MEI
Policy Center

CHINESE TECHNOLOGY IN THE MIDDLE EAST: A THREAT TO SOVEREIGNTY OR AN ECONOMIC OPPORTUNITY?

THOMAS BLAUBACH
MARCH 2021

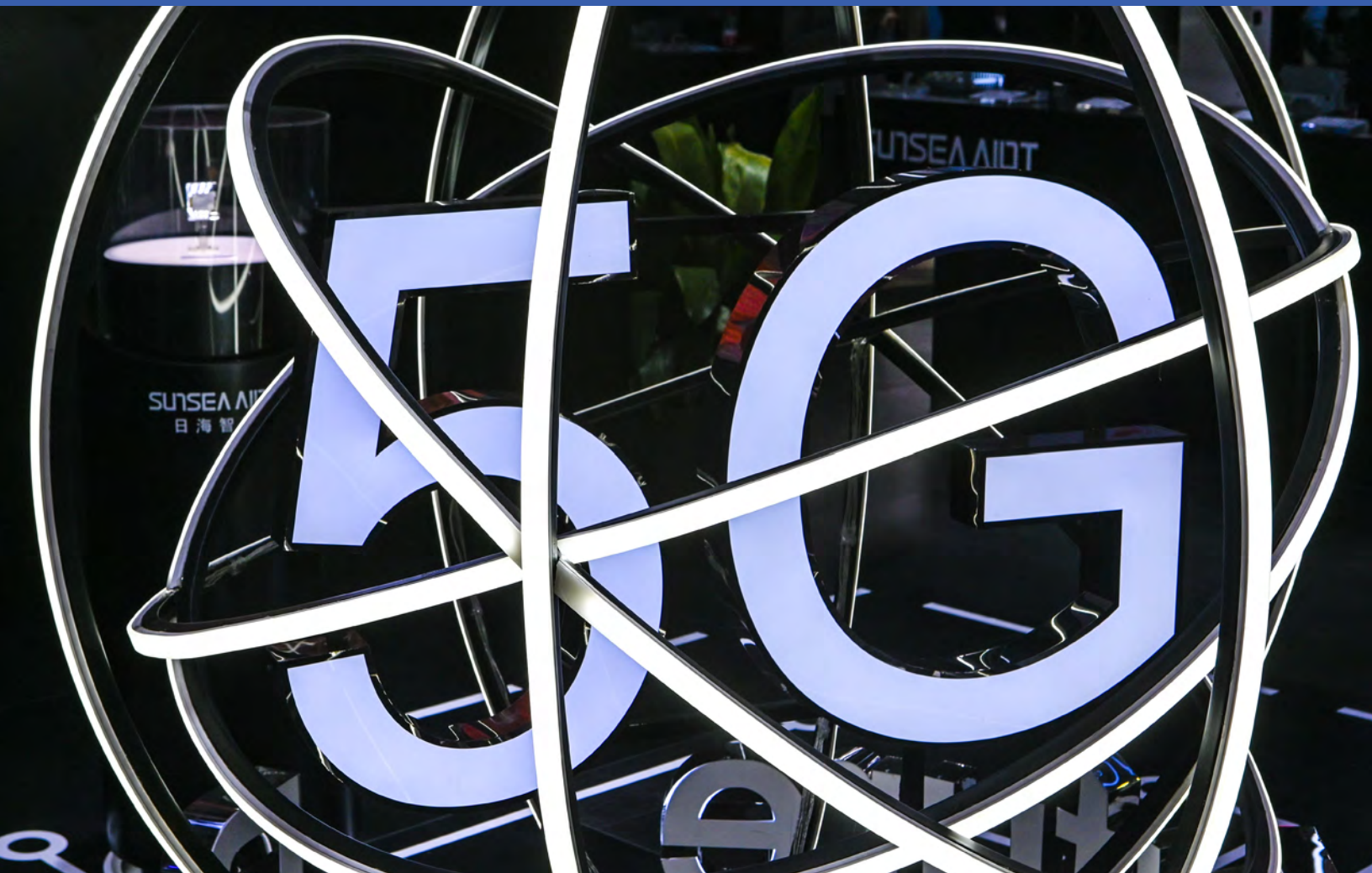

Photo above: Hikvision security cameras are seen on July 31, 2020 in Guangyuan, Sichuan Province of China. Photo by VCG/VCG via Getty Images

> **A major concern about Chinese technology is surveillance.**

Recent moves by Chinese tech giants like Huawei, ZTE, and Hikvision have raised concerns in Washington about Beijing's technological outreach to developing nations. To stem the international growth of these companies, the U.S. has discouraged countries from adopting Chinese technologies through efforts like promoting the Clean Network Initiative. Countries across the globe often must choose between Chinese or Western technology, and these choices have broad implications. The intense Chinese and American competition over the future of next generation technologies, e.g., 5G, has made it unclear if U.S. opposition stems from the actual risks of Chinese engagement or mere political considerations. Nations considering Chinese technologies and infrastructure projects must take a realistic viewpoint of China's global rise and ambitions to understand the benefits and risks. Among these nations are those of the Middle East and North Africa (MENA). These countries will have to navigate the Chinese Belt and Road (BRI) mega-project. China's BRI looks to reorient the Eurasian-African economy toward Beijing through various infrastructure deals, including railroads, energy projects, and ports. Over 60 countries have committed to participating in the

“Some critics have viewed BRI projects in low-income nations as ‘debt traps.’”

BRI with Chinese companies through Memoranda of Understanding (MoUs), plans, and resources for projects. Today, these projects stand at different stages, from conception to completion. Perhaps the BRI’s most consequential component will be the Digital Silk Road (DSR), which seeks to connect the global economy using Chinese technology infrastructure, led by companies like Huawei.

The Digital Silk Road

China has presented the DSR to MENA states in the form of various projects, such as fiber-optic cables, “safe city” projects for monitoring and securing urban public spaces, and new or expanded 5G communication networks. In essence, China’s digital initiatives promote strong “cyber sovereignty,” meaning strict control by states over digital information within their borders. Consequently, the risks of unwelcome or authoritarian surveillance and practices have dominated the debate about adopting Chinese technology, on top of issues of overwhelming debt or economic domination. Though these deals have varied widely in terms of their plausibility and completion status, DSR outreach has undoubtedly looked to transform the technological field in the greater Middle East region.

