*Expertise*

# The Present and Future of Chinese Private Security Companies

MATTHIAS SCHACHTLER

**Abstract** With the Belt and Road Initiative (BRI), China launched major infrastructure projects, mainly in the global South. Many of these projects, such as roads or pipelines, run through contested territory (for example in Pakistan or Myanmar). Several Chinese have lost their lives in attacks on BRI projects. The Chinese government passed a law early on that requires Chinese companies in hazardous areas to draw up appropriate security concepts, train their employees on security-related topics and have some zones actively guarded. The Chinese government recommends that companies hire Chinese security companies. To date, however, these companies are nowhere near as militarily armed and trained as the Wagner Group, for example. This article examines why this is the case and what strategies Chinese security companies could pursue in the future.

**Abstract** Mit der Belt and Road Initiative (BRI) lancierte China grosse Infrastrukturprojekte, hauptsächlich im globalen Süden. Viele dieser Projekte wie Strassen oder Pipelines verlaufen durch umkämpftes Gebiet (beispielsweise in Pakistan oder Myanmar). Bei Angriffen auf BRI-Projekte sind mehrere Chinesen ums Leben gekommen. Früh erliess der chinesische Staat ein Gesetz, das chinesischen Firmen in Gefahrengebieten vorschreibt, dass sie entsprechende Sicherheitskonzepte ausarbeiten, ihre Mitarbeiter zu sicherheitsrelevanten Themen ausbilden und manche Zonen aktiv bewachen lassen müssen. Dabei empfiehlt der chinesische Staat den Unternehmen, chinesische Sicherheitsfirmen zu beauftragen. Diese Firmen sind bis dato aber bei weitem nicht gleich militärisch bewaffnet und ausgebildet wie beispielsweise die Gruppe Wagner. Dieser Beitrag geht der Frage nach, weshalb dies der Fall ist und welche Strategien chinesische Sicherheitsfirmen in Zukunft verfolgen könnten.

**Schlüsselbegriffe** Chinas Sicherheitsstrategie; private Sicherheitsunternehmen; private Militärunternehmen; Belt and Road Initiative; Cybersicherheit
**Keywords** China security strategy; private security companies; private military companies; Belt and Road Initiative; cyber security

## Introduction

In March 2023, gunmen stormed a Chinese gold mine in the Central African Republic (CAR) and killed nine Chinese workers[1]. In an unusually aggressive tone, Xi Jinping called for the aggressors to be severely punished (Peltier 2023). This was only one of the most recent security incidents that Chinese companies and their workers have fallen victim to in recent years: In July 2021 the Pakistani Taliban killed nine Chinese engineers in a bus bombing (Shahzad 2021); in April 2022 a female suicide bomber attacked a Confucius Institute in Pakistan (Shahzad and Hassan 2022); and in December 2022 a hotel in Kabul often frequented by Chinese business people was bombed (Baptista and Heavens 2022).

With the launch of the Belt and Road Initiative (BRI) in 2013 as many as 30 000 Chinese companies started to work along the "New Silk Road"[2] (Sukhankin 2023). Some of the BRI's biggest projects are situated in hostile environments. The China-Pakistan Economic Corridor (CPEC), for example, is one of the BRI's flagship projects. It is a 62-billion-dollar infrastructure project with more than 30 000 Chinese nationals working onsite in Pakistan. The goal of CPEC is to connect the BRI's Maritime Silk Road with the land-based Silk Road Economic Belt (Legarda and Nouwens 2018). To do this, a 3000 km long system of roads, railways and pipelines is being constructed to connect the Port of Gwadar on the Arabian Sea with the city of Kashgar in China's Xinjiang region (Legarda and Nouwens 2018). The CPEC runs through some of Pakistan's most dangerous areas. Pakistan (on a regional and national level) has devoted considerable resources to protecting CPEC. Several different Pakistani military and police units (in total well over 25 000 units) have been tasked to protect CPEC (Legarda and Nouwens 2018). The Chinese government has also demanded that companies operating in hostile environments work together with security companies (preferably Chinese) to train their employees, draw up security plans and hire extra protection.

The goal of this paper is to provide an overview of how Chinese Private Security Companies (PSCs) have been utilised in the past to protect Chinese nationals and assets overseas. I will also discuss the definitional issue of what constitutes a PSC in comparison to a PMC (Private Military Company). Further on, I will provide a brief historical overview of the development of these PSCs and the way the Chinese Communist Party (CCP)

**MATTHIAS SCHACHTLER,** MA,
arbeitet an der Militärakademie an der ETH Zürich, wo er zu den chinesischen Streitkräften forscht. Er ist ausserdem Doktorand an der Ludwig-Maximilians-Universität in München (LMU) an der Forschungsstelle für Neurophilosophie und Ethik in den Neurowissenschaften. Er studierte an der Universität Zürich Philosophie, Politik und Arabisch. Später wechselte er an die LMU, wo er Philosophie und Sinologie studierte (BA). An der LMU absolvierte er ebenfalls einen Master (MA) in Philosophie mit Fokus auf künstliche Intelligenz. In der Schweizer Armee ist er Hauptmann bei den Sprachspezialisten. Matthias Schachtler ist in Taiwan geboren und aufgewachsen.
E-Mail: Matthias.Schachtler@vtg.admin.ch

has been handling them. Finally, I will show how Chinese security companies differ from other established PSCs and how their future development may be more oriented towards previously underdeveloped security sectors in the Global South, such as cybersecurity and digital surveillance.

