''China and the Middle East''

Testimony before the U.S.–China Economic and Security Review Commission

April 19, 2024

China's Security Interests Panel III

Dr Alessandro Arduino,

Affiliate lecturer Lau China Institute King's College London, visiting professor Geneva Graduate Institute

I want to start by thanking co-chairs Commissioner Aaron Friedberg and Commissioner Jonathan Stivers, as well as all the Commissioners, for giving me the opportunity to testify today. The views I'll be presenting are solely my own and should not be seen as representing any organization I'm affiliated with.

Setting the Stage. Chinese Private Security Companies Presence in the Middle East

Once more, the Middle East teeters on the edge, stirring China's unease over escalating regional instability. With porous borders, rampant transnational crime, attacks on the sea lanes of communications, and the relentless spread of terrorist networks, the threat to China's Belt and Road Initiative (BRI) looms large. While Beijing is gradually moving away from its longstanding policy of non-interference and becoming more reactive, it remains cautious about actively involving itself in the Middle East security quagmire.[i]

To address security concerns without committing Chinese military personnel, China is turning to private security companies (PSCs) as a convenient security gap filler. In the Middle East, Chinese oil and gas state-owned enterprises (SOEs) have been utilising these firms to protect Chinese engineers from kidnapping and to safeguard infrastructure from attacks by terrorist or criminal groups. This approach predates the specific security needs of the BRI. Still, the evolution and expansion of the Chinese private security sector, especially from the Middle East to Africa, is indicating China's proactive stance in mitigating risks without the necessity to deploy the People's Liberation Army (PLA) overseas. Initially, the Chinese private security sector defending Chinese oil fields in the Middle East aimed to emulate the role played by US Private Military Companies (PMCs) in Iraq. At that time several security companies from the US, UK and Israel supported with armed guards, security analysis and training the Chinese PSCs protecting national energy companies, mostly in the southern part of Iraq. Yet, increasing tensions with the US have made Chinese SOEs more hesitant to engage with Western security contractors. In this respect, the emergence of Russian quasi-PMCs and especially the Russian Wagner Group presented a

novel approach, combining mercenary activities with quasi-private proxy services for authoritarian regimes. In this respect, Russian quasi-PMCs attempted to enter the profitable market of safeguarding the BRI in the Middle East, especially against maritime piracy from the Red Sea to the Gulf of Guinea. However, this approach lost its allure relatively quickly, particularly after Wagner's boss Yevgeny Prigozhin's armed mutiny cast a shadow over the Wagner Group's loyalty, raising concerns in Beijing about the potential threats spanning from unaccountable heavily armed contractors returning home.

The growing presence of Chinese PSCs along the Belt and Road Initiative in the Middle East reflects Beijing's desire to cultivate a professional private security sector capable of operating effectively in complex environments far from China's borders while keeping intact the decades-old principle of non-interference. In this respect, the challenge lies not in determining the presence of Chinese PSCs overseas, but rather in distinguishing where the involvement of the State ends and the private sector starts.

In the Middle East, China's PSCs have a lesser presence compared to their activities in Asia and Africa. For example, in the affluent Gulf States, Chinese PSCs are primarily tasked with guarding offices and warehouses, as local police adequately ensure the safety of Chinese workers. However, in more volatile environments like Iraq, experienced Chinese PSCs support national oil and gas companies by leveraging longstanding relationships with Iraqi popular mobilization units (PMU), particularly when direct support from Baghdad is not feasible. In Syria and Yemen, Chinese investments have dwindled amid civil wars, with the possibility of seeing a surge in the Chinese private security sector only once Beijing commits to participating in post-conflict reconstruction efforts. Despite claims from various quarters, including Beirut, Damascus, and Sana'a, that Chinese billions in foreign direct investment (FDI) will revolutionise national economies' rebuilding, Beijing remains cautious. Simultaneously, Israel holds significance for Chinese PSCs not primarily as a market, but rather as service providers. Israeli companies and individuals possess valuable expertise in counter-terrorism and cybersecurity, which they can transfer to Chinese PSCs seeking to enhance their capabilities on a global scale.

