中国简报 China Brief
a journal of analysis and information
The JAMESTOWN FOUNDATION

VOLUME 18 • ISSUE 13 • JULY 24, 2018

IN THIS ISSUE

Censorship, Geopolitical Time Bombs, and China's Islamophobia Problem

By Matt Schrader

China has a serious and worsening Islamophobia problem. While relations between China's Muslim minorities and its Han majority have been fraught since 2009's deadly inter-ethnic riots in the far western city of Urumqi, recent years have seen the normalization of online hate speech directed at Muslims. The rise of Islamophobia inside China is a product both of government action, and of the government's failure to act. Commentary on the recent death of a prominent Muslim leader in the western province of Qinghai highlights the extent to which the situation has deteriorated, and suggests the ways in which China's warped online discourse could blunt its efforts to build influence and win friends in countries across the Muslim world.

The Death of an Imam

On July 16, Ma Changqing (马长庆), a prominent imam and a leader among the Muslims of China's far western province of Qinghai, passed away at the age of 83 (Xinhua, July 19). Ma was also a member of the China People's Political Consultative Congress (CPPCC), a consultative legislative body used by the Chinese Communist Party (CCP) to understand, engage with, and co-opt those parts of Chinese society not under direct Party control. Ma had a brief brush with national notoriety in 2014, when, during a CPPCC plenary session, he failed to stand during a moment of silence meant to commemorate the victims of a fatal knife attack by homegrown Islamic terrorists (China News, March 10 2014).

Although it later emerged that Ma may have failed to stand because of age-related infirmities—he reportedly attended the session in a wheelchair—the supposed slight was neither overlooked nor easily forgotten by many in

China (Wen Wei Po, March 7). When news of large crowds attending Ma's funeral to pay their respects began to spread on China's internet, a disturbing proportion of responses contained shockingly blunt hate speech.

"Filthy swine … it's good he's dead!", read one (the Islamic prohibition against pork makes pig references one of Chinese Islamophobes' favorite forms of insult). "Go see Allah, and bring some of your followers with you!", said another (Weibo, June 18). Another netizen, reacting to videos of crowds at the funeral, said, "Are those 200,000 [Muslims] people? They look more like time bombs to me."

Ma was, by all accounts, a compliant member of the party-state structure. That netizens would attack him and his fellow Muslims on such slight grounds reveals the degree to which the CCP's campaign to stamp out Islamic terrorism in China's far west has turbocharged latent xenophobic tendencies.

That campaign has seen hundreds of thousands of Uighurs—a Muslim minority group—rounded up and interred in "reeducation camps" meant to purge them of "extremist" behaviors (China Brief, May 15). It has also increasingly affected the Hui—China's other large Muslim minority—despite Hui communities having co-existed peacefully alongside China's Han majority throughout the country for hundreds of years (AP, April 10 2017). At the same time it has ramped up this campaign of coercion and control, the CCP has singularly failed to publicly condemn Islamophobic rhetoric engendered by state media's tendency to associate China's Muslim minorities with terrorism and extremism (Asian Journal of Communication, March 28).

Fostering Islamophobia

This shortfall exists because, in the CCP's eyes, the real issue is not the undue harshness of its policies, or Islamophobia among China's Han majority, but rather the inability of some of China's Muslims to hew to acceptable, state-sanctioned, "modern" expressions of Islamic faith.

Even specialists on Islamic culture publicly toe this line. For example, at a high-level Sino-Arab dialogue last year Xue Qingguo (薛庆国), a professor of Arabic at one of Beijing's top universities and secretary of the China Arabic Literature Studies Association, delivered a speech in Arabic on "Extremism and Islamophobia" to officials from 16 majority-Arab countries (Baidu Zhidao; Hongse Guxiang, September 4 2017). In his speech, Xue lauded the achievements of Islamic civilization, and admitted that "Islamophobia has gotten some traction in China in recent years". But he placed the blame for this squarely on Chinese Muslims themselves, condemning those who would "distort a civilization that produced significant advances in all fields of scientific endeavors, a civilization steeped in humanism, into a mass of trivial minutiae about beards, veils, and clothing".

Xue's speech is emblematic of a party-state that preaches ethnic unity, but abhors any self-reflection that could be interpreted as criticism of the party line, or as support for greater political autonomy for China's minorities. The problem is exacerbated by the way the CCP's online censorship apparatus functions.

China's censors take their cues from party leaders, scrubbing the internet of views that leaders find unacceptable, promoting those they espouse, and leaving untouched those about which leaders have expressed no opinion. The party-state's failure to strongly condemn Islamophobia thus places anti-Islamophobic voices at a disadvantage in public debate, since a vocal defense of China's Muslims could also be read as implicit criticism of the government's failure to speak out on their behalf. And since CCP leaders brook no criticism of their hardline policy towards Muslim minorities, all but the most anodyne expressions of support for China's Muslim citizens have a difficult time gaining purchase in wider discourse. By the same token, the censorship bureaucracy interprets top leaders' failure to condemn vile expressions of Islamophobia as a tacit sanction for their existence, allowing Islamophobic views to circulate more or less freely, and to go largely unchallenged.

The Real Time Bomb

While China's domestic politics offer little prospect for change, external factors could hold out more hope. If China's treatment of its Muslims minorities caused its ties with Gulf countries to deteriorate, it might, for example, prompt the CCP to rethink how it shapes the public conversation around Muslims—for China, the Gulf is an important market for weapons, and an important supplier of oil.

But despite the worsening situation in China's far west, there is little indication that Gulf rulers or their publics will turn against the PRC. Gulf countries recently rolled out the welcome mat for Xi Jinping during his tour of the region, and were generally positive towards Xi's call for China to serve as a "keeper of peace and stability in the Middle East" during a speech before the Arab League—suggesting a possible willingness on Xi's part for China to take on a larger security role in the region (South China Morning Post, July 10).