## Literature Overview

Surprisingly little has been written about the development of Chinese PSCs, and the subject has not been discussed at length in political circles. Max Markusen from the Center for Strategic and International Studies (CSIS) laments that the spread of Chinese PSCs remains a subject remarkably absent in more recent reports of the U.S. Department of Defense (DoD) and the U.S. Congress (Markusen 2022). Few news articles in Western media mention Chinese PSCs and they often get numbers wrong or make unfounded and exaggerated claims about their capabilities (discussed later in this paper). Only a few scholarly articles by a small number of authors who have researched the subject (specifically regarding Chinese PSCs) extensively currently exist. Notably, Helena Legarda together with Meia Nouwens wrote one of the earliest and most comprehensive papers on the subject in 2018 in which they explored how the expansion of the BRI has also led to an expansion of overseas Chinese PSCs. Most recently (January 2023) Sergey Sukhankin published a paper as part of the James Town Foundation's *Guardians of the Belt and Road Project* in which he researched extensively Chinese media and academic articles in order to verify and provide updates on many of the findings from Legarda and Nouwen's 2018 contribution to the subject (Sukhankin 2023). What the literature review also brought to light is that the literature used in military studies circles and China studies circles seldom overlap. Most of the authors who wrote about Chinese PSCs come from a China analysis background and are often not associated with the military community. Consequently, their papers mentioned little to no literature that would otherwise be seen as essential reading on the subject in military circles. One such underdiscussed work is Singer's Corporate Warriors (Singer 2008). His book has long been regarded as one of the seminal works on the subject in military circles, at least in the U.S.

## Differentiating between PSCs and PMCs

Legarda et al. argue that the primary difference between a PSC and a PMC is that a PSC provides protection for assets and personnel and is not equipped to actively engage in a conflict where the adversary is using military equipment and tactics. A PMC, on the other hand, is equipped not just to protect assets and people in volatile situations, but also to conduct attacks in a dynamic hostile environment and can either support or replace other military units (Legarda and Nouwens 2018).

Singer argues that the binary definitions of PMCs and PSCs are not sufficient. Even guarding valuable economic assets can be seen as aggressive behaviour that is more closely associated with the actions of a PMC than a PSC. He writes: "Some firms protect corporate sites that serve as primary funding sources for sides in civil wars or lie across critical lines of communication" (Singer 2008, 89). With China, this may, for example, be the case in Balochistan (Pakistan), where oil and gas pipelines run through territory that the Taliban consider to be theirs. However, it could also be argued that if most Chinese security companies are unarmed, then they must truly not be participants in any military-style operations. But Singer notes that companies which may describe themselves as security companies may still "[…] often perform military roles, with military consequences" (Singer 2008, 90). Examples here could include training allied combatants, providing intelligence from satellite images, or disabling enemy equipment through cyber operations. This leads to a definition according to which all security companies are theoretically capable of military operations, thus compromising the conceptual distinction between PSC and PMC.

Singer goes on to argue that instead of differentiating between only two labels it may be more accurate to define security companies (he uses the word *firms*) according to their respective Areas of Activity (Area of Operations, Theatre of Operations and Theatre of War). He then differentiates between three types of military firms that are each active in one of the three Areas of Activity: Military Provider Firms (in Area of Operations), Military Consulting Firms (in Theatre of Operations) and Military Support Firms (in Theatre of War). Direct kinetic combat is limited to the Area of Operations. Only Military Provider Firms are active in the Area of

Operations as they are the only type of firm that engages in direct kinetic combat. Military Consulting Firms and Military Support firms do not engage in direct kinetic combat and are thus exclusively to be found outside of the Area of Operations. These non-combat-oriented firms may, for example, assist with logistics or provide information and training on the fringes of the Area of Operations or further away. Provided below is an overview of the respective Areas of Activity.

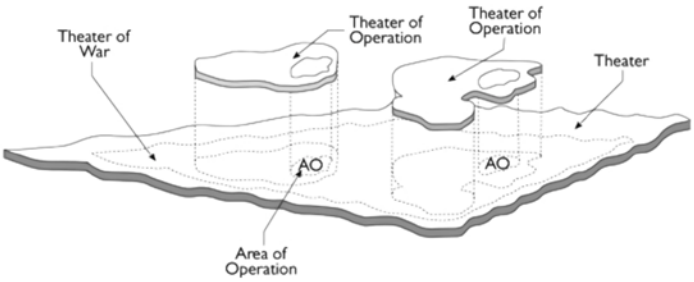


**Figure 1:** Source: (Singer 2008, 92)

There is, however, also a problem with Singer's definitions. NATO, in its *Allied Joint Doctrine for Force Protection,* writes: "The operational environment may have no discernible 'front-lines' or 'rear area' and an adversary may be expected to target Allied vulnerabilities anywhere with a wide range of capabilities" (NATO 2015, VII) (edited in December 2022 after the war in Ukraine began). What the war in Ukraine and, more recently, in Gaza has shown is that drones can, for instance, be used for attack and reconnaissance missions that allow for the precise targeting of both military and non-military personnel, as well as equipment far beyond any clear-cut front lines (far beyond the Area of Operations). Force protection guidelines then state that all forces, including forces far away from the Area of Operations, are required to protect themselves. This means that all forces in all Areas of Activity need to be prepared for potential kinetic combat. This leads to a situation in which kinetic combat is not exclusive to Singer's Area of Operations, which in turn leads to a breaking down of the clear definitional borders between Singer's Areas of Activity (no clear front lines), thus effectively weakening the usefulness of Singer's definitions. Cyber warfare also further complicates his definition since the Area of Operations in cyber warfare is diffuse. It would only be fair to state that since the release of Singer's book (the last edition released during the Iraq War), the nature of warfare has changed significantly. Due to the reduction in price and the broad availability of consumer electronics that have dual civil and military use, modern battlefield tactics have had to be adjusted accordingly. This has inevitably led to many military manuals being updated in recent years, including the above-mentioned NATO manual.

