GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES
A GERMAN - AMERICAN PARTNERSHIP

GPCSS#4, December 14, 2021
'Russia and China's Intelligence and Information Operations Nexus:
Implications for Global Strategic Competition?'

Context:
It is difficult to make coherent distinctions between Chinese and Russian influence operations and political warfare. The reality in late 2021 is complex. Russian and Chinese intelligence agencies are best characterized not in terms of friends and enemies ('Frenemies') but friends and rivals ('Frivals'). The intelligence nexus between the two is compartmentalized and the balance is changing, with the FSB becoming more wary and the GRU more cooperative. Whereas a self-identified beleaguered Russia focuses on a defensive push-back against the West and the glories of its Great Power past ('imperial nationalism'), China looks inward at modernization and the promises of restored future global hegemony. Although China currently carries out intelligence operations in Russia, Russian or any other states' intelligence operations in China are inherently extremely difficult, with risk often outweighing gain, though Russian intelligence operations against Chinese diplomats or citizens outside of China are possible. (Instead, Russia relies heavily on 'hands-off' intelligence gathering by satellite, ELINT and cyber, as well as open source.)

Russian Approaches: Russian intelligence services (GRU, SVR, FSB) are competitive, effective but show the impact of the intense tempo of operations, ready to deploy A, B and C teams and willing to accept a number of failures. In this sense, for example, the SVR's analogue is not the CIA but rather than OSS or SOE, given it is placed on war footing. Intelligence is perceived not simply as an adjunct of policy but an instrument to change the world. Career-wise, intelligence culture promotes 'doers' and risk takers.

- The **SVR** has a formal relationship with China's military intelligence but not the Ministry of State Security. Nonetheless, it does have bilateral and SCO-mediated contacts, ready to pragmatically share/trade specific intelligence and tradecraft, especially in operations against the West. The SVR is committed to a wider range of partners than just China, and relations with third parties such as India, can limit cooperation with China.
- By contrast, though the **GRU** has been historically more cautious of collaboration with China, particularly given the nature of Sino-Russian geopolitical competition in Central Asia and elsewhere, recently a shift is discernable. At the Moscow International Conference of 2021 the head of the GRU echoed Defense Minister Shoigu's language around the value of cooperation with China and the threat of the US in the Pacific. Military-technical espionage and information operations are areas in which Russia has a lead, with GRU unit 54777 or the 72nd Special Service Center sharing techniques and tradecraft with the PLA's Strategic Support Force.
- The **FSB** cooperates with China's Ministry of State Security, especially in efforts to counter *jihadism* (leaning heavily on Central Asia intelligence servicers to do so) and on sharing intelligence against domestic threats. China does carry out intelligence operations in Russia and recently the FSB has become more vocal in its public statements, for example the FSB and *Rostelecom* blamed Chinese cyber mercenaries for hacks against Russian government targets, suggesting they were state-backed, thereby alerting political masters that there is a problem.

President Putin is on record as having identified Chinese presence in Russia as a potential 5th column.

Chinese Approaches: China under Xi Jinping seeks to restore the 'Middle Kingdom's' centrality to and primacy in global affairs. To that end China focuses on three pillars of effort, all of which have an intelligence/espionage component: the Belt and Road Initiative; 'Made in China 2025'; Civil-Military Integration or fusion (CMI), which translates into military modernization.

- **BRI**: China has codified and put into practice a national security intelligence system overseas which is led by the Ministry of Public Security. This intelligence collection system uses Private Security Companies (PSC's) for tactical and force protection of Chinese investments in over 60 BRI states, reporting through Chinese diplomatic missions. China leverages information gathered by China's space Information Corridor to sell/trade with BRI states, as well as the BRI's Digital Silk Road.
- **'Made in China 2025':** China identifies 10 key technologies that must be indigenously produced by 2025 if China is to gain global primacy. Of 700 open source cases of Chinese espionage (intellectual property theft) that can be identified, 500 relate to these 10 sectors.
- **Military Modernization and CMI:** China integrates the manufacture of commercial components and innovation in, for example, advanced robotics, aircraft engines, marine systems, space infrastructure etc., into China's national military modernization. China takes a Whole of Society approach, to achieve this end, combining the efforts of the Ministry of State Security, the PLA, PSC's, state enterprises and entrepreneurs.

Conclusions: GPCSS#4 offers four key takeaways:

- First, the Sino-Russian intelligence nexus is strongest when the foci of intelligence agencies in both states is anti-Western. This reflects a shared paranoia in both states against the specter of 'color revolution' inspired regime change. However, in China at least liaison officers are considered by their counter-intelligence services as the weakest link, inhibiting deeper cooperation.
- Second, the role of the governing party in both states – United Russia and the Chinese Communist Party (CCP) - is totally different, as is the role of security services in the state. Russia can credibly be characterized as a counter-intelligence state ruled by a *Chekistocracy;* even if China devolves into a digital Leninist and algorithmic authoritarian state, the CCP not China's *siloviki* have primacy.
- Third, if third parties in Russia's orbit, such as Belarus or Kazakhstan, may instrumentalize links with Chinese intelligence to pushback against Russia and maintain their own strategic autonomy, then it is likely the opposite occurs in China's orbit.
- Fourth, when it comes to the Sino-Russian axis (non-aggression pact), or coordinated alignment and then full alliance schema – the focus of the GPCSS - intelligence relations proves to be an outlier, transcending such categories. Human intelligence is by definition an intensely personal and emotional endeavor and every intelligence agency competes against every other. Intelligence cannot be artificially shoe-horned into wider the IR state-based categories of axis, alignment and alliance.

GCMC, December 15, 2021.