

**Sveva Musumeci****Gregorz Szczepański**

# China's Dual Strategy in Myanmar

## Leveraging Civil War Instability

### 3 Main Points

- Does China's simultaneous provision of cyber capabilities to the Myanmar military junta and tacit approval of actions that empower anti-junta groups constitute a deliberate strategy of "managed instability" designed to advance Beijing's economic and strategic interests? - China negotiates with



both factions allowing it to maintain good relations with both sides while securing its interests, such as the development of the BRI. - Not deliberate but has no interest in peace

### **About the Authors**

Grzegorz Szczepański is a soldier and licensed private investigator. He leads the „Venator” Foundation and works with organizations such as the Royal United Services Institute Next Gen Initiative, Conflict Research Society, and European Guanxi. His research focuses on China’s role in global security, the Middle East, and the activities of violent non-state actors (VNSAs) in modern warfare.

Sveva started her academic path in Maastricht where she studied European Studies and got interested in security and defence. This led her to narrow her academic interest specifically on security concerns and for this reason she choose the master in International Security Studies at Charles University in Prague. During her master, she got engaged with AI safety and security, which is currently her research focus.

### **China's Dual Strategy in Myanmar**

Since gaining independence from British rule in 1948, Myanmar has been engulfed in a complex civil war—the longest in modern history (Sadovschi, 2024; Roy, 2022). In February 2021, the military junta staged a coup d’état, abruptly ending a decade of civilian rule (Bächtold, 2022). Conflict escalated rapidly afterwards, involving not only drones and rifles but also internet shutdowns and surveillance to silence the resistance. This made the digital domain central to the conflict. In this context, it appears that the military junta has access to Chinese equipment and technology, calling into question its commitment to achieving peace in Myanmar (Hinz, 2022). Conversely, China seems to support anti-junta groups by providing weapons and acting as their primary trading partner (Roy, 2022; Hein, 2025). Indeed, Myanmar serves as a key peripheral state to Beijing’s foreign policy ambitions (Roy, 2022). From this, the primary question underpinning this article is whether China’s simultaneous provision of cyber capabilities to the Myanmar military junta and tacit approval of actions that empower anti-junta groups constitute a deliberate strategy of “managed instability” designed to advance Beijing’s economic and strategic interests.

Historical and Political Context



Myanmar's military, the Tatmadaw, has governed for decades, switching between direct dictatorship and a semi-civilian government while maintaining entrenched constitutional powers (Sadovschi, 2024; Roy, 2022). Since independence from Britain in 1948, the armed forces have positioned themselves as the ultimate guarantor of national unity, using the country's ethnic diversity and ongoing insurgencies to justify their dominance. This has led to the world's longest ongoing civil war, lasting nearly eight decades. The latest developments in the civil war occurred in 2021, when the military junta staged a coup d'état, nullifying the results of the 2020 election, detaining civilian leaders, and violently suppressing peaceful protests (Sadovschi, 2024). These actions abruptly ended a decade-long experiment with semi-civilian rule and reasserted the armed forces' monopoly on power.

Therefore, the military junta, along with its allies – notably the State Council Administration (SAC) – instigated or supported the military coup. Conversely, resistance quickly materialised, including anti-SAC efforts that emerged after the coup to oppose the military, consisting of the People's Defence Force (PDFs) and Ethnic Armed Organisations (EAOs) such as the Kachin Independence Army (KIA), Karen National Union (KNU), and Arakan Army (AA) (Sadovschi, 2024; The International Institute for Strategic Studies, n.d.). For the first time in decades, these groups began to work more systematically with Bamar-led forces, despite longstanding mistrust.