In this paper, I have chosen to stick with the binary labels of PSCs and PMCs as they are easier to use and understand. I would, however, plead for regarding the PSC and PMC labels as part of a bipolar spectrum. Here the PMC pole represents the most militarised version of a security company (in extreme cases completely substituting for entire military units) and, on the opposite side, the PSC pole represents the least militarised version (for example unarmed security advisors or logistics providers). What matters for the relative positioning on the bipolar spectrum is what the day-to-day business of a company is. In most cases, the day-to-day business of Chinese security companies can more clearly be associated with the PSC pole than with the PMC pole, especially in comparison to companies such as the defunct (and recently re-established) South African Executive Outcomes3 or the Russian Wagner PMC (both clearly situated on the PMC side). It is important to note that according to this definition, calling Chinese security companies PSCs does not preclude them from occasionally performing activities associated with the PMC end of the spectrum. They can still be referred to as PSCs if their day-to-day activities are more clearly associated with the PSC pole. Of course, conceptually the labels remain binary (either PSC or PMC). In any case, any alternative devising of a multipolar spectrum definition with labels for each degree on the spectrum would still require (even more) arbitrary definitional cut-off points and would thus quickly degenerate into an incomprehensible definitional mess. For these reasons, I will stick with the binary labels of PSC and PMC, while keeping the door open for a more nuanced definitional approach through individual placement of security companies in relation to each other on the bipolar spectrum.

## A Brief History of Chinese PSCs

Under Mao's communist rule, private companies were not allowed and thus no PSCs existed. With the later introduction of decentralised market mechanisms in the 1980s, some