However, if the United States' experience is any guide, a superpower's deepening involvement in Middle Eastern politics can complicate ties with the Muslim world in unexpected ways. For China, the real time bomb may not be the way it treats Muslims at home, but how that treatment is perceived abroad.

Matt Schrader is the editor of the Jamestown China Brief. Follow him on Twitter at @tombschrader.

***

Beijing Bids to Extend its Global Clean Energy Lead

By Ashley Feng and Sagatom Saha

China has firmly established itself as the world's dominant manufacturer of clean energy technologies, having been the largest producer of solar photovoltaic cells and modules for at least a decade (Energy Policy, February 2011). The country now accounts for half of all solar manufacturing (International Energy Agency, October 4, 2017) globally and leads wind turbine (Renewable Energy Policy Network for the 21st Century, 2018) and lithium-ion battery production as well (Bloomberg, June 28, 2017).

As a result, Beijing is well-poised to benefit economically and strategically from the global shift toward clean energy technologies as countries—particularly those in the developing world—seek to decarbonize their economies and reduce pollution without sacrificing growth. Beijing is seeking to capitalize on this positioning by investing in and acquiring foreign power companies overseas, including a recent, high-profile attempt by a large Chinese power generation company to purchase outright Energias de Portugal, Portugal's largest utility company. At a time when protectionism is on the rise globally, these overseas acquisitions may provide Beijing a global foothold in the growing offshore wind market, as well as backdoor cyber-access to foreign grids, and—most importantly—the ability to influence other countries' power generation decisions in ways that benefit Chinese own firms and national clean energy strategy.

Sun Belts and Roads

China's quest for clean energy domination has been enshrined in national strategy—in 2006, the Chinese government released the Medium- to Long-Term Plan for the Development of Science and Technology, identifying energy as priority for technological development, as well as economical, efficient, and clean energy as a frontier technology that the country should focus on (State Council, February 9, 2006). The government continued its support for energy technology in the Twelfth Five-Year Plan, covering the years 2011-2015, then put its interest in green energy front and center starting in 2015 with Made in China 2025 (State Council, May 19, 2015). Beijing has promised so much support to clean energy companies that, by 2020, the government will owe companies $30.2

billion (Reuters, October 8, 2017) in unpaid subsidies—for comparison, the PRC government paid out $25.4 billion in renewables subsidies in 2017 (World Economic Forum, May 22). Government support for Chinese clean energy technology paid off—China became the world's largest exporter of environmental goods and services in 2012 (Bloomberg, December 5, 2017).

The ramping up of Made in China 2025 will coincide with the continued rollout of the Belt and Road Initiative (BRI), China's amorphous foreign policy plan to connect continents through development and infrastructure projects. BRI has also served a vehicle for China to increase its exports in the advanced clean energy sector. According to the Ministry of Industry and Information Technology's green industry development plan, China should "grasp the opportunity of BRI to comprehensively promote industrial green development," and actively participate in the investment, construction, and operation of new energy projects, including wind, solar, and nuclear energy, and power grids (Ministry of Industry and Information Technology, July 18, 2016).

Despite a broader slowdown (Radio Free Asia, April 23) in outward foreign direct investment (FDI), Chinese investment in BRI countries has been growing—the value of acquisitions in those countries surpassed 2016 levels by August 2017 (Reuters, August 15, 2017). Clean energy has been a particular bright spot. By one estimate, China's large international clean energy projects and takeovers totaled more than $44 billion in 2017, compared to $32 billion in 2016 (Carbon Brief, January 9).

Investments abroad could allow China to export its domestic overcapacity in clean energy industries to other countries, where it can win market share while walking back expensive domestic policy support for clean energy. In many cases it is a question of survival for the companies involved; they have to secure new projects abroad to stay afloat as China's National Energy Administration has announced plans to cut expensive subsidies for solar energy (Green Tech Media, June 6). As part of this push, Chinese companies, both private and state-owned, are buying larger stakes in power companies that put generation assets onto national grids such as Energias de Portugal.

Three Gorges in Portugal

The latest step in China's overseas clean energy plans has been the attempt by Three Gorges Corporation (CTG), a state-owned enterprise and one of the world's largest energy companies, to take over Energias de Portugal (EDP), Portugal's largest utility, as part of its Belt and Road corporate strategy (China Three Gorges, July 29, 2017). This would allow CTG to access new technologies and hard-to-reach markets—EDP serves almost 10 million clients across North America, Europe, and South America, and runs more than 205,000 miles of transmission lines globally (South China Morning Post, May 12).

CTG bought its first stake in EDP in 2011 amid the eurozone sovereign debt crisis, paying $2.5 billion for 21.4 percent of the company (Publico, December 22, 2011). Now, seven years later, CTG is looking to take over the entire company, whose portfolio includes wind, hydro, and solar power projects in twelve countries in Europe and the Americas (Energias de Portugal). At the end of 2017, EDP had businesses in forty countries, with a total contract value of $15 billion (Bloomberg, May 12). Through this possible acquisition, China would be able to gain on-the-ground experience and technical skills, as well as increased access to power markets in Europe and the Americas.

Although EDP rejected CTG's initial offer of $3.83 per share, along with a $8.48 per share offer for the purchase of EDP's renewable subsidiary alone, the company has indicated that it is still open to acquisition by CTG for a higher price (South China Morning Post, May 12, 2018). In the meantime, Portuguese Prime Minister Antonio Costa has indicated that he will not interfere with the deal (South China Morning Post, May 12, 2018).

Because of EDP's operations of wind farms in the United States, CTG's takeover would typically require review by the Committee on Foreign Investment in the United States (CFIUS), which may be strengthened to more closely scrutinize Chinese investment in critical infrastructures and technologies. However, CTG may convince other European utilities to buy EDP's US renewables portfolio, avoiding CFIUS while still expanding its business in other fast growing renewables markets (Reuters, June 26). It has since been revealed that the State Administration of Foreign Exchange, an arm of the People's Bank of China, owns 5 percent of EDP, giving Beijing even more leverage in negotiations (Financial Times, June 19).