The resistance, operating in exile, coordinates political and military opposition, including the landmark Operation 1027 in 2023, where PDFs and EAOs jointly captured strategic towns (Rejwan and Romaniuk, 2025). Operation 1027 is widely regarded as a pivotal moment in the conflict. On the one hand, the resistance succeeded in gaining control of peripheral and rural regions; on the other hand, it dismantled scam centres established by Chinese-led crime networks (Rejwan and Romaniuk, 2025). This achievement not only resulted in tacit Beijing's support but also effectively dismantled a significant source of revenue for the military (Michael, 2025; Paing, 2024; The International Institute for Strategic Studies, n.d.). Today, Myanmar's landscape is fractured: the junta holds urban centres and military bases, while EAOs and PDFs dominate peripheral and rural regions. The result is a mosaic of shifting frontlines and contested governance, where neither side has been able to achieve a decisive victory.



The use of modern technology has become a crucial part of the ongoing civil war in Myanmar. The organisation of the resistance has been supported by connectivity and social media, which have been opposed by the military through aggressive strategies of digital repression and surveillance, including internet shutdowns and new cybersecurity laws.

Digital activism, especially on social media platforms like Facebook, played a crucial role in the Spring Revolution that followed the coup d'état (Lwin et al., 2025; Bächtold, 2022). Activists use digital platforms to report human rights abuses, organise protests, and counter state-sponsored misinformation. For example, they share information about logistics, including digital live maps showing police and military deployments across the country (Bächtold, 2022). In response, the military junta has aimed to establish extensive state surveillance and exert considerable control over digital spaces, often utilising technology and support from foreign entities (Justice for Myanmar, 2024; Bächtold, 2022; Sriyai, 2025; Hinz, 2022). Particularly, new cybersecurity laws enable the military to monitor online activities, detain dissidents, and restrict digital freedom (Khine, 2023; Lwin et al., 2025; Sriyai, 2025). Consequently, this involves not only importing Chinese equipment but also adopting the principles of "cyber sovereignty" – the idea that states have the exclusive right to control their digital domain (Hinz, 2022). Beyond surveillance, cybercrime has become a significant battleground. Criminal scam centres have emerged as major sources of revenue tolerated by the junta. Resistance groups, especially PDFs, have started targeting these hubs to weaken military finances and disrupt exploitative networks that prey on ordinary people (Justice for Myanmar, 2025; Michaels, 2025; Paing, 2024; The International Institute for Strategic Studies, n.d.). These measures have turned the online sphere into a vital front in the conflict.

### China's Strategic and Economic Engagement in Myanmar

China holds significant interests in Myanmar. The country is a strategic hub for the development of the Belt and Road Initiative (BRI), which explains substantial investments across economic, strategic, technological, and ideological spheres (Hinz, 2022; Hein, 2025; Roy, 2022; Bächtold, 2022). Beijing's engagement should not be seen merely as support for the military junta; rather, it reflects a carefully balanced approach aimed at maximising leverage and safeguarding long-term interests. Economically, Myanmar is a vital link in China's BRI, especially via the China–Myanmar



Economic Corridor (CMEC), which features key infrastructure such as the deep-sea port at Kyaukphyu, rail links connecting Yunnan to the Indian Ocean, and pipelines carrying oil and gas (Hein, 2025). Controlling these corridors is crucial for China's energy security, trade access, and regional influence. A fragmented Myanmar increases reliance on Chinese investment, secures influence over critical infrastructure projects, and prevents the country from pursuing independent economic or foreign policies, thus maintaining Beijing's negotiating power and project oversight.

Strategically, Myanmar acts as a buffer state, allowing China to extend its influence into South and Southeast Asia while keeping Western powers away from its borders (Michaels, 2025). Besides Myanmar's importance in terms of economic infrastructure, Beijing's approach is focused on deep engagement with the aim of widening its geopolitical sway (Roy, 2022; Michaels, 2025; Rejwan and Romaniuk, 2025). Through providing surveillance technologies, facial-recognition systems, encrypted communications infrastructure, and drones, China increases the Tatmadaw's dependency, reinforcing a form of strategic reliance. Simultaneously, selective tolerance of ethnic armed organisations (EAOs) and operations such as Operation 1027 demonstrate Beijing's use of proxy governance, permitting resistance activities to continue at a level that weakens the junta without disrupting Chinese interests (Michaels, 2025; Paing, 2024; Sadovschi, 2024). This multifaceted strategy keeps Myanmar divided enough to remain pliable, yet sufficiently functional to protect China's long-term projects, energy routes, and access to the Indian Ocean.