According to Chinese scholars, since the onset of ''the Arab Spring, optimism can still be hard to find in the Middle East.''[ii] Russia returning to the Middle East as a major power through the military intervention in Syria and the US reorienting its Middle East strategy is accompanied by regional powers such as Saudi Arabia, Turkey, and Iran striving for power and security. Nevertheless, due to the large influx of capital and Chinese workers[iii], ''the protection of overseas Chinese citizens has emerged as a new diplomatic imperative."[iv] The 2018 State Council Report on the Protection of Overseas Chinese Rights and Interests emphasises that "the overseas Chinese have an irreplaceable and vital role in realising the Chinese dream," therefore for China, safeguarding nationals in the Middle East has become a cornerstone of its foreign policy. Amid rising terrorist threats and conflicts, the interconnectedness between China's human and economic presence in the Middle East and its security policy is of growing significance.

Compared to their Western counterpart the Chinese PSCs are latecomers into the international private security arena. In 1993 the operational scope of PSCs with ''Chinese characteristics'' was restricted, primarily allowing former military and police personnel to register such companies. However, since 2009, subsequent laws have broadened their operational horizons. These changes include loosening restrictions on weapon access and easing the stringent registration procedures that were in place earlier. However, the majority of the several thousand Chinese PSCs operating in mainland China are still established and managed by former security officers, with key personnel recruited from the People's Liberation Army, People's Armed Police, and the police force. Simultaneously, while there exists a

detailed law governing the operation of PSCs within China, there is a lack of precise rules and regulations for those operating overseas. This ongoing legal vacuum exposes the entire sector to competition from semi-legal Chinese private security companies that establish themselves overseas without proper licensing domestically[v]. Nevertheless, while the Chinese private security sector is increasing its professionalisation, it's improbable that Chinese PSCs will attain in the short term the same level of expertise and capability as their Western counterparts[vi].

The Party Controls the Gun. Regulating the Evolution of the Chinese Private Security Sector

Prior to President Xi Jinping's flagship foreign policy initiative, the Belt and Road, Chinese investments in the Middle East and North Africa (MENA) primarily targeted natural resource extraction and trade. However, since 2013's surge in infrastructure investments driven by the BRI, aiming to connect the MENA region with Chinese trade routes like the estimated 63 billion US$ China-Pakistan Economic Corridor (CPEC), Central Asia, the Red Sea, the Indian Ocean and the Mediterranean basin has also heightened risks and threats to Chinese personnel and infrastructures. In this respect, Beijing's position on MENA is ''shifting away from harvesting economic benefits while avoiding political entanglements … albeit in a cautious way''[vii]. Therefore, China is gradually increasing its political, security[viii] and economic presence in the region, with economic cooperation still the centrepiece of this effort.

While China trails behind the US as the primary security provider in the MENA region and across Africa, it stands as one of the leading economic actors. In 2018, the MENA region ranked second globally in terms of investment and Chinese construction projects, following closely behind Europe, with this trend on the rise. However, security remains a significant challenge. Complicating Beijing's development-security approach is the increasing presence of over one million Chinese expatriates in the region, spanning from construction workers to businesspeople, students, and even religious pilgrims visiting Saudi Arabia and Iran.

In this respect, Chinese security pundits are increasingly vocal on Chinese social media that it is time that China's private security sector increases its capability and footprint abroad to protect Chinese nationals against terrorist threats. Yet, the Chinese Communist Party (CCP) remains resolute, adhering to the Maoist principle that "the party controls the gun."[ix] Despite Beijing's scepticism, Chinese private security firms are poised to assume an important role in safeguarding Chinese interests overseas and bolstering security capabilities in a domain where the boundary between private and public realms is often blurred.

While the private security sector with ''Chinese characteristics'' is adapting to meet increasing challenges abroad[x], Beijing's imposed limitations on access to weapons are still forcing the Chinese PSCs to rely on armed personnel hired from local or international sources. Consequently, Chinese PSCs primarily engage in passive roles such as asset protection against various threats like riots, theft, kidnapping for ransom, terrorism, and maritime piracy. This restriction has prompted numerous Chinese security experts over the past decade to advocate for the professionalisation and restructuring of the sector, potentially modelling it after Western private military frameworks or incorporating elements from the Russian approach to PMCs[xi].