CTG's bid to take over EDP, a company that generates, supplies, and distributes electricity globally, is not an isolated case. Rather, multiple Chinese SOEs have developed a habit of buying stakes in power companies, especially those in debt-laden countries. Amid Brazil's economic downturn in 2017, China's State Grid, the largest utility in the world, bought a controlling stake in CPFL Energia, Brazil's third largest utility (China Daily, September 1, 2017). It has employed the same tactic in Europe's more financially-vulnerable countries including Greece, Italy, and Portugal, acquiring ownership stakes in power grid companies (Xinhua, June 21, 2017).

Buying In to Offshore Wind

The EDP acquisition reflects a larger pattern of purchases by Chinese SOEs, not only in foreign power grids, but in foreign companies with large offshore wind portfolios and technical know-how. Although China leads in nearly all other clean energy technologies, it lags in offshore wind development.

Beijing has ambitious plans to increase its offshore wind capacity, but has so far lacked the technical capacity to achieve them (Reuters, June 24, 2016). CTG is still developing its first offshore wind farm, even as dramatic drops in the levelized cost of offshore wind energy have made the technology accessible elsewhere (China Three Gorges, December 30, 2017).

In this respect, EDP would be a valuable acquisition—its renewables arm installed the fourth-most wind capacity globally in 2017, and has offshore wind projects under development in the United Kingdom and France (Energias de Portugal, June 2018). In the long term, the company aims to become a leading offshore wind company globally and is developing innovative new technologies like floating wind farms. If the acquisition were to go through, EDP itself has flagged the Chinese domestic offshore wind market, where CTG plans to play an active role, as a potential area for growth (China Daily, February 9).

Other Chinese state-owned companies have been buying into companies driving offshore wind development forward—in December 2017, China Resources, a state-owned Chinese company, bought a 30 percent stake in the Dudgeon offshore wind farm in England from Statkraft, a Norwegian company, in an explicit bid to improve Chinese knowledge and experience with the technology (South China Morning Post, December 19, 2017).

Concerns: Innovation, Cybersecurity, and Control

The fact that China is strengthening its knowledge of offshore wind technology is not a problem in and of itself. China's ability to produce cheap solar panels helped fuel solar's explosive growth globally. However, its domination of the solar industry has also resulted in incremental improvements that have stifled demand for and the ability to invest in more disruptive technologies in the energy sector (Vox, April 18, 2016).

PRC companies acquiring positions in foreign power grids also brings cybersecurity risks associated with grid infrastructure, especially as that infrastructure becomes more advanced.

Power grids are becoming increasingly intelligent and networked, potentially allowing those with access to not only disrupt electricity supply, but to also conduct espionage through detailed monitoring of power use. Advanced behind-the-meter technologies can track information as granular as opening a refrigerator or turning on a shower, allowing anyone with access to monitor private activities (Council on Foreign Relations, June 2018). Countries will likely have a difficult time maintaining secrecy in critical infrastructure like military installations if Chinese companies control the power systems that supply them.

China's focus on acquiring electric companies overseas will also make it easier to shape the global clean energy market to its liking. An outsized role in a country's power sector will give China the ability to influence decisions regarding that country's future generation mix in a way that could benefits PRC state-directed firms.

For example, State Grid's large investments in Brazil have allowed it to showcase high-voltage transmission lines, which allows electricity to travel over longer distances with lower losses to resistance (Global Energy Interconnection Development and Cooperation Organization, October 13, 2017). Beijing aims to popularize and export this technology globally, creating large regional country-spanning power grids (South China Morning Post, January 21, 2016). Through their foreign power-sector acquisitions, Chinese companies are directing procurement toward specific clean technology products that Beijing aims to deploy, maintaining and eventually strengthening China's broad state-directed influence in the market. If CTG's acquisition of EDP goes through, Portugal may find itself acquiescing to the needs of Chinese state-owned enterprises before those of its own national energy strategy.

Ashley Feng is a research associate at the Council on Foreign Relations, focusing on Chinese foreign policy. She can be found on Twitter @afeng79. Sagatom Saha is an independent energy policy analyst based in Washington, D.C. His writing has appeared in Foreign Affairs, Defense One, Fortune, Scientific American and other publications.

***

Taiwan's Emerging Push for "Cyber Autonomy"

By Philip Hsu

On May 11, Taiwan's Legislative Yuan passed the Cybersecurity Management Law, Taiwan's first national cybersecurity law (iThome, May 22). This law, which mandates cybersecurity requirements for Taiwan's government agencies and operators of critical infrastructures, represents the latest initiative in the Tsai administration's push for cyber security under the policy "Cyber Security is National Security." As part of this push, the administration is also working to develop Taiwan's indigenous cybersecurity industry through a policy of "cyber autonomy" (资安自主).

The cyber threats to the island are substantial. Taiwan has been ranked as one of the top targets of advanced cyber attacks in the world, mainly from state-initiated or state sponsored Advanced Persistent Threats, or APTs (FireEye, January 14, 2014). These APTs conduct cyber espionage against government agencies and corporate entities in Taiwan, most of which can be traced back to China. In April, the Department of Cybersecurity of Taiwan's Executive Yuan revealed that China's "internet army" accounted for 288 successful attacks against Taiwan's government agencies in 2017 (Liberty Times, April 5). Last March, the Director of Taiwan's National Security Agency admitted to the Legislative Yuan that China's cyber penetration of Taiwan's networks is "worse than before" (Liberty Times, March 9, 2017).

Cyber Autonomy and National Security

Given this backdrop, it may come as no surprise that Taiwan's push to support its cybersecurity industry through cyber autonomy has a national security bent. In one sense, the word autonomy (自主) is connected to Taiwan's ongoing efforts at "defense self-reliance" (国防自主) to reduce the island's reliance on foreign arms. Such efforts to indigenously design and build military jets, missiles, and armored vehicles have been ongoing for decades, but the Tsai administration has made self-reliance a central component of its defense policy, most notably including Taiwan's new plans to deploy indigenously developed attack submarines.