### China's involvement in the conflict

Beyond Beijing's foreign policy ambitions in Myanmar, the PRC's involvement in the conflict can be seen through infrastructure, ideological, and economic levels. At the infrastructure level, China's provision of advanced surveillance technologies from companies such as Huawei, Dahua, and Hikvision has significantly increased the military's capacity for monitoring civilians and opposition groups (Justice for Myanmar, 2024; Bächtold, 2022; Sriyai, 2025; Hinz, 2022). Hundreds of facial recognition cameras were initially installed in Naypyidaw and Yangon under the "safe city" initiative before the 2021 coup, with subsequent expansion to cover all 14 states and regions (Hinz, 2022). These systems, boosted by artificial intelligence, can automatically scan faces and vehicle



licence plates, alerting authorities to wanted individuals. For activists, journalists, and resistance fighters, this network represents a new level of digital authoritarianism, compelling them to adapt to a regime that monitors both physical and cyber spaces (Justice for Myanmar, 2024). Moreover, following Operation 1027, Beijing's alignment with the resistance increased due to the dismantling of scam centres at the border between China and Myanmar and the acquisition of territorial gains deemed essential for the development of the China–Myanmar Economic Corridor (Rejwan and Romaniuk, 2025). This development marked China's emergence as the primary trading partner of opposition forces, including the procurement of weapons (Paing, 2024; Hein, 2025).

At the ideological level, as previously noted, Beijing promoted the concept of “cyber sovereignty”. The supply of technological and surveillance equipment to the military junta facilitated the creation of systematic control over the digital space, aiming to suppress opposition groups (Hinz, 2022; Justice for Myanmar, 2024; Lwin et al., 2025; Sriyai, 2025). The fundamental idea behind this control indicates that the state has the right to exert authority within the cyber realm. At the same time, the People's Republic of China (PRC) took a stance of distancing itself from pro-democratic factions, which showed greater alignment with Western interests, although it did not offer any tangible support to resistance groups (Hein, 2025).

Finally, at the economic level, the conflict facilitated the development of scam centres along the Myanmar-China border, often targeting Chinese citizens (Paing, 2024). Since the coup, these centres have grown. The military junta has not taken direct action against them, as doing so would have led to a loss of revenue. However, the junta's hesitation to launch a large-scale anti-scam operation created a significant opportunity for the resistance, which was seen as tacit approval from the Chinese government for Operation 1027 in late 2023 (Justice for Myanmar, 2024; Rejwan and Romaniuk, 2025). Furthermore, Operation 1027 enabled resistance forces to seize control of key territories along the border with China, elevating their strategic importance for China due to the development of the China–Myanmar Economic Corridor (Rejwan and Romaniuk, 2025). Besides scam centres, Beijing fuelled a war economy by providing weapons and cyber tools to both sides and participating in illegal trading in Northern Myanmar, further complicating its peace support (Roy, 2022).



By balancing support for the junta with tolerance of select anti-junta activities, Beijing maintains control over strategically important areas for the development of its own infrastructure. This sophisticated approach illustrates how technological, economic, and ideological tools are integrated to achieve strategic goals without direct military intervention.

## Conclusion

Despite the apparent lack of a deliberate 'managed instability' strategy by China, considering the simultaneous destabilisation of its own investments, it is clear that Beijing has no genuine interest in peace or stability in Myanmar. It seems that the People's Republic of China is supporting the faction that is demonstrably in a stronger position, mainly to safeguard its own commercial and strategic assets within the country. Immediately after the military coup of 2021, the People's Republic of China unwaveringly supported the military junta by supplying technological equipment and surveillance systems. This move was primarily aimed at gaining access to strategic territories, generating revenue from a war economy, and effectively introducing the concept of 'cyber sovereignty' into the nation. Furthermore, the opposition was more aligned with Western ideals of democracy, a stance that Beijing did not endorse. However, along the border between China and Myanmar, several scam centres emerged that also targeted Chinese citizens. The military junta did not act against them, as this would have resulted in a loss of revenue. Operation 1027 was a pivotal moment because the resistance gained control of these territories and, with tacit support from Beijing, dismantled these centres. As a result, China began strengthening its ties with EAOs, becoming their primary arms supplier and trading partner. Therefore, it can be argued that China's involvement in the current conflict is more complex than simply supporting one faction; the choice of which to support depends on which can better secure its economic and strategic interests.