Following the launch of the BRI, the Chinese private security sector briefly experimented with a model akin to Blackwater. This was evident in the establishment of Frontier Services Group (FSG), a Hong Kong-

based joint venture co-founded by Erik Prince the founder of US PMC Blackwater in collaboration with the Chinese state conglomerate CITIC. However, as tensions between China and the US escalated, the prominence of the Blackwater-inspired model began to decline.

Also, the Russian model did not find fertile ground. Before the Wagner Group armed mutiny, several Chinese security firms had started contemplating collaborations with Russian counterparts. They were attracted to three main advantages offered by Russian security providers: skilled contractors with a demonstrated combat track record, a lack of evident Western ties that might jeopardize the confidentiality of SOEs, and competitive pricing. Nevertheless, Chinese foreign investments demand stability while the Wagner Group's promise of ''armed stability'' thrives in chaos. This presents a paradoxical challenge for Beijing and Moscow's "no-limits friendship," while simultaneously making it difficult for the Chinese private security sector to maintain a low profile.

In the Middle East, wherever there are Chinese economic interests, Chinese PSCs are there operating alongside local or international armed contractors. These Chinese contractors usually consist of a small number of unarmed security managers who serve as contact points between the Chinese company's workers located in a gated compound and the local security forces. In cases where regulations in the host country prohibit the registration of independent Chinese PSCs or joint ventures with local private security firms, it's not uncommon for a limited number of Chinese security managers to operate under working visas granted to the Chinese SOE. The risk management approaches of Chinese companies vary, with state-owned enterprises (SOEs) in natural resource exploitation being better funded and equipped to procure necessary security services[xii].

Maritime Security: From Anti-piracy to Anti-drones.

Since the surge of piratical activities along the Somali coast the Chinese private security sector has provided guards to Chinese commercial vessels, mostly related to Chinese commercial shipping lines and China's State energy companies. Since 2019, with Somali pirate activities nearly eradicated due to the efforts of Combined Naval Task Force 151, Chinese PSCs have shifted their focus to addressing the maritime security needs of the BRI in response to the increase in piracy incidents in Western Africa.

The most common maritime incidents in the region involve boarding ships to steal valuables from crews, but hijackings and kidnappings also occur. Various types of pirates still operate around maritime chokepoints, leaving vessels with limited options for navigation. However, rising insurance costs to protect sea lines of communication from piracy are compelling the private security sector to enhance their capabilities at sea. Nevertheless, in 2024, the Middle East is back in the global spotlight after a Yemeni militant group, the Houthis, began engaging in marauding activities in the Red Sea. The Bab al Mandab chokepoint is a crucial link in one of the world's most important maritime routes connecting the Mediterranean to the Indian Ocean facilitating the continuous transportation of millions of barrels of oil daily and contributing to 12% of global trade.

In this respect, the Chinese PSCs have been forming their own response to armed drone attacks and hijack attempts on Red Sea shipping. Providing security service in the maritime domain entails logistic constraints to carry weapons onboard when commercial vessels dock into national waters. In contrast to Chinese PSCs operating on land, a select few engaged in maritime security boast a vast international network of partners. This includes offering logistical services aimed at bolstering maritime security, exemplified by the presence of floating armouries. In the past decade, the proliferation of floating

armouries has increased in response to rampant piracy in high-seas areas and stringent national regulations regarding the transportation of heavy firearms. These armouries play a vital role in coping with the restrictions on private security forces carrying firearms into the ports of numerous countries.

The onslaught of Houthi attacks has intensified the imperative to safeguard the crucial sea lanes responsible for over 40% of China's hydrocarbon transport. In response, Chinese PSCs are getting ready to deliver advanced services, including deploying jammers to disrupt transmission signals between controllers and drones, along with kinetic options such as anti-aircraft guns.