A national defense-centric interpretation of cyber autonomy, a response to an uncertain environment for international cyber technology transfers and the clear threat from China, is one impetus for building up an "autonomous" domestic cybersecurity industry. New Frontier Foundation, a Democratic Progressive Party (DPP) think tank, first described cyber security as one of Taiwan's "Core Defense Industries" along with the aerospace and shipbuilding industries in its Blue Paper No. 7 from 2014 (New Frontier Foundation, October 2, 2014). It argued that Taiwan's Ministry of Defense should assist in the development of Taiwan's cybersecurity industry and create a local market for cyber products by opening up its cybersecurity contracts to small and medium-sized cyber companies.

President Tsai herself joined the effort to enlist the private sector in Taiwan's national defense efforts as early as 2016. As a keynote speaker at the Hacks in Taiwan Conference (HITCON), an annual gathering of Taiwan's hacker community, she highlighted how the "hacker spirit" could aid in her government's goal of elevating cyber security to a matter of national security (iThome, December 1, 2016). In particular, Tsai expounded upon her government's policy of encouraging indigenous cybersecurity innovation by creating a domestic market for cybersecurity services, including plans to recruit the private sector to bolster the capabilities of Taiwan's military cyber forces. At a cybersecurity awareness event hosted at the Presidential Palace in Taipei last December, Tsai again declared that the power of Taiwan's white hat hackers should be "unleashed" to drive growth and innovation in Taiwan's cybersecurity industry, a clear nod to cyber autonomy (China Times, December 11, 2017).

The national defense-oriented interpretation of cyber autonomy acquired more definition through the efforts of Taiwan National Security Council Member Lee Der-tsai, who has become one of the primary spokespersons for the Tsai government's cybersecurity initatives. Following President Tsai's example of promoting cyber autonomy policy positions at major cybersecurity conferences, Lee listed promoting "defense-based autonomous cybersecurity research" as one of the government's strategic goals at the March 2017 Taiwan Cyber Security Summit (iThome, March 16, 2017). He further compared Taiwan's situation with that of Israel, another victim of constant cyber attacks that promotes its domestic cybersecurity industry through government policy, including subsidies and extensive cooperation between the private cybersecurity sector and military.

A Different Interpretation of Cyber Autonomy

Yet by the time of the Taiwan Cyber Security Summit a year later in March 2018, another interpretation of cyber autonomy may have gained traction. In his keynote at the Summit, Lee again referenced the development of the cybersecurity industry through national defense projects. However he indicated that these efforts would henceforth be led by Taiwan's Ministry of Economic Affairs (MOEA), as that agency begins to take a leading role in developing Taiwan's cybersecurity industry as a whole (Liberty Times, March 14).

The basis for MOEA's leading role in a cyber autonomy policy stems from the National Cyber Security Program of Taiwan for 2017 to 2020, which was released in November of 2017 by the Executive Yuan's National Information and Communication Security Taskforce, or NICST (NICST, November 14, 2017). NICST is an inter-agency task force

founded in 2001 at the behest of Taiwan's National Security Council to secure Taiwan's government networks and critical infrastructure.

MOEA has long been responsible for executing specific policies and goals related to "cybersecurity industry autonomy" (资安产业自主). This phrase first appeared in the 2013 to 2016 National Cyber Security Program in reference to boosting Taiwan's indigenous cybersecurity research and competitive capabilities (NICST, February 2, 2016).

MOEA Takes Over

As has long been the case, MOEA is focused on non-defense efforts to promote the development of Taiwan's cybersecurity industry. One of its main related initiatives is the propagation of security standards for mobile applications developed in Taiwan. Though MOEA's Industrial Development Bureau (IDB) had supported these efforts since at least 2015, the standards gained traction in 2017 when IDB began promoting these standards for adoption by Taiwan's government agencies and banks (MOEA, February 22).

IDB has similarly promulgated domestic IoT security standards for internet-connected video surveillance systems. In addition, it plans to open up the testing of domestic cybersecurity industry products on critical infrastructures and other selected industries in 2018, to allow domestic companies to "gain product experience and build skills" (MOEA, February 22).

IDB also sponsored the Cyber Taiwan Expo at this year's Taiwan Cyber Security Summit. The expo included "autonomous research and skills exhibition" show booths for 38 domestic cybersecurity companies to demonstrate their capabilities to expo attendees (China Times, March 16). Participating companies presented to government officials, including Taiwan's Vice President Chen Chien-jen.

Taiwan's National Cyber Security Program for 2017 to 2020 explicitly states that MOEA is to "develop the domestic cybersecurity industry ecosystem by connecting it with national defense needs" (NICST, November 14, 2017). Given the innate vulnerability of mobile, surveillance, and critical infrastructure systems, the Ministry's efforts so far to elevate the value of Taiwan's cybersecurity industry do appear to be aimed at improving national security and fulfilling President Tsai's broader policy of cyber security as national security. However, it remains to be seen how or whether the ministry will fulfill its mission of bringing together private industry and national defense needs in the military sector.

National Defense Still a Focus

In a recent poll of 374 public agencies and industries, general public and private sector spending on cybersecurity services in Taiwan grew by seventy-three percent between 2017 and 2018, led by the financial and services sectors (iThome, April 4). Though increased private sector investment in cyber security services is a promising development, Taiwanese companies may have difficulty competing with better-resourced multinational cybersecurity companies, a challenge that has been highlighted in both the DPP's aforementioned Blue Paper No. 7 and Taiwan's National Cyber Security Programs. In this regard, defense-based cybersecurity spending may be an attractive option for developing Taiwan's homegrown cyber industry, since foreign firms are likely to be excluded from competing for national defense contracts.

