estimated at only 70%, with remote regions still using 2G services. Telkom's mobile division boasted 168m subscribers in mid-June 2019, two-thirds of them using smartphones. Communications Minister Johnny G. Plate stated that the government was working on the provision of adequate spectrum availability and that there would be a level playing field for foreign providers including Huawei. He dismissed security concerns over Huawei saying, 'everyone is spying on each other

these days,' and that Indonesia did not share the same concerns as the US.⁴⁰ Indonesia was drafting a law for data protection for parliamentary approval in 2020, and had studied the European Union's General Data Protection Regulation (GDPR) as a model. According to Plate, legislation would be crafted to address cyber security and cyber crime, as well as content causing civil unrest and social disharmony.

Indonesia's cyber vulnerability

Indonesia's ICT ecosystem remains fertile ground for cyber attacks and network exploitation. Given the disparity between demand and supply in the indigenous ICT talent pool, Indonesia has struggled to implement a coherent cyber strategy given the rapid modernisation of the ICT sector and the government's lofty ambitions to achieve ICT primacy within ASEAN. Until relatively recently, government and businesses appeared to be turning a blind eye to national and commercial cyber vulnerabilities. However, with the establishment of Indonesia's BSSN in 2018, the government has acknowledged the need to establish nascent cyber-resilience and -defence mechanisms and to engage with foreign powers to establish best practice in policymaking.

Australia and Indonesia signed a cyber-cooperation MOU in September 2018 witnessed by President Widodo and Prime Minister Scott Morrison. At the 2019 IISS Shangri-La Dialogue special session on defence implications for cyber-security development, Agung Nugraha, then-BSSN acting deputy for protection, stated that the Indonesian government was still in the process of creating a Cybersecurity Act.⁴¹ He described the importance of collective responsibility through information sharing with stakeholders and operators in mitigating cyber threats but conceded that the private sector was more knowledgeable about cyber security than government regulators. Nugraha said that his government was concerned about the use of social media for underground and terrorist activities, fake news and cyber crime. However, he did admit that Indonesia had learned from US National Security Agency Director General Paul Nakasone how to handle cyber attacks through its months-long participation in an effective voluntary vulnerability-disclosure programme.

Despite concerns about Indonesia's vulnerability to cyber threats, discussions in Indonesia's House of Representatives about its over-reliance on Chinese ICT investment remains absent from the parliamentary debate. Indonesia's proposed Cybersecurity and Defense Bill – scheduled to be debated and passed in 2019 – was postponed to the 2020 legislative term agenda and is yet to be tabled. The bill was proposed by the House following repeated warnings about the vulnerability of Indonesia to cyber threats and concerns over a potential cyber war.⁴² Public debate and scrutiny of the bill is permitted under Indonesian law. The delay in a debate in the House of Representatives appears to be a result of an overburdened legislative process causing a long backlog of draft bills. According to Deputy House Speaker Fahri Hamzah, the Special Committees for numerous bills, including the Cyber Security Bill, have been unable to complete their work. Legislative experts say that government ministers, including the minister of communication and information technology, failed to attend a House of Representatives meeting to discuss the bill on 27 September 2019,⁴³ allegedly because the president had called an urgent cabinet meeting on that day.⁴⁴

The large-scale student protests of September 2019 and their fallout may partially explain the postponement of the bill to the 2020 term. There was widespread attention and concern over breaches of privacy and freedom of expression. Some articles of the draft bill will allegedly furnish the BSSN with considerable power as the implementing body in coordination with Indonesia's armed forces (TNI), the police, the Attorney General's office and intelligence agencies. Opponents of the bill are concerned that the BSSN would be granted draconian powers if it passed in its current form.

Cyber-security concerns are well understood by President Widodo, who recently warned of vulnerabilities in Indonesia's fintech sector, following BSSN reports that 88m cyber attacks occurred against Indonesian entities during the first four months of 2020. Indonesia's private sector appears to be keenly aware of the problem, as 84% of Indonesian companies planned to raise IT budgets in 2020, though of these less than 50% allocated half of their IT budget to cyber security, according to a survey by Palo Alto Networks in February.⁴⁵

The lack of legislation, repeated concerns and private-sector pressure have created an 'open season' for the Indonesian presidency to consolidate deals with the Chinese telecoms sector by signing a plethora of agreements with Huawei. This situation has been compounded by Huawei – under pressure from the US global Clean Network campaign – redoubling its efforts to exploit the Indonesian telecoms US\$27bn digital-services market. According to Indonesia's National Investment Coordinating Board (BKPM), Chinese investments doubled to US\$4.7bn in 2019, second only to Singapore, with the greater proportion of investments in the telecoms and transportation sectors.

In October 2020, the Presidential Staff Office signed a deal for Huawei to provide ICT vocational training to 100,000 Indonesians. A senior presidential adviser coordinated and presided over the agreement, observing that Indonesia needed to collaborate to boost its lagging ICT human-resource sector. Another key influence has been Minister Luhut Pandjaitan, who was tasked with coordinating Indonesia's participation in China's DSR projects under the Belt and Road Initiative. According to Ardi Sutedja, chairman and founder of the Indonesia Cyber Security Forum, the Indonesian telecoms providers are so inextricably enmeshed with Huawei that even if the Indonesian government were to call for ICT disentanglement it would be extremely difficult and prohibitively expensive to do so.⁴⁶

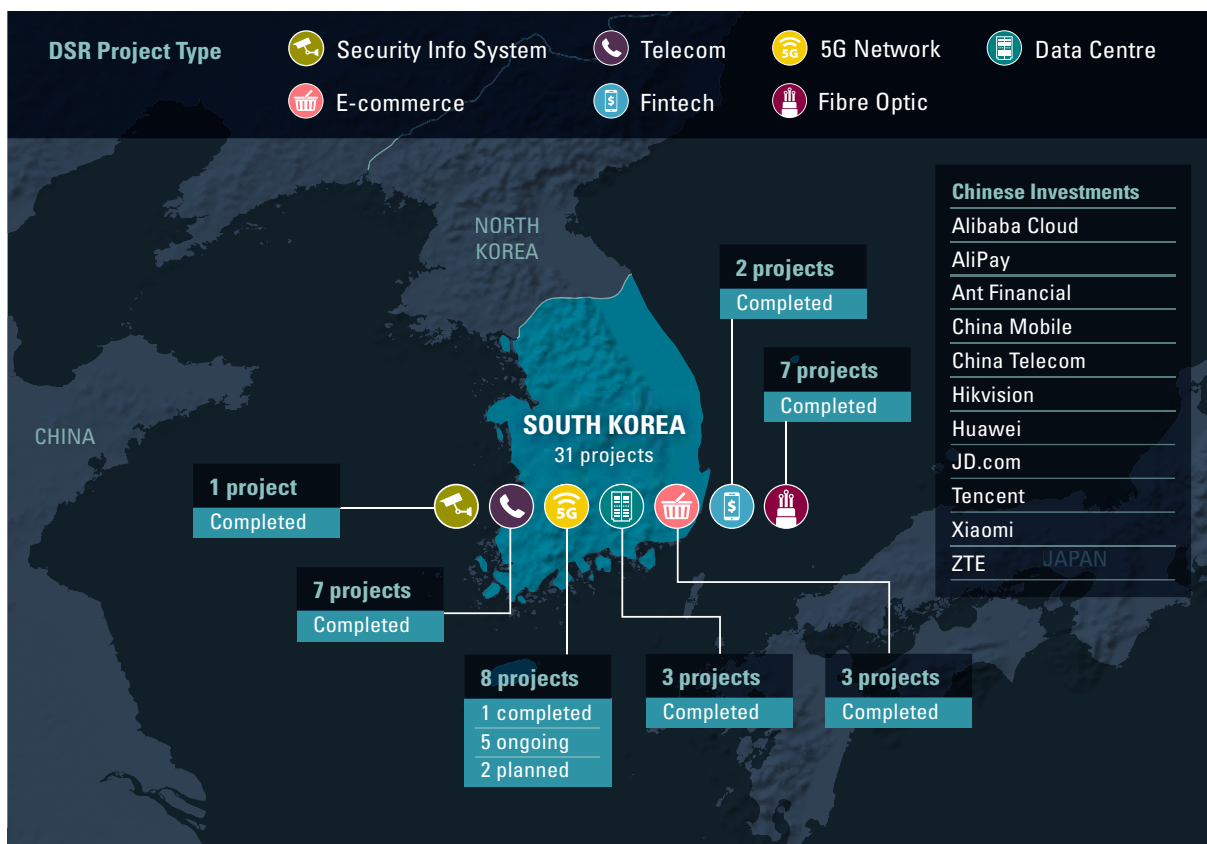
Conclusion

Indonesia is on the cusp of a digital awakening, redressing an imbalance in both internet penetration and indigenous ICT resources, allowing the country to become one of the biggest digital economies and ecosystems in Asia. From the start of this project, Jakarta has been overwhelmingly reliant on Chinese ICT investment and hardware. Huawei is ubiquitous across all aspects of Indonesia's digital infrastructure – from fibre-optic cable networks thousands of kilometres long to the latest smartphones. Chinese-designed localised apps are prevalent among Indonesian smartphone users, whose communications are transmitted and relayed by Chinese-designed base-station technology and data centres. Much of the Indonesian cloud is apparently Chinese

engineered. For at least a decade Huawei has served as a crucible for nurturing Indonesian ICT talent, preparing Indonesia for the advent of 5G, which is still apparently some way off; and it would seem that China has built Indonesia's critical digital infrastructure. Meanwhile, China's biggest web enablers have invested heavily in the ICT sector. Chinese products are so heavily embedded in Indonesian digital architecture that senior government officials appear

to be dismissive of, if not resigned to, any potential threat from China. Indonesia's leaders are rightly concerned that social media might enable terrorist, criminal or subversive activities. Any future bilateral tension could prompt Beijing to wield the strong arm of Chinese nationalism via its pervasive presence in the ICT sector. This may leave Indonesia's critical national infrastructure exposed and could curtail its ambitions for the regional digital economy.

2.2 Republic of Korea



Map 2: Chinese digital investments in Republic of Korea, IISS China Connects, 2020

The Republic of Korea (ROK) is at the heart of the fourth industrial revolution's strategic competition. Amid escalating rivalry in the digital domain between China and the US, Korea is caught between both powers' quest to conquer the digital future. For Korea the historical resonances of Chinese actions in the region go back centuries, and treading the line between

dependence and autonomy today remains equally central to Korean policymaking in its technological engagement with China. Overshadowing this dynamic is the ROK-US security alliance and the presence of a 28,500-strong US garrison on Korean soil, United States Forces Korea (USFK), and its own information- and cyber-security requirements.

Global ICT export power

The ROK is an ICT exporting giant. Korean companies have established complex supply chains across the Indo-Pacific region. The importance of ICT for Korea is reflected in the US\$2.2bn the Moon Jae-in administration allocated for the Digital New Deal in 2020, Korea's five-year plan to accelerate its leading role in the global ICT supply chain. According to Korea's Ministry of Trade, Industry and Energy (MTIE) Korean ICT exports in September 2020 increased to a year-on-year growth of 11.9% to US\$17.6bn.⁴⁷ ICT exports to China grew 5.6% to US\$8.2bn driven by strong sales of semiconductors and computers. Korea's semiconductor industry is heavily dependent on the Chinese ICT market. Korean chip makers rely on exports to China and in particular to Chinese telecommunications champion Huawei. China's share in Samsung Electronics, annual revenue is estimated to be close to 20%, while SK Hynix's dependence may be even deeper – in 2018 nearly 50% of its exports were to China, amounting to 3.1trillion won (US\$2.8bn).

Despite this impressive figure, Korea is by no means self-sufficient in fulfilling its ICT demands. China is a vital supplier to Korea's ICT manufacturing base. Imports of ICT have been steadily rising too. In September 2020, imports also rose 9% to US\$9.6bn with a trade balance showing a surplus of US\$8.1bn. Of total imports, China enjoyed a significant share amounting to 31%. This figure has remained consistent throughout 2020, averaging a little over 30%. China's total share of Korean ICT imports in 2019 was 42.5%. By comparison, the United States' and the EU's shares of Korea's ICT imports have both remained at around 6%.

Chinese ICT in Korea

Chinese attention towards the ICT market in Korea surged in 2015 with Chinese web-portal giants Alibaba and Tencent competing for shares of Korean online-shopping and payment-service markets.⁴⁸ Alibaba sought to make inroads into the messaging and content sector while Tencent targeted digital retail services. Tencent gained a 10% stake in Kakao, Korea's biggest messaging app. Meanwhile, Alibaba established a branch in Korea and invested US\$90m in the content industry. China's telecommunications giants have taken an avid interest in a broad spectrum of Korea's ICT

sector, including Korean start-ups, tapping into Korean technological, innovation incubator programmes. China Telecom has maintained a strong presence in Korea since mid-2012, aiming to encourage joint development as a conduit for market entry of both countries' telecommunications industries and facilitating integration.

Chinese companies also joined the competition for a stake in Korea's cloud market – foreign companies occupied 51% of the market in 2019, increasing their market share by 40%. Korea's Internet and Security Agency (KISA) granted an information-security management-system certification to Tencent in January 2020 as the company readied itself to launch services in Korea. In September 2020, Alibaba Group signed a contract in collaboration with Korean cloud managed service provider Megazone Cloud to introduce Alibaba Cloud Intelligence Brain into the Korean market. China Unicom established a venture fund specifically for the purpose of exploiting Korean tech innovation. In June 2016, SK Telecom revealed that China Unicom had invested US\$1.5m in two Korean start-ups involved in high-speed video transmission and 3D imaging. Both companies were participants in SK Telecom's Dream Venture Star programme run jointly with Korea's Center for Creative Economy and Innovation in Daejeon.

Chinese and Korean companies have also embarked on major silicon-chip foundry ventures, expanding into high performance computing (HPC) chips used for cloud-to-edge computing. In December 2019, Samsung Electronics announced it would mass-produce an AI chip for Baidu, named Baidu Kunlun. The chip is Baidu's first cloud-to-edge AI accelerator, built into the company's own processing architecture, along with Samsung's solutions. This cooperation has enhanced Baidu's AI capability, including search ranking, speech recognition, image processing, natural language processing, autonomous driving and deep learning platforms. On the user end, Baidu is also making successful forays into the Korean app market – 41% of Baidu's photo-processing app Photo Wonder users are Korean.

China is keenly focused on Korea's 5G roll-out. By the middle of the decade, 66% of mobile connections in Korea will be 5G.⁴⁹ A 2019 Internet Usage Survey conducted by the Ministry of Science and ICT and KISA revealed remarkable levels of mobile internet

penetration – 90% of the country’s population aged 3 years and older are internet users, with 95% of them connecting to the internet via smartphone and the same proportion using instant-messenger apps.⁵⁰ Korea’s younger generation are being offered increasingly wider choices of smartphone. Chinese brands are no exception, and in early 2019 Xiaomi’s launch of a new model priced more than 50% cheaper than other smartphones sold out almost instantaneously. Korea’s and China’s telecommunication giants are already collaborating on cutting-edge 5G services. KT and China Mobile announced in late 2019 the joint development of a blockchain-based real-time roaming-charge system called B.Link which can self-analyse roaming data from both carriers in real time. ZTE’s intent to penetrate the Korean smartphone market is evident, but early news suggested that the company was taking a cautious approach bordering on obfuscation of its brand within the Korean market.

Huawei and 5G Korea

Huawei is determined not to be sidelined in Korea owing to US pressure there and is doing as much as possible to remain at the cutting edge of 5G development. Huawei has recently launched an open laboratory (OpenLab) for next-generation 5G wireless networks in Korea. In light of the sanctions announced by the US, it was a deliberately low-key launch without a media presence. Huawei announced plans to invest US\$5m in the OpenLab in Seoul’s Jung Gu district, designed to focus on building a 5G ecosystem through cooperation with a number of South Korean ICT small and medium enterprises (SMEs). The laboratory was Huawei’s first open-5G services development centre allowing companies to test their platforms, focused on four major sectors: Cloud Virtual Reality and Augmented Reality, connected vehicles, robots, and intelligent manufacturing. Huawei’s OpenLab boasts end-to-end 5G network equipment including 5G base stations, core networks and transport networks for its partners to use free of charge. Meng Shaoyun, Huawei Korea’s then-CEO, stated that plans to establish a fully fledged R&D centre in Korea were still on the table but Huawei was committed to the principle of ‘In South Korea, for South Korea’.⁵¹ Huawei’s then-head of global media and communications, Karl Song

Kai, stated that US close-mindedness would present opportunities for South Korea and that Huawei would be increasing investment there.⁵² Song’s sentiment was echoed by China’s state media in September 2020 following a visit to Busan by Chinese politburo member and director of the Central Foreign Affairs Commission Yang Jiechi, at the invitation of Korea’s National Security Advisor Suh Hoon. China’s *Global Times* reported that despite intensifying strictures imposed by the US on Huawei, it would be possible for Huawei and Samsung to cooperate in a low-profile manner.⁵³

Huawei’s low-key approach appeared to be taking on a more public tone this year when Huawei Korea signed a partnership with the Korean Artificial Intelligence Association aiming to boost Korean AI-sector start-ups’ business abroad, including a programme of events and educational programmes. Huawei stated that it intended to support a healthy AI ecosystem in Korea and to support AI-related computing infrastructure. Huawei Korea also appointed a new chief security officer (CSO), Lee Joon-ho, a former chief information security officer at major Korean web portals Daum and Naver, in early June 2020. Despite the considerable threat to Korean exports following the 15 September US trade ban, LG Uplus, the only telecommunications carrier incorporating Huawei technology, stated that this was unlikely to have any major effect on its new 5G network, 70% of which had already been completed.⁵⁴ While the Korean 5G dilemma has been at the forefront of strains in the US–Korea relationship, Huawei’s ubiquitous presence in wired networks across Korea’s business community has been largely overlooked. Many, if not most, of Korea’s corporations including banks and financial services companies use Huawei for their internal networks.

Compartmentalised USFK communications

Inter-alliance communications between the defence ministries and the entire command and control (C2) and command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) networks are managed and secured by the US. Unclassified information on the equipment used in these networks is unavailable but it would be inconceivable that any of these systems, both within the USFK intranet and its connectivity with the ROK Ministry of National

Defense (MND), would contain Huawei equipment. US security concerns over the presence of Huawei equipment in South Korean networks are not new to Seoul. The US Senate highlighted its concern in 2013, but other US government agencies would have harboured such concerns much earlier. By 2014, the ROK government was engaged in low-key discussions with the US government over these issues. The potential threat falls into two categories: firstly, the security of inter-alliance communications, and secondly, the threat posed by LG UPlus 5G networks incorporating Huawei equipment in close proximity to US bases in Korea.