More broadly, China’s projects under the BRI have led to concerns over Beijing’s intentions. Some critics have viewed BRI projects in low-income nations as “debt traps”. These projects have also been identified as a way for China to challenge American power worldwide by exerting its influence over its close allies. China’s BRI efforts are not examples of a purely virtuous diplomacy of “South-South” cooperation nor are they exclusively attempts to dominate its economic partners. The underlying impetus for China’s BRI is to continue the nation’s rapid economic development. By accessing new markets and their resources, China can continue reaching the high levels of economic growth demanded by its massive and growing middle class. BRI projects in the Middle East play the crucial role of continuously supplying energy resources to China and, to a lesser extent, providing access to the Western European market via the Mediterranean, Turkey, and the Caucasus. In terms of the DSR, China’s focus in the Middle East is to digitally connect the region to a global Eurasian-African economy and to upgrade current technological infrastructure using Chinese blueprints.

Although most of China’s BRI projects serve important economic and diplomatic purposes, it is essential to examine associated short-falls, concerns, and risks. The BRI and DSR initiatives are complex and overarch the fields of technology, economics, and policy-making. This assessment found four major risks associated with the global expansion of Chinese technology:

- Surveillance technology uses
- Fusion of Chinese tech companies with the Chinese Communist Party (CCP) & the People’s Liberation Army (PLA)
- Chinese influence over future technology markets and tech norms
- Chinese technological/economic dominance leading to political coercion or perpetuating authoritarian regimes in other countries

It is critical to examine BRI projects and foresee possible impacts. As nations around the world slowly center their societies around next-generation (5G) technologies, adoption (or non-adoption) of Chinese technology will have lasting implications for geopolitics, cyberspace, and economics.

The issue of surveillance

A major concern about Chinese technology is surveillance. Critics claim that Huawei systems and Hikvision cameras allow governments to spy on citizens and political opponents.[1] [2] Some even claim that this technology gives the CCP the ability to conduct espionage against foreign targets and governments.[3] Although these claims are plausible and carry some truth, Chinese companies are not the only ones that engage in undemocratic surveillance. Several American, European, and Israeli tech companies have created tools or partnered with Chinese companies that have been met with disapproval from Western governments and civil rights groups.[4]

Western tech companies have responded by claiming that the products or services were limited in their surveillance capabilities and that technologies are inherently multi-purpose.[5] They state that their products only connected to targeted Wi-Fi networks and couldn’t decrypt messages, that any training of local buyers was limited, and that buyers were solely responsible for non-democratic uses of the

Photo above: General view of the deserted Badshahi Mosque closed amid concerns over the spread of the COVID-19 novel coronavirus, in Lahore on March 16, 2020 Photo by ARIF ALI / AFP via Getty Images

“Projects in Lahore and Islamabad demonstrate the shortcomings of the project and the often corrupt practices in payments and implementation.”

“In MENA’s expanding metropolises, there is a growing need to make public spaces more secure to promote commerce, mitigate security threats … and ease growing pains.”

technology. Representatives from both Western and Chinese tech companies argue that their products are not inherently democratic or authoritarian but can be either, depending on the laws and institutions of the user country.[6]

“Safe Cities”

Huawei’s “Safe Cities” program — a system of surveillance cameras and products — has been launched in numerous cities around the world with ranging scopes and levels of performance. Opponents of Huawei’s “Safe Cities” program view it as a first step in regimes establishing a “surveillance state.” But most “Safe Cities” programs outside of China are too incomplete to foresee the future implications of the program. The opaque dealings and ambiguous terms make the progress of the initiative hard to assess. Huawei has claimed that it has set up 230 “safe cities” in 90 countries, but a Center for Strategic and International Studies (CSIS) report could only verify 73 programs in 52 countries,[7] demonstrating the difficulty in determining the true breadth and impact of the initiative.

In MENA’s expanding metropolises, there is a growing need to make public spaces more secure to promote commerce, mitigate security threats (theft, mobs, smuggling, etc.), and ease urban “growing pains” like traffic jams. Such problems often discourage business and lower confidence in governance. One can gauge the chances that Huawei’s “Safe Cities” program might ameliorate some of these problems by looking at the country with the greatest investments in the BRI: Pakistan. In Peshawar, for example, local officials hoped that the 5,000 CCTV camera system would help reduce corruption and crime in the city’s streets and that the consequent “peace” would attract further investment and economic prosperity.[8] Projects around Pakistan and MENA aim at these objectives, but the outcomes of the “safe city” plan are often exaggerated. Projects in Lahore and Islamabad demonstrate the shortcomings of the project and the often corrupt practices in payments and implementation. Evidence suggests that the cameras did not achieve their primary objective. After 8,000 cameras were installed in Lahore, total crime actually rose in the city, and Islamabad also soon saw a crime increase after several years of falling rates.[9] Perhaps more worrisome are reports of price-gouging and corruption in the implementation of the Islamabad “safe city” plan.[10] From an espionage perspective, local sources from the Punjab Safe City Authority (PSCA) reported that Wi-Fi transmitting cards had been found in city CCTV cabinets that were installed by Huawei. Although the company said there was a misunderstanding and that transmitters were mentioned in the bidding document, PSCA said that the reference to the cards was unclear and that the functionality of the cards was redundant and not needed for local use, raising the question of why the transmitters were installed.[11]

In the earliest deployment of “safe cities” in MENA, the project has largely not become the authoritarian tool some feared. Instead, issues stem from exaggerations of the project’s effectiveness and corruption surrounding the bidding and implementation of projects. However, this early implementation of project components does act as a warning signal. While “safe cities” could enjoy increased security and economic opportunity, they could also become vulnerable to authoritarian overreach, corruption, and Chinese espionage. Regardless of the immediate outcomes and controversies, surveillance has become a major part of the DSR initiative and will undoubtedly play a large and controversial role in the future use of technologies in the Middle East.

“

Huawei’s ‘Safe Cities’ program — a system of surveillance of cameras and products — has been launched in numerous cities.