Connecting Taiwan's cybersecurity industry with its military will require the participation of Taiwan's Ministry of Defense (MoD). For its part, the Ministry is actively employing private sector cybersecurity firms in defense projects as part of its defense self-reliance efforts, including prioritizing the use of homegrown cyber products and services. In

addition, the Executive Yuan remains committed to developing Taiwan's cybersecurity industry through building its connections with national defense. It now considers Taiwan's cyber industry as part of the national defense component of the $3.6 billion "Five Plus Two" economic development plan that the Tsai administration has proposed to develop new industries and small to medium-sized businesses (Executive Yuan, May 4; AmCham, May 8, 2017).

These funds will prove crucial to achieving the Executive Yuan's goal of doubling the size of Taiwan's cybersecurity industry from $1.3 billion currently to more than $2.6 billion by 2025. If private sector cyber security is effectively matched to national defense needs, then Taiwan's military spending will also come into play. The Tsai administration has plans to increase military spending to $12.6 billion by 2025, from the current level of $10.9 billion, or about 1.84% of GDP (Taiwan News, January 12). While this level of spending remains below the 3% of GDP proposed by DPP Blue Paper No. 7 in 2014, it does highlight investment in cyber security and continued emphasis on the defense self-reliance project.

Conclusion

The Tsai administration has delivered support and promised additional funding for cyber autonomy. So far these efforts have gained some momentum on multiple tracks led by the Executive Yuan, MOEA, and MoD. The ultimate goal of these initiatives is to simultaneously help Taiwan's cyber firms become globally competitive and defend against the Chinese and other cyber threats, which will require both the whole-of-market approach of MOEA and targeted industry approach of MoD.

Cyber autonomy could provide a springboard and help develop a local market for Taiwan's cybersecurity industry, but the reach of MoD's cyber funding may be limited in the market, and Taiwan's cyber firms will still face tough competition internationally. Both Taiwan's public and private sector have suggested that Taiwan's unique threat environment gives rise to a competitive autonomous industry through increased expertise on a variety of cyber tactics, techniques and procedures, but there is uncertainty about whether this environment is relevant to the rest of the world's cyber needs.

Finally, defending against the concerted cyber challenge from China will require a determined and organized inter-agency response. If successful, mobilizing Taiwan's private cybersecurity sector in defending government agencies, private companies, military and other sectors of Taiwan's "digital territory" (数位国土) will be a good start.

Philip W Hsu is a Technology Consultant at FTI Consulting and a graduate of Columbia University's School of International and Public Affairs. He tweets @philipwhsu.

***

The Belt and Road Initiative: A Road to China's World Cup Dreams?

By Emily Weinstein

Since its inception at a 2013 speech in Kazakhstan, CCP General Secretary Xi Jinping has touted his One Belt One Road (OBOR) initiative as a platform for "peace and cooperation, openness and inclusiveness, mutual learning and mutual benefit," through economic and cultural exchange. (State Council Information Office, May 4, 2016). Sports tourism, especially that surrounding soccer, has been an important albeit lesser-known component of OBOR. Chinese media have argued that the sports industry is growing into one of China's most dynamic sectors, as Chinese entities have begun to invest heavily in international teams, arenas, and events (Xinhua, April 2, 2016).

A number of paramount Chinese leaders have shown interest in soccer; however, none have expressed it to the same degree as Xi Jinping. Since Xi's ascension to power, China has seen a soccer reawakening. In 2014, Xi announced his three World Cup dreams: "qualifying for the World Cup," "hosting the World Cup," and "winning a World Cup title" (China Soccer Observatory, April 5, 2018). Since this announcement, Xi has been working to utilize soccer as a tool for relationship building and diplomacy with other soccer-fanatic countries (People's Daily, June 19, 2014).

Throughout the 2018 FIFA World Cup in Russia, China has worked to ensure it remains in the international spotlight, despite its national team having not made the cut for this year's competition. US companies such as Castrol and Johnson & Johnson backed out of FIFA sponsorships for this year's cup, citing concerns surrounding not only a 2015 FIFA corruption scandal, but also increased tension between the US and Russia. However, where the US saw potential conflict, China saw opportunity, and has treated the World Cup as one of the most significant marketing opportunities for Chinese brands this year, with a diversity of Chinese firms supporting this year's Cup (Lanxiong Sports, March 6, 2018). While commercial rationales are undoubtedly at work, Chinese firms' eagerness to demonstrate their support also underscores their support for Xi Jinping's World Cup and OBOR aspirations, thus demonstrating China's understanding that soccer—in addition to cultural exchanges, loans and infrastructure projects—may be another way to win hearts and minds in other countries.

FIFA's PRC Bailout

The 2018 World Cup has been a difficult one for FIFA sponsorship. A number of well-known Western companies chose to part ways with the organization following the arrest of several high-level FIFA officials in the midst of a corruption scandal in 2015 (BBC News Chinese, June 14, 2018). FIFA sponsors continued to drop left and right as tensions between Russia and the United States worsened in 2016; as a result, the organization's advertising revenue dropped by $170 million from 2015-2018 compared with the three-year period prior (Nielsen, June 11, 2018).

Salford University Professor Simon Chadwick noted that the lack of demand from potential Western sponsors left FIFA desperate for cash (Xinhua, June 14, 2018). The organization found itself with a $369 million net loss for 2016 and a shortage of corporate sponsors for the 2018 World Cup (Deutsche Welle, July 4, 2017). This dearth, however, presented Chinese entities with an opportunity for a cost-effective way to promote their brands globally.