The security of ROK–US defence communications is governed by a memorandum of agreement between the two ministries of defence on communications interoperability and security. The agreement stipulates that US standards define interoperability parameters, and that the US DoD provides and maintains communications-security equipment to the ROK MND. The agreement includes the establishment of a Command and Control Interoperability Board (CCIB) which meets twice a year. In addition, the two sides hold an annual command, control, communications, computers, and intelligence (C4I) summit. A trilateral C4I annual meeting, which is considerably more complex, is also convened between Korea, Japan and the US. Historical differences between Korea and Japan have at times threatened this relationship. In August 2019, Korea announced that it would cease participation in the General Security of Military Information Agreement (GSOMIA) trilateral intelligence-sharing mechanism,⁵⁵ prompting USFK Commander General Robert Abrams to warn against historical differences undermining the alliance.

USFK runs an Interoperability Program between the ROK Joint Chiefs of Staff and USFK as well as United States Indo-Pacific Command (US INDOPACOM) J61 (C4) staff. This programme directly supports USFK J6 with information technology, architecture and engineering, and C2 networks. The C2 networks enable the Commander Combined Forces Command (CFC) and USFK and subordinate commanders with a capability to effectively command and control nearly 690,000 combat-ready troops on the Korean Peninsula via network-centric high-speed connectivity among sites supporting ROK and US forces. USFK J6 Combined IT support

services are maintained by US defence contractors who recruit network engineers and administrators holding US citizenship and clearances up to TS/SCI (Top Secret/Secret Compartmented Information). For example, the US defence contractor Tribalco supports USFK C4ISR by deploying multilayered National Security Agency (NSA) compliant solutions, enabling USFK to share and protect classified data.

Huawei equipment in close proximity to US bases

The US has been concerned with Huawei and its proximity to its communications for some time, and the relationship between Korean conglomerate LG and its telecommunications companies and the USFK community have at times been strained. In 2007, USFK agreed a deal to prevent Korean telecoms provider LG Dacom from blocking US Voice over Internet Protocol (VOIP) companies' services at USFK bases.⁵⁶ US concerns about LG Uplus's relationship with Huawei are not limited to the former Trump administration. As early as 2013, senators from the Foreign Affairs and Intelligence committees wrote to former secretary of state John Kerry expressing their concern over LG's deal with Huawei. Anecdotal evidence suggests that 10,000 USFK personnel changed carriers when LG Uplus introduced Huawei-enabled 4G services. In 2014, following closed-door discussions with the US, Seoul agreed that no sensitive Korean government communications or US interaction would take place by networks incorporating Huawei equipment.⁵⁷ At that time, LG Uplus clearly viewed USFK as an important customer and was ready to ensure that US military bases would not be connected to networks containing Huawei equipment.

The US maintained its pressure on the Korean government to eschew Huawei following the migration of USFK command, CFC and United Nations Command (UNC) from the Yongsan garrison in the heart of Seoul to the more remote US Army Garrison Humphreys at Pyongtaek in 2018. LG Uplus was one of the providers of mobile and internet services to the mega-garrison, which consists of 50,000 military personnel, their families and contract workers providing services to the base. Their communication needs presented a considerable communications security challenge to USFK.

Meanwhile, Korean news media reported that US diplomats were mounting an intensive lobbying campaign to prevent the installation of LG Uplus 5G equipment in sensitive areas.⁵⁸ The US has maintained consistent pressure on Seoul to counter Huawei's influence. Randall Schriver, former assistant secretary of defense for Indo-Pacific Security Affairs, warned in the Korean media against embracing Huawei and the possible loss of confidence in sharing sensitive information with the ROK government.⁵⁹ While LG Uplus prepared to roll out Huawei-enabled 5G services via 30,000 base stations in the Seoul, Incheon, Gyeonggi and Gangwon regions in early 2019, Korean media said that US requests had ensured there would be no Huawei equipment installed in areas with a USFK presence.⁶⁰ The Trump administration continued to exert pressure on the Korean government to exclude Chinese telecommunications companies from its 5G networks as late as mid-October 2020. According to South Korean officials, the 5th ROK-US Senior Economic Dialogue on 14 October 2020 saw the US emphasise that Korea must subscribe to former secretary of state Pompeo's Clean Network programme.⁶¹

Seoul's reluctant acceptance of US concerns

While the Korean national-security community is keenly aware of the Huawei security dilemma and has likely undertaken numerous closed-door discussions with the US, little light has been shed on just how LG Uplus has set about distancing its networks from USFK facilities. Some Korean commentators have suggested that President Moon Jae-in himself has not fully grasped the gravity of the threat. The Korean government has continued to stress the autonomy of telecommunications companies in addressing security concerns,⁶² encouraging companies to use third-party security assessors to monitor networks. To this end, LG Uplus announced in April 2019 that it would employ the services of S-1, a Korean network-security provider, to oversee network-security concerns.⁶³

In the aggregate, government acquiescence on the Huawei dilemma suggests deference to Korea's *chaebols* – the powerful family-run conglomerates – who in turn pay their own deference to China as a huge ICT market for Korea. The financing arrangements for LG's

partnership with Huawei are, as with most strategic deals between Chinese companies and Korea's *chaebols*, opaque. It is possible that government officials have conflated USFK communications-security concerns with the US Clean Network campaign and are hedging that a Biden administration will be less tenacious over the Huawei concerns. Then South Korean foreign minister Kang Kyung-wha declared in July 2020 that South Korea would ensure 'strategic openness while working to maintain technological security' in the technology sector, which is shorthand for deference to China. A 2020 policy paper by the Center for New American Studies lists several reasons driving Korea's 'digital entanglement' with China.⁶⁴ These include the 'alliance dilemma' and the fallout of economic coercion by China in 2018 following the deployment of the Terminal High Altitude Area Defense (THAAD) missile-defence system in Korea.

It should also be noted that geopolitical risk and national-security concerns have not necessarily permeated from the government into the private sector. This is clearly evidenced by the delegation of responsibility for security assessments over the inclusion of Huawei into Korean networks to the telecommunications companies themselves. While there appeared to be some willingness by Seoul to accept the veracity of US security concerns in conjunction with the US Clean Network campaign, policies have since been more contradictory. South Korea's minister of science and ICT urged telecommunication providers to use domestic equipment for the 5G network in January 2018, but changed his position six months later citing fears over disputes with Beijing. In the wake of the 5th ROK-US Strategic Economic Dialogue last year, a South Korean official again stated that the ICT equipment used by telecoms operators was the company's own decision and that the government would not interfere in the decisions of private companies.

In practical terms, USFK has created a closed network in Korea, which includes an interface with Korea's MND and CFC. The network uses US communications-security standards and is maintained by US-cleared engineers only. It is air-gapped from ROK military networks, perhaps for good reason. A TV Chosun expose in October suggested that 48,000 AI smart speakers purchased by the Korean military and installed at military

facilities across Korea contained chips produced by a Huawei subsidiary, HiSilicon.⁶⁵ In the absence of any public government debate, the Korean National Assembly appears to have forced the agenda. When National Assembly legislator Yun Ju-gyeong of Korea's People Power Party questioned the MND about the presence of Huawei chips in military equipment, the MND professed that it was unaware of the problem.

The security of communications within Korea's defence industry would be another key concern for both the US and the ROK given the need for alliance interoperability. Little light has been shed on the levels of communications traffic within Korea's domestic defence-industrial base conveyed over Huawei equipment or if USFK strictures are applied to Korean defence corporations. There is also the question of whether foreign defence vendors present in Korea, predominantly but not exclusively from the US, have banned Huawei equipment from their own corporate networks in Korea. It must be assumed that Korea-US intergovernmental communications concerning defence sales from the US to Korea would be carried over US classified networks, but it is less clear whether communications between defence contractors and their clients and Korea's *chaebol*s are carried over 'clean' networks.

Huawei and LG Uplus

Of Korea's three big telecommunications carriers, KT, SK Telecom and LG Uplus, LG is the only company committed to incorporating Huawei into its 5G networks. Concerns over LG Uplus's relationship with Huawei surfaced as early as late 2013 when reports emerged that Washington had successfully lobbied Korea to take measures to ensure that USFK-ROK military-to-military communications remained secure.⁶⁶ According to the reports, Seoul would not use Huawei in important communications with the US, and USFK communications would not be carried on Huawei equipment. LG Uplus acknowledged that USFK was an important client but admitted that it had not withdrawn from its relationship with Huawei.

South Korea's National Assembly, through the Expert Advisory Council on 5G Security, has scrutinised 5G security and potential Huawei equipment vulnerabilities since early 2018. The decision to adopt and launch

5G services significantly pre-dated the Trump administration's anti-Huawei campaign. Huawei has made a public statement that it will fully comply with Korean government demands to examine the security of its 5G equipment.⁶⁷ The company acquired a Common Criteria EAL4+ certificate for its 5G base station equipment in June 2020 and declared it had secured international credibility for its 5G wireless-network equipment.⁶⁸ As US pressure mounted, then-prime minister Lee Nak-yeon instructed Korea's Ministry of Foreign Affairs to launch a seven-member task force to deal with Korea, US and China relations. Emphasising corporate autonomy, the ministry insisted any solution would not impact the security of military communications, adding that no security flaws had been detected in Huawei products.

The president is the final arbiter of China's involvement in Korea's ICT ecosystem, and President Moon's national-security adviser, Suh Hoon, plays a particularly important role in weighing up US security demands against the lobbying power of Korea's powerful *chaebol* leaders. Underlying this is a complex system of policymaking and advisory channels comprising industry associations, labour unions, National Assembly groups and government agencies. Despite early efforts by the Korean government to mitigate security concerns over Huawei's current and future presence in the Korean telecommunications ecosystem, US sanctions on Huawei have caused anxiety within Korea's semiconductor sector. Huawei was added to the US Department of Commerce Entity List in May 2019. One year later, enhanced US sanctions prevented companies from using US software and machinery to design or produce chips for Huawei or its affiliates. Anxiety over pressure by the US was reportedly rooted in Korea's experience of being shunned by China in the wake of a land sale by Korea's Lotte group to USFK for the deployment of the controversial THAAD anti-ballistic missile system deployed in the south of the country to counter North Korea's burgeoning missile threat. Lotte and its affiliates suffered huge losses along with several other Korean business giants, including Hyundai.

ROK-US bilateral tension

As US strictures against Huawei started to take a toll, the Korean media reported that the US had raised concerns that 5G networks could jam military

communications and radar operations, a capability which had been downplayed by government officials.⁶⁹ In a background brief for the Korean media, an anonymous official insisted there was little security risk in using Huawei equipment, which amounted to less than 10% of Korea's 5G infrastructure. The official observed that Huawei was isolated from Korea's defence and security telecoms networks and that there would be no impact on South Korea-US military and security interests.⁷⁰ Then-US ambassador to Korea Harry Harris had stressed the importance of good communications between Seoul and Washington in a meeting with then South Korean National Security Office chief Chung Eui-yong on 7 June 2019, warning that Washington would be reluctant to share sensitive information with Korea unless it eschewed Huawei's presence in its networks. Harris warned that collaborating with untrustworthy 5G providers would have long-term implications for national security and stressed that in the interest of cyber security the US and allies must prioritise trustworthy vendors over cost cutting.⁷¹ The Korean government complained to Washington that the move had no basis in international law, and Korean newspaper editorials accused the US of being egocentric. Former under secretary of defense John Rood warned of the risks of the installation of Huawei equipment in Korea's networks in a statement to the US House Armed Services Committee in January 2020.⁷² Robert Strayer, then US deputy assistant secretary for cyber and international communications and information policy, directly called for LG Uplus to abandon its use of Huawei equipment in favour of trusted vendors on 21 July 2020.⁷³ Despite LG Uplus's decision to push ahead with Huawei equipment in its 5G base stations, US pressure has had some effect. Both KT and LG UPlus decided not to use Huawei in planned 5G optical backbone network upgrades, allegedly at the request of USFK. Nonghyup bank was also reconsidering a US\$100m Huawei-KT consortium to install a wired network, and Korea Electric Power Corporation was also assessing removal of Huawei equipment from its own networks.

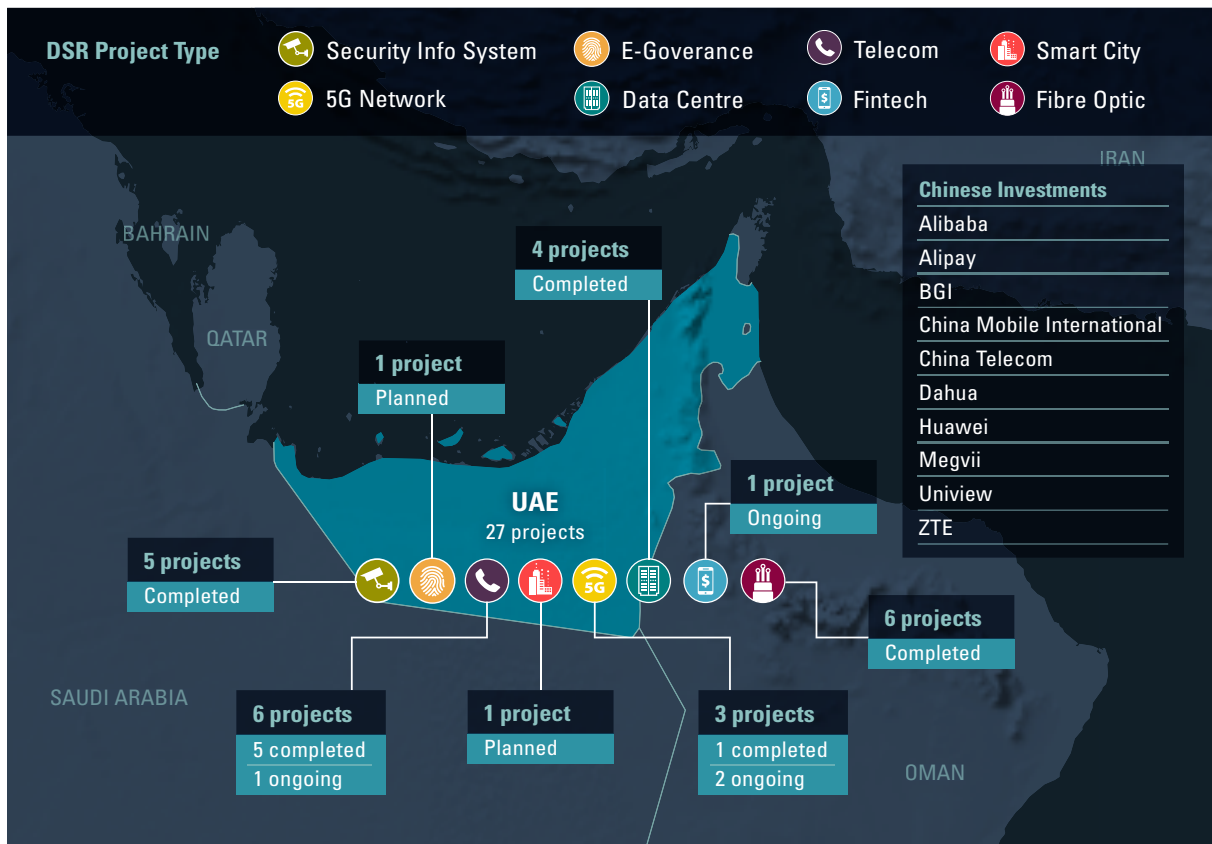
Huawei has meanwhile pressed on with courtship of Korean business, inviting a large delegation to tour its headquarters in Shenzhen, including Samsung Vice-Chairman Yoon Boo-keun and Min Byung-doo,

Democratic Party Member of Parliament. As of mid-October 2020, the Korean government was continuing to resist US pressure to remove Huawei equipment from its networks, repeating the similar messaging from several months earlier. Korea's three major telecoms operators had dismissed the exclusion of Huawei from 5G networks in May. On 13 October, officials from the Moon administration had rejected US pressure on the Korean government to exclude Huawei equipment during high-level economic discussions.

Conclusion

China's foreign direct investment (FDI) in Korea is a carrot-and-stick tool for the Chinese leadership during times of political tension. For example, when bilateral tensions over the US deployment of THAAD radar in Korea were deemed to have eased in 2018, Chinese FDI in Korea surged 240% to US\$2.74bn.⁷⁴ Korea's ICT exports to China have been centre stage in the Sino-US silicon-chip war, revealing an intricate, complex and enormously lucrative national asset which the Korean establishment will apparently defend at some cost to ROK-US relations. The Korean government has faced pressure from the US on two fronts: firstly, extricating itself from a deeply entrenched ICT supply chain with China as a result of successively punitive US sanctions against Huawei, and secondly, eschewing Huawei's presence in Korea's new 5G mobile-communications networks. The ROK government is keenly aware of red lines regarding the security of USFK and inter-alliance communications. However, China's ICT footprint in Korea, like much of Asia, is much broader than the vagaries of chip wars and Huawei's presence in Korea's 5G roll-out. The debate has ignored the weight of global Chinese ICT behemoths, the enablers of internet commerce, the likes of Tencent, Alibaba and Baidu, and their impact on Korea's ICT ecosystem and society at large. All of China's national ICT champions, Huawei included, seem entranced by Korea's ability to innovate in the ICT sector, its ultra-competitive semiconductor industry and Korean society's addiction to digital connectivity and commerce. Beneath the tectonic stresses of Sino-US information rivalry, all these Chinese ICT giants have quietly invested in Korea's digital ecosystem and China continues to absorb the insights of this hyper-connected society.

2.3 United Arab Emirates



Map 3: Chinese digital investments in United Arab Emirates, IISS China Connects, 2020

Over recent years, the UAE has sought to position itself on China's Digital Silk Road. Driven by the need to both diversify its geopolitical relationships and to propel its economy beyond hydrocarbons, the small Gulf state has been eager to develop its ties with China in a wide range of sectors, including new technologies. For the UAE, China's ambitious Digital Silk Road aligns well with its own agenda to build a more digitalised and knowledge-driven economy. Western companies have long been key partners of the UAE's digital transformation, but as China emerges as a new global leader in new technologies, it is increasingly becoming a partner of choice for the UAE and other Gulf Cooperation Council (GCC) states. While still mainly centred on the transactional export of Chinese technologies to the UAE, this relationship is slowly moving towards greater strategic cooperation, including in R&D. However, as the US–China rivalry ramps up and risks of technological decoupling loom, cooperation on such strategic – and potentially sensitive

– sectors could crystallise tensions and put the UAE under growing pressure.

The UAE's digitalisation agenda and its deepening partnership with China

Recently, the UAE has been at the forefront of an important push made by GCC countries to digitalise their economies and societies. Building technology-driven knowledge economies has become a high priority on government agendas within broader efforts towards economic diversification. AI, IoT, cloud-computing services, biotech, e-commerce, and financial technologies, as well as improved broadband and digital infrastructures, appear as promising vectors of this transition. GCC societies are already familiar with digital tools. The UAE's smartphone penetration is the highest in the world at 73.8%, with more than 90% of the population having access to the internet.