## References

- Bächtold, S. (2022). The smartphone and the coup. *International Journal of Public Policy*, 16(5).  
<https://doi.org/10.1504/IJPP.2022.10046665>



- Hein, Y. M. (2025, April 17). China's Double Game in Myanmar. Foreign Affairs. <https://www.foreignaffairs.com/china/chinas-double-game-myanmar>
- Hinz, E. (2022, July 28). How Myanmar's junta uses Chinese surveillance technology. Dw.com; Deutsche Welle. <https://www.dw.com/en/how-myanmars-junta-is-using-chinese-facial-recognition-technology/a-62624413>
- Justice for Myanmar. (2024). The Myanmar junta's partners in digital surveillance and censorship | Justice For Myanmar. Justiceformyanmar.org. <https://www.justiceformyanmar.org/stories/the-myanmar-juntas-partners-in-digital-surveillance-and-censorship>
- Khine, N. K. (2023). Digital rights in the post-coup Myanmar: Enabling factors for digital authoritarianism. *Journal of Human Rights and Peace Studies*, 9(2), 186–216. [https://www.researchgate.net/publication/377337004\\_Digital\\_Rights\\_in\\_Post-coup\\_Myanmar\\_Enabling\\_Factors\\_for\\_Digital\\_Authoritarianism\\_Journal\\_of\\_Human\\_Rights\\_and\\_Peace\\_Studies](https://www.researchgate.net/publication/377337004_Digital_Rights_in_Post-coup_Myanmar_Enabling_Factors_for_Digital_Authoritarianism_Journal_of_Human_Rights_and_Peace_Studies)
- Lwin, T., Aye, N., Tar, K., Sett, A., Aung, P., & Soe, K. (2025). Digital resistance Understanding perceptions of online spaces and tools in political activism in Myanmar. <https://secdev-foundation.org/wp-content/uploads/2025/07/K4DM-MDR-18-Digital-Resistance.pdf>
- Michaels, M. (2025). Myanmar's war to nowhere - IISS Myanmar Conflict Map. IISS Myanmar Conflict Map. <https://myanmar.iiss.org/analysis/war-to-nowhere>
- Paing, T. A. (Victor). (2024, August 26). China in Myanmar: How the Game-Changing Neighbor Would Continue to Maintain Its Influence • Stimson Center. Stimson Center. <https://www.stimson.org/2024/china-in-myanmar-how-the-game-changing-neighbor-would-continue-to-maintain-its-influence/>
- Romaniuk, S. N., & Rejwan, K. T. (2025, April 22). China's Geopolitical Balancing Act in Post-coup Myanmar. Geopolitical Monitor.



<https://www.geopoliticalmonitor.com/chinas-geopolitical-balancing-act-in-post-coup-myanmar/>

Roy, C. (2022). China's grand strategy and Myanmar's peace process. *International Relations of the Asia-Pacific*, 22(1), 69–99. <https://doi.org/10.1093/irap/lcaa012>

Sadovschi, A. (2024). Post-colonial Identity and Power Politics. The Case of Myanmar's Civil War. *EIRP*2024, 19(1), 255–266. <https://dp.univ-danubius.ro/index.php/EIRP/article/view/490>

Sriyai, S. (2025, January 24). Myanmar's Internet Shutdowns: Silencing Resistance in the Battle for Connectivity | FULCRUM. FULCRUM. <https://fulcrum.sg/myanmars-internet-shutdowns-silencing-resistance-in-the-battle-for-connectivity/>

The International Institute for Strategic Studies. (n.d.). Dashboard. IISS Myanmar Conflict Map. <https://myanmar.iiss.org/>