The 2018 FIFA World Cup has arguably presented China with its largest branding platform since the 2008 Summer Olympics, as it provides Chinese companies with the opportunity to share airtime with Western powerhouses like Coca-Cola and Adidas. The new crop of PRC-based World Cup sponsors invested $835 million in advertising for this summer's World Cup, accounting for 35 percent of total sponsorship deals. Both Wanda Group (万达集团), a large real estate developer, and Mengniu (蒙牛), one of China's largest dairy brands, are among the biggest sponsors of this year's Cup. In the absence of a Chinese soccer team, official Chinese media outlets have referred to these sponsors such as Mengniu, Hisense and Wanda Group as "China's National Team" in this year's World Cup (CCTV, December 25, 2017).

FIFA sponsors benefit from a number of exclusive advantages, including product category exclusivity, the use of official FIFA logos in conjunction with their own brand logos, and brand exposure at World Cup matches and events, as well as FIFA publications and the official FIFA website (Journal of Contingencies and Crisis Management, September 2016). In 2016, Wanda spent $150 million on Tier 1 sponsorship; Mengniu and two other companies opted for Tier 2 sponsorship, accounting for 60 percent of the total Tier 2 investments (新芽 New Seed, June 9, 2018). More specifically, the Chinese dairy product manufacturer and distributor, Mengniu, has made significant moves to position itself at the forefront of World Cup advertising. In addition to becoming the "official drinkable yogurt" of the 2018 World Cup (Outlook News [前瞻网], June 8, 2018), the company announced in February 2018 that it had signed Argentinian soccer superstar Lionel Messi as its new brand ambassador (Yutang Sports, February 25, 2018).

Unlike Mengniu, Wanda Group has already established a worldwide presence. Instead of using the World Cup for purely business tactics, Wanda Group is looking to export elements of soft power such as "public interest and cultural self-confidence". Wanda Group's leadership has also discussed playing the "public welfare card" in order to create a positive global image of Chinese enterprises and highlight social responsibility (People's Daily, June 20, 2018). The Chinese government over the past decade has pushed for stronger and more transparent corporate social responsibility (CSR), especially in cases involving Chinese enterprises operating abroad (Berkeley Journal of International Law, 2010). Since Wanda Group has come under recent scrutiny for financial misdoings in both overseas and domestic projects (South China Morning Post, August 2017), the company may be using the World Cup in part as a face-saving measure, and to demonstrate its ongoing support for Xi Jinping's soccer ambitions on the largest stage imaginable.

OBOR and Sports Tourism

In July 2017, the State General Administration of Sports (国家体育总局), in conjunction with China's State Administration of Tourism (国家旅游局), released the 'Belt and Road' Sports Tourism Development Action Plan ('一带一路'体育旅游发展行动方案) aimed at incorporating the central themes of China's OBOR initiative into the country's nascent sports tourism industry (State General Administration of Sports, July 7, 2017). More specifically, China hopes to use sports tourism as a way to localize its OBOR ambitions. The Action Plan states that Chinese entities should encourage countries along the Belt and Road region to develop distinctive sports tourism models based on their individual resources and market conditions. Once those models have been sufficiently established, the Plan advocates integration of international and domestic (Chinese) forces, forming "an open and mutual-beneficial sports tourism development model." (State General Administration of Sports, July 7, 2017).

China's intent to integrate sports tourism and OBOR has been on display at a number of soccer exhibitions held in China over the past year. For instance, on April 6, 2018, the China Football Association (中国足球协会) hosted its Second Annual "Belt and Road" Cup ("一带一路" 杯) in Hainan, inviting teams from China, Azerbaijan, the Czech Republic and Hungary to compete in friendly matches. The Cup was founded on the eve of the 2017 "Belt and Road" International Cooperation Forum and is designed to use soccer to establish people-to-people exchanges between China and other OBOR countries. At the tournament's opening ceremony, Deputy Mayor of Haikou Ren Qinghua spoke of the strategic significance of Haikou, one of China's most popular tourism destinations, to China's OBOR strategy, and said Hainan Province has and will continue to use tourism to drive cultural cooperation and exchange. Mayor Ren also emphasized the importance of soccer in providing a platform for shared common interests across international borders, demonstrating its applicability to "One Belt One Road" (People's Daily, April 6, 2018).

In other instances, China has paired soccer with traditional educational exchange platforms in its OBOR toolbox. From January to February 2018, China hosted the first "Belt and Road" Culture and Soccer Winter Camp in Shanghai. The event, hosted by Shanghai Sports National University and other local sponsors, sought to promote China through cross-cultural interaction among children from OBOR countries, including Serbia, Sri Lanka, Kenya, and Panama. In addition to providing soccer training and activities, the program also included an OBOR cultural exchange tour throughout key historical landmarks across China. At the closing ceremony, top players from one of Shanghai's professional soccer teams were invited to speak to the children.

The biggest Chinese sponsors in this year's world cup have also made significant contributions to China's OBOR and have been working to actively promote the Chinese government's message. Mengniu in September 2017 was awarded the "OBOR Constructive Case Award ("一带一路" 建设案列奖) at the People's Daily OBOR Media Cooperation Forum, where it was commended for its dedication to promoting China's OBOR. During the event, Mengniu Party Secretary Wu Wenting gave the keynote speech, noting that over the past few years, the spirit of OBOR has provided Mengniu with a "rich foundation for development and has helped to company develop an internationally renowned brand" (Xinhua, September 20, 2017).

China World Cup 2030?

Just as China utilized "ping pong diplomacy" (乒乓外交) [1] in the early 1970s to begin to ease tensions between a slowly-opening China and the rest of the world, Beijing is now exploiting the world's love of soccer as a means to win over hearts and minds in other countries. OBOR and the World Cup are both global stages from which China can communicate what it views as its humanitarian and inclusive values. It was thus a natural that, after Chinese entities stepped in to bail out FIFA prior to the 2018 World Cup, they chose to portray themselves as the "saviors" of this summer's tournament; Wanda Group Chairman Wang Jianlin told reporters that Wanda Group "gladly extended their hand to FIFA during a difficult time" (China Venture, June 16, 2018). The support provided by PRC entities to FIFA's most important event could make a Chinese World Cup—a long-standing dream of President Xi—a reality, potentially as early as 2030.