Separation of business and state

China's leading tech companies, especially Huawei, have had difficulty convincing foreign governments and businesses of their independence from Beijing. Due to the CCP's authority over the state-controlled economy, tech giants like Huawei have grown under the auspices of the central government. Beijing's security complex, largely run by the PLA, has also played a central role in the development of the country's technology industry. These close relationships, interdependencies, and forms of collaboration have created a complex that has helped turn China into a global economic and political juggernaut. Every Chinese company is required by law to have a CCP committee that ensures that "moral and social values" are being maintained.[12] The PLA has allegedly contracted with tech companies like Huawei and has connections with its top leadership — Huawei CEO and founder Ren Zhengfei served as a director of Basic Civil Engineering Corps in the PLA. [13] Beyond Huawei, China has a controlling stake through subsidiaries of Hikvision.[14] One project, PLA-863, through which Huawei and ZTE provide switches, routers, and mobile and fiber networks, also demonstrates the collaboration between the military and industry leaders.[15] This party-military-industry complex (PMIC)[16] has cast doubt on the independence of industry leaders and the aims of their global strategies. Specifically, Chinese tech companies' role within the PMIC has come under scrutiny because of:

- Government subsidies and active promotion
- Previous examples of opaque, unusual, or corrupt dealings
- Possible CCP/PLA-sponsored espionage through companies and contracts

A clear challenge to Huawei's claim of independence is the subsidies and promotion it enjoys from the central government and state-owned banks. Huawei received $228.2 million in government grants between 2008 and 2011 and since 2012, has secured around $9 billion in state-owned bank financing for overseas projects.[17] State subsidies allow Huawei to become a global competitor by providing markets with high-quality but inexpensive technology products. In addition to giving Huawei a global market advantage, the Chinese government has taken political positions that point to strong state support for the company. One can see the proximity between Huawei and the Chinese government in the events surrounding the arrest of Meng Wanzhou, the CFO of Huawei and the daughter of Huawei founder and CEO Ren Zhengfei. She was arrested in Canada and charged by U.S. authorities with conspiracy to commit fraud for circumventing sanctions on Iran through a company called Skycom Tech.[18] Shortly after Wanzhou's arrest, the Chinese government detained two Canadians on espionage charges in an apparent retaliation and blocked certain agricultural imports from Canada.[19] This episode illustrates China's willingness to retaliate on both political and economic levels when the integrity of a corporate entity of the state's PMIC is threatened.

Given the immensity of the operations carried out by Huawei and other Chinese industry leaders in telecommunication, incidents of corrupt and/or opaque business practices are inevitable. A few such incidents in MENA are worth mentioning, especially in light of the industry's close ties to the state. In 2012, Algeria banned Huawei and ZTE for two years after a $10 million bribery scandal involving two ZTE employees, one Huawei employee, and an official from Algeria Telecom.[20] In Pakistan, the corruption allegations around Islamabad's Safe City Project have also challenged Huawei's dealings in the Middle East. Examples from Algeria and Pakistan are only a few in a global web of malpractice by Chinese tech giants that has called the actions and standards of their international projects into question.[21] The fusion of business and the state through the PMIC has raised suspicions about Chinese tech companies being involved in or facilitating espionage. Specifically, the source of suspicion is Article 7 of China's National Intelligence Law (2017):

> "All national bodies, military forces, political parties, social groups, enterprise and undertaking organizations, as well as citizens, shall support, cooperate with and collaborate in national intelligence work, and maintain the secrecy of national intelligence work they are aware of … Relevant departments in all levels of People's Governments, enterprise and undertaking work units, other organizations and citizens shall provide the necessary assistance to national intelligence work organs lawfully carrying out their work, and maintain secrecy."[22]

Article 28 of the same law states that those who do not comply can be detained and investigated. [23] These provisions legalize and formalize the cooperation between industry and state, increasing the probability of Huawei's covert cooperation with the CCP/PLA.

An example of the PMIC being used for state espionage is the Guangzhou Boyu Information Technology Company, Boyusec, and the advanced persistent threat group APT3. Listed as a "cooperative

Photo right: Huawei CFO Meng Wanzhou leaves BC Supreme Court during a break in her hearing where she is fighting extradition to the United States on September 28, 2020 in Vancouver, Canada. Photo by Rich Lam/Getty Images

“A clear challenge to Huawei’s claim of independence is the subsidies and promotion it enjoys from the central government and state-owned banks.”

partner,” Huawei has helped Boyusec build its security services.[24] Boyusec shares individual actors with the APT, also known as the “Gothic Panda” group, which has reportedly conducted espionage on behalf of the Ministry of State Security (MSS).[25] The activities and relationship between Huawei-Boyusec-APT3-MSS has been confirmed by the Pentagon and the Permanent Select Committee on Intelligence, as well as the Department of Justice, which indicted a Boyusec executive for hacking into the American credit rating company Moody’s, the German manufacturer Siemens, and the American technology company Trimble.[26] This dynamic displays the complicated relationship between state, industry, and cyber actors and how they operate to achieve Chinese state goals. Looking forward, the National Intelligence Law and Huawei’s enmeshment in the PMIC will increasingly become a point of tension between the company and its international clients.

Technology dominance and influence

China seeks to establish itself as the world’s primary technological power in order to lead the economy of tomorrow, which will be fueled by 5G technologies and data. As part of this mission, Beijing has been attempting to reformulate global technological norms –– the rules for using the digital sphere –– and hopes to supply the future’s digital infrastructure. The “China Standards 2035,” which was released by the Chinese government in June, 2020, summarizes China’s goals and articulates Beijing’s desire to become the leader in emerging 5G technologies in the near future.[27] Nonetheless, China will not be able to unilaterally redefine tech standards due to Beijing’s likely compliance with international regulation-setting organizations like the 3rd Generation Partnership Project (3GPP) and the International Telecommunications Union (ITU).[28] [29] With the global market and society speeding toward a 5G digital economy, a future Chinese-dominated global 5G digital infrastructure would secure Beijing’s power. Through a world-wide network of technical expertise, “safe city” technology, and global digital infrastructure, China looks to gain digital primacy.

One can see the proximity between Huawei and the Chinese government in the events surrounding the arrest of Meng Wanzhou, the CFO of Huawei.

Photo above: Chinese Ambassador to Egypt Liao Liqiang speaks via a video call during a ceremony to celebrate China's National Day in Cairo, Egypt, Oct. 11, 2020.. Photo by: Ahmed Gomaa/Xinhua via Getty

> **Huawei's vision to establish its ICT norms and become a pillar of the global economy is on full display in North Africa.**

Using Huawei to export its technological vision and business, China has made the world's largest telecommunications provider and second-largest smartphone manufacturer the fulcrum of its global digital expansion and influence. Through Huawei's developmental IT programs like "Seeds for the Future" and high-level meetings with foreign officials, the city of Shenzhen has become the launching pad for China's mission to reshape the digital landscape. The "Seeds for the Future" draws international talent from across the globe to gain technical expertise from Huawei, which they can then bring home – along with positive feelings for China.