Chinese PSC as Chinese Security Technologies Ambassadors

In China's Arab Policy Paper of 2016[xiii], Beijing outlined its strategy for economic and cultural development with Arab states, emphasizing enhanced connectivity within the BRI. The paper discusses security cooperation briefly, focusing on enhancing capabilities to address nontraditional security threats and supporting efforts against piracy, cyber security, and maintaining maritime security in the Gulf of Aden and off Somalia. Although China's defence cooperation in the Middle East remains limited compared to the United States and Russia, there is a growing trend in military cooperation. Chinese PSCs are positioned as ambassadors for Chinese high-tech security products. According to the Stockholm International Peace Research Institute (SIPRI), China accounted for only 5% of arms transfers to the MENA region between 2014 and 2018, significantly lower than the United States (54%) and Russia (9.6%)[xiv]. However, China's military hardware sales and transfers in the region focus on niche sectors, including combat-armed and scouting drones and missiles, such as the transfer of an armed drone production line to Saudi Arabia.

While the Chinese private security sector is a latecomer in the international private security market, the Chinese PSCs, could lean toward a high-tech evolutionary model. Chinese PSCs are becoming ambassadors of China's crowd management technologies, such as facial recognition and sooner could be the entry point for Chinese AI's ''safe cities'' product.

In the Middle East, when States have the option to choose a partnership with China in the cyber realm it is possible to predict that it will follow an ongoing trend of relations balancing with Beijing and Washington. For example, ''the UAE is a small yet ambitious state, both powers are crucial to its strategy for maintaining security and diversifying its economy.''[xv] As the UAE prioritizes its security ties with the US, particularly concerning the Iranian threat, it's one of only five countries in the Middle East and North Africa to have a 'comprehensive strategic partnership' with China. In navigating this dynamic, the UAE effectively balances between relying on the US security umbrella and leveraging Chinese ICT and AI technologies, which are pivotal to its development policies and contribute significantly to digital advancements in the region.

The UN's 2022 call for enhanced oversight on the trade of military-grade cybertechnologies is a case in point, with at its core the reevaluation of the conventional regulatory approach toward dual-use technologies[xvi]. Given that most technologies have multiple potential applications, there's an urgent need for revised regulations that clearly distinguish between commercial uses and national security imperatives.

However, the real challenge lies in distinguishing between legitimate private cybersecurity firms and cyber mercenaries, and determining when private sector initiatives to enhance government espionage capabilities cross ethical boundaries. The inherently chaotic nature of the Internet only exacerbates this challenge.

In the realm of cyber security, both state and non-state actors are tapping into defensive and offensive capabilities provided by the private sector. Nevertheless, distinguishing between offensive and defensive cyber services is even more complex[xvii] due to the inherent opacity of the sector. Since the inception of the Internet, states have sought to leverage cyberspace for intelligence and coercive power. Nonstate cyber operators can traverse borders with minimal digital traces and at low costs, presenting an attractive option for states aiming to wield influence in cyberspace. In both times of peace and conflict, certain cyber activities blur the lines with mercenary-like activities. In this respect, the emergence of Big Data applied to border management profiling and new surveillance technologies is already prone to abuses.

The emergence of cyber mercenaries is already evident, although they are not yet formally recognized as such. In this respect, the UN Working Group on Mercenary Activities defines cyber mercenaries as companies using military-grade cyber weapons to carry out tasks for foreign powers, nonstate actors, or even criminal and terrorist groups[xviii].

In the Western world, particularly in the US, the liberal attitudes towards cyberspace create a vast grey area ripe for exploitation. This isn't just by cyber mercenaries but also by PMCs and PSCs seeking to capitalize on a lucrative and rapidly expanding market. Conversely, authoritarian regimes provide no insight beyond their firewalls, tightly guarding Big Data under the guise of national security.

Cyber Security and Cyber Mercenaries

The expansion of the Digital Silk Road within the BRI is promoting "digitization with Chinese characteristics." This initiative aims to position China at the forefront of the fourth industrial revolution, encompassing digital security, e-services, and integration into smart cities. It involves various components, ranging from underwater fibre-optic cables to the Beidou satellite navigation system[xix].