The UAE is by far the most advanced country of the region on this path. The country launched a series of

national strategies for National Innovation (2014), for the Fourth Industrial Revolution (2017), for Artificial Intelligence (2017), and for Blockchain 2021 (2018), building a comprehensive framework to support the state's digital-transformation agenda. The country appointed a dedicated Minister for Artificial Intelligence in 2017, an Ambassador of the Fourth Industrial Revolution in 2019, and introduced a Ministry of Industry and Advanced Technology in 2020. The country aims to become a major hub of tech start-ups and hosts several large international conferences around cyber and information security such as the Gulf Information Security Expo & Conference (GISEC) in Dubai.

On 5G infrastructure, considered key to unleashing the full potential of digitalisation, the UAE is again spearheading GCC efforts and appears well positioned on global rankings. As early as 2016, the UAE's Telecommunications Regulatory Authority had formed its four-year-long 5G roadmap and established a steering committee to facilitate the deployment of 5G. In December 2019, the UAE announced that 5G coverage in 'populated areas, main cities' was 80%.⁷⁵ The UAE ranked first in the Arab region and fourth globally in the launch and use of 5G networks, according to the Global Connectivity Index issued by Carphone Warehouse in 2019.

These efforts are starting to pay off. Oxford Insights' 2019 government AI readiness index ranks the UAE within the top 20 countries globally, ahead of China and Israel. In the 2019 IMD World Digital Competitiveness ranking, the UAE climbed five places to 12th. In 2018, the UAE reached the 21st rank globally in the UN's E-Government Development Index (EGDI), ahead of many European countries.⁷⁶

The path to the UAE becoming a full-on innovation hub is still long. The country relies heavily on highly educated foreign engineers and entrepreneurs, and is struggling to develop the human capital of its national workforce. The UAE leadership is also focusing a lot on the PR aspect of its investments in new technologies, sometimes missing the long-term vision needed for a comprehensive development strategy. Government voluntarism is strong, however, and the coronavirus pandemic is likely to compound this trend. Social distancing has accelerated the adoption of digital tools by

the public, the state and private companies, and the collapse of oil prices has further highlighted the urgency of economic diversification in the Gulf.

Western companies are key partners of this push for digital transformation in the Gulf, with US companies especially long dominating the global ICT market and digital innovation. However, as China is emerging as a new global leader in high-tech, it is increasingly becoming a partner of choice. In December 2017, the UAE was among the eight countries co-launching the China-led Digital Economy International Cooperation Initiative on the margins of the World Internet Conference held in Wuzhen. The initiative aims to foster digital cooperation along the Chinese Belt and Road on a wide range of sectors from e-commerce to cyber security and international standardisation.

This UAE-China technology partnership is developing in a broader context of deepening ties between the two countries. Over the past decade, China has become a key player in the Gulf, through its energy imports but also the BRI. In a context of perceived US disengagement from the Middle East, China has appeared for the countries of the region as a tool of strategic hedging. The UAE has therefore sought to engage China beyond the energy sector, to slowly bring the relationship to a more diversified and strategic level. While China's Digital Silk Road focuses mainly on exporting Chinese technologies and services to the rest of the world, the UAE seeks to become more than just a consumer of Chinese technologies and has the ambition to establish itself as an equal partner of China in the field of tech innovation.

The UAE's cooperation with China and Huawei on its 5G roll-out

The 5G and GCC countries' partnership with Huawei is what has gathered most international attention recently. GCC countries, especially the UAE and Qatar, have been competing to be among the first countries in the world to launch their 5G networks. In this race to 5G, Huawei appeared as a partner of choice, able to provide rapid and low-cost solutions. The UAE's two main telecom companies, Etisalat and Du, both announced their cooperation with Huawei for network supply in early 2019, alongside similar deals with Nokia and Ericsson. Although all telecom companies in the GCC

are diversifying their 5G partnerships to avoid full reliance on Huawei, Huawei has secured more 5G deals than its competitors – 13 in the GCC as of December 2020, against six for Ericsson and four for Nokia – and is present in all the countries of the region.

Far from being newcomers to the region, Chinese telecom companies, mainly Huawei and ZTE, already have a long history of cooperating with Gulf operators. Huawei had already partnered with Etisalat and Du to develop their 3G, 4G and 4.5G networks. The partnership with Huawei had allowed the UAE to be the first Arab state to launch its 3G network in 2003. This long-standing relationship with Huawei is a key factor behind the decision of Emirati telecom companies to contract Huawei on 5G projects. On top of Huawei's already competitive prices, it is much faster and cheaper to opt for 'non-standalone implementation', building out the first wave of 5G on top of existing 4G infrastructure. Representatives from telecom companies in the Gulf also acknowledge that Chinese providers are not only cheaper but have also over recent years significantly upgraded the quality of their technologies and services, in a way that makes them increasingly attractive and competitive.⁷⁷

Huawei has also unrolled a long-term strategy to integrate itself in the digital landscape of Gulf countries. Since the early 2000s, the Chinese ICT giant has had regular knowledge-sharing engagements with Emirati political and business decision-makers. It has developed and conducted training programmes, young leaders' initiatives, and organised ICT competitions and study trips to Shenzhen, in cooperation with almost all GCC governments, to support the identification and formation of local engineers and ICT talents in the Gulf. In the UAE, the Huawei ICT Academy signed partnerships with the American University of Ras Al Khaimah and the University of Sharjah, and provided free ICT skills training and certification exams during the COVID-19 pandemic. Those trainings aimed to foster people-to-people ties and prepare a generation of engineers and digital entrepreneurs in the UAE that perceive China positively.

Another element in Huawei's advantage in the GCC has been its involvement in a wide range of projects beyond 5G, including in smart- and safe-city projects in cooperation with different Emirati government authorities. The

broader cooperation with Huawei at the highest levels of the state has likely weighed on the internal Huawei 5G debate, making it more difficult for the UAE government to abide by US pressures to ban Huawei. The US anti-Huawei campaign has, however, pushed GCC telecom companies to diversify their partnerships and avoid full reliance on a single provider. In the UAE, Du and Etisalat have both signed 5G contracts with Huawei but also with Ericsson for Etisalat, and Nokia for Du.

Beyond 5G: Towards a more strategic UAE-China tech partnership?

While 5G and Huawei have gathered a lot of media attention, they are far from being the only aspects of the UAE's digital cooperation with China. Many other Chinese tech companies have appeared on the UAE market, working on a wide range of sectors and projects, from e-commerce and fintech to AI, smart cities, cloud computing information-security in systems. But more importantly, increased cooperation on R&D and high-level engagement on digital issues also signal the creation of a relationship that aims to go beyond the simple exchange of services and reach more strategic levels.

Mutual investments in the high-tech sector from both China and GCC countries have increased over recent years. In an interview in June 2020, Mubadala's CEO Khaldoon Al Mubarak – who is also the UAE's special envoy to China – declared his intent to explore investment opportunities in Asian markets in the technology sector.⁷⁸ In October 2019, the Dubai Chamber of Commerce and Industry revealed its plan to open a new office in Shenzhen, the Chinese hub for technology companies, signalling a willingness to foster mutual investments.

The telecoms market, e-commerce and fintech are key areas of fruitful business cooperation and joint investments between Chinese and Emirati companies and institutions. Huawei, Xiaomi and OPPO's smartphones, as well as Chinese apps and platforms such as TikTok, AliExpress and Jollychic, are already popular in the UAE. Alibaba Group has made significant headway in the UAE, attracted by the fintech and e-commerce potential of the region. It partnered in 2014 with the Dubai Chamber of Commerce and Industry to launch an e-commerce platform ahead of Expo 2020. In 2017, it announced the construction of a

US\$600m 'Tech Town' near Dubai's Jebel Ali. The cloud-computing division of the company, Alibaba Cloud, also partnered with several Emirati institutions and companies on their cloud solutions and launched in 2016 with Meraas a data centre which is the first full-fledged public cloud company in the Middle East. Emirati financial institutions such as the Dubai International Financial Centre (DIFC), the First Abu Dhabi Bank and the Abu Dhabi Global Market (ADGM) made a series of partnerships on fintech innovation and cooperation with Chinese companies such as Alipay, as well as with Chinese financial institutions.

Another area of fruitful cooperation between the UAE and Chinese companies is smart-city solutions. Huawei has positioned itself at the forefront of these efforts. In 2019, it signed MOUs with the Dubai municipality for smart-city cooperation in Smart Dubai and South Dubai. Both Huawei and Alibaba Cloud cooperate with the Dubai Electricity and Water Authority (DEWA) to develop smart-city solutions. In 2016, Huawei chose Dubai to launch its first OpenLab in the Middle East and North Africa, in cooperation with the Emirati Telecommunication Regulatory Authority, where it develops and promotes a wide range of AI, IoT-enabled solutions such as smart cities, public safety, smart transportation, digital oil & gas and smart electric power.

Biotech and healthcare technologies are also an area of promising partnership between China and the UAE. In December 2019, Abu Dhabi-based AI company G42 launched the Population Genome Program in partnership with the Beijing Genomics Institute (BGI) and the Emirati Department of Health. According to their official website, the programme aims 'to provide citizens with their own high quality genome as a baseline and incorporate genomic data into healthcare management'.⁷⁹ In the following months, as the coronavirus pandemic developed, G42 furthered this partnership with BGI and Chinese Sinopharm to jointly develop a vaccine and a detection lab. The Inception Institute for Artificial Intelligence (IIAI), created in Abu Dhabi in 2018 has a specific research focus on healthcare tech, and cooperates with leading hospitals in the country, such as Cleveland Clinic Abu Dhabi, VPS Healthcare Group and Abu Dhabi Health Services Company.

As the UAE–China tech partnership is deepening, the countries are also starting to cooperate in the academic and research realm. The newly created Mohammed bin Zayed University of Artificial Intelligence counts among its founding board of trustees Dr Kai-Fu Lee, founder and CEO of Sinovation Ventures, and Andrew Chi-Chih Yao, from Tsinghua University, as well as Group42 CEO Peng Xiao, and it is presided by Professor Dr Eric Xing. The Executive Vice President and Provost of the University is Professor Ling Shao, who is also the founding CEO of the Inception Institute for Artificial Intelligence (IIAI). In the IIAI, two of the four members of the Scientific Advisory Committee are Chinese, and 50 of the 67 researchers and engineers (three-quarters) are Chinese or of Chinese descent. The IIAI also created a specific grant to fund Chinese doctoral students to study in some of the AI-related programmes of the New York University of Abu Dhabi. In 2019, Chinese AI unicorn UBTECH Robotics, backed by Chinese internet giant Tencent, inked a deal worth US\$362.4m to step up AI teaching labs for students in the UAE.

As Chinese researchers and engineers become more present in the UAE's AI research landscape, the partnership between the two countries is slowly moving beyond transactional interactions towards a deeper, more strategic partnership. For the UAE, which actively seeks to develop human capital and indigenous research, such cooperation is crucial.

A digital cooperation largely based on the security sector

Beyond commercial opportunities, a more strategic dimension of this cooperation for the Emirati leadership is the applications of these new technologies to enhance state control and security. In the UAE, state control over the population has gradually tightened over the past decade, and on repeated occasions, the UAE has praised China for its counterterrorism efforts in Xinjiang,⁸⁰ as well as for its handling of the COVID-19 crisis.⁸¹

As a result, an important part of the UAE's tech partnership with China has a security edge. The UAE is an important client of Chinese video-surveillance and facial-recognition tools, supplied by companies such as Hikvision, Dahua, Megvii and Yitu. Some of the UAE's biggest investments in Chinese digital companies have

been in the field of security systems. In 2019, the Abu Dhabi Investment Authority invested heavily in Megvii, and Mubadala invested in the facial-recognition firm SenseTime in 2017. The Abu Dhabi Investment Office also signed a deal with SenseTime in 2019 to open an R&D centre in Abu Dhabi, and Dahua opened its Middle East branch in Dubai in 2015. This cooperation on security technologies goes beyond transactional purchases and is being integrated in a broader effort by the government to digitalise its capabilities. Overall, Huawei's smart-city solutions provided to Smart Dubai, South Dubai and promoted through its OpenLab all have an important security component.

In 2017, Huawei signed an MOU with Dubai Civil Defense, the Ministry of Interior and the Emirati cyber-security firm Pegasus (a subsidiary of Dark Matter) for the development of 'safe city' solutions, including smart video surveillance and big-data applications. The CEO of Pegasus at that time, Peng Xiao, is now the head of another Emirati AI company. This continuity of actors involved in different branches of the state apparatus, from the health sector all the way to the security sector, suggests a comprehensive approach by the Emirati state to the control of its population, similar to the Chinese governance model. This growing partnership with Chinese companies for the procurement of security solutions has also developed greatly in neighbouring Saudi Arabia, where the government notably partnered with Huawei to develop a Hajj and Umrah app tracking all pilgrims entering the country. Here again, the relationship is slowly moving beyond the transactional purchase of Chinese technologies towards greater cooperation involving the highest spheres of the Gulf governments.

Security and geopolitical debates and implications

The deepening UAE-China partnership on new technologies is raising new questions about its potential geopolitical and security implications. So far, most security concerns have been voiced by the US. As part of a broader global campaign against Huawei, US officials have repeatedly expressed their concerns to the Emiratis about the ramifications of such a partnership with China and have attempted to prevent them from

using Chinese technologies in their 5G networks. While Emirati officials and telecoms companies initially saw it as another traditional commercial competition between the US and China, they are taking increasingly seriously the potential political risk this could engender. Originally very centred on purely commercial interests, the calculations around technology partnerships are increasingly developing a strong political connotation.

In September 2019, during a visit to the UAE, Saudi Arabia and Bahrain, the US State Department's deputy assistant secretary for cyber, international communications and information policy and the Federal Communications Commission Chair raised their security concerns to their interlocutors.⁸² A few months later, in June 2020, the US embassy in the UAE declined an offer from the UAE government to test its staff at the testing centre established in cooperation with the Chinese. While US officials have been less vehement than they have been with Israel – mainly because the UAE is less technologically advanced and less exposed to sensitive US military technologies than Israel – pressures are likely to increase as the UAE's relationship with China deepens.

The UAE is an important security partner for the US in the region. It hosts a US Air Force presence at its base at Al Dhafra, US ships in Fujairah and Jebel Ali, receives important military assistance and training from the US, and imports 7% of US global arms sales.⁸³ Current discussions about the possible sale of F-35s to the UAE following the normalisation with Israel – agreed to by the Trump administration and put on temporary hold by the incoming Biden administration – could bring this military-technology transfer to another level if confirmed.

From an American perspective, the main fear is strategic US technologies, especially military or dual-use technologies, being transferred to or spied on by the Chinese. Experts have highlighted the existence of connections between Chinese technology companies such as Huawei and the Chinese government or military. The use of Chinese technologies within the UAE's digital infrastructure, and the cooperation with Chinese companies and universities on technology research and development, make the UAE more prone to IP theft or cyber espionage by China. US concerns are further

reinforced by the fact that the UAE is slowly deepening its security relationship with China, including the import of Chinese armed drones – the *Wing Loong 1* and 2 – at a moment when the US Congress has blocked the export of such sensitive technologies from the US to Gulf countries. In 2019, Chinese Minister of National Defence Wei Fenghe visited the UAE.

From the UAE's perspective, however, the risk perception is much different. China is not considered a major cyber threat in the region. GCC countries have faced numerous cyber attacks over recent years, but most of them were coming from Russia, mainly for commercial intelligence in the energy sector, or from Iran. To the contrary of Israel, the UAE is also not technologically advanced enough to be a target of IP theft from China, and it does not enjoy the same level of access to cutting-edge US military technologies. The lack of Chinese investments in UAE tech companies and R&D cooperation – in comparison with Israel – signals that the UAE is still very much a technology importer and is not considered by China as strategically important on its DSR in the way Israel could be. The establishment of a SenseTime R&D office in Abu Dhabi is reported to be a more cosmetic, heavily financed and initiated move by the UAE, rather than the result of a Chinese initiative.

Finally, when it comes to internet governance and data privacy, GCC countries have more congruence with China than with the West. Emirati officials and telecoms companies have long been rather unconvinced by US warnings about possible security risks posed by Chinese technologies, considering those claims as the result of a simple commercial competition between the two powers. However, US pressures are starting to change the internal debate in the UAE. While Emirati telecom companies and officials continue to publicly voice their support for Chinese technologies, wary not to antagonise Beijing, they acknowledge in private that they are increasingly worried about maintaining the right balance between their economic, strategic and security interests.⁸⁴ More than seeing China as posing a security threat in itself, the main dilemma for GCC states comes from US pressures and the fear that their security relations with Washington could be downgraded. The US remains the uncontested security guarantor of GCC countries.

From a regional perspective, the UAE's race towards digitalisation and towards Chinese investments falls within the context of an acute competition with its own neighbourhood. Whether it is in relation to Iran, Turkey, Qatar or even its own GCC allies, the UAE is keen to stay a step ahead. It was the first GCC country to normalise ties with Israel in September 2020, and is likely to use this new opportunity to foster a tech triangle with Israel and China in the region. The company G42, already closely connected to Chinese tech companies, will be the first Emirati company to open an office in Tel Aviv.

As US–China tensions rise, GCC countries will find it increasingly challenging to balance both powers. A full-on confrontation between the two powers could lead to a digital decoupling that would put Emirati companies in a difficult situation. The US decision to tighten sanctions on Huawei and the sale of critical chips could compromise Huawei's ability to deliver on current 5G demand beyond the first half of 2021, a time when some analysts have warned it could run out of essential components.

Emirati companies and universities would also not want to risk losing crucial cooperation with Western entities. Overall, Western countries remain the UAE's main partners in its digitalisation efforts. On the website of the UAE's Strategy for Artificial Intelligence, the majority of partners mentioned in the different programmes and initiatives are from the US, Europe, India and South Korea (Microsoft, IBM, Dell, Oxford University, Berkeley University, Samsung), not China.

More significantly, the UAE's tech cooperation with China could also impact Abu Dhabi's security partnership with the US. At the date of writing this piece, the Biden administration has put the agreement with the UAE to purchase American F-35s on hold. This sale would constitute a significant upgrade in the military technology exported by the US to the UAE. So far, debates about the sale have not mentioned the China angle much, focusing rather around the question of Israel's quantitative military edge (QME). China's deepening relationship with the UAE is seen as an argument in favour of the sale rather than against it, as the US seeks to avoid its Gulf allies turning to China to import sensitive military technologies, as they have done in the past for uninhabited aerial vehicles (UAVs) when the

US refused to make those exports. It seems, however, that if the sale is confirmed the risk of US technology theft by China in the UAE would become greater, and that the US would have an additional means of pressure to constrain the UAE in its relationship with China.

The limits of the China–UAE tech partnership

The UAE–China partnership in the tech sector has been developing rapidly over recent years. However, the strategic importance of this relationship should not be overestimated. From Beijing’s perspective, the UAE is one partner among others along its Digital Silk Road. The eagerness of the small Gulf country to cooperate with China has made good publicity for Beijing’s initiatives in the region, and its ability to finance cutting-edge projects is an asset. However, no matter how much money it invests in its own digitalisation, the UAE still has a long way to go before it bridges the gap with more advanced nations such as Israel, Japan or Western countries. The UAE still lacks the human capital, engineers, entrepreneurs, and R&D centres to develop a solid indigenous high-tech industry.