Huawei in North Africa

Huawei's vision to establish its ICT norms and become a pillar of the global digital economy is on full display in North Africa. "Seeds for

“Chinese investments in North Africa are a part of a the country’s larger goals for controlling future world trade”

the Future” has established programs with Tunisia and Egypt as part of broader MoUs in North Africa.[30][31] In Tunisia, Huawei has trained over 1,000 Tunisian ICT professionals and has established a talent center, a service resource center, and a “Huawei ICT Academy” to serve as a regional educational hub for the company.[32] Nearby in Egypt, over 5,000 Egyptian ICT professionals have trained with Huawei and the company has built the first “OpenLab” in Cairo, in addition to four centers for training and ICT smart city solutions.[33]

Huawei sees North Africa as a critical part of its global strategy. In February 2018, Huawei signed a memorandum with Telecom Egypt to establish a $5 million data center for a cloud computing network as part of its mission to develop one of the five largest cloud networks in the world.[34][35] The cloud computing network is slated to be the first in MENA. In Morocco, the Chinese Communications Construction Company (CCCC) broke ground on the Mohammad VI Tangier Tech City. The project, which is projected to be the largest Chinese investment in North Africa, will further develop Morocco’s ICT capabilities under Chinese construction and guidance.[36]

Chinese investments in North Africa are a part of the country’s larger goals for controlling future world trade. Adel Abdel Ghafar and Anna Jacobs of the Brookings Institution explain that for “Chinese diplomats … North African countries are especially attractive prospects for economic cooperation due to their proximity to European, African, and Asian markets, high number of industrial zones, and high levels of investment in infrastructure development. [37]” The economically developing North African region will be an increasingly important place for investment by both Huawei and the larger Chinese PMIC.

Fiber-optic cables

The DSR initiative sets out to build the necessary infrastructure for the digital future. This requires the roll-out of 5G telecommunication technology and expansion of fiber-optic cables.

About 350 fiber-optic cables on the world’s seabeds process around 95% of intercontinental data traffic.[38] Huawei has participated in about 90 projects to build or upgrade undersea fiber-optic cables across the globe to become a primary operator. A region of particular interest in terms of fiber-optic construction is MENA. Huawei’s subsidiary, Huawei Marine Networks, has finished several cables connecting the Mediterranean. including the “Hannibal” cable between Tunisia to Italy and another linking Libya to Greece.[39][40] Elsewhere in the region, Huawei has built cables connecting Oman to East Africa and Pakistan.[41]

Dwarfing these cable lines is Huawei’s Pakistan and East Africa Connecting Europe (PEACE) cable.[42] Starting in Gwadar and Karachi, Huawei plans to connect MENA to Europe and Africa by a cable that extends through the Indian Ocean, Red Sea, and Mediterranean, reaching as far as France, Kenya, and possibly South Africa.[43] It is no surprise that the major nodes of the cable are Pakistan, Djibouti, and Egypt — major participants of the BRI in the region. The PEACE cable is a linchpin in China’s DSR initiative. The cable will further promote Huawei in the countries most active in BRI projects and allow China to capitalize on their transition to the digital economy.

COVID-19 may increase Huawei’s ambitions in the Middle East and around the world with the steep surge in the demand for telecommunications during a prolonged time of social-distancing. Furthermore, developing countries are facing greater debt burdens so they are drawn to tech-oriented projects, which are cheaper and completed more quickly than traditional infrastructure projects, such as ports and railways. Due to these factors and China’s relatively fast recovery, COVID-19 could accelerate Chinese market share in MENA’s vital telecommunications industry.

China (via Huawei) has also played an active role in developing the region’s 5G communication’s framework. Huawei has spearheaded initial national 5G programs in the UAE, Lebanon, and Pakistan. Deals range from launching 5G and IoT (Internet of Things) OpenLab programs in the UAE to providing ten base stations to Lebanon’s initial 5G program. With Huawei’s already high level of technological involvement in the region, the company can be expected to seek a major role in bringing 5G to countries like Egypt and Algeria once their tech markets become sufficiently mature.

Photo above: People visit the Huawei booth during the Mobile World Congress (NWC) Shanghai 2021 at Shanghai New International Expo Center on February 24, 2021 in Shanghai, China. Photo by VCG/VCG via Getty Images

> **COVID-19 may increase Huawei's ambitions in the Middle East and around the world.**

With the exception of the Gulf, the region will not see the full impact of 5G technologies for a while. Initial investments and infrastructure are crucial. Once 5G infrastructure is implemented, it is logistically difficult and cost-prohibitive to remove.[46] This gives a telecom provider, such as Huawei, significant influence over the growth of its initial investments in a country's nascent 5G network. If Huawei can corner the market early, it can prevent local business from competing.[47] Local manufacturers in North Africa already have intense competition from Chinese phone makers like Oppo and Vivo. [48] Chinese dominance in MENA's future tech industry stands to eliminate local industry leaders and give China control of the future economy's biggest asset: data. From a commercial standpoint, data allows Chinese tech companies to better understand markets and eventually outcompete local and foreign players. Controlling the flows of data allows Chinese tech companies and the PMIC to "monitor, manipulate, and disrupt information flows." [49] [50] In addition, early Chinese tech dominance could also block Western companies and government partners

“China has economically driven relationships with the countries it dominates in trade, with a politcally hands-off approach”

from gaining important market share and from interacting with regional MENA partners in the digital sphere. It is essential for the countries of the Middle East to consider the future economic and security risks of a predominant Chinese digital infrastructure with Chinese control over data flows.

COVID-19 may increase Huawei’s ambitions in the Middle East and around the world with the steep surge in the demand for telecommunications during a prolonged time of social-distancing. Furthermore, developing countries are facing greater debt burdens so they are drawn to tech-oriented projects, which are cheaper and completed more quickly than traditional infrastructure projects, such as ports and railways.[51] Due to these factors and China’s relatively fast recovery, COVID-19 could accelerate Chinese market share in MENA’s vital telecommunications industry.

Chinese neocolonialism?

Critics of China’s aggressive BRI foreign policy strategy have also criticized it for being a debt trap that will inevitably make debtor developing nations economic dependents of Beijing, opening them up to Chinese neocolonialism. This claim, however, requires a comparison between China’s current foreign policy and European colonial regimes. Unlike European colonial regimes, the Chinese have not taken an explicit role in the politics of their client states. China does not look to create a “Greater China” and dominate debtor nations politically, socially, or linguistically. Instead, China has an economically driven relationship with the countries it dominates in trade, with a politically hands-off approach. An apt comparison is with the mercantilism of the early British Empire, which created small British-controlled enclaves to facilitate a global trade regime. Similarly, China uses the ports and bases that it has acquired in Djibouti and Sri Lanka to extend its global economic power rather than politically dominate the host countries.