Amidst escalating strategic rivalry between the United States and China, Beijing is increasing its strategic presence in the MENA region not only to safeguard its energy security but also to assert its dominance in the digital realm. While many countries are striving to balance the utilization of Chinese technology against American efforts to block such systems, Chinese PSCs are a component of Beijing’s push in the digital domain.

The smart cities sector presents a potential clash of interests between China, the US, and regional actors. The integration of Chinese sensors, Big Data analytical software, and narrow AIs into smart cities has broader national security implications. For instance, Chinese PSCs are transitioning from offering basic guarding services to providing comprehensive high-tech solutions, such as semi-autonomous patrol robots equipped with sensors and narrow AI. However, this raises concerns about privacy issues stemming from the use of collected video feeds and biometric data.

China's ambition to become a "cyber great power" and its implications for data access fuel suspicions regarding Chinese PSCs operating high-tech equipment abroad. While China's role as a security provider

in regions like the Middle East is still evolving, its digital influence in the region, from 5G to cybersecurity and Big Data analytics, is rapidly expanding. Consequently, the operational space for Chinese PSCs venturing abroad is increasing.

Chinese security companies are transitioning from offering low-cost bids to providing additional high-tech services, leveraging competitively priced AI-enabled facial recognition and surveillance drones, which are unavailable in the US market due to regulatory restrictions. The use of CCTV and Big Data analysis is shifting the private security sector toward a more proactive approach, focusing on predictive analysis and preventive solutions.

However, challenges arise from the Chinese National Cybersecurity Law, especially in countries with their own cybersecurity frameworks. Concerns about the gathering and processing of personal data by Chinese PSCs abroad persist, with doubts lingering regarding the security of sensitive information. The ongoing algorithm weaponization is reshaping the development of smart cities and society, prompting Middle Eastern monarchies to weigh their exposure to Chinese technologies within the Digital Silk Road.

Blurring the distinction between security and military roles presents a significant risk, particularly in the realm of cyberspace, where private security firms often operate. These firms, untroubled by potential labels like "private military entities" or even "cyber mercenaries," operate without fear of consequences. Unlike PSCs with boots on the ground, who can face swift repercussions for bolstering the military capabilities of sanctioned governments or non-state actors, those operating in cyberspace do not fear backslashes.

On the global stage, while mercenaries on the ground sow disorder, their cyber counterparts capitalise on the demand for easily deployable offensive cyber capabilities. These professionals, enticed by lucrative opportunities in the private sector, often prioritize financial gain over national allegiance. However, in China, monetary gain and nationalistic pride are closely intertwined. As China increasingly favours the use of private security firms with boots on the ground to protect President Xi’s flagship foreign policy initiative, it appears to also be employing the same strategy in cyberspace. In this respect, Beijing is discovering the hard way[xx], as the West has, the perils and advantages of outsourcing security to private companies to maintain plausible deniability. A February 2024 data dump of files from a Chinese cyber security firm revealed alleged hacking exploits. Like the West, Beijing is finding out the hard way the perils and advantages of outsourcing to private cyber security firms to maintain plausible deniability.

As it is happening in the boots on the ground private security sector, there's a similar trend occurring in the cyber security sector in China. The debate is anchored on whether to follow a Western approach or a Russian one. In China, there's been some interest in the idea of privatizing cybersecurity, however, adopting the Russian model would be more challenging for China as Beijing heavily emphasizes control over its security providers. On the contrary, Moscow's cyber capabilities rely on a close relationship with skilled cybercriminal organizations. This relationship is based on two principles[xxi]: first, the state protects criminal hackers who avoid targeting national interests, and second, hackers must carry out operations for the Kremlin when needed.

Moreover, amidst the ongoing debates within the Chinese government regarding the increased involvement of private security firms in protecting Chinese interests globally, also in the digital realm, it revolves around the extent of "the Party control the cyber gun," echoing the longstanding Maoist principle.