The Emirati government’s eagerness to achieve rapid outcomes makes it prioritise prominent turnkey projects over long-term comprehensive development strategies. Therefore, while the UAE appears as a good entry point to the GCC market for Chinese ICT companies, it does not appear particularly strategic nor to be bringing cutting-edge technologies. By contrast with Israel, China is not investing much in UAE tech companies, and the UAE is still very much a technology importer. The cooperation on research and development also remains at its early stages. Very few Emirati researchers and engineers are involved in the different research projects of the New York University in Abu Dhabi or of the IIAI.

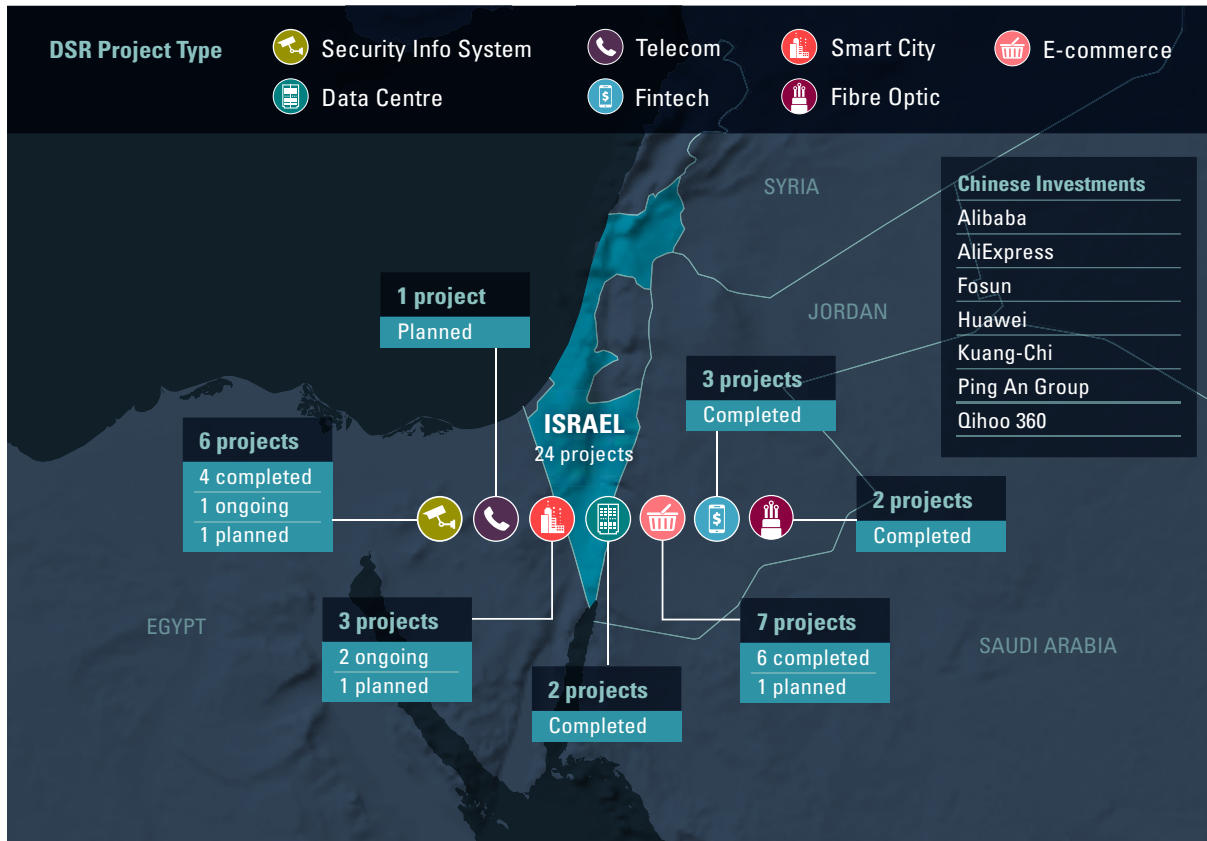
The presence of Chinese researchers appears rather motivated by the willingness to penetrate the region and cooperate with non-local researchers employed by those institutions.

Conversely, Chinese tech companies have a lot to bring to the UAE, but the West remains by far the leader in the market. Abu Dhabi-based Mubadala Investment Company has invested some US\$2bn across China, including in the tech sector, partly through the Softbank Vision fund; but this number is dwarfed by the US\$100bn in investments it made in the US over the same period. Reports of the Gulf’s sovereign wealth funds’ tech shopping spree over recent years mainly mention investments in US companies in Silicon Valley.⁸⁵

Conclusion

As both China and the UAE are seeking to digitalise their economies and position themselves as emerging global leaders in the field of cutting-edge technologies, the two countries have found each other natural partners in the technology field. Originally based on the transactional export of Chinese technologies to the UAE, the relationship is starting to evolve towards greater cooperation. Joint R&D, but also the development of security and population-control technologies, with cooperation at the highest levels of the Emirati state, are gradually bringing the cooperation to a more strategic level. The growing US–China rivalry is, however, challenging this blossoming relationship, with the US putting its Gulf allies under increasing pressure. While the tech cooperation between the UAE and China is only at its very early stages and does not pose the same direct threats to the US as in the case of Israel, close monitoring is still needed.

2.4 Israel



Map 4: Chinese digital investments in Israel, IISS China Connects, 2020

Israel occupies a special place along China's Digital Silk Road. It is the only country in the world to have signed a Comprehensive Innovation Partnership with Beijing, putting a strong focus on science, technology and innovation cooperation since the early stages of the relationship. It is also one of the few countries along the DSR where China is less interested in selling its own technologies than in trying to acquire another's innovation. Often branding itself as a 'start-up nation', Israel's vibrant tech ecosystem has benefited from a highly educated population, coupled with government incentives and investments from multinational companies. This model of innovation-led development, but also the strong synergies between Israel's tech and defence industries, are particularly interesting to China, whose companies have dramatically increased their investments in Israeli tech companies over recent years. However, Israel's special partnership with the US is a major challenge to this blossoming relationship. As China makes headway in Israel's tech ecosystem, the

strong pushback from the US is putting Israel in an increasingly difficult position.

The Israeli high-tech ecosystem

Israel has established itself over the past few decades as a global hub for cutting-edge technologies and innovation. In 2020, it was ranked 6th globally in Bloomberg's Innovation Index and 13th in the Global Innovation Index. A highly educated workforce, combined with a coherent national policy of competitive grants and tax incentives, and the support of the local defence industry, foreign high-tech firms and sophisticated research centres, have made Israel a unique model of development in the world. It has the world's most research-intensive business sector, and Israel invests 2.2% of its GDP in R&D, the third-highest level in the world.

In 2017, the ICT sector represented 20% of Israel's total exports of goods and services. Israel's high-tech companies cover a wide range of sectors, from digital health, biotech and foodtech, to AI, cyber security,

cloud computing, fintech, data analytics and robotics. It has been particularly efficient at attracting investments from big foreign companies. Israel is one of the biggest venture-capital centres in the world outside the US. According to the Israeli Innovation Authority, the amount of high-tech capital raised in 2019 reached a new peak of US\$9bn, a 450% increase since 2005.

One specificity of the Israel model is the close synergy between its defence industries and its high-tech industries. In the 1980s, R&D was mainly aimed at developing military communications and electronics, and was largely funded by the defence and aerospace industries. Between 1980 and 1989, Israel devoted an average of 16.5% of its GDP to military spending. Considered a strategic asset against a Soviet threat, Israel also enjoyed high amounts of US military support, which reached a new high of US\$1.3bn in 1979. Civilian spin offs from military technology created the basis of Israel's first generation of high-tech enterprises. After the Cold War, the decline in global defence spending compelled many Israeli defence companies to expand into civilian markets. Many of Israel's high-tech products in the fields of medical electronics and robotics were developed by adapting technologies developed by the Israel Defense Forces. The government also financed and encouraged cyber research and dual military-civilian R&D through its National Cyber Bureau, and through the establishment of a CyberPark in 2014.

Israel's partnership with the US and Europe has been key to the development of this high-tech ecosystem. According to the Israel Venture Capital Database, 300 foreign research centres are currently active in Israel. Many of these centres are operated by large multinational companies such as Apple, Google, Intel, Microsoft, HP, IBM and eBay, some of them having been present for over three decades. These foreign companies play a crucial role in the local industry. In 2011, 30% of employees in the Israeli high-tech industry were employed by foreign-owned companies, and these companies represented 43% of production.

A fast-emerging China-Israel partnership, strongly focused on technologies

While the US has long been the paramount partner and investor in Israel's high-tech sector, China has emerged

over recent years as a new significant player. The two countries started business relations under the radar in the late 1970s, even before they formalised diplomatic ties in 1992. Relations took off substantially only after Prime Minister Benjamin Netanyahu's visit to Beijing in 2013. In just a few years, China became Israel's second trade partner for both imports and exports. As Beijing developed the BRI after 2013, Chinese construction companies gradually became key players in Israel's infrastructure sector.

From the beginning, however, new technologies and innovation were at the centre of the relationship. Coming back from his visit to Beijing in 2013, Netanyahu declared that China was interested in 'three things: Israeli technology, Israeli technology and Israeli technology'.⁸⁶ The two governments created a task force to advance technology cooperation in 2013, a China-Israel Joint Committee on Innovation Cooperation (JCIC) in 2014, and in 2017 they signed an Innovative Comprehensive Partnership that puts a specific focus on science, innovation and technology cooperation. The two countries agreed 'to closer exchanges among young technological personnel, and cooperation in joint labs, a global technology transfer center, innovation parks and an innovative cooperation center'.⁸⁷ According to data collected by RAND on 87 Chinese investments made in Israel between 2011 and 2018, 75% of those investments went to the technology sector.

Originally, technology relations between the two countries mainly revolved around the defence sector, and the Israeli Ministry of Defense exerted strong influence over this relationship. During the 1980s and 1990s military-technology transfers between Israel and China were estimated to range between US\$1bn and US\$2bn, with Israel selling or helping to upgrade aircraft, tanks, missiles, airborne early warning (AEW) systems, radars and navigation systems to China. For China, the Israeli symbiosis between defence and technology industries, as well as Israel's close cooperation with the US, was perceived as particularly attractive. This blossoming relationship hit a wall in the late 1990s-early 2000s when the US pressured Israel to cancel two major deals over fears about the transfer of sensitive military technology to China. The first deal in 2000 concerned the selling to China of the *Phalcon* AEW radar system,

which US pressures forced it to cancel. The second incident occurred in 2005 when the US prevented Israel from repairing and possibly upgrading the *Harpy* UAVs it had previously sold to China. The Pentagon was reportedly concerned that American technology could be leaked to the Chinese. The two incidents led to a dramatic severance of Israel–China defence relations and to major changes in the structure of Israel’s export-control regime. In 2007, Israel consequently passed the Export Control Law, increasing the restrictions on exports of arms and dual-use technologies.

While Israel is not likely to return to the previous status quo, it started to slowly resume its defence relations with China in the 2010s, with visits of military delegations and maintenance cooperation. However, this cooperation remains very limited and under the shadow of US scrutiny.⁸⁸ China responded pragmatically to this shift and continued to develop the relationship through other civilian sectors such as technologies related to agriculture, health, biology and water. The Israeli government also played a key role in incentivising the development of Sino-Israeli cooperation. Resolution 251 adopted by the Knesset in 2013 called for the expansion of those ties and was followed by additional government directives, incentivising different ministries to cooperate with Chinese companies. Chinese activity in Israel was also enabled by a relatively permissive investment environment that only regulates foreign investment in Israeli companies that produce military or dual-use goods and services. As a result, since the mid-2010s, China has started investing substantially in Israel’s tech start-ups. According to a report by Tel Aviv-based research firm IVC Research Center, the number of Chinese companies investing in Israeli high-tech entities rose from 18 in 2013 to 34 in 2017, and the annual Chinese investment in start-ups from 2015 to 2017 was in the range of US\$500–600m, 12% of all capital raised by Israeli start-ups during that period.⁸⁹

For many Israeli companies, China’s huge market and fast-growing economy appear to be the future for their technology exports. They hope that by deepening their ties with their Chinese counterparts, they will obtain greater access to the Chinese market, which is reputedly difficult to penetrate. Many of the investment funds channelling Chinese investments into Israeli tech

companies promise to assist these investment companies in ‘penetrating the Chinese market and identifying a Chinese strategic partner’.⁹⁰ In a report published in December 2019, the Israeli Ministry of Finance also highlighted the strong dependence of Israel’s high-tech sector on US funding, leaving the Israeli economy very exposed to external economic downturns, and called for greater diversification.⁹¹

Perhaps more important than the commercial opportunities, Israel is also seeing its growing relationship with China through a political and strategic lens. Israel is increasingly seeking to diversify its partnerships away from its traditional partners, the US and Europe. Netanyahu’s visit to Beijing in 2013 came only a few months before the official launch of Beijing’s ambitious Belt and Road Initiative. This was amid growing debates about China’s emergence as a new global power, and strained relations with the Obama administration. Important disagreements with the US administration on the Israeli–Palestinian peace process, and on how to manage the Iranian challenge, pushed Israel to hedge its strategic dependence on the US. China’s good relations with Iran are also perceived by Israel as another potential lever towards the Islamic Republic.

From China’s perspective, Israel appears as a unique model of innovation-led development and military–civilian synergy. Beijing is eager to learn from Israel’s policies and practices as it is itself trying to shift its economy from labour-intensive mass manufacturing to high-tech innovation and services. The civilian–military synergy of the Israeli model interests China at a moment when it is also advancing its own military–civil fusion (MCF) strategy. China is also interested in acquiring some of Israel’s most advanced technologies. Compared with markets in the US and Europe, there are fewer barriers to entry in Israel to Chinese investors. The US has adopted strong screening instruments to control foreign investments and acquisitions such as the Committee on Foreign Investment in the United States (CFIUS) and the Foreign Investment Risk Review Modernization Act (FIRRMA), and the EU launched an investment-screening plan in 2018, with all these measures specifically targeting China. Israel therefore appears as a weaker entry point to obtain advanced technologies, including technologies originally from

the US. From a broader political point of view, China sees Israel as an important player in the Middle East. In 2020, the historical normalisation of ties between Israel and some Arab Gulf states – which are also important Chinese partners in the region – further reinforced the importance of this strategic axis. Making economic headway into these countries allows Beijing to slowly weaken the network of US partners in the region, without having to commit more substantially on the security side.

China's growing tech cooperation with Israel

Sino-Israeli cooperation in the high-tech sector has kept increasing over the past ten years. The channels of transfer of Israeli technology to China have multiplied, taking three main forms: exports of Israeli technologies to China with a significant number of deals involving the transfer of production technology, Chinese investments in Israeli tech companies, and R&D and academic cooperation.

Israel's exports to China have increased significantly over recent years to reach US\$4.6bn in 2019. Most of these exports were in the high-tech sector, such as software, computing and R&D services. In 2018, 57% of Israel's total goods exports to China were machinery and electrical equipment, most coming from Intel Israel. In the context of US sanctions over semiconductor chip makers' exports to China, Israel has started emerging as a significant exporter of chips to China. Israel is also an important exporter of technology patents to China, with the annual number of Israeli patents granted to China growing from about 200 in the early 2000s to over 700 in 2015. According to sources, some of these deals involved the transfer of the technologies exported, such as the revealing of the source code of product software. Therefore, these deals have the potential to contribute to the development of China's telecommunications, aerospace and other industries, possibly including China's military modernisation. In relative terms, however, Israeli exports of high technologies to China remain limited due to the competitive business environment in China and the concerns over IP rights violations.

A potentially more important aspect of the growing tech relationship between China and Israel has been

the acceleration of Chinese investments in, and acquisition of, Israeli tech companies after 2010. According to a report by the Tel Aviv-based research firm IVC Research Center, Chinese investments into Israeli tech start-ups have been increasing rapidly over recent years, reaching US\$325m in the first three-quarters of 2018.⁹² Chinese entities invest either directly in Israeli companies, or through Israeli venture-capital (VC) funds, which themselves invest in other Israeli technology companies. Israeli VC firms such as Singulariteam, Viola Ventures, Catalyst, OurCrowd and others have received significant funding from Chinese investors. Several Israeli–Chinese funds were also created with the specific aim of investing in Israel's high-tech sector. These included Infinity I-China Fund created in 2007, Go Capital & EOC (GEOC) founded in 2013, and Mizmaa Ventures in 2017, which alone had a target of US\$100m in Chinese investments. In 2016, Kuang-Chi launched a US\$300m Global Community of Innovation (GCI) Fund, with its headquarters based in Tel Aviv. These funds and joint ventures aim to foster Israel–China cooperation, with the Israeli partner providing the technology while the Chinese partner is responsible for the introduction of the product to the Chinese market.

The most active Chinese investors in Israel's high-tech sector include investment firms such as Horizons Ventures, China Everbright, Go Capital and Kuang Chi, as well as large Chinese private companies such as Alibaba, Xiaomi, Lenovo, Tencent, Baidu and Huawei. Investments supported by Chinese policy banks such as the China Development Bank, or from Chinese state-owned enterprises, have been much less frequent, which signals that Chinese private entities see a clear commercial and financial interest in investing in Israel without the government having to intervene very much. However, due to the connections between big Chinese tech companies and Beijing, this does not rule out the influence of the government's strategic objectives in those investments.

Chinese investments have targeted companies working on a wide range of emerging technologies such as foodtech, biotech, data analytics, computer vision, AI, cyber security, fintech, cloud computing and robotics. Chinese investors were involved in about 12% of all the

high-tech deals taking place in 2018, which is relatively modest, but the numbers have increased over recent years, and when participating, Chinese investors capture from 30 to 40% of the total capital raised. In 2018, Chinese investors participated in six of the 17 largest funding deals in the Israeli venture market.

Another substantial channel of Israeli technology transfer to China is through their academic and R&D cooperation, which has developed greatly over recent years. The Three-Year Cooperation Action Plan signed in 2015 by China and Israel proposed the founding of the China–Israel 7+7 Research-Based University Alliance to promote research and academic cooperation between research universities in Israel and China. The Technion-Israel Institute for Technology, Israel's leading university of new technologies and innovation, in cooperation with Shantou University and with US\$130m in financial support from the Li Ka Shing Foundation, established the Guangdong Technion-Israel Institute of Technology (GTIIT) in 2015. Israel has signed R&D cooperation agreements with the Chinese government, as well as with Chinese state agencies and provinces such as Shanghai, Shenzhen and Jiangsu. Several Chinese companies, such as Techcode and DayDayUp, have opened innovation and R&D centres in Israel. In 2017, Kuang-Chi opened its International Innovation Headquarters in Tel Aviv, and in the same year Alibaba Group opened the Alibaba Israel Machine Vision Laboratory in Tel Aviv, as part of its multi-billion-dollar DAMO global Academy. In September 2019, the Jiangsu-based Wujin Hi-Tech Industrial Zone launched a Tel Aviv innovation centre, shortly after partnering with Israel's Innovation Authority (IIA) on the China–Israel Changzhou innovation-park initiative, set up to promote joint tech ventures.