With less than a decade of progress, it is difficult to forecast the unintentional consequences of BRI and the DSR, but the projected economic and technological dominance of China over participating Middle East states is hard to dismiss. As of present, the comparison between China and the British Empire is far-fetched, but it is possible that in the future China will have client states in the Middle East that resemble the early British imperial system with domination by control of trade. Emerging risks from BRI and DSR that will certainly impact the future of MENA can be summarized as:

- Chinese-held debt from infrastructure and loans
- Dependence on trade with Beijing
- Chinese 5G dominance in Middle Eastern markets

Debt traps

A growing worry surrounding the BRI is the debt taken on by participating countries. The implications of debt stress can indeed be severe for a nation’s sovereignty, but a 2018 report from the Center for Global Development (CGD) found that only eight of over 60 participating nations are at high risk for debt stress from BRI projects.[52] Four of these nations are in the Greater Middle East and surrounding regions –– Djibouti, Pakistan, Tajikistan, and Kyrgyzstan. In some cases, China has implemented debt-for-equity schemes that provide debt relief in exchange for control over infrastructure. Thus, the inability of indebted nations to pay loans can lead to a loss of critical infrastructure that could otherwise be a major source of economic development and income. Countries with high levels of debt-stress can find themselves in a zero-sum game when participating in China’s BRI.

Sri Lanka, Djibouti, and Pakistan all provide examples of the negative effects of indebtedness to China. The Chinese takeover of the Hambantota port in Sri Lanka has become an infamous case study for China’s strategy. The Sri Lankan government agreed to lease the port to China for 99 years when it was unable to service its $8 billion loan at 6 percent. Djibouti is severely indebted to Beijing and hosts a Chinese foreign military base. China provided almost $1.4 billion of funding, equivalent to 75% of the East African nation’s GDP. The port of Gwadar, the centerpiece of the China-Pakistan Economic Corridor (CPEC), is another strategic site in the Greater Middle East with heavy Chinese involvement. Resonating with the outcome of the Hambantota Port, Gwadar was leased to

Photo above: Bunkering ship in operation at Hambantota International Port, Sri Lanka, a Sri Lanka-China joint venture, Hambantota International Port on April 6 2020. Photo by Liu Hongru/Xinhua via Getty Getty Images

“A rising superpower, China can use its new international ports to project its military might in the Indian Ocean and Red Sea.”

the China Overseas Port Holding Company (COPHC) for 40 years. It is estimated that COPHC will receive a 91% share of revenue from operations to recover its capital investment. China may very well attempt a debt-for-equity swap with heavily indebted Islamabad. China's acquisition of regional port infrastructure through debt-for-equity swaps is part of a strategy to secure trade and energy routes in the greater Indian Ocean region.

China's military base in Djibouti and allegations that Beijing seeks to implement intelligence gathering components at the Hambantota port suggest a second risk of Chinese debt[56]: the dual use of infrastructure for politico-military purposes. Along with securing energy supplies and facilitating trade, the infrastructure obtained from debt-for-equity swaps could be used for a growing Chinese military presence. As a rising superpower, China can use its new international ports to project its military might in the Indian Ocean and Red Sea. With a loss of sovereignty and economic potential, high-stressed nations could find themselves as mere hosts to the Chinese military.

The social, political, and especially economic fallout from the COVID-19 pandemic in the developing world is exacerbating the "debt-trap" worries. As they fall further into debt, MENA countries currently classified as having "significant" stress-risk will begin to fall into the category of "high risk." CGD report identified eight countries that they classified as being part of the greater MENA region — Armenia, Syria, Lebanon, Iraq, Jordan, Egypt, Yemen, and Afghanistan — as having significant debt stress before the pandemic. The added financial burden on these countries will further intensify their financial relationship with China. In the future, we may see further debt-for-equity swaps on the region's critical infrastructure.

China as a primary trading partner

Not only is China becoming a major lender to many countries in the region, it is also becoming their primary or secondary trading partner. China will benefit from greater leverage and demand for its products as the infrastructure projects begin to operate. China already is the top energy importer from many of the region's largest energy markets including Saudi Arabia, Iran, Kuwait, and Oman.[57] Outside the Gulf, China is the top trading partner of Algeria and Egypt.[58] In Egypt, China has taken an active economic role with a focus on the country's biggest economic-political assets, the Suez Canal and the mega-city of Cairo. Chinese companies played a crucial role in Egypt's Suez Canal economic zone project and will be heavily involved in building the new capital city outside Cairo, the "New Administration Capital."[59] While Chinese projects in Egypt have occasionally fallen short of expectations, Egyptian President Abdel Fattah el-Sisi has prioritized strengthening ties with Beijing, as evidenced by his six visits to China.[60] Given heavy investment in Egypt by China, strong bilateral trading ties, and Beijing's indifference to human rights abuses, el-Sisi's illiberal regime may wish to turn Beijing into its primary partner for more than just trade. China's ability to shape the region economically and technologically will increase in tandem with China's energy imports and industrial exports.

Not only is China becoming a major lender to many countries in the region, it is also becoming their primary or secondary trading partner.

5G-Tech Dominance

5G technology is penetrating the very fabric of MENA economy. If Beijing builds the necessary infrastructure for this transformation, it could play a dominant economic and possibly political role in the region.

Dependence on China's finance, trade, and tech will diminish the sovereignty of BRI participants and their ability to act independently from Beijing. This trend is evident from claims of Chinese espionage in the building of the African Union's (AU) headquarters in Addis Ababa. As part of China's growing outreach, Beijing pledged $200 million for the AU headquarters, while using Chinese contractors.[61] In 2018, *Le Monde Afrique* reported that the headquarters' computer system had been hacked and that data had been transferred to servers in Shanghai every night for the past five years.[62] Publicly, both Chinese and AU officials dismissed the claims as lies. But in private, African officials raised concerns about the hack and the consequences of the continent's growing dependence on trade with China.[63] The hack at the AU in Ethiopia demonstrates the vulnerabilities associated with overdependence on China in trade, infrastructure, and technology.

Considering these factors, a patron-client relationship might develop between China and MENA BRI-participating nations. Under such circumstances, Beijing could encourage or even practice "digital authoritarianism" and surveillance abroad. China could take a mostly passive role in the affairs of these client states and intervene through technological means or economic pressure when the client state moves against Beijing or asks for China's assistance politically. This approach could perpetuate cycles of authoritarianism and corruption in client countries. Although not a current reality, signs of this dystopian future of Chinese-exported digital authoritarianism and surveillance have already manifested themselves in Africa, in Iran, and in China itself.