Recommendations

China primarily expands its influence in the Middle East through economic means, leveraging its economic prowess as a key tool. Meanwhile, the region is open to the idea of increasing China's cultural soft power footprint, as long as it doesn't pose a challenge to existing local power dynamics. In this respect, China believes that its vision of global order and the solutions it proposes could find fertile ground in the Middle East. China is steadfast in out-competing the West, and given the region's perceived openness to China's global ambitions, its engagements on the continent are expected to intensify. Nevertheless, Beijing's economic tools are severely constrained by a rapidly deteriorating security environment and unpredictability.

Apart from the recent brokered detente between Saudi Arabia and Iran, Beijing is hesitant to actively involve itself in the security complexities of the Middle East.

The rise in violence against Chinese nationals abroad has prompted a call for the professionalisation of the private security sector. While some top Chinese security firms operate internationally, most PSCs struggle due to late entry into the global security sector and difficulty in finding competent Chinese contractors, often relying on local fixers. Challenges include training personnel with local knowledge and security skills, limited lucrative contracts, and few PSCs providing internationally accredited training certifications to staff. Moreover, the notion of "private" in China is influenced by the pervasive presence of the CCP in businesses, dealings with SOEs, and government bureaucracy shaping the private sector.

While Chinese PSCs may not pose an immediate challenge to Western counterparts in shaping the Middle Eastern private security sector, their presence demands a clearer understanding of their role and future development trajectories. Therefore, to compete effectively in the region, strategic policies must be crafted, focusing on three pivotal aspects.

Firstly, there's the imperative of ongoing monitoring of the Chinese private security sector. Across the expanse from the Middle East to Africa, the progression of Chinese PSCs adhering to global standards and attaining internationally recognised certifications could prove advantageous not just for China but also for local stakeholders and the international community. A small window of opportunity for collaboration with Western counterparts still exists in promoting transparency and accountability. For example, the maritime domain along the Red Sea presents a prime opportunity to enhance existing collaborations that vertically integrate security services, risk mitigation, negotiation, and the insurance sector. However, neglecting to seize this chance promptly might crack the door open to alternative evolving models for the Chinese private security sector, such as the assertive Russian approach, which already forcefully imposes its Wagner model in supporting autocratic regimes to stay in power in exchange for local resources and access to strategic logistic hubs. Regulating the ascent of Chinese PSCs through comprehensive norms reduces the risk of adverse consequences overseas and amplifies potential advantages, particularly in situations where China must uphold its proclaimed "principle of peaceful rise."

The second aspect revolves around the cyber realm. While there might be room for cooperation with the Chinese private security sector boots on the ground in cyberspace is far more complex. The murky nature of cyber operations blurs the lines between state and private entities, particularly when passive security measures morph into active military engagements. Hence, strengthening international regulations is paramount to curb and punish cyber actors who cloak themselves as private cybersecurity

entities but function as cyber mercenaries, especially as AI integration in cybersecurity becomes ubiquitous.

The last aspect pertains to the potential integration of Chinese PSCs in the Middle East, particularly those assigned to guard logistic hubs, into the PLA's multi-domain operations. Although Chinese PSCs currently maintain a passive stance, primarily focused on supporting the economic and trade endeavours of Chinese SOEs and companies abroad, there exists the possibility of future involvement in safeguarding ports, collecting local intelligence and providing ground support for non-combatant evacuation operations. Such developments could further blur the distinction between private security and private military services.

[i] Alessandro Arduino, ''Chinese private security companies in the Middle East.'' in Routledge Handbook on China–Middle East Relations. Edited By Jonathan Fulton. Routledge, September 2023. (Part VI, Cap.21)

[ii] Dandan Zhang, China's Security Protection of Chinese Nationals in the Middle East. Asian Journal of Middle Eastern and Islamic Studies, (2023) 17(1), 66–82. https://doi.org/10.1080/25765949.2023.2196194

[iii] Dandan Zhang and Degang Sun,"China's consular protection in the Middle East: innovation in concept, practice and mechanism,"West Asia and Africa (4), (2019)

[iv] Shaio Zerba,"China's Libya evacuation operation: a new diplomatic imperative—overseas citizen Protection," Journal of Contemporary China 23(90), (2014), p. 1094