Emily Weinstein is a research analyst at Pointe Bello and an M.A. Candidate in Security Studies at Georgetown University. Her research focuses on Chinese industrial and political espionage and foreign policy. She can be found on Twitter @emilysw1.

Notes

[1] For more information on "ping pong diplomacy," see the following excerpt from a 1971 Global Times article: http://www.people.com.cn/GB/historic/0410/1145.html

***

China May be Unprepared for the End of the Syrian War

By Joseph Hope

In early 2017, Secretary-General and President Xi Jinping announced his desire to build a "Great Wall of Iron" to promote security and peace in China's Xinjiang Uighur Autonomous Region (Xinhua, March 10, 2017), an intensification of Beijing's strict security measures in the region since the 2009 Urumqi riots. While Xi's focus may be largely domestic, the move towards stricter security in Xinjiang coincides with a new potential challenge to China's national security: Syrian-trained Uighurs potentially returning to Xinjiang as the war in Syria winds down (China Brief, September 21, 2017).

China's returning fighter challenge is linked with the al-Qaeda affiliated Turkestan Islamic Party (TIP), which has been active in Syria and may have been affiliated with as many as several thousand Chinese Uighur members (South China Morning Post, December 12, 2017). The Islamist radicalization of some of these fighters while abroad has also helped build links of solidarity between them and the broader global Islamic militant community.

Pressure may be mounting on Uighurs in Syria as the forces of Syrian President Bashar al-Assad close in on Idlib, the last major rebel-held area of the country, where Uighur fighters are believed to be concentrated. Idlib lies within an agreed multi-party de-escalation zone, but Syrian government forces have violated such agreements in other areas, and a recent government-rebel prisoner swap and evacuation may foreshadow increased pressure on rebel groups (Al Jazeera, July 19).

As Assad consolidates power over Syria's remaining territory, Chinese nationals fighting alongside al-Qaeda may leave the fighting and attempt to return to China. How Beijing responds to these returning fighters may dramatically alter the security situation in Xinjiang and the rest of China.

Uighurs at War

China has long accused the TIP and the East Turkestan Islamic Movement (ETIM), the two main Uighur terror groups, of connections to al-Qaeda. Before 2009 this was a dubious assertion, since the majority of Uighur fighters and terrorists espoused separatism rather than Islamic fundamentalism **[1]**. The 2009 Urumqi riots changed by drawing the attention of al-Qaeda (Terrorism Monitor, July 12, 2013). This was followed soon afterwards by assertions in PRC media that Uighurs had begun to leave Xinjiang to join the fighting in Syria (Global Times, October 29, 2012). Shortly after Islamic State (IS) leader Abu Bakr al-Baghdadi's declaration of the Caliphate in 2014, IS released the first edition of its main propaganda magazine, *Dabiq*, in which China and several other nations were singled out as threats **[2]**. A subsequent wave of Uighur-language propaganda, as well as Uighurs leaving China for Syria, have helped to deepen the Xinjiang-Syria connection.

Estimates of the number of Uighurs in Syria. The Syrian government reportedly informed Beijing there were 5,000 as of May, 2017 (Reuters, May 11, 2017). Another Dubai-based media outlet reported the number as 10,000 to 20,000, mostly in Idlib province (Asia Times, May 21, 2017). A ledger recently recovered by US forces providing information on women within the Islamic State gives rare first-hand information on the question. Of 1,139 women who had joined the Islamic State, 76 reported Xinjiang as their place of origin, making Xinjiang the third most common place of origin behind Dagestan with 200, and Turkey with 124 **[3]**. Similarly, data on 290 IS child soldiers shows that 12 are Chinese. Four originated in Aksu (阿克苏), a city in Xinjiang, making it the seventh-most common city of origin in the data set **[4]**. Since the number of Uighurs in IS is believed to be much smaller than that of TIP, this would seem to support the contention that there is a large number of Chinese Uighurs in Syria.

While ETIM and TIP have traditionally espoused separatism from China, some Uighurs in Syria appear to have become indoctrinated in Islamic militancy. Some Uighurs fighting in Syria have even reportedly directly threatened to "return to Xinjiang to wage Jihad" (South China Morning Post, September 7, 2016). A key indicator of this shift in motivation was the 2016 bombing of the Chinese Embassy in Bishkek, Kyrgyzstan, in which an Uighur rammed the embassy gates with a vehicle, then detonated the explosives inside. Although the attacker was a suspected member of ETIM, both the attacker and the cell that planned the attack were believed to be affiliated with Jabhat al-Nusra, al-Qaeda's Syrian branch at the time that the attack would have been planned (Xinhua, September 6, 2016). The attack came only three months after a call to action among Uighurs was made by al-Qaeda's leader, Ayman al-Zawahiri (The Diplomat, September 29, 2016).

There are indications that some Uighurs in Syria view China as a target. An early 2017 Islamic State video showed a group of Uighurs making threats to China, and ended with a shot of a Uighur fighter executing a prisoner (Al Jazeera, March 1, 2017). In an interview another Uighur fighter said, "we didn't care how the fighting went or who Assad was… We just wanted to learn how to use the weapons and then go back to China (AP, December 23, 2017)." Malhama Tactical, a for-profit Jihadist military training group, also made a threat against China in early 2017 and claimed to have added Chinese nationals to its instructor ranks. Importantly, the group is known to operate in Idlib, where there may be a large Uighur population, and has trained numerous TIP fighters. While the group itself does not carry out terror attacks, it is providing training to Uighur fighters and apparently marketing itself to Uighurs in Xinjiang (Terrorism Monitor, November 27, 2017). While official PRC figures on Uighur fighters returning are not available, Jacques Neriah of the Jerusalem Center for Public Affairs claims that the Chinese government has arrested around 100 returning fighters as of the end of 2017(JCPA, December 20, 2017). Moreover, the number of returning fighters intercepted at the Chinese border reportedly increased "ten-fold" in 2017, according to Ji Zhiye of the China Institute of Contemporary International Relations (South China Morning Post, January 8).