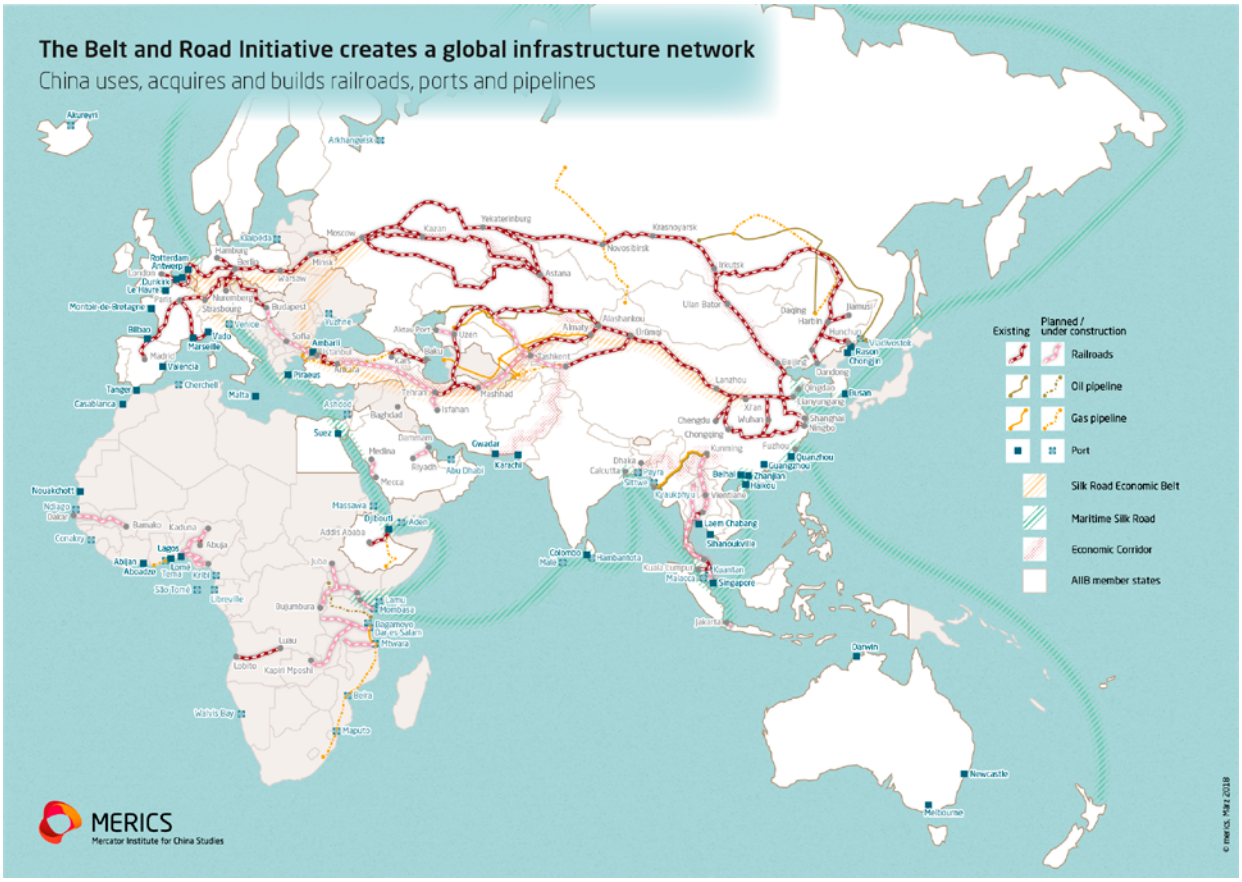


**Figure 2:** Source: MERICS (2018)

*click on the image to enlarge (web)*

early domestic private security providers emerged. However, these were always closely tied to the Public Security Bureau and thus under strict control of the CCP. Additionally, there was a strong conviction in the CCP that the Chinese government should have a monopoly on the use of firearms. This can be summarised as the principle of "the party holds the gun" (党指挥枪) (Sukhankin 2023), which is still broadly upheld to this day, meaning that there are virtually no armed domestic PSCs. The law, however, does not govern overseas PSCs. Nonetheless, according to unofficial government statements, such PSCs are strongly discouraged from using firearms (Legarda and Nouwens 2018). With the gradual opening of the Chinese economy to the world in the 1990s, an increasing number of Chinese companies started to establish themselves overseas. Sukhankin argues that two main events broadly discussed in Chinese media eventually led to the legalisation of PSCs domestically and then later also led to growing support for the use of PSCs to guard Chinese economic interests overseas (Sukhankin 2023). The first event was the 2004 killing of eleven Chinese road construction workers in their tents while they were sleeping, supposedly by the Taliban (Gall 2004). This event was arguably pivotal for the 2009 domestic legalisation of PSCs and the de facto endorsement of their operations overseas. What also followed in 2010 was a new law forcing overseas Chinese companies to follow strict security procedures and in many cases to provide their workers with security training and personnel to protect their work sites and their workers (Legarda and Nouwens 2018). This led to a further proliferation of Chinese PSCs overseas. The second event that Sukhankin mentions occurred more recently in 2019. This was an attack by the separatists of the Baluchistan Liberation Army that directly targeted Chinese investors who frequented the Zaver Pearl Continental Hotel in Gwadar Pakistan. The separatists specifically stated that China should expect further such attacks (Masood 2019). This arguably led to a further hardening of the perception that Chinese PSCs are necessarily needed to protect Chinese economic interests overseas.

## Past Focus on BRI Large Infrastructure Projects

In the last decade, most overseas Chinese PSCs were hired to protect Chinese assets and personnel working on large BRI infrastructure projects. The initial spread of overseas Chinese PSCs is thus inextricably linked to the BRI. Provided below is a map of some of the larger infrastructure projects of the BRI in Asia, Africa and Europe.

*"In the last decade, most overseas Chinese Private Security Companies were hired to protect Chinese assets and personnel working on large Belt and Road Initiative infrastructure projects."*

Funding for larger BRI infrastructure projects had already slowed significantly before the COVID-19 pandemic years and dwindled even more during and after the pandemic. More recently, China has shifted a big part of its BRI funding to what it calls the Health Silk Road (providing medical equipment during the COVID-19 pandemic and investing in medical infrastructure) and more notably the Digital Silk Road (DSR) (Nouwens 2023). The new focus on the DSR is prompting new concerns on how the Chinese security sector may be shifting its focus away from protecting large physical infrastructure to protecting and developing digital infrastructure along the BRI corridors (cell towers, satellites, surveillance technology etc.) The worry is that such technology may, for example, be equipped with software backdoors which could allow the Chinese government to monitor or manipulate data. This is not unprecedented. In one example, a legitimate Chinese software used for paying taxes, which businesses in China were required to use, had a backdoor installed which allowed the government to extract data (Cordey 2023). It is also likely that some countries in the Global South may be interested in hiring specialised Chinese security companies to help monitor and censor the internet to control local narratives and help track down dissidents.

*"It is also likely that some countries in the Global South may be interested in hiring specialised Chinese security companies to help monitor and censor the internet to control local narratives and help track down dissidents."*

## Can Chinese Security Companies be Private?

There are many misconceptions about private ownership of Chinese companies, including PSCs. It is true that for a long time under the Mao regime, private companies were not allowed. In modern China, however, companies can be privately owned. Renewed enforcement of previously introduced laws has, however, further muddled the distinction between the private and the governmental spheres. A law from 1993 mandated that all companies with three or more communist party members were required to form a party organisation within privately owned companies, which would be responsible for overseeing and enforcing the implementation of CCP laws and nurturing CCP values. For a long time, this law was not followed closely, but more recently the CCP has started enforcing it more strictly. By 2018 over 70% of companies had a party organisation (Livingston 2021). It is important to remember that domestic PSCs are mostly made up of ex-PLA soldiers who, when recruited, are strongly encouraged to join the CCP (the military is the military of the party, not of the country, and fielty is thus sworn to the party). Thus, it is likely that most if not all domestic PSCs are to a large extent made up of CCP members (especially if they employ ex-PLA officers) and thus the 1993 law would certainly require them to form party organisations, which would in turn allow the CCP to exert greater influence over them. Of course, this is not the same as being a government-owned company. Private companies with integrated CCP control elements are still factually privately owned. However, the fact that they have CCP members embedded in them who monitor the company and enforce the demands of the CCP does not correspond well with the understanding of private company ownership in Western countries.

Of course, all these regulations technically do not count for overseas PSCs founded by Chinese citizens. Such companies can, for example, be registered in the Bahamas or the United Arab Emirates as offshore companies, which is not an unusual practice for modern PSCs and PMCs (Singer 2008). But the reality is that most if not all Chinese PSCs have parent companies that are registered in China or, in the past, often in Hong Kong. But since Hong Kong is also slowly becoming more aligned with China, the same mechanism of party organisations becoming established within Hong Kong companies has also started appearing (Goldenziel 2023).