While China is interested in Israeli technology, Israeli companies and administrations are also contracting Chinese tech companies for several projects. Chinese security systems and cameras from Hikvision and Nuctech are used by the Israeli administration and along the Israel–Palestine borders. Huawei partners with Israel-based Zing Energy to install inverters in solar farms. It seems, however, that there is more demand for Israeli technologies from China than the other way around.

Assessing the risk of Sino-Israeli technology cooperation

While cooperating with China on technologies brings opportunities, it also comes with increasing challenges for Israel. The Israeli Ministry of Defense, more attuned to US concerns, has been monitoring and raising concerns about China's activities since the early 2000s, long before the issue reached the level of public debate in Israel. The Ministry of Defense's emphasis on the relationship with the US means that Israel's technology interactions with China remain heavily subject to the influence of the US. However, China's emergence as a global power, including in the field of technology, makes it impossible for Israel to completely ignore China. The multiplication of channels of technology transfer to China complicates Israel's ability to control those transfers and guarantee their non-military use. Israel's business community and part of the political leadership want to preserve their relations with China despite the warnings from the US and the defence establishment.

The risk associated with partnering with Chinese companies or including Chinese technologies in the country's network involves several elements. First is the risk of transferring, voluntarily or not, strategic or sensitive technologies to China that, in the long run, could provide China with a technology edge. Most major Chinese companies have ties with the Chinese government, formal or informal, and are expected to cooperate with the government when requested, including by handing over their users' data hosted on their servers. Huawei Technologies and ZTE Corporation have come under significant scrutiny in the US for their opaque connections to the Chinese government and military, and many executives from companies like Tencent, Xiaomi and Lenovo have served as delegates to the National People's Congress (NPC). This is combined with Chinese companies' weak record on IP rights enforcement.

As a result, Chinese investments in Israeli technology companies or the Chinese purchase of Israeli technologies could facilitate the transfer or theft of strategic sensitive technology. From a commercial perspective this could, in the long term, lead to Israel losing its technology edge to China. From a security perspective, this could lead to an increase in China's military edge, and the potential transfer of American technologies to China

via Israel. While Israel severed its defence relationship with China in the early 2000s, many technologies such as semi conductor chips, AI, satellite communications and others can have a dual civilian–military use, and the limit of what has a solely military use is becoming increasingly blurred.

The controversial Chinese telecom giant Huawei, while not involved in the development of Israel’s telecom networks, has still been active in the country. Since the late 2000s, Huawei has been developing technologies, some potentially sensitive, through a locally registered company called Toga Networks Ltd. At Toga, Israeli engineers – many of them having previously served at Israel’s elite technology army units – are developing a range of software and equipment, including tools that can help telecommunication providers examine data moving through their routers. It was recently reported that Huawei opened a representative office in Israel to sell equipment and maintenance services to companies that build solar-power facilities. According to several reports, this could allow Chinese access to data about the Israeli electricity sector. Huawei also acquired the Israeli cloud-security firm HexaTier in 2016, and invested in cloud-storage company Elastifile. According to Reuters, ‘Huawei will use HexaTier to set up a research and development center in Israel for databases in the cloud’.⁹³

Another risk of contracting Chinese vendors to develop the country’s digital infrastructure is the potential exploitation of certain security vulnerabilities for cyber espionage and surveillance purposes. According to the US National Counterintelligence and Security Center (NCSC), China, along with Russia and Iran, is the most active foreign power engaged in the illegal acquisition of US technology. Several of the Chinese technology companies investing in Israel, such as Tencent, Alibaba, Baidu and Xiaomi, have received attention due to perceived security vulnerabilities in their products. There is no evidence so far to determine whether these vulnerabilities are the result of voluntary practices to enable government surveillance. Chinese security risks are also a concern due to China being a close partner of Iran, one of Israel’s main rivals in the region. By partnering with China, Israel could face the risk of some of its technologies or data being transferred to Iran via China.

Those risks not only pose a threat to Israel’s national interests, but also to its close ally, the US, which sees the transfer of US defence-related technologies to China via Israel as a key security concern. In 2014, there were reports that Chinese hackers had stolen the data of Israel’s missile-interception system known as *Iron Dome*. The hackers also targeted three major defence-industry companies, Elisra Group, Israel Aerospace Industries and Rafael Advanced Defense Systems, stealing ‘intellectual property pertaining to Arrow III missiles, Unmanned Aerial Vehicles (UAVs), ballistic rockets and other technical documents in the same field of study’.⁹⁴ These attacks were a major concern in the US.

Balancing security risks with economic and strategic opportunities

In light of security concerns regarding Chinese involvement in Israeli technologies, the Shin Bet is believed to have unofficially imposed restrictions on the use of Chinese technologies for the development of national communication infrastructure as early as 2006 or 2007.⁹⁵ In contrast with most countries in the Middle East, Chinese technology has not been used previously for Israeli digital infrastructures such as 4G and 3G, and a partnership with Huawei on 5G appears very unlikely. In August 2020, Israel was reportedly close to joining the US Clean Network Initiative, therefore renouncing the use of Chinese technology in its 5G networks. In February 2020, the Israeli Cyber Directorate issued a directive, under the initiative of the Shin Bet and following important US pressures, to bar all Chinese-made systems and components in communications and security systems used in sensitive infrastructure.

For technology related to the defence sector or characterised as dual-use, the regulation has been strongly tightened following the *Harpy* incident in 2005. Foreign purchases of military, defence and dual-use technologies are regulated by the Israeli defence Export Controls Agency. However, Israel’s defence companies are regularly lobbying the government to ease those regulations as they face increasing difficulties in selling their equipment to the Ministry of Defense. According to reports, Israeli officials, particularly in the Prime Minister’s office and the Foreign Ministry, have been seeking to open a debate about how to ease those restrictions.⁹⁶

Those efforts have so far been met with strong opposition from the Defense Ministry which seeks to avoid harming the relationship with the US. Having entered its third ten-year military-aid MOU with the US in 2016, which consists of US\$33bn in Foreign Military Financing grants and US\$5bn in missile-defence appropriations, the Israeli Ministry of Defense remains the main stumbling block to closer technology cooperation between Israel and China. According to some critics, it even takes a harsher line on China than Washington itself, forbidding security-technology exports that are permitted by the US.⁹⁷

Despite those strict regulations, the dual-use nature of many advanced technologies makes it increasingly difficult to draw a clear line between the technologies that fall under this regulation and those that do not, and the exports of and foreign investment in Israeli civilian technologies lack scrutiny. Israel does not have a coherent mechanism to assess the political or security implications of transactions in the high-tech sector. Pressures from the US and from the head of Shin Bet led the Israeli government to adopt a screening mechanism for foreign investments made in the country in October 2019. This mechanism, however, does not cover the high-tech sector, especially emerging technologies such as biotechnology, AI, machine learning and data analytics, which constitute a major part of Chinese investments in Israel today. According to some reports, the mechanism also lacks real leverage, and the Israeli government has been struggling to find a balance between pressures from the US and Israeli defence establishment on the one hand, and on the other the business community which seeks to avoid any extra procedures complicating the conclusion of deals with Chinese companies. Although awareness has been rising within the Israeli government, scrutiny remains weak. For example, Chinese surveillance cameras provided by Hikvision and Nuctech are still installed in many Israeli government and police buildings, according to some sources.⁹⁸ According to a cyber and strategy expert at the Israeli Institute for National Security Studies (INSS), 'Washington is furious at the lack of safeguards in Israel against Chinese cyber activities'.⁹⁹

Awareness about the potential risks of Chinese involvement has been slow to develop among the Israeli political and business elite. For economic elites,

the opportunities presented by the Chinese market outweigh the potential security risks, and they see American pressures as just another commercial competition between China and the US. Business leaders have lobbied against stronger monitoring of Chinese investments, which would add to already existing bureaucratic burdens. In the opinion of much of the political elite, China appears as an emerging global player that they do not want to antagonise completely, although the relationship with the US remains a priority. Therefore, most concerns for Israeli economic and political elites seem to revolve around avoiding US pressure or sanctions, rather than around a clearly defined threat to Israel's national interests. While some of them are scaling back their cooperation with China due to fears of threatening their relationship with the US, others are likely to exploit the loopholes in Israeli regulations to continue doing business with China under the radar.

Nuancing China's influence in Israel

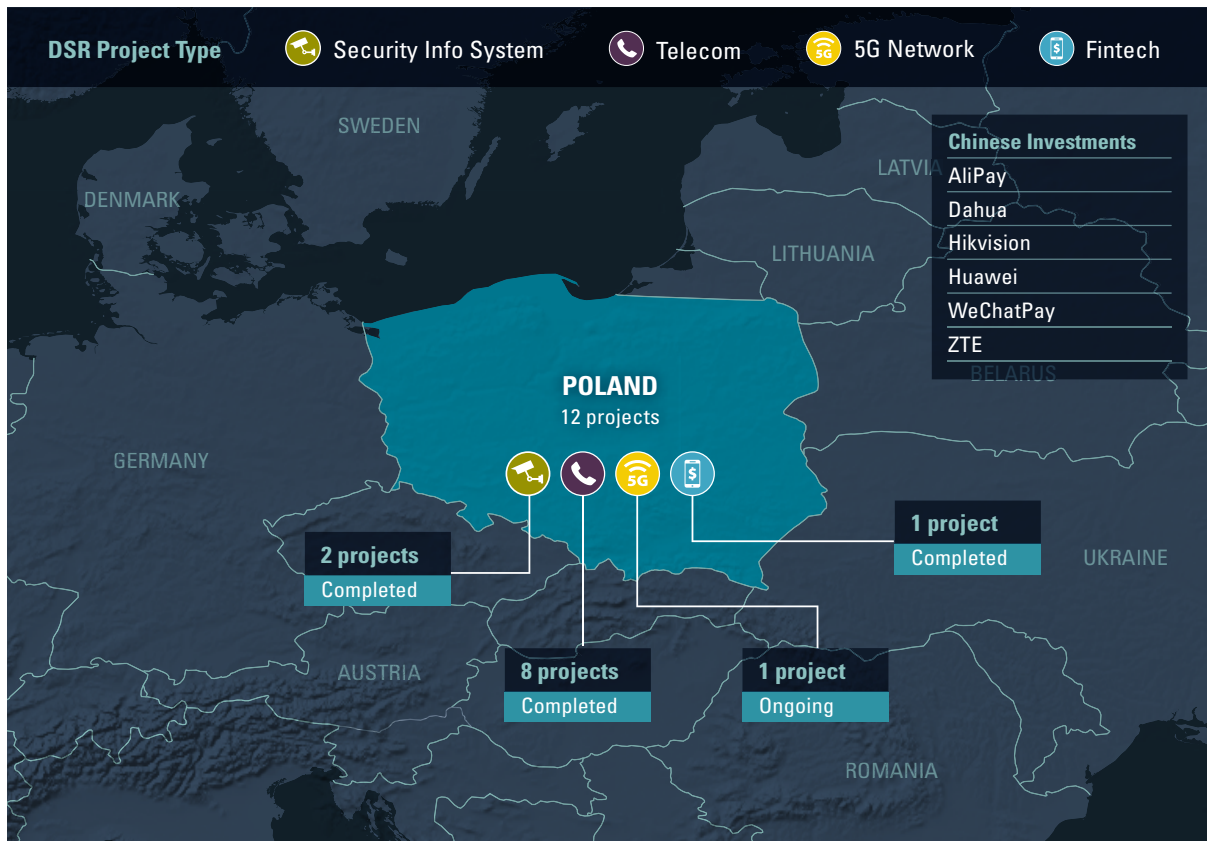
Growing Chinese investment in the Israeli tech sector has come under important scrutiny over recent years. Concerns about heightened surveillance risks or possible transfers of sensitive technologies have raised red flags among the Israeli defence establishment and have put the US-Israel relationship under mounting pressure. While those risks should be better monitored and assessed, China is still far from becoming a substantial competitor to the US in Israel. As stated by a report by IVC, 'in recent years China has become a more significant player in Israel's technology sector, but it remains a relatively minor player'.¹⁰⁰

American investments in Israel's tech sector largely outsize those made by China. US venture-capital investors alone accounted for 35% of all investors in Israeli tech in 2018. Today, most research and development centres in Israel are still operated by Western multinational companies such as Apple, Google, Intel, Microsoft, HP, IBM and eBay, and some of them have been present in the country for more than three decades. For Israeli tech companies, it is far more prestigious to cooperate with American or European companies than with the Chinese. Moreover, some Israeli companies have come to realise that cooperation with Chinese companies and access to the Chinese market were more difficult

than initially expected. China's record of weak IP rights enforcement and security vulnerabilities are starting to raise red flags. As tensions between the US and China are mounting, many Israeli companies do not want to threaten their cooperation with the US, and several reports suggest that even companies that export products that are not dual-use prefer not to export to China out of fear of harming their sales in the US.¹⁰¹

Politically, the relations between Israel and China have remained limited. China's good relations with Iran make it difficult for Israel to envisage a deeper strategic relationship with China. China is also a traditional supporter of the Palestinian cause. Therefore, while Israel has been keen to diversify its partnerships, the US remains its main ally and it will not take the risk to threaten this relationship.

2.5 Poland



Map 5: Chinese digital investments in Poland, IISS China Connects, 2020

There are numerous Chinese technology companies currently active in Poland, including several – Dahua, Hikvision, Huawei, ZTE – that are on the US Entity List of proscribed companies. But while the key foreign-policy driver for Poland, apart from its often fraught EU membership, remains keeping the US relationship strong as a counter to Russia, Polish monitoring and regulation of Chinese DSR companies is modest and uneven. Private and local-government contracts with Chinese

technology companies are common and lightly regulated, with the exception of Huawei. However, Huawei is deeply embedded in Polish networks, has cultivated support among both the public – Polish football legend Robert Lewandowski has been Huawei's spokesman since 2015 – and government agencies, and has been the object of intense focus by the United States. At numerous levels, Polish opinion has turned against Huawei, with Prime Minister Mateusz Morawiecki urging Europeans

in July 2020 to stand with the US against the company. However, Poland's policies towards the DSR are a work in progress and will remain one as the EU refines its own approach to 'digital sovereignty' and the US under a Biden presidency develops its own post-Trump approach to Chinese 'techno-authoritarianism'.¹⁰²

Huawei at centre stage

Awareness of the DSR in Poland has centred on Huawei, which played an important role in building Poland's mobile-Internet infrastructure and hopes to participate in 5G and later buildouts. Huawei came to Poland in 2004 and made Warsaw its Central and Eastern Europe (CEE) regional hub in 2008. By 2019, the company said it had over 900 employees in Poland and had invested more than US\$1.3bn. Huawei's state-owned rival, ZTE, helped build Poland's fibre-optic national backbone network beginning in 2001 and continues to participate in the Polish market. However, most of the focus has been on Huawei.

In Poland as elsewhere, Huawei did not limit itself to technology projects. For example, beginning in 2014 it sponsored prize programmes for tech students at as many as a dozen Polish universities, the prize being a week of workshops at Huawei headquarters in Shenzhen, a second week to visit Beijing and a complimentary smartphone.¹⁰³ As recently as June 2020, Huawei signed a partnership agreement with a major Polish university.¹⁰⁴ China also has six Confucius Institutes in Polish universities.¹⁰⁵

Although Polish military and intelligence services were aware of the potential dangers of having Poland's telecommunications networks built and maintained by Chinese companies, whether private or state-owned, there was also cooperation with Huawei through 2018. The Military-Technical Academy, for example, is the research and education arm of the Polish Ministry of National Defence, and its faculty of cybernetics is charged with cryptology and 'counteracting threats in cyberspace'.¹⁰⁶ In 2014, two academy students were among the first group of ten Polish students to win the two-week trip to China and Huawei headquarters. The students' projects were judged by military-academy faculty; one of the winning entries was on the integration of ICT tools and platforms into combat operations. The following year, Huawei representatives met with officers and professors at the academy to discuss

deepening cooperation, particularly on mobile technologies and the possibilities for military students' further participation in the Huawei competition. The Huawei competitions were under the patronage of Naukowa i Akademicka Sieć Komputerowa (NASK), a government agency that has broad responsibility for ensuring the security of Poland's telecommunications networks, including the management of threat-response teams as well as maintenance of a domain-name system.

In January 2019, Polish national Piotr Durbajlo was arrested for espionage, along with Weijing 'Slawomir' Wang, a Huawei employee and former Chinese government official.¹⁰⁷ Wang and Durbajlo had known each other at least since a 2013 visit by Polish government officials to Huawei's headquarters in Shenzhen, and the two men later vacationed together in China. Durbajlo had been an officer of the Internal Security Agency (ABW), Poland's domestic-intelligence agency, since 2009.¹⁰⁸ He worked on telecommunications and cyber security, including a project on encryption of official communications.¹⁰⁹ The ABW assigned Durbajlo to work with Poland's telecoms regulatory agency in May 2012. That was also the year Durbajlo began work at the Military-Technical Academy on a project concerning protection of fibre-optic networks from intrusions aimed at collecting classified material. The project ran to 2015, when Wang and Durbajlo accompanied another delegation from Poland to China.¹¹⁰ Durbajlo was also a senior adviser to the Office of Electronic Communications (UKE), which regulates various aspects of telecommunications, including use of radio frequencies by wireless providers like Huawei. He left government service and in 2017 joined Orange, the French telecommunications company, which has a large share of the Polish market. The investigation of Durbajlo dates from around that time.^{111 112}

The Wang and Durbajlo arrests were a blow to the reputations of Poland's security services and of Huawei. They also reflected the almost unique political exposure of Huawei — and its policy of establishing ties, by many different means, with various levels of government in its markets. The development of Polish policies on vetting of DSR companies was quickened by the arrests as well as by concurrent policy reviews in the EU and intensified US focus on excluding Huawei from allied-country networks.

The Chinese presence

ZTE, which unlike Huawei is directly controlled by the Chinese government, keeps a much lower profile as a rule, including in Poland. The same is true of other Chinese technology companies active in Poland, including some under forms of Chinese government ownership or on the US proscribed Entity List. The main Chinese technology companies in Poland apart from Huawei and ZTE are Hikvision, Dahua, TCL, Aliexpress and Nuctech.

Dahua is a large private Chinese company specialising in security and surveillance systems, whether in the relatively benign forms of traffic monitoring and smart-city infrastructure or in the less attractive form of state surveillance aimed at the repression of dissent and other forms of political control. Hikvision is effectively a state-controlled company, specialising in similar technologies to Dahua including facial recognition. Both companies have followed the familiar path of developing their products in the protected, but internally competitive, Chinese market then expanding abroad. Both are tightly linked to the Chinese state and are on the US Entity List, chiefly for their involvement in Chinese state surveillance in the province of Xinjiang. They operate through Polish subsidiaries without Polish ownership. They have become chosen suppliers for private and public Polish security providers, and have corporate strategies aimed at integrating surveillance technology with 5G platforms and IoT networks.