Domestic Security Readiness

China will likely attempt to arrest and imprison as many returnees as possible; a task made easier by PRC pressure on neighboring nations such as Kyrgyzstan, Kazakhstan and Afghanistan as well as nations on known Uighur transit

routes like Thailand and Malaysia to deport Uighurs to China (Global Times, February 11; Global Times, November 21, 2017; Al Jazeera, January 8, 2017; Al Jazeera, February 19, 2015; Uyghur Human Rights Project, May 19, 2006). However, this will do little to stabilize communities in Xinjiang or to account for those who manage to return to Xinjiang without apprehension by authorities. Furthermore, ongoing harsh treatment of Uighurs may sharpen foreign extremist groups' focus on China. Stabilizing Xinjiang and neutralizing radicalization is made more difficult the pervasive economic, workplace, and even interpersonal discrimination that Uighurs face (Radio Free Asia, May 14, 2015) **[5]**. Other countries' experience with radicalized individuals and returning fighters suggests this may not be the most effective approach. This is a particularly important consideration given the growing influence of Islamic militancy upon Uighurs within groups such as ETIM and TIP.

Tightening security policies in Xinjiang since 2009 have aimed to limit Uighurs' movement, control their access to weapons, and make inaccessible meeting areas where radicalization, organization and attack planning could take place. Other measures have sought to address religious fundamentalism by banning beards, prohibiting children from observing Ramadan, and closing mosques. Despite, or perhaps because of, these measures, attacks in Xinjiang have continued to occur (China Brief, February 6, 2017; China Brief, September 21, 2017).

Authorities have also chosen to enlist Uighurs and other local citizens in pervasive low-level security deployments. In addition to the already ubiquitous "convenience police stations", Xinjiang authorities recruited an enormous number of informal security agents in 2016 (China Brief, March 14, 2017). Many of the more than 30,000 new hires were positioned within convenience police stations, where they closely monitor surrounding communities. One of the benefits, from the authorities' point of view, of using local manpower stationed close to the communities where they live, is their unique ability to identify the sudden reappearance of individuals who have been away for long periods of time, making it more likely that any returning fighters will be discovered and apprehended.

A newly built network of "re-education" camps and pervasive electronic surveillance will also be used to combat the problem of returning fighters, but in some cases may be ineffective, or create as many problems as they solve (China Brief, May 15). Re-education in many cases may not be permanent detention, and if the program is not successful in de-radicalizing an individual, they may simply re-engage upon release because of a lack of reintegration and community-based programs. In other countries confronting Islamic militancy, prisons are known to be fertile grounds for radicalization **[6]**. It is not currently known whether China detains captured returning fighters separately from individuals placed in re-education programs. Uighur returnees may also be able to avoid electronic detection in while in Xinjiang, since electronic surveillance evasion is also a skill practiced by terrorist groups in Syria and elsewhere **[7]**.

Conclusion

While many Chinese Uighurs have travelled to Syria to fight, it remains unknown how many of those who remain alive intend to return to China. Those who return may bring with them a newly Islamized ideology distinct from the predominantly separatist ideology that drove attacks by Uighur radicals. To be clear, China does not face a threat of thousands of fighters returning to wage an open battle. Rather, the real risk is that a small number of returning fighters slips through the cracks to re-enter their communities, or exit detention programs without renouncing violence. Once back in their communities, those individuals could become powerful force multipliers, who could introduce leadership, technical and tactical knowledge, resources, and radicalization methods to the community **[8]**.

Past PRC deradicalization measures have not fully addressed the threat, and will likely continue to prove inadequate in the face of evolving threat. While pervasive on-the-ground surveillance and patrols by community members may prove effective in detecting returned fighters, it will do little to counter the religious ideology that could prove the new face of terrorism in Xinjiang, or to neutralize the influence of those who are not apprehended. Given its traditional preference for coercive measures, it is unlikely that Beijing will adopt a softer approach that promotes reintegration,

community bonds, and religious education. Instead, heightened security measures may be in store for Xinjiang, and are likely to bring heightened tensions with them.

Joesph Hope holds an MSc from the University of Essex, where his dissertation focused on analyzing the Islamic State's magazine, Dabiq, for signals that a criminological theory may be applicable in the behavior of foreign fighters. He lives in Chengdu, Sichuan, and is preparing to begin a PhD in 2019.

Notes

[1] For more, see Chris Zambelis. (2010). "Uighur Dissent and Militancy in China's Xinjiang Province". *CTC Sentinel.* 3(1). p 16-19.

[2] For more, see Dabiq. (July, 2014). Return of the Kilifa. *Dabiq.* Retrieved from The Clarion Project at http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq

[3] For more, see Brian Dodwell and Daniel Milton. (2018). "Jihadi Brides? Examining a Female Guesthouse Registry from the Islamic State's Caliphate". *CTC Sentinel*. 11(5). p. 16-22.

[4] For more, see Dakota Foster and Daniel Milton. (2018). "Children at War: Foreign Child Recruits of the Islamic State". *CTC Sentinel*. 11(6). p. 11-17.

[5] For more, see Xiaowei Zang. (2011). "Uyghur-Han Earnings Differentials in Urumchi". *The China Journal*. (65). p. 141-155.

[6] For more, see James Brandon. (2009). "The Danger of Prison Radicalization in the West". *CTC Sentinel*. 2(12). p. 1-4.

[7] For more, see Aaron Brantly and Mohammed al-Ubaydi. (2015). "Extremist Forums Provide Digital OpSec Training". *CTC Sentinel*. 8(5). p. 10-13.

[8] For more, see United Nations Security Council. (2018). "The Challenge of Returning and Relocating Foreign Terrorist Fighters: Research Perspectives". *UNSC Counter-Terrorism Committee Executive Directorate*