In summary, overseas Chinese security companies can be privately owned. There is, however, far more potential governmental control over Chinese privately owned companies than would otherwise be common

The largest and most active Chinese PSCs all claim to operate worldwide

| | China Security and Protection Group (中安保实业有限公司) | HuaXin ZhongAn (花信中安保安服务有限公司) | Beijing DeWe Security Services Limited Company (北京德威保安服务有限公司) | Frontier Services Group (先丰服务集团) | China Overseas Security Group (中国海外保安集团) |
|---|---|---|---|---|---|
| Number of employees | +30,000 | +15,000 | Total unknown, +350 based abroad | Total unknown, 432 in headquarters | +20,000 |
| Top leader-ship | Liu Wei (刘伟) (Chairman) | Yin Weihong (殷卫宏) (Founder) | Li Xiaopeng (李晓鹏) (Chairman) | Erik D. Prince (Chairman) | Jiang Xiaoming (蒋晓明) (Managing Director) |
| Date established | 1994 | 2004 | 2011 | 2014 | 2015 (consortium formed by 5 Chinese PSCs) |
| Where they claim to work | Global, with a BRI focus | Global | Global | BRI focus | Global, with a BRI focus |
| Website | http://www.cspbj.com/ | http://www.hxza.com/ | http://www.dewesecurity.com/sy | http://www.fsgroup.com/index.html | http://www.cosg-ss.com.cn/ |
| Logo | 中安保实业有限公司 | 华信中安 | | FRONTIER SERVICES GROUP | COSG |

© MERICS

*click on the image to enlarge (web)*

**Figure 3:** Source: MERICS (Legarda and Nouwens 2018)

among Western privately owned companies. It is hence reasonable to assume that most, if not all, Chinese PSCs operate in the interests of the CCP, which is not necessarily the case for other non-Chinese PSCs. The Wagner PMC, for example, operated counter to Russian government orders on several occasions, even before its uprising in Russia. All of this, however, does not change the fact that most PSCs and PMCs are often seen as extensions of certain governments, no matter what their form of ownership. Singer, for example, noted that Dyncorp, a PMC that fought against Columbian rebels, was always referred to as being made up of "Yankees" (Singer 2008).

This can be the case even if the company is not registered in the U.S. If most of its personnel come from one specific country and fulfil the wishes of the government of that country, then they are in essence the extension of that government, even if privately owned. To further complicate things, any overseas PSC or PMC can work with or for the local host government, in which case they could in parallel also be considered to be an extension of that government (Dyncorp's work aligned with the interests of both the U.S. and the Colombian governments).

## Chinese PSCs Today

The Chinese domestic PSC market is one of the biggest in the world, with over 7000 companies (Sukhankin 2023). The overseas Chinese PSC market is minuscule in comparison. Only around 20 companies are active overseas (Sukhankin 2023). It is difficult to gauge how active these PSCs are and how many personnel they employ. Researching their websites or contacting them for information usually does not lead to any useful insights and academics have cited widely varying numbers. Nonetheless, some academics have attempted to investigate specific modern overseas Chinese PSCs more thoroughly. Attached above is an image from the 2018 Legarda & Nouwens paper (Legarda and Nouwens 2018). It provides a short overview of some of the largest and most active overseas Chinese PSCs.

In many cases, overseas Chinese PSCs do not provide active security personnel themselves but function as advisors and liaisons between Chinese companies and other local security providers (private or governmental). This is arguably often necessary as the cultural and language barriers represent a significant obstacle for Chinese companies, which, by extension, also makes understanding local security issues more difficult (Sukhankin 2023). The strategy of employing Chinese PSCs as advisors and liaisons can be perceived as being less threatening and more favourable in terms of projecting a benign (non-offensive) image of China (Sukhankin 2023).

Most overseas Chinese PSCs hire ex-PLA soldiers and officers, as is the case with many other international

PSCs and PMCs who also recruit ex-military personnel. This reliance on specifically ex-PLA personnel may, however, constitute a problem for some overseas Chinese PSCs. Since most overseas Chinese PSCs provide advisory and liaison work, it would be important for them to better understand the security situation of their host country in order to optimally research and predict potential security threats. Chinese experts have, however, noted that ex-PLA personnel often exhibit very low levels of literacy and "struggle to even write a single report" (Rolland 2019). Sukhankin argues that for the roles overseas PSCs perform, their personnel are often critically unqualified. In their most common employment as liaison officers, it would be far more important for them to have, for example, studied security management and have a generally broader and higher level of general education. Security studies are, however, seldom taught at Chinese universities (only very few provide such curriculums) (Sukhankin 2023). This results in a situation where overseas PSCs employ personnel that can hardly communicate in any other language than Chinese and often lack the tools to analyse and understand the complex security situations of their host countries (including but not limited to ethno-religious divides, geography, local customs etc.). However, because the Chinese companies employing PSCs often also operate mostly in Chinese, they require Chinese-speaking counterparts in the security sector, and ex-PLA soldiers both have a security background and speak Chinese, thus fitting the bill, even if their abilities to interact with local security personnel and to understand local security issues are limited. Another problem is that because China has not been engaged in any military conflicts in recent history (last in 1979 with Vietnam), ex-PLA soldiers lack real-world conflict experience compared to other PSCs and PMCs, which, for example, recruit ex-soldiers from the U.S., Russia or Israel who have seen active service.

The unregulated nature of overseas Chinese PSCs also remains a significant problem. Compared to the domestic PSC market, the overseas market is not regulated at all (Legarda and Nouwens 2018). Overseas PSCs mostly follow unofficial guidelines derived from the comments of CCP officials. This means that overseas PSCs staffed with Chinese nationals could in theory legally turn themselves into PMCs if they wished, provided they follow the legal framework of their host countries. It is important to understand, however, that most if not all overseas Chinese PSCs have their headquarters in China and if their overseas activities are deemed problematic by the CCP, their domestic offices could be held accountable (for example, by blacklisting a specific PSC to deter them from working with overseas Chinese companies). In 2017 the CCP planned to release a white list of overseas PSCs that are deemed to have a sufficient quality standard to be employed by overseas Chinese companies (Sukhankin 2023). This would go a long way towards guaranteeing and to some degree regulating the work quality of overseas Chinese PSCs. Such a list has, however, not yet materialised.