Warnings from Uganda, Iran, and Xinjiang

Beijing has assisted African governments in suppressing political opposition. Events in Uganda and Zambia have demonstrated the possibility of digital authoritarianism under a Chinese-led digital sphere. *The Wall Street Journal* in August 2019 reported that Huawei technicians helped suppress protests associated with Ugandan political opposition figure Robert Kyagulanyi Ssentamu, better known as Bobi Wine, and accessed phones and social media pages of bloggers connected to a pro-opposition news site in Zambia.[64] In both instances, Huawei technicians gave local security forces the technical and hacking expertise that they lacked.

The Ugandan government contracted an Algerian team, including an Algerian expert trained at Huawei's headquarters in Shenzhen, to implement a Huawei surveillance program. Kampala's decision came after the company suggested looking at Algeria's "Huawei's intelligent video surveillance system" that was adopted by Algieria's former long-time president, 'Abd al-'Aziz Bouteflika.[65] In Zambia, Huawei technicians associated with the Zambia Information & Communications Technology Authority (ZICTA) were reportedly helping officials to combat opposition news sites.[66]

In addition to providing technical expertise to suppress political opposition, China looks to establish new global tech norms of digital authoritarianism. That China is creating an international web to spread these norms is made evident by the fact that an Algerian technician was sent to Uganda after having been trained in Shenzhen. The norms and expertise taught in Shenzhen to non-Chinese technicians and officials — including African intelligence officials who attended meetings at the company's headquarters with Chinese government agents[67] — are impacting political movements in Uganda and Zambia. Secondly, China is cementing itself in foreign technology infrastructure and institutions. On top of supporting foreign communication infrastructure, Chinese tech companies like Huawei have built centers and have established themselves in state institutions. For example, the company built 11 monitoring centers in Kampala and based technicians inside state agencies like ZICTA in Zambia.[68] These efforts are then complemented by China's push to dominate the technology industries of these countries. Initiatives like "Smart Zambia" and an agreement with the Ugandan government for Huawei to become the government's "sole information-communications partner"[69] have propagated China's tech norms, ideology, and business as these developing countries become more technologically advanced. The recent events and trends in Sub-Saharan Africa, should serve as a warning to those invested in seeing democracy in the Middle East.

Previously, China was willing to break global norms by helping the Islamic Republic of Iran to suppress political opposition through technological means. Since the exodus of Western tech companies

Photo right: With a security surveillance camera above the teacher's podium, university professor and member of the Uighur minority, Ilham Tohti, lectures in a classroom in Beijing on June 12, 2010. Photo by FREDERIC J. BROWN/AFP via Getty Images

“In addition to providing technical expertise to suppress political opposition, China looks to establish new global tech norms of digital authoritarianism”.

due to the crackdown on the Green Revolution of 2009, Huawei and ZTE filled the gap by partnering with state communication businesses like MTN Irancell and Iranian tech leaders like Zaiem Industries Co.[70] An opaque contract for “managed services” guided Huawei’s operations overseeing parts of MTN Irancell’s network.[71] Huawei’s “managed services” to the majority state-owned Iranian telecom company, and it has been claimed that MTN Irancell ordered Huawei to suspend text messages and block Skype.[72] ZTE also sold to Tehran its ZXMT system, which monitors voice, text messages, and internet communications; it was marketed as a monitoring system and a solution for “lawful interception” to Tehran. [73]Although ZTE and Huawei distanced themselves to an extent after these operations surfaced, Chinese tech companies continue to assist the Iranian government, as shown by Meng Wanzhou’s recent arrest for helping Iran to avoid sanctions. With a newly signed MoU, China will most likely play an increasingly large role in Iran, leading from the digital sphere.

The risky transition to an omnipresent “digital authoritarianism” as seen in Uganda and Zambia is coupled with warnings of a Chinese-style “surveillance state.” The contours of such a surveillance can best be seen in China’s restive Xinjiang province. Located in Western China, Xinjiang Province is home to a Turkic Muslim ethnic group, the Uighurs, who have been at odds with the CCP over cultural, religious, and political rights. Between 2009 and 2014, a series of terrorist attacks by militants from Xinjiang Province turned the issue of Uighur autonomy into a national security imperative for Beijing.[74] In 2014, Beijing implemented a “Strike Hard Campaign against Violent Terrorism” that would eventually lead to the incarceration of up to one million Uighurs in camps, centers, and prisons in the region.[75]

The oppressive measures of the “Strike Hard” campaign were enforced by the creation of a surveillance state of unprecedented magnitude. Ethnic Uighurs in the region were systematically targeted by a vast expansion of police checkpoints equipped with biometric sensors and CCTV to monitor the movements of the population and collect

“Ethnic Uighurs in the region were sytematically targeted by a vast expansion of police checkpoints equipped with biometric sensors and CCTV to monitor movements of the population.

Photo above: Passengers wait at the Hyderabad Junction railway station. Beijing is set to upgrade a 1,163-mile track from Karachi to Peshawar near the Afghan border with an $8 billion loan to Pakistan. Photo Asim Hafeez/Bloomberg via Getty Images Makram

> **Using loans ... along with technology and infrastructure, China attempts to reestablish itself as a global superpower.**

DNA and eye scans. To further track and monitor Uighurs, spyware was sometimes forcibly installed on their smartphones, all vehicles were required to install Beidou (China's version of GPS) and security forces deployed small surveillance drones to assist the coverage of CCTV cameras. The comprehensive digital tracking and surveillance technologies used to suppress the Uighur community could also be used on a global scale. At this point, most "safe city" programs are not developed enough to subdue entire populations as seen in Xinjiang. But with rapidly changing socio-political and economic climates, we could eventually see the expansion of this model beyond China.

China's foreign outreach in the form of BRI and DSR has various facets. Using loans and other economic tools along with technology and infrastructure, China attempts to re-establish itself as a global superpower. Though the hawkish narratives in Washington over the proliferation of Huawei technology and the "debt traps" of BRI have yet to manifest in an international

"The economic and political influence of Beijing will grow wherever Huawei, ZTE, Hikvision, and other Chinese tech companies are primary suppliers."

and systematic way, the examples of Chinese-sponsored digital authoritarianism in Africa, Iran, and Xinjiang should raise alarms in countries considering further, large-scale adoption of Chinese technology or infrastructure projects.

Takeaways

- Shift to More Political Coercion: Beijing has historically been apolitical in its foreign policy since the end of Mao Zedong's regime, but a shift to a larger political role is possible as China becomes a dominant financial, tech, and economic partner in MENA and adopts bolder positions as a superpower.
  - — *No Recourse*: Chinese dominance in these fields could leave BRI-participant countries with little power or ability to counter unwanted Chinese action or espionage, as seen in the silence over the AU headquarters hack.