TCL is best known as a manufacturer of television displays, including at a facility in Poland. TCL is a global player in smart TVs, which are integrated with the internet; it also has a content arm. It is partly government-owned and has the People's Liberation Army (PLA) as a client through its shareholding interest in Tianjin 712 Communication and Broadcasting. TCL is a major actor in China's effort to gain independence from US suppliers in semiconductor manufacture, in part through its purchase of Tianjin Zhonghuan, and has adopted a strategy of integrating its products with 5G networks and the IoT. It has been hiring in Poland for a new artificial-intelligence laboratory.

Nuctech is a government-controlled airport-security company whose capabilities include facial recognition and big-data analysis. It has had a sizeable operation since 2005 at its Polish subsidiary. It has long-established

relationships with Chinese security agencies concerned with border control. Aliexpress is an e-commerce arm of privately owned Alibaba. It enables small businesses and individuals in China to reach buyers abroad, whether middlemen or consumers. In 2019 it was the 15th-most popular app in Poland. Through a deal between Polish Post and China Post in 2017, Aliexpress became able to sell Chinese goods to Polish consumers with the benefit of tax leniency, favourable postal rates (Chinese outgoing postage for parcels is set at a very low developing-economy rate) and local subsidies to small businesses. Aliexpress is integrated in Poland, as in much of Europe, with Alibaba's smart-logistics arm Cainiao. Alibaba's 2015 joint venture with Norinco, China's leading, state-owned defence contractor, has in turn been devoted to integrating global smart logistics with the BeiDou satellite navigation system, the Chinese military's GPS alternative. Polish transport and logistics companies have expressed some interest in using BeiDou; it is likely this will be done for them, as Alibaba and its subsidiaries and partners integrate their networks with BeiDou. The Alibaba/Norinco venture, Qianxun, is already the leading low-speed autonomous vehicle (AV) positioning system in China, aimed at coordinating AV commercial transport networks.

All these companies are part of China's approach to the fourth industrial revolution: building an integrated digital network for the observation and movement of goods, people and money, with as little friction as possible and therefore a minimum amount of energy consumed — in that sense, it is a 'green' policy. However, with the exception of Huawei, Chinese technology companies in Poland, even those with Chinese government ownership and close military ties, receive minimal attention outside specialist circles.

The China price

The overarching narrative of China's Belt and Road Initiative in Poland has been one of initial enthusiasm, followed by high expectations and much bilateral and multilateral foregathering, followed by disappointment. This has been alongside surging political effort, differently led by the US and the EU, at separating Poland, and indeed the entire CEE region, from China. The main battlefield turned out to be communications technology.

China made the first moves. Huawei and ZTE built internet infrastructure in Poland and the region from the mid-2000s. Chinese diplomacy followed on with the '16 + 1' initiative for CEE countries, begun in 2011. This was a multilateral experiment in regional organisation sponsored by a foreign power, and the first regional summit was held in Warsaw in 2012. The most active participants, with the status of Chinese 'strategic partners', were Hungary, Poland, Serbia and the Czech Republic. The region, with a combined population of over 100 million, has enjoyed strong growth, relative to the core EU economies, since 2012 — based not least on EU 'cohesion' transfers, which have amounted to more than 50% of public investment in large economies like Poland's and Hungary's — and frequent political distancing from Brussels. That independent-mindedness could be seen as a vindication of China's CEE policy.

However, Chinese FDI has not been that large, and it has been concentrated in Hungary, followed by Poland, the Czech Republic and Slovakia. Much of the promised BRI heavy infrastructure was very slow to materialise and wariness developed quickly in Poland. An unsuccessful road project in 2012 got the relationship off to a poor start. By 2015, Poland had passed an anti-takeover regulation that included energy production and distribution, petroleum production, processing and distribution, and telecommunications among sectors where any foreign buyer would not be allowed to buy a 'significant share' of Polish enterprises. Investments were to be screened by both the ABW and Poland's Foreign Intelligence Agency (AW). This law was directed more against Russia than China. Nonetheless, it was part of a legislative and regulatory pattern with implications for China. Poland had observed the process of BRI investment in other small economies, and it did not want Chinese investment that only led to employment in Poland of Chinese nationals, nor did it want to fall into debt traps. By 2017, Polish minister Henryk Kowalczyk was saying

We want investments to be under Polish control — obviously in cooperation with China. We would like to avoid the situation in which projects ... are entirely financed by China. ... Infrastructure investments must be

carried out with caution, with the predominance of Polish capital. This applies not only to Chinese capital, but to every other. We believe that capital has nationality. It would be unreasonable at this point to 'let' investors enter into the infrastructure projects, giving them all the funding possibilities.¹¹³

In line with the disappointing flow of Chinese value-creating investments, Polish enthusiasm for the 16+1 grouping — 17 + 1 with the addition of Greece in April 2019 — declined. At the same time, Poland needed investment. At one point China seemed to provide Poland and the CEE region with leverage in their negotiations with the EU and major European states, particularly Germany and France, and a similar role could be envisaged regarding the US after the 2016 presidential election, as President Trump's administration refocused US foreign policy with China as the principal strategic competitor and Russia as a distant second. The US had long been Poland's principal strategic partner after the EU, and Polish strategic culture regards the US as the most effective guarantor of its own security against Russia. This goes a long way to explain why Huawei went from being a valued partner in Poland in 2012–17 to an embattled one beginning in 2018.

The American turn

The pivot from China to the US might be dated from a summit meeting in Dubrovnik on 28 August 2016, as Poland, under a new government, settled into Euroscepticism and a heightening of its already considerable enthusiasm for US ties. The Three Seas Initiative (3SI), derived from a Polish diplomatic concept (*intermarium*) from the interwar years, was launched with the assistance of both US General James Jones and China's Liu Haixing. Gen. Jones and the Atlantic Council, mainly with Polish partners, had brought out a report in 2014 on North-South integration of the region between the Baltic, Adriatic and Black seas — the 'Three Seas'. The report's main concern was energy, directed not least at reducing dependence on Russian supplies, but it also focused on transport and digital connectedness. The report said very little about China, and Jones's presence alongside the Poles signalled both

US interest in strengthening CEE and the CEE interest, especially in Poland, in keeping the US in the region. Central European coverage portrayed it as a means for regional unity and a way to pressure the European Union. Liu nonetheless gamely connected the 3SI to the broader BRI.

It was not to be. The next meeting of the 3SI was in Warsaw and was addressed by President Trump in July 2017, on his second European visit. China was put to one side. Trump did not mention the digital aspect of 3SI, instead stressing energy supplies 'so Poland and its neighbors are never again held hostage to a single supplier of energy', that is, Russia.¹¹⁴ (Poland had recently received its first shipment of American liquefied natural gas.) Trump's other main interest was military contracts: in March 2018, Poland signed the largest military procurement deal in its history, spending US\$4.75bn on Raytheon's *Patriot* missile system. In January 2020, Poland agreed to buy 32 of Lockheed's F-35A jets for US\$4.6bn. These would join its existing fleet of 48 F-16 fighters and replace Soviet-era Sukhoi planes. This was the first F-35 sale in the CEE.

The digital side of 3SI was revived in 2018, partly through a group of think tanks led by Krakow's Kosciuszko Institute and supported by the Polish government as well as Google and Microsoft, which are the dominant US tech multinationals in the Polish market. The idea of a unified digital CEE network in line with US digital policy was now explicit. The 3SI was being distanced from the DSR and being brought into line with both the US National Cyber Strategy and the EU Network and Information Systems (NIS) directive of 2016 and subsequent legislation. The CEE was becoming a digital battleground. The Digital Three Seas Initiative complemented American diplomatic efforts to convince CEE states to reject Chinese technology. By August 2019, the Romanian and US presidents were agreeing to 'seek to avoid the security risks that accompany Chinese investment in 5G telecommunications networks'.¹¹⁵ Similar agreements with the US soon followed in Poland and over the next year with Estonia, Latvia, Lithuania, Slovenia, Slovakia, Bulgaria and North Macedonia.

Poland's security services, particularly after the spy arrests in January 2019, seemed to have come a considerable distance since the last free trips to Huawei

headquarters by cyber-oriented military cadets in 2018. On a visit to Washington in December 2019, Poland's minister-coordinator for security services, Mariusz Kaminski, described dependence on Chinese networks for 5G as 'a monstrous risk, a monstrous irresponsibility'.¹¹⁶

A strategic-autonomy synthesis?

The EU, particularly with former German defence secretary Ursula von der Leyen as Commission president, has embraced a doctrine of strategic autonomy. While this move was security-driven it has become as much or more about technology. Europe's multiple efforts at establishing its own viable tech companies and platforms, protecting its citizens' privacy and securing its own networks grew up in opposition to US tech dominance but are growing to maturity in opposition to China as well. European strategic autonomy and digital sovereignty have become jumbled together.

Poland participated, like Estonia and others, in the design of the EU 'toolbox' and related regulatory and legislative efforts aimed at maximisation of European autonomy in technological innovation and the establishment of platforms in cloud computing and other technologies that might shape the fourth industrial revolution to serve European interests. Not surprisingly, given the size of their economies, Huawei chose to single out Poland and Romania in a letter sent to EU Commission Executive Vice President Margrethe Vestager, complaining that those countries' US-inspired agreements to, in effect, block Chinese technology companies from their territory violated EU laws designed to keep digital-platform decisions at some distance from political considerations, like assessing state control of foreign tech investors or forbidding foreign investors who were tied to human-rights violations by their home countries, for example in Xinjiang, Tibet or Hong Kong. But China is going against a strong trend, even after the completion of negotiations at the end of 2020 on a China-EU Comprehensive Agreement on Investments. The relevant language in Poland's draft law of 8 September 2020 might be watered down but it probably won't go away.

Whether keeping both Chinese and US tech companies at a guarded distance will benefit European innovation is a central question. Poland and the CEE states

face, on a smaller scale, the same challenge that major Western European states face of generating internal innovation that can compete with that of Chinese and American, as well as Korean and Japanese, tech multinationals. It is not an easy challenge to meet. In the short term, the weaponisation of the tech question would seem simply to favour companies domiciled in strategically allied states, like Google, Microsoft and Amazon (in the shape of Amazon Web Services, a major cloud-computing and data-centre player but one that is not yet present at scale in the Polish market), along with Samsung, NTT, and the Nordic duopoly of Nokia and Ericsson. It is unclear how much room there is for smaller players, or how much strategic autonomy or digital sovereignty can be built on a handful of American, Korean, Japanese and Nordic multinationals.

Within the 5G sector, there is growing enthusiasm in Poland, as there is in the United States and Japan, for Open Radio Area Networks (ORAN) as a type of technological shortcut around the problem of having just a few providers (Nokia, Ericsson, Huawei, ZTE, Samsung, perhaps Reliance Jio) capable of building vertically integrated hardware–software 5G networks based on current technology. ORAN seeks to disaggregate 5G platforms, minimising the role of hardware and maximising that of software systems that could create 5G and 6G ecologies that would enable multiple vendors at different points in the system. However, the market for ORAN remains somewhat notional, and telecoms vendors prefer to work with what is proven, which is the principal reason why vendors in Poland as elsewhere have resisted the move away from Huawei and ZTE. What's more, ORAN could have the effect of vitiating the current business models of Nokia and Ericsson, thus undercutting the European champions themselves.

Meanwhile the problem of indigenous innovation remains. Polish attempts to reform the process of monetising academic innovation – in essence, imitating the structure initiated at Stanford in the 1960s that allowed faculty to retain their posts while starting tech companies and benefiting directly from their growth – have stalled: Polish academic institutions insist on controlling such monetisation, which means that the cycle of innovation and monetisation stays at a low level. The general European trend is towards greater protection

of existing European companies, suggesting continued dampening of the local innovation that is nonetheless the ultimate goal.

Conclusion

From the perspective of defence contractors, the hold of US companies on Polish acquisitions remains very strong, with the bias of Polish buyers being towards American suppliers. The Biden administration shows every sign of continuing the policies that support this bias, and indeed hardening the US line against Russia, Poland's chief concern. The Biden campaign also stressed its preference for a league of techno-democracies to oppose techno-authoritarians, a global policy aimed squarely at China.¹¹⁷ This all fits neatly with Polish policy towards China's DSR and Polish foreign policy more generally.

There remains some question about the security of Polish networks. While the government security services appear to have turned a corner, provincial and city governments, and some other government agencies, remain engaged with Chinese tech firms like Hikvision and Dahua. According to former Polish government officials and Polish researchers, the degree of national-government awareness of and influence over such connections is not extensive. Private Polish companies as well, from security to transport and logistics, are working with Chinese technologies from companies like Aliexpress and Nuctech. Polish telecoms vendors are slow-walking the transition away from Huawei and ZTE, delaying the additional costs that will come with changing equipment suppliers. The strategic calculations may work out but the economic ones don't yet, and ultimately it was economics that allowed Chinese tech companies, subsidised and often directly controlled by the Chinese government, to lay networks across much of the world in the first place. The opposition to this process has been mostly strategic and, particularly in Europe, ethical. In Poland as elsewhere, the deepest need is for a local tech ecosystem capable of growing and sustaining companies – that is the real source of tech resilience. If it is not achieved, then Poland will be an observer at the fourth industrial revolution, its networks will be insecure, and China, pushed out through the strategic door, will be most likely to re-enter through the economic one.

3. Key findings and potential implications for Western defence industries and government

The preceding section considered in detail the level of integration of Chinese technology in five case-study countries, as well as the decision-making processes by government when considering further integration of new Chinese technology projects. It also considered whether this has had implications for the country's security and defence, and follow-on impacts on defence cooperation with Western defence industries and militaries. Lastly, the case studies also considered whether the governments in question had attempted to implement risk-mitigation strategies, as well as whether Chinese companies had diversified their approaches to securing tech contracts in the face of perceived pushback. This section will seek to compare the five case studies, identifying common themes and lessons learned for defence industry where possible.

3.1 Reach of Chinese tech investments in countries and sectors

The case studies examined the top-level integration of Chinese tech investments into national ICT ecosystems of each of the five case studies according to the DSR categories outlined in this report as well as R&D-related programmes. However, understanding the integration of Chinese technologies into lower levels of the ICT supply chains, for example the source of copper cables or components, was not possible. As this report has argued, all national ecosystems include the integration of foreign ICT from a variety of countries, and for most countries, understanding the extent of Chinese technological integration in physical infrastructure, software provision, content production and service delivery will be a complex task that is well beyond the scope of this work.

In all case studies examined, however, Chinese technology companies had an established presence that

preceded the launch of China's DSR initiative. Indeed, in all cases but the UAE, companies like Huawei based their current and future business on their long-standing investment history. Huawei's relationship with Indonesia dates back over two decades, while Huawei has located its CEE headquarters in Warsaw. These long-standing relationships allow Chinese companies to build on previous investments in order to continue to do business. For example, in the UAE Huawei marketed its 5G network roll-out as a follow-on project to previous projects in which Huawei rolled out pre-5G networks.

In all five case studies, Chinese companies also all invested in a variety of project types. 5G was thus part of a larger context of investment into a national ICT ecosystem, both in the private and public realms. This is a reflection of the diversity in projects undertaken as part of the DSR initiative, but also a reflection of the strength of domestic Chinese companies across a range of sectors and ICT technologies. As China's domestic market becomes increasingly competitive and saturated for Chinese technology companies, it is unsurprising that these companies would seek market opportunities abroad. The case studies represent developing and developed economies alike, but all five are attractive markets for Chinese companies looking for new opportunities. Indonesia is the fourth-most populous country in the world, with a young and increasingly urbanised population, while South Korea is at the heart of the fourth industrial revolution. Internet and mobile-phone usage in Indonesia is extensive, as is the case in South Korea, the UAE, Israel and Poland. However, Indonesia's example stands out as offering the most opportunity for Chinese companies in hard-infrastructure projects. This is particularly the case in the government's assessment that there are 'two Indonesias' – one that is digitally connected and one

that lacks digital connectivity. Hard-infrastructure projects, aside from undersea cables and 5G networks, are less prevalent in the other four case studies.

For South Korea, the UAE and Israel, engagement with Chinese tech companies includes both incoming Chinese investment into tech projects and collaboration between Chinese and local tech companies, governments and academic institutions. In the former, Chinese companies have particularly invested in local start-up industries. In Indonesia and Israel, Chinese venture capital increasingly makes its way into indigenous e-commerce, fintech and AI-related start-ups. In the UAE and Indonesia, Chinese tech companies have partnered in particular with local academic institutions or government agencies to build local human capital – either through establishing training centres led by Chinese companies, or by providing educational exchanges with companies and universities in China.

The majority of projects revolved around what China and Chinese companies could offer the recipient market economies and governments. However, not all case studies followed this one-way pattern of engagement. Poland, South Korea and Israel were each to a certain extent as much sources of technology, innovation and talent as they were markets for Chinese companies. In particular, Israel (a start-up nation) represented an opportunity to transfer innovative ideas from a country with close civil–military cooperation to China through investment in start-ups. This finding was made more interesting when noting the absence of Chinese telecommunications networks in the country, which in recent years has garnered the most attention in terms of intelligence risks. This would support the idea that Chinese investment in telecommunications networks should only be considered as part of a larger context of investment. Secondly, the case of South Korea highlighted the two-way trade flow of technology between tech companies. Chinese companies import South Korean semiconductor chips while exporting telecommunications-network technology and apps to the Korean market. Lastly, in Poland, technological scholarships were not just a means by which Chinese companies offered to build up local talent, but also highlighted their use to bring cyber- and tech-related talents to China.

3.2 Government debate, hedging and factors in decision-making

All case studies have at some level found themselves caught in the middle of the United States’ and China’s technological competition. All cases noted an increased effort on the part of the US government to influence national decision-making to ban Chinese technologies in 5G and other network roll-outs, and to a certain extent to also ban other Chinese tech investments. However, not all governments took heed of US warnings that the failure to restrict or ban Chinese technologies in national ecosystems would have dire consequences for bilateral relationships. While Indonesia was initially concerned about the consequences of accepting Chinese investments in the country for its bilateral relationship with the US, the government has deemed that the need for connectivity is more important. The government also noted that security risks exist with any telecommunications provider or technology company, and security risks are thus not limited to just Huawei. Ultimately, parliamentary discussions on the topic of the country’s national reliance on Chinese ICT were also absent.

While national debates in all case studies featured clear disagreement between government security interests and the private sector’s commercial interests, in the case of South Korea the parliament played a role in bringing security concerns to the fore of national debates. It did so by questioning the Ministry of National Defense about the presence of Huawei chips in 48,000 AI smart speakers across ROK military facilities.