## Spotlight on Frontier Services Group

Frontier Services Group (FSG) stands out in comparison to other overseas Chinese PSCs for its highly skilled and broadly specialised international employees and its global reach. It is one of the few (if not the only) Chinese PSCs comparable to other larger well established international PSCs or PMCs and thus it also has the most potential to tilt towards the PMC pole in the future. Until recently it was led by Erik Prince, founder of the former U.S. PMC Blackwater (Now called Academi and part of Constellis Holdings). What differentiates FSG from other overseas Chinese PSCs is that it employs highly educated (often Oxbridge and Ivy League) Chinese and Western security advisors and liaison officers and on occasion also employs international PSCs and PMCs as subcontractors. FSG has for example allegedly employed Western NATO fighter jet pilots to help train PLA Air Force Pilots (Sridharan 2023). Because of the activities of some of the local FSG branches, they have been sanctioned by the U.S. government in Kenya, Laos and the UAE (Department of Commerce 2023). There is also some contention about how much direct control the CCP has over FSG. The Chinese state-owned CITIC Group is by far the largest shareholder of FSG (with over 25%). Other smaller shareholders also have very close ties to the CCP.

## Current Chinese PSC Strategy

Some academics have argued that Chinese PSCs are still in their infancy and that their goal will inevitably be to develop into PMCs that can wage wars on behalf of the Chinese government. Weinbaum from the Rand Corporation, for example, mentions that one apparent strategy that overseas Chinese PSCs seem to utilise is to employ lo-

cal PSCs and then slowly acquire their know-how and copy their operating procedures in order to eventually supplant them. This reads like a common stereotypical narrative of how the Chinese are often seen as acting, especially in the economic sector, and arguably falls into the trap of yielding a compromised orientalist analysis. Weinbaum further argues that the Chinese government may for now want to seem more benign politically and would thus want to keep their overseas PSC operations at a threshold not quite equivalent to PMCs. But if the Chinese government wishes to pivot their strategy and become more aggressive, as has been observable in recent events in the South China Sea, this threshold could be crossed quickly, and PSCs turned into PMCs could be utilised to participate in wars overseas (Weinbaum 2022). The narrative of the CCP wishing to turn their PSCs into PMCs for future wars, however, contradicts the view of other academics. These researchers have instead emphasised that overseas Chinese PSCs mostly function in advisory and liaison roles and seldom use firearms themselves. Furthermore, they argue that this strategy is purposefully chosen and continuously endorsed by the Chinese government (Sukhankin 2023).

*"In summary, the Chinese government's strategy towards Private Security Companies is to try to make itself appear as benign as possible and to rely on local military and law enforcement if additional firepower is required."*

Would it be possible to rapidly turn overseas Chinese PSCs into PMCs? And could the CCP endorse such a pivot in the near future? In 2012 during the 11th Chinese People's Political Consultative Conference (中国人民政治协商会议), there were calls for the establishment of "security companies similar to Blackwater" (Sukhankin 2023). The Charhar Institute (察哈尔学会), a Chinese defence research institute, also noted that China does not yet have a company similar to Blackwater and that more needs to be done to provide security in volatile regions (Charhar Institute 2015). A few years later, however, the same Charhar Institute also strongly discouraged the use of firearms on a social media post on Baidu (Charhar Institute 2021). The CCP has also signalled its continued support for its "the party holds the gun" policy in recent years. Recently, Chinese scholars have also argued that the Wagner PMC mutiny in Russia would not have been possible in China exactly because of the aforementioned policy (Lau 2023). Some overseas Chinese PSCs have indeed acquired the licence to carry firearms from their host nations. Veteran Security Service (VSS) was, for example, allowed to carry firearms in South Sudan (Anthony and Hengkun 2015). This example seems, however, to be an exception rather than the norm.

In summary, the Chinese government's strategy towards PSCs is to try to make itself appear as benign as possible and to rely on local military and law enforcement if additional firepower is required. This means that overseas Chinese PSCs are also, by extension, not encouraged to provide the training and logistical support to their own personnel that would be required for a sustained military campaign. This diminishes the capacity for such PSCs to rapidly pivot towards performing military tasks more associated with PMCs.

Presently, a much more plausible scenario is that if the CCP deploys the PLA overseas, local Chinese PSCs could provide the PLA with intelligence and function in their roles as advisors and liaison officers in the PLA's favour (for example, by recruiting additional local combatants). Further improving Chinese technological surveillance and cyber operations of overseas PSCs would also help in gathering intelligence, especially if Chinese dual-use technology (for example in telecommunications) useful for intelligence gathering is already proliferated throughout the engagement zone. It is, for example, probably no coincidence that the Chinese government has recently bankrolled several communications satellite launches with several African governments (Nyabiage 2023). This entire strategy, however, hinges on the enhanced ability of overseas PSCs to gather intelligence locally across cultural and language barriers.

## Future Chinese PSC Strategy

As noted above, most overseas Chinese PSCs would have a hard time in seriously competing with the decades of experience