- The Permanence of 5G Infrastructure: The origin of 5G infrastructure is so critical partially because of the relative difficulty of replacing it once installed. Adopting Chinese 5G technology establishes the buyer as a long-term client. As 5G technology becomes deeply embedded in the global economy, the economic and political influence of Beijing will grow wherever Huawei, ZTE, Hikvision, and other Chinese tech companies are primary suppliers.

- Establishing New Digital Norms: Beijing does not brook domestic political opposition and uses surveillance technology to quash it. China now looks to promote this model in countries like Iran, Zambia, and Uganda and increase its tech influence abroad.
  - — *Cyber Sovereignty*: Through ICT training, deployment of "smart city" surveillance, and digital infrastructure, China seeks to impress upon its trading partners the benefits of tight control over data flows within its borders — strict "cyber sovereignty" — as opposed to Western cyber norms.[76] Although no other nation has implemented structures as sophisticated as China's "Great Firewall" or the surveillance state in Xinjiang Province, would-be digital authoritarians can look to China for guidance.
  - — *Perpetuation of Authoritarian Regimes*: China's main focus is economic expansion rather than political alignment. Thus, Beijing does not care if a regime is authoritarian or corrupt, as long as business remains lucrative. To maintain this business flow, China will assist regimes in maintaining the status quo, e.g., Huawei technicians suppressing political opponent, Bobi Wine, for Uganda's Museveni regime. In the future, regimes such as al-Sisi's in Egypt, Erdoğan's in Turkey, and the Gulf monarchies may bend less to Western demands if they have the backing of China.

- 5G and IoT Impact in Global Cities: With the development of MENA's digital 5G-oriented economies, telecom providers will have a major role in a society driven by data flows. The further urbanization of the Middle East will cement this digital transition and create influential spaces for suppliers like Huawei, especially in megacities like Cairo, Tehran, Lahore, and Karachi.

- Ambiguity and Strength of the PMIC - The multistranded, sometimes informal, and often secret relationships and dealings between party, military, and industry leaders make it difficult to assess the full impact that the PMIC has on China's economic-political progress and ambitions.

- A Spectrum of Outcomes - The level of domestic surveillance and domination of Chinese 5G tech in MENA countries is largely based on the domestic policies of those countries. No BRI participant is inevitably poised to experience digital political suppression like in Kampala or the level of surveillance in Xinjiang. Whether digital authoritarianism emerges will hinge on domestic politics and how much countries are willing to depend on China technologically, financially, and economically.

ENDNOTES

1. Lehman-Ludwig, Anna, "Hikvision, Corporate Governance, and the Risks of Chinese Technology," CSIS, August 6, 2020. https://www.csis.org/blogs/technology-policy-blog/hikvision-corporate-governance-and-risks-chinese-technology

2. Parkinson, Joe; Bariyo, Nicholas; Chin, Josh, "Huawei Technicians Helped African Governments Spy on Political Opponents," Wall Street Journal, August 15, 2019. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

3. Vaswani, Karishma, "Huawei: The story of a controversial company," BBC, March 6, 2019. https://www.bbc.co.uk/news/resources/idt-sh/Huawei

4. Parkinson; Bariyo; Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."

5. Ibid.

6. Feldstein, Steven, "The Global Expansion of AI Surveillance," Carnegie Endowment For International Peace, September 17, 2019. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

7. Prasso, Sheridan, "Huawei's Claims That It Makes Cities Safer Mostly Look Like Hype," Bloomberg, November, 12, 2019. https://www.bloomberg.com/news/articles/2019-11-12/huawei-s-surveillance-network-claims-face-scrutiny

8. Abbas, Syed, "Peshawar gets security boost with Safe City Project," Pakistan Forward, May 5, 2017 https://pakistan.asia-news.com/en_GB/articles/cnmi_pf/features/2017/05/31/feature-01

9. Prasso, "Huawei's Claims"

10. Mukhtar, Imran, "Govt paying on $124m loan since 2011," The Nation, September 18, 2013. https://nation.com.pk/18-Sep-2013/govt-paying-markup-on-124m-loan-since-2011

11. Kelion, Leo, Iqbal, Sajid, "Huawei wi-fi modules were pulled from Pakistan CCTV system," BBC, April 8, 2019. https://www.bbc.com/news/technology-47856098

12. Vaswani, "Huawei"

13. RWR Advisory Group, "A Transactional Risk Profile of Huawei," RWR Advisory Group LLC, February 13, 2018, 13,

14. Lehman-Ludwig, "Hikvision, Corporate Governance, and the Risks of Chinese Technology."

15. RWR Advisory Group, "Risk Profile of Huawei", 14.

16. The Party-Military-Industrial Complex (PMIC) mentioned above may be similar in name to the American "Military-Industrial Complex" (MIC) but they differ in function and structure. The American MIC is a mutually beneficial cycle between lawmakers, industry, and the military, where actors depend on each other on a relatively equal-power basis. The Chinese PMIC has a vertical power relationship. The CCP designates broad policy objectives in which the defense apparatus (PLA and MSS) look to accomplish by then giving specific directives to industry leaders (Huawei, ZTE) and subcontractors. The economic and political benefits of the industry then reach the military, in the form of completed contracts and channels for espionage, and the CCP, through the economic benefits from the industry's commerce and the industry's cooperation with the defense apparatus, directly contribute to the stability of the CCP's regime. In addition, relationships between actors in the complexes are different. In the American MIC, although actors in their career often transition between the military, politics, and industry, their roles are largely set at one time. I.e., a congressman cannot be a lobbyist while serving. In the PMIC, actors' roles between the establishments are more fluid and they can act in more than one at a single time. I.e. party officials are on the boards of state businesses and the military shares a very close relationship with the CCP.

17. RWR Advisory Group, "Risk Profile of Huawei," 11.

18. Greene, Jay, "U.S. Alleges Huawei CFO Hid Ties to Telecom With Iran Business," Wall Street Journal, Dec. 7, 2018. https://www.wsj.com/articles/canadian-prosecutor-lays-out-u-s-allegations-against-huawei-cfo-1544211957?mod=article_inline//&mod=article_inline

19. McNish, Jacquie, "Test to Seek Huawei Executive's Extradition," Wall Street Journal, May 27, 2020. https://www.wsj.com/articles/canadian-judge-rules-u-s-met-legal-test-to-seek-huawei-executives-extradition-11590604033

20. RWR Advisory Group, "Risk Profile of Huawei," 32.

21. Ibid.

22. Ibid. 12.

23. Ibid. 13.

24. Ibid. 15-16

25. Ibid.

26. Ibid. 15-16

27. Powers-Riggs, Aidan, "Covid-19 is Proving a Boon for Digital Authoritarianism," CSIS, August 17, 2020. https://www.csis.org/blogs/new-perspectives-asia/covid-19-proving-boon-digital-authoritarianism

28. Wilson, Naomi, "China Standards 2035 and the Plan for World Domination-Don't Believe China's Hype," Council on Foreign Relations, June 3, 2020. https://www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype

29. Kitson, Andrew, Liew, Kenny, "China Doubles Down on Its Digital Silk Road," CSIS, Nov. 14, 2019. https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/

30. Huawei, "Huawei Helps Tunisia Promote Industry's Digitalization Development," Huawei, July 31, 2018. https://www.huawei.com/en/news/2018/7/Huawei-Tunisia-Digitalization-Development.