[v] Alessandro Arduino, '' Money for Mayhem: Mercenaries, Private Military Companies, Drones, and the Future of War'' Rowman & Littlefield. October 15, 2023. https://rowman.com/ISBN/9781538170311/Money-for-Mayhem-Mercenaries-Private-Military-Companies-Drones-and-the-Future-of-War

[vi] Sergey Sukhankin ,''An Anatomy of the Chinese Private Security Contracting Industry'' The Jamestown Foundation January 3, 2023. https://jamestown.org/program/an-anatomy-of-the-chinese-private-security-contracting-industry/

[vii] Degang Sun, "China's Approach to The Middle East: Development Before Democracy," in *China's great game in the Middle East*, ECFR, October 21, 2019, https://www.ecfr.eu/publications/summary/china_great_game_middle_east

[viii] Cortney Weinbaum, John V. Parachini, Melissa Shostak, Chandler Sachs, Tristan Finazzo, and Kate Giglio, ''China's Weapons Exports and Private Security Contractors.'' Santa Monica, CA: RAND Corporation, 2022. https://www.rand.org/pubs/tools/TLA2045-1.html.

[ix] Daniel C. Mattingly, ''How the Party Commands the Gun: The Foreign–Domestic Threat Dilemma in China.'' American Journal of Political Science, October 21, 2021. 68: 227-242. https://doi.org/10.1111/ajps.12739

[x] Christopher Spearin ,''China's Private Military and Security Companies: "Chinese Muscle" and the Reasons for U.S. Engagement.'' National Defense University Press PRISM Vol. 8, No. 4 June 11, 2020

[xi] Alessandro Arduino, '' Money for Mayhem: Mercenaries, Private Military Companies, Drones, and the Future of War'' Rowman & Littlefield. October 15, 2023. https://rowman.com/ISBN/9781538170311/Money-for-Mayhem-Mercenaries-Private-Military-Companies-Drones-and-the-Future-of-War

[xii] "Report of the State Council of Protection of Overseas Chinese Rights and Interests,"the National people' sCongress, (25 April 2018),http://www.npc.gov.cn/npc/xinwen/2018-04/25/content_2053574.htm

[xiii] China's Arab Policy Paper January 2016. English version: http://www.china.org.cn/world/2016-01/14/content_37573547.htm

[xiv] Pieter D. Wezeman et al., "Trends in International Arms Transfers, 2019,"SIPRI Fact Sheet, March 2020, https://www.sipri.org/sites/default/files/202003/fs_2003_at_2019.pdf.

[xv] Mohamed Bin Huwaidin, '' UAE's Balancing Strategy Between the United States and China.'' Middle East Policy 2024;31:88–101. https://doi.org/10.1111/mepo.12724

[xvi] UN, "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE)," in Michael Smith, "The Sixth United Nations GGE and International Law in Cyberspace," Just Security, June 10, 2021, https://www.justsecurity.org/76864/thesixth-united-nations-gge-and-international-law-in-cyberspace/.

[xvii] Shane Harris, @War: The Rise of the Military-Internet Complex (Boston: Mariner Books, 2015).

[xviii] Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to SelfDetermination, "The Human Rights Impacts of Mercenaries, Mercenary-Related Actors and Private Military and Security Companies Engaging in Cyberactivities," A76/151, July 15, 2021, https://documents-ddsny.un.org/doc/UNDOC/GEN/N21/192/08/PDF/N2119208.pdf?OpenElement

[xix] Alessandro Arduino, '' Money for Mayhem: Mercenaries, Private Military Companies, Drones, and the Future of War'' Rowman & Littlefield. October 15, 2023. https://rowman.com/ISBN/9781538170311/Money-for-Mayhem-Mercenaries-Private-Military-Companies-Drones-and-the-Future-of-War

[xx] J. Edward Moreno, ''China's Hacker Network: What to Know.'' The New York Times, February 22, 2024 https://www.nytimes.com/2024/02/22/business/china-hack-leak-isoon.html

[xxi] Francesco Varese, ''La Russia in quattro criminali.'' Einaudi, 2022 https://www.einaudi.it/catalogo-libri/problemi-contemporanei/la-russia-in-quattro-criminali-federico-varese-9788858441046/