gained in classic security operations by other international PSCs and PMCs. Overseas Chinese PSCs may, however, develop other skill sets that could fill market gaps, especially if they go on to also advise foreign governments and companies in the areas of technological surveillance and cybersecurity. It is possible, though hardly definitive, that the CCP would strategically promote the above-mentioned scenario of overseas PSCs functioning as intelligence assets specialising in surveillance and cyber operations. In the Digital Silk Road Whitepaper, the CCP argues that the domains of digital, cyber and space are the new pillars of the BRI (National Development and Reform Commission (NDRC) 2015). This is also consistent with recent reports that China is, for example, developing a similar system to Elon Musk's Starlink, in which several thousand satellites would be launched into orbit to provide global internet coverage (Chen 2023). The first to receive this new high-speed satellite internet are some of the countries closely associated with the original BRI (Ma 2023). Such technology could, of course, also be used for surveillance and intelligence gathering. The CCP has identified these technological projects as areas where they could be the first providers of such services, hence potentially gaining long-term economic and security advantages of considerable impact, similar to how the U.S. did with the development of computers, smartphones and artificial intelligence with such companies as Google, Apple and Microsoft, whose services and devices can also be exploited for intelligence gathering. Nouwens also argues that this new focus on the DSR represents a shift in CCP thinking. In many countries, they could be the first to provide a digital infrastructure that may prove to be an effective platform for influencing and forming local narratives and values and to align them with Chinese narratives and values. Furthermore, the economic cost of the DSR is likely far lower than that of the BRI's initial large infrastructure projects. The effect and potential value that DSR projects have may, however, far outweigh that of previous BRI projects. Sukhankin argues that the Chinese government is still far from fully endorsing and supporting overseas PSCs in specializing in cyber conflict and surveillance. There seems, however, to be a general surge in PSCs becoming more specialised in these areas. Russia in the wake of the Ukraine war has, for example, already started to experiment with giving more cyber security tasks to PSCs (Sukhankin 2023). It would make sense for the CCP to follow suit, especially in light of the many young talented and educated university graduates in the field of cyber security and adjacent fields coming into the labour market and seeking jobs. Besides this, employing PSCs as cyber advisors for foreign companies and governments also creates more economic opportunities to sell civil-military dual-use technologies, which further advances their plans for the DSR.

***"In the Digital Silk Road Whitepaper, the Chinese Communist Party argues that the domains of digital, cyber and space are the new pillars of the Belt and Road Initiative."***

## Conclusion

With the Wagner PMC in recent years gaining international notoriety, many, especially in the mainstream news media, have asked if China also plans to utilise PMCs to wage future wars (see, for example, this article in The Diplomat (Lee and Wittman 2023)). Some of these news articles fail to differentiate between PSCs and PMCs and greatly exaggerate the capabilities of Chinese PSCs (see, for example, this VOA article (Bartlett 2023)). It can be argued that it might be strategically appealing to the Chinese government to develop their PSCs into PMCs. It seems clear, however, that for now, the CCP does not endorse this strategy. One CCP official commenting on the Wagner PMC uprising argued that Russia "raised a tiger and courted disaster" (a Chinese saying: "养护上身"). One reason for the CCP not wanting to help create Wagner-like PMCs may be that employing Chinese armed nationals abroad would not provide plausible deniability. Having talked to local people in several of the West African countries participating in BRI projects, what becomes clear is that it is common for them to think that the Chinese government itself is building the infrastructure in their country and that all Chinese companies working on those projects are simply an extension of said government. It is important to note here that the CCP does hold stakes in some of the bigger construction and resource extraction companies working within the BRI framework. Normally, plausible deniability is provided because PSCs or PMCs often do not wear uniforms or clearly identifiable markers. Ethnicity is, however, a strong identifiable marker. Arguably,

the Chinese government can only really profit from plausible deniability if it does not arm its citizens but instead uses them to recruit and arm local fighters instead. Overseas Chinese PSCs can, however, collect intelligence and provide solutions in the areas of surveillance and cybersecurity for other companies and governments. Operations in these areas provide far better plausible deniability and support the CCP's goal of focusing on controlling narratives around values and building digital infrastructure with its DSR projects.

***"Overseas Chinese Private Security Companies can collect intelligence and provide solutions in the areas of surveillance and cybersecurity for other companies and governments."***

In summary, there seems to be a lot of inaccurate and exaggerated information within mainstream news media and sometimes within academia as well with respect to overseas Chinese PSCs. This is problematic because it may hinder future analysts from uncovering the more subtle security strategies that the CCP is currently developing and will likely pursue in the future, which, as I have stated, are far more likely to be more closely associated with the recent focus on the Digital Silk Road. ◆

## Endnotes

**1** The CAR government has blamed a local rebel group. Controversially, however, that group has claimed that the gunmen were from the Russian Wagner group (Hong and Peltier 2023).

**2** The term *New Silk Road* is supposed to pay homage to the old silk road previously traveled by merchants in order to trade goods between China and Europe.

**3** The original Executive Outcomes was a South African PMC that was one of the largest and most active in its time. They were often hired for active combat roles mostly on the African continent and have in the past significantly influenced military operations in Angola and Sierra Leone. They disbanded in 1998 (and reestablished in 2020). The personnel of the original Executive Outcomes were mostly made up of South African ex-special forces troops from the Apartheid era of South Africa.

## References

Anthony, Ross, and Jiang Hengkun. 2015. "Forum: Security and Engagement: The Case of China and South Sudan". *African East-Asian Affairs* 0 (4). https://doi.org/10.7552/0-4-147.

Baptista, Eduardo, and Andrew Heavens. 2022. "Five Chinese Nationals Were Wounded in Kabul Hotel Attack – Chinese Foreign Ministry". *Reuters*, 13 December 2022, sec. Asia Pacific. https://www.reuters.com/world/asia-pacific/five-chinese-nationals-were-wounded-kabul-hotel-attack-chinese-foreign-ministry-2022-12-13/.

Bartlett, Kate. 2023. "How Chinese Private Security Companies in Africa Differ From Russia's". VOA. 31 March 2023. https://www.voanews.com/a/how-chinese-private-security-companies-in-africa-differ-from-russia-s-/7030946.html.

Charhar Institute. 2015. "私营安保公司: 中国海外安全的供给侧改革", December.

– – –. 2021. "海外安保的痛点与难点：既非打打杀杀，也不等同于看家护院". Social Media. Baidu. 20 July 2021. https://baijiahao.baidu.com/s?id=1705806385991854758&wfr=spider&for=pc.