31. Huawei, "Huawei executives met with Egyptian prime minister to promote digital ecosystem development in Egypt," Huawei, April 22, 2019. https://www.huawei.com/en/news/2019/4/huawei-egyptian-prime-minister-digital-ecosystem-egypt

32. Huawei, "Tunisia."

33.. Huawei, "Egypt."

34. RWR Advisory Group, "Risk Profile of Huawei."

35. Al-Youm Al-Masry, "Egypt, Huawei sign MoU for cloud computing, AI networks," Egypt Independent, February 26, 2019. https://egyptindependent.com/egypt-huawei-sign-mou-for-cloud-computing-ai-networks/

36. Ghafar, Abdel Abdel, Jacobs, Anna L., "Beijing calling: Assessing China's growing footprint in North Africa," Brookings, September 23, 2019.

37. Ibid.

38. Page, Jeremy, O'Keeffe, Taylor, Rob, "America's Undersea Battle With China for Control of the Global Internet Grid," Wall Street Journal, March 12, 2019. https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466

39. Ghafar, Jacobs, "Beijing calling."

40. Page, O'Keefe, Taylor, "America's Undersea Battle."

41. Ibid.

42. Diagram, http://www.peacecable.net/

43. Ibid.

44. Verma, Saurabh, Banik, Gourab, "State of 5G in the Middle East: Review and Future Outlook," International Teletimes, February 2020. https://teletimesinternational.com/2020/state-of-5g-middle-east/.

45. Ibid.

46. Hillman, Jonathan, McCalpin Maesea, "Watching Huawei's 'Safe Cities,'" CSIS, November 4, 2019. https://www.csis.org/analysis/watching-huaweis-safe-cities.

47. El Kadi, Tin Hinane, "The Promise and Peril of the Digital Silk Road," Chatham House, June 6, 2019. https://www.chathamhouse.org/expert/comment/promise-and-peril-digital-silk-road.

48. Ibid.

49. Blanchette, Hillman, "China's Digital Silk Road."

50. El Kidi, "The Promise and Peril of the Digital Silk Road."

51. Blanchette, Jude, Hillman, Jonathan "China's Digital Silk Road after the Coronavirus," CSIS, April 13, 2020. https://www.csis.org/analysis/chinas-digital-silk-road-after-coronavirus.

52. Hurley, John, Morris, Scott, Portelance, "Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective," Center for Global Development, March 2018. 16. https://www.cgdev.org/sites/default/files/examining-debt-implications-belt-and-road-initiative-policy-perspective.pdf

53. Ibid. 20

54. Ibid. 17

55. Kanwal, Gurmeet, "Pakistan's Gwadar Port: A New Naval Base in China's String of Pearls in the Indo-Pacific," CSIS, April 2, 2018. https://www.csis.org/analysis/pakistans-gwadar-port-new-naval-base-chinas-string-pearls-indo-pacific.

56. Ghafar, Jacobs, "Beijing calling."

57. Molavi, Afshin, "China's Global Investments Are Declining Everywhere Except for One Region," Foreign Policy, May 16, 2019. https://foreignpolicy.com/2019/05/16/chinas-global-investments-are-declining-everywhere-except-for-one-region/.

58. Ghafar, Jacobs, "Beijing calling."

59. Molavi, "China's Global Investments."

60. McManus, Allison, "Egypt And China's Telecoms: A Concerning Courtship," Power 3.0, February 20, 2020. https://www.power3point0.org/2020/02/20/egypt-and-chinas-telecoms-a-concerning-courtship/.

61. Vaswani, "Huawei."

62. Ibid.

63. Ibid.

64. Parkinson, Bariyo, Chin, "Huawei Technicians"

65. Ibid.

66. Ibid.

67. Ibid.

68. Ibid.

69. Ibid.

70. Stecklow, Steve, Fassihi, Farnaz, Chao, Lorretta, "Chinese Tech Giant Aids Iran," Wall Street Journal, October 27, 2011. https://www.wsj.com/articles/SB10001424052970204644504576651503577823210.

71. Ibid.

72. Ibid.

73. Muncaster, Phil, "ZTE winds down Iran biz after espionage claims," The Register, March 28, 2012, https://www.theregister.com/2012/03/28/zte_iran_sanctions/

74. Polyakova, Alina, Meserole, Chris, "Exporting digital authoritarianism: The Russia and Chinese models," Brookings, August 2019. https://www.brookings.edu/research/exporting-digital-authoritarianism/

75. Ibid.

76. Ibid.

77. Ibid.

Cover Photo: A 5G sign is seen during the Mobile World Congress (NWC) Shanghai 2021 at Shanghai New International Expo Center on February 24, 2021 in Shanghai, China. (Photo VCG/VCG via Getty Images)

ABOUT THE AUTHOR

Thomas LoCoco Blaubach is a Graduate Fellow with the Cyber Program at MEI, and a MA Candidate at the University of Chicago's Committee on International Relations. He received his B.A. in International Studies and Political Science, with certificates in Middle Eastern and African Studies from the University of Wisconsin-Madison. His research interests include 5G technologies in the context of geostrategic competition and regime use in the Middle East.

ABOUT THE MIDDLE EAST INSTITUTE

The Middle East Institute is a center of knowledge dedicated to narrowing divides between the peoples of the Middle East and the United States. With over 70 years' experience, MEI has established itself as a credible, non-partisan source of insight and policy analysis on all matters concerning the Middle East. MEI is distinguished by its holistic approach to the region and its deep understanding of the Middle East's political, economic and cultural contexts. Through the collaborative work of its three centers — Policy & Research, Arts & Culture, and Education — MEI provides current and future leaders with the resources necessary to build a future of mutual understanding.

MEI
Policy Center

MEI@75
Peace. Prosperity. Partnership.

WWW.MEI.EDU