Hedging between the US and China can particularly be seen in the cases of the UAE and South Korea – countries that particularly depend on US military technology and security guarantees but also have significant commercial interests in maintaining access to the Chinese market. In the case of South Korea, this meant restricting the integration of Chinese network technology and components to networks not used by the USFK or Korean defence forces. Networks that included Chinese components or technology would also not be used in proximity to US bases. In the case of the UAE, the government in private discussions acknowledged its concern for striking a balance between maintaining economic ties with Beijing and the UAE’s long-term strategic interest. While China is not considered a security

threat to the UAE, Emirati officials changed their perspectives from pure commercial interest to taking into account the possible consequences for the security relationship with the US.

Wider contexts of regional and international politics were also taken into account by governments when deciding whether to restrict Chinese tech investments into their markets. In the UAE's case, the disengagement of the US in the Middle East under the Trump administration meant that the GCC was careful not to create dependencies on the US. Furthermore, the UAE case study also noted the importance of maintaining national competitiveness as the UAE sought the quickest and most affordable roll-out of 5G networks in order to out-innovate its GCC neighbours.

In Israel's case study, government decision-making showed a tendency to favour security concerns and the maintenance of good relations with the US, its main security guarantor. While the private sector was eager to accept Chinese investment and export to China, the clear prioritisation of defence interests over commercial interests was noteworthy in this case study. This stands in stark contrast to the case of Indonesia, where commercial and development interests were prioritised.

3.3 Defence exports, defence integration and intelligence-sharing challenges

Countries with the deepest defence cooperation and alliance ties with the US considered the prioritisation of defence over commercial concern most strongly. In the case studies of Israel, Poland and South Korea, the governments were most concerned about maintaining military cooperation with the US as their primary security guarantor. However, this factor did not elicit the same responses from each government. Indeed, governments took different decisions to be able to either wholly comply with US demands for restricting Chinese tech investments, or partly address US concerns.

Israel's case presents the former scenario, whereby US security concerns were internalised into the government's own security considerations. However, in the case of South Korea, the government was able to make adjustments to national critical infrastructure to satisfy both domestic-commercial and US-security interests. By blocking off the communications channels used by the

USFK and the Korean military, Korean telecommunications companies were able to continue incorporating Chinese tech into their national networks and ecosystems. In Poland, defence arrangements with the US took priority over other national factors. The continued threat to national security presented by Russia further supported the Polish government's prioritisation of its alliance with the US. While the Polish government had already started shifting its opinion of Chinese investment due to lacklustre results of the 17+1 cooperation group, recent large procurement deals for US missiles and fighter aircraft coincided with the government's more vocal criticism of the security risks of Chinese technology.

In the case of Indonesia and the UAE, the link between procurement of US defence technology and the potential security risks posed by Chinese technology investments was not explicitly mentioned as part of public debates. In Indonesia's case study, concerns over cyber vulnerabilities, attacks and information security were acknowledged in general terms when debating the country's ability to share intelligence and sensitive information safely. However, these concerns were framed within greater threats posed by terrorist, criminal or subversive digital activities in cyberspace. The connection to Chinese actors did not feature specifically in these discussions.

In Israel and Poland, however, the link between threats posed by Chinese actors in cyberspace and through Chinese tech investments was clearer. This primarily was reported to be the result of past experience of IP theft and espionage, rather than the result of pressure from the US government. Chinese hackers have reportedly in the past stolen data on Israel's missile systems, while in Poland espionage cases involving Huawei employees have played a role in central-government decision-making.

It should be noted that despite the varying levels of integration of Chinese ICT technology in each of the national ICT ecosystems, the US did not act on threats to national-security cooperation, as far as is known in public open-source research. Furthermore, despite concerns about the impact of DSR activity on arms exports, in none of the case-study countries did the level of Chinese technology integration reach such a high level that the US even considered a change in arms exports to that country.

3.4 Change in strategy by Chinese companies to invest

In all case studies, Chinese companies have been flexible enough to adapt to periods of government push-back or public criticism in an effort to maintain bilateral commercial ties and continue in-country business. In some countries, companies like Huawei turned to philanthropic projects in order to maintain a positive image in the government's and the public's eyes. In South Korea and the UAE, Chinese companies funded and opened bilateral innovation labs in order to support local human capital and talent, and build people-to-people ties.

However, in some cases this was accompanied by relatively little fanfare, instead opting for low-profile launches without media presence. Such was the case for the launch of Huawei's OpenLab for next-generation 5G development in South Korea. In Poland, Chinese tech companies also opted to keep a low profile. ZTE, for example, was noted to skip the publicity that Huawei in the past had promoted.

In one case, Chinese companies shifted the sectors in which they invested following government restrictions. Chinese companies prior to the 2000s invested in defence-related companies and technologies; however, following restrictions by the Israeli government, Chinese companies shifted to civilian sectors thereafter. In the mid-2010s Chinese companies shifted focus again, this time towards Israel's start-up sector in particular.

3.5 Potential to mitigate risk?

Considering the importance of defence-industrial and political ties with the US for nearly all countries studied, it is striking that few governments took efforts to mitigate the potential risk of Chinese tech investments into their national digital ecosystems. Indeed, the only example in which a real compromise was made was in the ROK's case study, through the hiving off of a segment of their national communications networks specifically to secure communication with the US. However, the continued integration of Chinese components and technology in the wider South Korean digital ecosystem continues to be a point of contention between the US and South Korea.

Furthermore, even in cases where a central government took steps towards restricting Chinese technology in national digital infrastructure, this was at times undermined by limited knowledge and control over lower levels of government. This was particularly the case in Poland. Although the Polish government strongly supported the US Clean Network Initiative, provincial and city governments, as well as some other government agencies, remain engaged with Chinese tech firms like Hikvision and Dahua. The mismatch between awareness of and influence by central governments over the whole governmental system is thus not extensive. Furthermore, this does not even consider the degree to which private Polish companies also continue to work with Chinese technologies in areas such as security, transport and logistics.

Lastly, Indonesia has showed interest in promoting cyber-security standards, for example by drafting data-protection laws based on the EU's GDPR as a model or participating in voluntary vulnerability-disclosure programmes with the US NSA. While these laws and programmes aim to address cyber security, cyber crime, content causing civil unrest, and social disharmony, they might still address some of the data-security concerns potentially posed by Chinese companies.

Conclusion

The implications of China's global digital investments for US and Western defence industries is an understudied subject that deserves greater attention. The technological strategic competition between the US and China shows no signs of abating. Furthermore, China's global digital investments, despite US government rhetoric, continue to expand in technological and geographic scope. The intersection between technologies, alliance structures and defence cooperation will thus likely come increasingly to the fore.

This report has aimed to address this gap in current analysis by firstly outlining the potential risks posed by China's global digital and technological investments to defence industries. Secondly, the report analysed the extent of Chinese DSR activity in five case-study countries across Asia, the Middle East and Europe that are of high security and defence importance to the US: Indonesia, the Republic of Korea, Israel, the United Arab Emirates

and Poland. In doing so, the report aims to provide greater insight into government decision-making and lessons learned for Western defence industries.

Countries still hedging against the possibility of complete bifurcation of the global digital ecosystem

The US has argued that the integration of Chinese technology in national digital ecosystems will have significant consequences for national security and defence cooperation with the US, including defence-industrial cooperation. However, with the exception of Israel, this report found that in all case-study countries Chinese ICT investment was prevalent across almost all sectors of the national ICT ecosystems, from physical infrastructure to service provision and ‘over the top’ platforms. All case-study countries, it would seem, are to a certain extent still hedging against the possibility of a fully bifurcated global digital ecosystem.

The report found that although all five case-study countries were recipients of largely the same diversity and scale of Chinese technological investments, government responses to the campaign by the US to further restrict Chinese technologies in national ecosystems were diverse. Predictably, governments struggled to find a balance between commercial and security interests. Perhaps more surprising was the observation that even in countries where governments were dependent on the US as their only security guarantor, this struggle was no more decisive to prioritise security concerns. Also of note was the lack of governmental and public debate in some countries as part of decision-making processes around accepting Chinese tech investments.

Challenges for alliance intelligence and defence cooperation?

Despite the varied and, in some instances, deep integration of Chinese ICT investments into national ICT ecosystems, this did not seem to impact the defence and intelligence cooperation between the US and the countries studied. In some cases, the security relationship with the US played a stronger role in governmental

decision-making than in others. However, the decision to exclude or limit the integration of Chinese technology by any of the governments analysed was based purely on the hypothetical consequences of not doing so for defence and intelligence cooperation with the US and allies. It could be possible that evidence of this is classified and thus outside the scope of this paper, which is based on open-source intelligence research.

What level of integration should be considered significant?

This report has argued that it is difficult to examine in full the exact level of integration of Chinese ICT technologies throughout the national ICT ecosystems of each case-study country examined. Doing so is well beyond the remit of this report and requires further detailed examination. However, it is interesting to note that in all case studies, decisions made by national governments seemed to largely centre around discussions of Huawei 5G networks and other physical infrastructure. Debates also focused largely on whether to accept top-level Chinese physical infrastructure and did not, for example, seem to delve into debates around whether to rely on imports of copper wire from China, or whether to permit Chinese investment into local start-up industries. It would thus seem from this research that it is difficult for national-level governments to precisely determine what level of integration of Chinese ICT technologies should be considered significant.

Can security risks to companies doing business abroad be mitigated?

An important lesson learned for defence industries is that efforts by national governments to mitigate security risks were found lacking in the majority of cases studied. Furthermore, central-government decision-making appeared not to account for the reality of national investment landscapes at lower levels of government. Chinese tech companies in all case studies were also quick to adapt to new measures imposed by central governments that would otherwise restrict their business in-country.

Notes

- 1 'Vision and Actions on Jointly Building Silk Road Economic Belt and 21st Century Maritime Silk Road', National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce of the People's Republic of China, March 2015, <http://www.chinese-embassy.org.uk/eng/zywl/t1251719.htm>.
- 2 Yamei, 'Full text of President Xi's speech at opening of Belt and Road forum', Xinhuanet, 14 May 2017, http://www.xinhuanet.com/english/2017-05/14/c_136282982.htm.
- 3 "'Working Together to Deliver a Brighter Future for Belt and Road Cooperation": Keynote Speech by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second Belt and Road Forum For International Cooperation', Consulate-General of the People's Republic of China in Belfast, 26 April 2019, http://belfast.chineseconsulate.org/eng/zgxw_1/t1658424.htm.
- 4 Denghua Zhang and Jianwen Yin, 'China's Belt and Road Initiative, from the inside looking out', *The Interpreter*, 2 July 2019, <https://www.lowyinstitute.org/the-interpreter/china-s-belt-and-road-initiative-inside-looking-out>.
- 5 'China Connects: From coal to code', The International Institute for Strategic Studies, 2020, https://www.iiss.org/topics/geo-economics/belt-and-road#anchor_1588777861331.
- 6 Samantha Hoffman, 'Engineering global consent: The Chinese Communist Party's data-driven power expansion', Australian Strategic Policy Institute, 14 October 2019, <https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion>.
- 7 The National People's Congress of the People's Republic of China, '中华人民共和国国家情报法' ('Zhonghua Renmin Gongheguo Gguojia Qingbao Fa'), 中国人大网 (*Zhongguoren da Wang*), 12 June 2018, <http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml>.
- 8 Nigel Inkster, 'Huawei debacle throws spotlight on China's technology ambitions', The International Institute for Strategic Studies, 10 December 2018, <https://www.iiss.org/blogs/analysis/2018/12/huawei-china>.
- 9 Erica D. Boghard, 'The Overlooked Military Implications of the 5G Debate', Council on Foreign Relations, 25 April 2019, <https://www.cfr.org/blog/overlooked-military-implications-5g-debate>.
- 10 Patrick Wintour, 'US defence secretary warns Huawei 5G will put alliances at risk', *The Guardian*, 15 February 2020, <https://www.theguardian.com/us-news/2020/feb/15/us-defence-secretary-warns-us-alliances-at-risk-from-huawei-5g>.
- 11 Lesley Wroughton and Gergely Szakacs, 'Pompeo warns allies Huawei presence complicates partnership with U.S.', Reuters, 11 February 2019, <https://www.reuters.com/article/us-usa-pompeo-hungary-idUSKCN1Q0007>.
- 12 Milo Medin and Gilman Louie, 'The 5G Ecosystem: Risks & Opportunities for DoD', US Defense Innovation Board, 3 April 2019, p. 21, https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF.
- 13 Eleanor Shearer, Richard Stirling and Walter Pasquarelli, 'Government AI Readiness Index 2020', Oxford Insights, September 2020, p. 11, <https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/5f7747f29ca3c20ecb598f7c/1601653137399/AI+Readiness+Report.pdf>.
- 14 Bill Marczak and John Scott-Railton, 'Move Fast and Roll Your Own Crypto', The Citizen Lab, 3 April 2020, <https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/>.
- 15 National Defense Industrial Association, 'Vital Signs 2020: The Health and Readiness of the Defense Industrial Base', 2020, p.41, https://www.ndia.org/-/media/vital-signs/vital-signs_screen_v3.ashx?la=en#:~:text=Vital%20Signs%202020%3A%20The%20Health,for%20regular%20monitoring%20and%20assessmen.
- 16 Brin Mathew, 'US blacklists Xiaomi and Cnooc in flurry of actions to counter China', *Financial Times*, 14 January 2021, <https://www.ft.com/content/5a7aac48-1b1f-41a0-8fb7-e4253b730782>.
- 17 Joe Gould, 'US government's Huawei ban moving

- too fast, contractors say', *Defense News*, 9 July 2020, <https://www.defensenews.com/congress/2020/07/09/us-governments-huawei-ban-is-too-fast-contractors-say/>.
- 18 Mathew, 'US blacklists Xiaomi and Cnooc in flurry of actions to counter China'.
- 19 Wroughton and Szakacs, 'Pompeo warns allies Huawei presence complicates partnership with U.S.'.
- 20 'Lockheed Martin Poland', Lockheed Martin, <https://www.lockheedmartin.com/en-pl/index.html>.
- 21 'IAI Inaugurates New Line for F-35 Wing Skins', Lockheed Martin, 24 December 2018, <https://www.lockheedmartin.com/en-il/israel-news/iai-inaugurates-new-line-for-f-35-wing-skins.html>.
- 22 Ayman Falak Medina, 'Indonesia's Palapa Ring: Bringing Connectivity to the Archipelago', ASEAN Briefing, 28 January 2020, <https://www.aseanbriefing.com/news/indonesias-palapa-ring-bringing-connectivity-archipelago/>.
- 23 Fathiya Dahrul and Rieka Rahadiana, 'Indonesia Working on 5G Airwave Sale Leaves Door Open for Huawei', BloombergQuint, 15 November 2019, <https://www.bloombergquint.com/business/indonesia-working-on-5g-airwave-sale-leaves-door-open-for-huawei>.
- 24 'Digital technology to Indonesia: Trends and opportunities', Australian Trade and Investment Commission, 2020, <https://www.austrade.gov.au/Australian/Export/Export-markets/Countries/Indonesia/Industries>.
- 25 Teresa Umali, 'Indonesia proposes a budget increase for ICT, HR and digital literacy in 2020', OpenGov Asia, 25 June 2019, <https://opengovasia.com/indonesia-proposes-a-budget-increase-for-ict-hr-and-digital-literacy-in-2020/>.
- 26 'Huawei aims to have 73 local Indonesian apps in AppGallery by March', *The Jakarta Post*, 28 February 2020, <https://www.thejakartapost.com/news/2020/02/28/huawei-aims-to-have-73-local-indonesian-apps-in-appgallery-by-march.html>.
- 27 Ma Jingjing, 'Chinese tech companies flock to Indonesia to capitalize on booming internet economy', *Global Times*, 23 December 2018, <https://www.globaltimes.cn/content/1133239.shtml>.
- 28 Apoorva Bansal, 'Huawei donates 'qurban' to needy across 15 cities in Indonesia', Marketing Interactive, 3 August 2020, <https://www.marketing-interactive.com/huawei-donates-qurban-to-needy-across-15-cities-in-indonesia>.
- 29 'Huawei Indonesia, Batik Air, Garuda Indonesia among the most reputable brands in Indonesia fighting the COVID-19', Isentia, 3 March 2020, <https://www.isentia.com/latest-reads/huawei-indonesia-batik-air-garuda-indonesia-among-the-most-reputable-brands-in-indonesia-fighting-the-covid-19/>.
- 30 Muh Iqbal Marsyaf, 'Canggih, AI Besutan Huawei Bakal Jadi Pengawas Hutan di Indonesia', *SINDOnews*, 26 October 2020, <https://autotekno.sindonews.com/read/209794/207/canggih-ai-besutan-huawei-bakal-jadi-pengawas-hutan-di-indonesia-1603732251>.
- 31 Rossie Indira, 'Huawei Indonesia: Reaching for No 1', *China Daily*, 9 September 2011, https://www.chinadailyasia.com/news/2011-09/09/content_106637.html.
- 32 'Huawei proposes ultra-broadband for Indonesia', *Telecom Review Asia Pacific*, 25 April 2016, <https://www.telecomreviewasia.com/index.php/news/network-news/230-huawei-proposes-ultra-broadband-for-indonesia>.
- 33 Luffhi Anggraeni, 'Huawei Indonesia Luncurkan Learn On untuk Pendidikan Digital', Medcom.id, 7 July 2020, <https://www.medcom.id/teknologi/news-teknologi/Rb109OYN-huawei-indonesia-luncurkan-learn-on-untuk-pendidikan-digital>.
- 34 Stuart-Crowley, 'Huawei and BPPT to develop cloud, 5G and AI in Indonesia', W.Media, 16 October 2020, <https://w.media/news/huawei-and-bppt-to-develop-cloud-5g-and-ai-in-indonesia/>.
- 35 Petir Garda Bhwana, 'Huawei Partnership to Advance Indonesia's Digital Ecosystem', *Tempo*, 14 October 2020, <https://en.tempo.co/read/1395789/huawei-partnership-to-advance-indonesias-digital-ecosystem>.
- 36 'Huawei wins ICT award in Indonesia', Xinhuanet, 16 July 2019, http://www.xinhuanet.com/english/2019-07/16/c_138231909.htm.
- 37 Winston Qiu, 'Huawei Marine Deploys SeaX-1 Cable System connecting Indonesia, Singapore and Malaysia', Submarine Cable Networks, 11 September 2016, <https://www.submarinenetworks.com/systems/intra-asia/seax-1/huawei-marine-deploys-seax-1-cable-system-connecting-indonesia-singapore-and-malaysia>.
- 38 Cindy Silviana and Fanny Potkin, 'Indonesia cannot 'be paranoid' about curbing Huawei as telcos sign deals: minister', Reuters, 27 February 2019, <https://www.reuters.com/article/us-indonesia-huawei-idUSKCN1QG1C7>.
- 39 'Indonesia's top phone carrier leaves door open for Huawei 5G', *South China Morning Post*, 26 September 2019, <https://www.scmp.com/news/asia/southeast-asia/article/3030446/southeast-asias-largest-carrier-telkom-indonesia-adopts>.
- 40 Dahrul and Rahadiana, 'Indonesia Working on 5G Airwave Sale Leaves Door Open for Huawei'.