Chen, Stephen. 2023. "China Is Supersizing Its Rocket Industry – and It's Coming for Starlink". South China Morning Post. 25 May 2023. https://www.scmp.com/news/china/science/article/3221831/china-supersizing-its-rocket-industry-and-its-coming-starlink.

Cordey, Sean. 2023. "Software Supply Chain Attacks: An Illustrated Typological Review". Application/pdf. ETH Zurich. https://doi.org/10.3929/ETHZ-B-000584947.

Department of Commerce. 2023. "Rules and Regulations". *Federal Register* 88 (No. 114). https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3289-88-fr-38739/file.

Gall, Carlotta. 2004. "Taliban Suspected in Killing of 11 Chinese Workers". *The New York Times*, 11 June 2004, sec. World. https://www.nytimes.com/2004/06/11/world/taliban-suspected-in-killing-of-11-chinese-workers.html.

Goldenziel, Jill. 2023. "Chinese Communist Party Demands Employees At Western Firm Show Their Support". Forbes. 27 February 2023. https://www.forbes.com/sites/jillgoldenziel/2023/02/27/chinese-communist-party-demands-employees-at-western-firm-show-their-support/.

Hong, Nicole, and Elian Peltier. 2023. "Mysterious Killing of Chinese Gold Miners Puts New Pressure on Beijing". *The New York Times*, 15 May 2023, sec. World. https://www.nytimes.com/2023/05/15/world/asia/china-africa-miners-wagner.html.

Lau, Jack. 2023. "China's Communist Party Confident in Military Grip after Russia's Wagner Rebellion, Experts Say". News. South China Morning Post. 1 July 2023. https://www.scmp.com/print/news/china/military/article/3226172/chinas-communist-party-confident-military-grip-after-russias-wagner-rebellion-experts-say.

Lee, Jong Min, and Samuel Wittman. 2023. "Will China's Private Security Companies Follow the Wagner Group's Footsteps in Africa?" *The Diplomat*, 24 June 2023. https://thediplomat.com/2023/06/will-chinas-private-security-companies-follow-the-wagner-groups-footsteps-in-africa/.

Legarda, Helena, and Meia Nouwens. 2018. "Guardians of the Belt and Road: The Internationalization of China's Private Security Companies". *Merics*, August. https://www.merics.org/en/report/guardians-belt-and-road.

Livingston, Scott. 2021. "The New Challenge of Communist Corporate Governance". *CSIS*, January. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210114_Livingston_New_Challenge.pdf.

Ma, Sylvia. 2023. "China Launches Satellite Internet That Could Challenge SpaceX's Starlink". South China Morning Post. 30 November 2023. https://www.scmp.com/news/china/science/article/3243351/china-launches-high-orbit-satellite-internet-could-challenge-spacexs-starlink.

Markusen, Max. 2022. "The Quiet Expansion of Chinese Private Security Companies". *CSIS Briefs*, January.

Masood, Salman. 2019. "Gunmen Attack Pakistan Hotel Used by Chinese and Vow Further Violence". *The New York Times*, 11 May 2019, sec. World. https://www.nytimes.com/2019/05/11/world/asia/pakistan-hotel-attack-gwadar.html.

MERICS. 2018. "Mapping the Belt and Road Initiative: This Is Where We Stand". MERICS. 7 June 2018. https://www.merics.org/en/tracker/mapping-belt-and-road-initiative-where-we-stand.

NATO. 2015. "Allied Joint Doctrine for Force Protection". NATO. https://www.cimic-coe.org/resources/external-publications/ajp-01-edf-v1-f.pdf.

Nouwens, Meia. 2023. "China's Belt and Road Initiative a Decade On". In *Asia-Pacific Regional Security Assessment 2023*, 90–114. London: The International Institute for Strategic Studies. https://doi.org/10.4324/9781003454724-5.

Nyabiage. 2023. "How China's 'Very Intentional' Push to Expand Africa's Space Industry Works". South China Morning Post. 21 November 2023. https://www.scmp.com/news/china/diplomacy/article/3242162/how-china-ties-space-projects-africa-climate-and-security-priorities.

Peltier, Elian. 2023. "Xi Condemns Killings in African Nation Where Russian and Chinese Interests Compete – The New York Times". 20 March 2023. https://www.nytimes.com/2023/03/20/world/europe/central-african-republic-russia-china.html.

Rolland, Nadège. 2019. "Securing the Belt and Road Initiative: China's Evolving Military Engagement Along the Silk Roads". *NBC Special Report (The National Bureau of Asian Studies)* 80 (September).

Shahzad, Asif. 2021. "Pakistan Says Attack That Killed Chinese Was a Suicide Bombing". *Reuters*, 12 August 2021, sec. Asia Pacific. https://www.reuters.com/world/asia-pacific/pakistan-foreign-min-says-bus-attack-that-killed-9-chinese-workers-was-suicide-2021-08-12/.

Shahzad, Asif, and Syed Raza Hassan. 2022. "Insight: Alarmed by Suicide Attack, China and Pakistan Work Together on Probe". *Reuters*, 31 October 2022, sec. Asia Pacific. https://www.reuters.com/world/asia-pacific/alarmed-by-suicide-attack-china-pakistan-join-hands-probe-2022-10-31/.

Singer, Peter Warren. 2008. *Corporate Warriors: The Rise of the Privatized Military Industry*. 10987654321. New York: Cornell University Press.

Sridharan, Harish. 2023. "Frontier Services Group Denies U.S. Allegations on Training Chinese Military Pilots". *Reuters*, 13 June 2023, sec. World. https://www.reuters.com/world/frontier-services-group-denied-us-allegations-training-chinese-military-pilots-2023-06-13/.

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

Weinbaum, Cortney. 2022. "China's Security Contractors Have Avoided the Fate of Russia's Military Contractors, So Far". *Rand Corporation*, March.