- 41 'The IISS Shangri-La Dialogue 2019 Special Sessions', The International Institute for Strategic Studies, 2 June 2019, <https://www.iiss.org/events/shangri-la-dialogue/shangri-la-dialogue-2019/special-sessions>.
- 42 Markus Juniarto Sihalo and Nur Yasmin, 'Cybersecurity Bill Postponed Until House's Next Term', *Jakarta Globe*, 27 September 2019, <https://jakartaglobe.id/news/cybersecurity-bill-postponed-until-houses-next-term/>.
- 43 'Indonesia: Government and DPR cancel discussion on cybersecurity bill', DataGuidance, 28 November 2019, <https://www.dataguidance.com/news/indonesia-government-and-dpr-cancel-discussion-cybersecurity-bill>.
- 44 Markus Wisnu Murti, 'Cybersecurity Draft Bill Officially Dropped', *Tempo*, 27 September 2019, <https://en.tempo.co/read/1253238/cybersecurity-draft-bill-officially-dropped>.
- 45 Eisy A. Eloksari, 'Indonesian businesses ramp up cybersecurity budget amid rampant attacks', *The Jakarta Post*, 23 July 2020, <https://www.thejakartapost.com/news/2020/07/22/indonesian-businesses-ramp-up-cybersecurity-budget-amid-rampant-attacks.html>.
- 46 Resty Woro Yuniar, 'Is Indonesia becoming too reliant on Huawei?', *South China Morning Post*, 4 December 2020, <https://www.scmp.com/week-asia/economics/article/3112634/indonesia-becoming-too-reliant-huawei>.
- 47 'Korea's ICT exports rise for 4 straight months, up 11.9% to \$17.6 billion in September', Ministry of Trade Industry and Energy Republic of Korea, 16 October 2020, http://english.motie.go.kr/en/tp/tradeinvestment/bbs/bbsView.do?bbs_seq_n=805&bbs_cd_n=2&view_type_v=TOPIC&¤tPage=1&search_key_n=&search_val_v=&cate_n=2.
- 48 Jack H. Park, 'Chinese ICT Companies to Make Full-scale Investment in Korean Market', *BusinessKorea*, 5 January 2015, <http://www.businesskorea.co.kr/news/articleView.html?idxno=8367>.
- 49 Douglas Busvine, 'USA, China, Japan and Korea to dominate 5G: study', Reuters, 7 November 2019, <https://uk.reuters.com/article/us-telecoms-5g-idUKKBN1XH0RC>.
- 50 Eujin Oh, 'APAC Market Spotlight: The Mobile Landscape in Korea', *Nativex*, 5 August 2020, <https://www.nativex.com/en/blog/apac-market-spotlight-the-mobile-landscape-in-korea/>.
- 51 Huawei Technologies, 'Huawei Opens its First 5G OpenLab in South Korea, Partnering with Korean SMEs to Build the 5G Ecosystem', *GlobeNewswire*, 3 June 2019, <https://www.globenewswire.com/news-release/2019/06/03/1863641/0/en/Huawei-Opens-Its-First-5G-OpenLab-in-South-Korea-Partnering-with-Korean-SMEs-to-Build-the-5G-Ecosystem.html>.
- 52 Teresa Taylor, 'Huawei Looks For More Investments And Product Purchases In South Korea Due To US Sanctions', *FinanceSecond*, 20 December 2019, <https://www.financesecond.com/huawei-looks-for-more-investments-and-product-purchases-in-south-korea-due-to-us-sanctions/>.
- 53 'Huawei decisions tests Samsung's wisdom', *Global Times*, 21 August 2020, <https://www.globaltimes.cn/content/1198457.shtml>.
- 54 Li Na and Meng Xing, 'Huawei Ban Is Likely to Have Huge Knock-On Effect on Korea's Chip Industry, Analysts Say', *Yicai Global*, 10 September 2020, <https://www.yicai.com/opinion/columnist/huawei-ban-is-likely-to-have-huge-knock-on-effect-on-korea-semiconductor-industry-analysts-say>.
- 55 'Seoul-Tokyo row risks sending 'wrong message': USFK chief', *Yahoo Sports*, 12 November 2019, <https://au.sports.yahoo.com/seoul-tokyo-row-risks-sending-wrong-message-usfk-210248117--spt.html>.
- 56 Erik Slavin, 'USFK deal keeps VoIP access for troops', *Stars and Stripes*, 18 January 2007, <https://www.stripes.com/news/usfk-deal-keeps-voip-access-for-troops-1.59207>.
- 57 Adam Entous, 'U.S.-South Korea Communications Won't Use Huawei Gear', *The Wall Street Journal*, 13 February 2014, <https://www.wsj.com/articles/SB10001424052702303704304579381742601220138>.
- 58 'US reportedly urges South Korea to reject Huawei products', *CNBC*, 22 May 2019, <https://www.cnn.com/2019/05/23/us-urges-south-korea-to-reject-huawei-products-report.html>.
- 59 John Power, 'US pressure on Seoul over Huawei taps into fears of North Korea', *South China Morning Post*, 26 June 2019, <https://www.scmp.com/week-asia/geopolitics/article/3016028/us-pressure-seoul-over-huawei-taps-fears-north-korea>.
- 60 Lee Sang-Jai, 'Huawei's woes in U.S. give pause to Korea, too', *Korean JoongAng Daily*, 20 December 2018, <https://koreajoongangdaily.joins.com/2018/12/10/industry/Huaweis-woes-in-US-give-pause-to-Korea-too/3056724.html>.
- 61 Kim Seung-yeon, 'U.S. renews calls on S. Korea to join economic security campaign against China', *Yonhap News Agency*, 14 October 2020, <https://en.yna.co.kr/view/AEN20201014008400325>.
- 62 J. James Kim and Hong Sanghwa, 'Opportunities and Challenges for South Korea in the New Era of 5G', *The Asan Institute for Policy Studies*, 21 March 2019, <http://en.asaninst.org/contents/opportunities-and-challenges-for-south-korea>.

- in-the-new-era-of-5g/.
- 63 Nagyung Lee, 'South Korea Should Not Disregard Huawei Security Concerns', *The Diplomat*, 4 June 2019, <https://thediplomat.com/2019/06/south-korea-should-not-disregard-huawei-security-concerns/>.
- 64 Kristine Lee et al., 'Digital Entanglement: Lessons Learned from China's Growing Digital Footprint in South Korea', Center for a New American Security, 28 October 2020, <https://www.cnas.org/publications/reports/digital-entanglement>.
- 65 'Huawei's Chips Banned by the U.S. in South Korean Defense Ministry's 40,000 Smart Speakers, Ministry "Didn't Know"', East Asia Research Center, 7 October 2020, <https://eastasiaresearch.org/2020/10/07/huaweis-chips-banned-by-the-u-s-in-south-korean-defense-ministrys-40000-smart-speakers-ministry-didnt-know/>.
- 66 Adam Entous, 'U.S. Raises Concerns About South Korea Deal With China's Huawei', *The Wall Street Journal*, 4 December 2013, <https://www.wsj.com/articles/us-warns-south-korea-about-chinese-telecom-firm-1386101980>.
- 67 Juan Pedro Tomás, 'Huawei willing to work with South Korea over 5G security concerns', RCR Wireless News, 9 October 2018, <https://www.rcrwireless.com/20181009/5g-huawei-willing-work-south-korea-over-5g-security-concerns>.
- 68 Michael Herh, 'Korean Telecom Industry Caught in Middle of U.S.-China Tug of War', BusinessKorea, 30 July 2020, <http://www.businesskorea.co.kr/news/articleView.html?idxno=49756>.
- 69 Park Han-na, 'Experts call for cautious approach to Huawei row', *The Korea Herald*, 17 June 2019, <http://www.koreaherald.com/view.php?ud=20190617000663&mod=skb>.
- 70 Park Chan-kyong, 'Using Huawei for 5G in South Korea presents 'little security risk'', *South China Morning Post*, 7 June 2019, <https://www.scmp.com/news/asia/east-asia/article/3013622/using-huawei-5g-south-korea-presents-little-security-risk>.
- 71 *Ibid.*
- 72 Tony Bertuca, 'DOD worried South Korea could use Huawei to build 5G network', Inside Defense, 28 January 2020, <https://insidedefense.com/insider/dod-worried-south-korea-could-use-huawei-build-5g-network>.
- 73 Kim Jae-seob, 'US cranks up pressure on S. Korean telecoms to abandon Huawei and Chinese technology', *The Hankyoreh*, 24 July 2020, http://english.hani.co.kr/arti/english_edition/e_business/955114.html.
- 74 Jung Suk-yee, 'China's FDI in South Korea Soars 240% in 2018', BusinessKorea, 4 January 2019, <http://www.businesskorea.co.kr/news/articleView.html?idxno=27991>.
- 75 Faisal Masudi, 'UAE 5G coverage now 80% in cities, footprint to grow', *Gulf News*, 8 December 2019, <https://gulfnews.com/uae/uae-5g-coverage-now-80-in-cities-footprint-to-grow-1.68349744>.
- 76 United Nations E-Government Survey 2018: Gearing E-Government to Support Transformation towards sustainable and resilient societies (New York: United Nations, 2018), p. 89, available at https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf.
- 77 Interview with a senior representative of an Emirati telecom provider, 28 October 2020.
- 78 Sarmad Khan, 'Mubadala looks to beef up tech investments and boost Asia portfolio', *The National*, 22 June 2020, <https://www.thenational.ae/business/economy/mubadala-looks-to-beef-up-tech-investments-and-boost-asia-portfolio-1.1037473>.
- 79 'Department of Health unveils world's most comprehensive Genome Program, Transforming health and well-being with genomics and Artificial Intelligence, the nation's leading strengths', Department of Health-Abu Dhabi, 10 December 2019, <https://doh.gov.ae/en/news/Department-Of-Health-unveils-worlds-most-comprehensive-Genome-Program>.
- 80 Haisam Hassanein, 'Arab States Give China a Pass on Uyghur Crackdown', *The Washington Institute for Near East Policy*, 26 August 2019, <https://www.washingtoninstitute.org/policy-analysis/view/arab-states-give-china-a-pass-on-uyghur-crackdown>.
- 81 'His Highness Sheikh Mohamed bin Zayed, Chinese President discuss strengthening relations', United Arab Emirates Ministry of Foreign Affairs & International Cooperation, 26 February 2020, <https://www.mofaic.gov.ae/en/mediahub/news/2020/2/26/26-02-2020-uae-china>.
- 82 Alexander Cornwell, 'US flags Huawei 5G network security concerns to Gulf allies', *Reuters*, 12 September 2019, <https://www.reuters.com/article/us-huawei-security-usa-gulf-idUSKCN1VX241>.
- 83 SIPRI Arms Transfers Database, accessed 24 January 2021, <https://armstrade.sipri.org/armstrade/page/values.php>.
- 84 Interview with a senior representative of an Emirati telecom provider, 28 October 2020.
- 85 Naushad K. Cherrayil, 'Gulf's SWFs on a tech-shopping spree', *Gulf News*, 6 January 2018, <https://gulfnews.com/technology/gulfs-swfs-on-a-tech-shopping-spre-1.2152491>.

- 86 'Prime Minister Benjamin Netanyahu's Remarks at the Israeli Presidential Conference', The Prime Minister's Office, 20 June 2013, https://www.gov.il/BlobFolder/news/speechtomo200613/en/english_mediacenter_speeches_documents_tomoeng200613.doc.
- 87 'China, Israel announce innovative comprehensive partnership', Xinhuanet, 21 March 2017, http://www.xinhuanet.com/english/2017-03/21/c_136146441.htm.
- 88 Hiddai Segev, 'Sino-Israeli Security Relations: In America's Shadow', Middle East Institute, 15 May 2018, <https://www.mei.edu/publications/sino-israeli-security-relations-americas-shadow>.
- 89 Gil Press, 'China and Israel: A perfect match, growing steady', Forbes, 26 February 2018, <https://www.forbes.com/sites/gilpress/2018/02/26/china-and-israel-a-perfect-match-growing-steady/#10ff8a345ec9>.
- 90 'What is GEOC?', GEOC, 2020, <http://www.gocapitalgp.com/Strategy>.
- 91 Hagar Ravet, 'The Israeli Tech Industry Is too Dependent on U.S. Economy, Says Israeli Finance Ministry', *CalCalist Tech*, 30 December 2019, <https://www.calcalistech.com/ctech/articles/0,7340,L-3776754,00.html>.
- 92 'Chinese Investment in Israeli Tech Is Growing, Report Says', *CalCalist Tech*, 12 November 2018, <https://www.calcalistech.com/ctech/articles/0,7340,L-3749619,00.html>.
- 93 'Huawei in talks to buy Israeli cyber company HexaTier: sources', Reuters, 20 December 2016, <https://www.reuters.com/article/us-huawei-tech-hexatier-m-a-idUSKBN1491O6>.
- 94 CyberESI, 2020, Home – CyberESI; Zachary Keck, 'Chinese hackers target Israel's Iron Dome', *The Diplomat*, 2 August 2014, <https://thediplomat.com/2014/08/chinese-hackers-target-israels-iron-dome/>.
- 95 Interview with an Israeli expert on China-Israel tech relations, 8 October 2020.
- 96 Ora Coren, 'Washington obstructing Israeli high-tech exports to China', *Haaretz*, 22 January 2014, <https://www.haaretz.com/israel-news/business/.premium-u-s-barring-israeli-tech-export-to-china-1.5313832>.
- 97 Yoram Evron, 'Between Beijing and Washington: Israel's Technology Transfers to China', *Journal of East Asian Studies*, vol. 13, 2013, pp. 503–28.
- 98 Interview with an Israeli expert on China-Israel tech relations, 8 October 2020.
- 99 Arie Egozi, 'Furious' US presses Israel to bar Chinese gear from sensitive systems', *Breaking Defense*, 18 February 2020, <https://breakingdefense.com/2020/02/furious-us-presses-israel-to-bar-chinese-gear-from-sensitive-systems/>.
- 100 Press, 'China and Israel: A perfect match, growing steady'.
- 101 Coren, 'Washington obstructing Israeli high-tech exports to China'.
- 102 On the latter, see Antony J. Blinken and Robert Kagan, 'America First' is only making the world worse. Here's a better approach', *Washington Post*, 1 January 2019, https://www.washingtonpost.com/opinions/america-first-is-only-making-the-world-worse-heres-a-better-approach/2019/01/01/1272367c-079f-11e9-88e3-989a3e456820_story.html.
- 103 'Seeds for the Future Polska 2018 – an opportunity for students of technical universities', Telix press release, <https://www.telix.pl/inne/konkurs/2018/03/seeds-for-the-future-polska-2018/>.
- 104 Politechnika Warszawska, 'Huawei Polska i Politechnika Warszawska podpisały porozumienie o współpracy', 6 August 2020, <https://www.pw.edu.pl/Aktualnosci/Huawei-Polska-i-Politechnika-Warszawska-podpisały-porozumienie-o-wspolpracy>.
- 105 'Confucius Institutes Around the World – 2020', DigMandarin, 15 February 2020, <https://www.digmandarin.com/confucius-institutes-around-the-world.html>.
- 106 Wojskowa Akademia Techniczna (WAT), Wydział Cybernetyki, <https://wcy.wat.edu.pl/pl/50lecie/obchody-jubileuszu>.
- 107 Joanna Plucinska et al., 'How Poland became a front in the cold war between the U.S. and China', Reuters, 2 July 2019, <https://www.reuters.com/investigates/special-report/huawei-poland-spying/>.
- 108 Lukasz Sarek, 'Arresting Huawei's march in Warsaw', *Sinopsis*, 2 February 2019, <https://sinopsis.cz/en/arresting-huaweis-march-in-warsaw/>.
- 109 Bojan Pancevski and Matthew Dalton, 'Spy Case Linked to China Raises Red Flags for Poland and US', *The Wall Street Journal*, 24 January 2019, <https://www.wsj.com/articles/spy-case-linked-to-china-raises-red-flags-for-poland-and-the-u-s-11548357192>.
- 110 'Zinfiltrowano Kluczowa Uczelnia Wojskowa w Polsce?', 12 January 2019, <https://osluzbach.pl/2019/01/12/ustalenia-o-sluzbach-kluczowa-uczelnia-wojskowa-w-polsce-mogla-zostac-zinfiltrowana-przez-chinskie-sluzby/>.
- 111 'Zatrzymany przez ABW Piotr D. pełnił ważne funkcje w MSWiA, ABW i UKE', *Forsal*, 11 January 2019, <https://forsal.pl/artykuly/1391757,zatrzymany-przez-abw-piotr-d-peelni-wazne-funkcje-w-mswia-abw-i-uke.html>.
- 112 'Zinfiltrowano Kluczowa Uczelnia Wojskowa w Polsce?'

- 113 'Henryk Kowalczyk o współpracy z Chinami Co ze zwiększeniem eksportu I inwestycjami w Polsce?', Money.pl, 1 June 2017, <https://www.money.pl/gospodarka/wiadomosci/artikul/henryk-kowalczyk-polski-eksport-do-chin-nowy,94,0,2328158.html>.
- 114 See 'Remarks by President Trump to the People of Poland', speech delivered by Donald Trump, US President, , 6 July 2017, <https://www.president.pl/en/news/art,494,remarks-by-president-trump-to-the-people-of-poland.html>.
- 115 Alina Grigoras, 'Update: US, Romanian Presidents Adopt Joint Statement to Strengthen The Strategic Partnership', Romania Journal, 21 August 2019, <https://www.romaniajournal.ro/politics/upate-us-romanian-presidents-adopt-joint-statement-to-strengthen-the-strategic-partnership/>.
- 116 The speech was at the Wilson Center and is available on YouTube: <https://youtu.be/LrMfXiBL9ks>. The translation here is different from the live translation on the video.
- 117 Jacob M. Schlesinger, 'What's Biden's New China Policy? It Looks a Lot Like Trump's', *The Wall Street Journal*, 10 September 2020, <https://www.wsj.com/articles/whats-bidens-china-policy-it-looks-a-lot-like-trumps-11599759286>.



The International Institute for Strategic Studies – UK

Arundel House | 6 Temple Place | London | WC2R 2PG | UK

t. +44 (0) 20 7379 7676 **f.** +44 (0) 20 7836 3108 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas

2121 K Street, NW | Suite 600 | Washington, DC 20037 | USA

t. +1 202 659 1490 **f.** +1 202 659 1499 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia

9 Raffles Place | #49-01 Republic Plaza | Singapore 048619

t. +65 6499 0055 **f.** +65 6499 0059 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Middle East

14th floor, GBCORP Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain

t. +973 1718 1155 **f.** +973 1710 0155 **e.** iiss-middleeast@iiss.org
