THE REGIONALIST
INSTITUTE FOR REGIONAL SECURITY

CLASHING DOCTRINES AND STRATEGIC CULTURES: THE NEED FOR SINO-AUSTRALIAN CYBER COOPERATION

Nicholas Lyall

SYNOPSIS

To achieve mutually beneficial outcomes in the Australia-China military cyber relationship, Australia must use Lyle Goldstein's 'cooperation spirals' theory. This process involves starting with small, seemingly insignificant, cases of dialogue and partnership and gradually increasing the size and significance of these cases until a level of mutual understanding and cooperation has been established that is highly conducive to ongoing stability. Such a policy would greatly help to ensure that cyber, as the 'new frontier of warfare', does not become a military setting prone to excessive volatility and conflagration.

INTRODUCTION

In late June, Australia definitively announced its arrival on the military cyber scene with the establishment of the Australian Defence Force's (ADF) Information Warfare Division (IWD). The move is a crucial addition to Australia's cyber capability. However, if the IWD hopes to be a successful force for stability in the Asia Pacific cyber balance then it is crucial that a thorough understanding is generated by ADF policymakers and IWD officials of the concepts and mindsets that govern the operations of its main counterpart and potential adversary – China's People's Liberation Army (PLA) Strategic Support Force (SSF).

The SSF's concepts and mindsets present some potentially destabilising factors within the military balance of the Asia-Pacific. The IWD and ADF must engage the SSF and the PLA in cooperation initiatives. The aim of this engagement would be to increase mutual understanding in order to minimise the risk of unwarranted escalation of future tensions. The opportunities to constructively engage with China on this front will increase if officials and policymakers are equipped with such an understanding. At the very least, knowing how best to approach the challenge in order to avoid unnecessary conflagrations should be achievable.

CLASHING CYBER DOCTRINES AND ITS IMPLICATIONS

Working across the ADF's three service branches, the IWD is tasked with protecting Australia's military networks as well as engaging in offensive cyber operations against foreign targets. The IWD has a broad mandate; military cyber operations, military intelligence, joint electronic warfare, information operations, and the military's space operations are all covered under the unit's remit. The mandate for active defence and offensive operations powers is a clear announcement of Australia's intent to become a strong player in cyber warfare.

Similarly, the SSF was created in December 2015 to form an 'information umbrella' which would integrate space, cyber and electronic warfare in future PLA joint operations. Chinese officials described these three domains as the 'new areas that determine whether our army can win in the future battlefield'. Upon its creation, the SSF's assumed control over many elements of the PLA General Political Department, which include information operations, propaganda and psychological warfare. This development was salient because it positions the SSF as a prime political vehicle through which the CCP may pursue its ideological aims overseas, a mandate in competition to the ADF.

The mandate of the SSF was captured in a statement by its commander, General Gao Jin, where he asserted that the SSF will 'protect the high frontiers and new frontiers of national security,' while aiming to 'seize the strategic commanding heights of future military competition.' The SSF is viewed by Beijing as a flagship entity within the Chinese push to establish an asymmetric advantage over the US in the Western Pacific.

The SSF and IWD are approaching the cyber domain from incredibly different angles. Failure to build understanding risks escalating the likelihood of misinformed threat perceptions. Such misinformed perceptions can lead to volatile outcomes like cyber arms races.

CHINA'S 'OFFENSIVE DEFENCE' STRATEGY

PLA cyber 'retaliations' in response to perceived malicious foreign 'political or strategic motives' will probably increase. Active Defence – a cornerstone of PLA strategy – mandates PLA retaliation in defence of the nation in reaction to something as nebulous and nondescript as an adversary's political or strategic motives. Much of the PLA believes that the West is seeking to actively undermine the CCP.

Active Defence defines much of current PLA action, as displayed consistently over the previous decade in the East and South China Seas. The planned SSF joint integrated operations abilities are capabilities that Chinese strategists are intending to deploy in these theatres to further China's territorial sovereignty claims.

China's understanding of deterrence (wēishè - 威慑) will create further risk of escalation and conflict. In contrast to the western understanding of deterrence, wēishè is a military posture that is geared both to dissuade an adversary from threatening China's interests the PLA (deterrence) and also postured to compel an adversary to do something (compellence). China's posture against Freedom of Navigation Operations in the South China Sea is an example of wēishè.

In the context of the SSF, the combination of wēishè with the concept of Active Defence generates obvious escalatory potential vis-à-vis other nations or militaries. Being perceived, rightly or wrongly, as a military whose posture is more offensive than defensive may result in SSF actions being viewed by the IWD as overtly antagonistic, when in fact they may be more defensively minded. This is because the opacity of cyberspace makes the true intentions of a cyber actor hard to decipher, meaning it is often left up to whatever background knowledge the responder has of the initial actor in order to attribute intentions. Compounding this unstable status quo is the apparent lack of a clear Chinese model for de-escalation in case tensions do boil over.

AN ADF–PLA CYBER COOPERAITON SPIRAL – POLICY DIRECTION

The cyber relationship between Australia and China has a history of tension – as shown by the ASIO building plan and Bureau of Meteorology incidents. Australia must take a proactive stance in attempting to bulletproof the relationship as much as possible in order to prevent future cases of tensions from escalating unnecessarily. Australian policy must be to build an environment where cooperative measures in Sino-Australian military cyber affairs gradually proliferate and grow. A potential military cyber cooperation spiral that both nations should engage in could take the following steps:

Stage 1: Include the SSF and IWD in the Australia–China Defence Strategic Dialogue

The annual Australia–China Defence Strategic Dialogue presents an opportunity to begin addressing the chasm in cyber philosophies and mindset that exists between both nations. The dialogue typically includes initiatives like high-level officer visits, strategic policy forums, and cultural exchanges. In the cyber realm, this engagement could take the form of SSF-IWD staff exchanges, joint involvement in each other's low-level staff courses, and presentations to each other on the respective doctrines and strategies of both bodies as they pertain to cyber.

Stage 2: Invite China to observe joint exercises in the Singapore-Australia cyber agreement

Australia might invite China to observe joint exercises, such as those exercises planned in the new Singapore-Australia cyber security collaboration agreement. As this agreement was only established in June 2017, Beijing may view this gesture as a sign that Australia and the IWD aims to be a responsible and stabilising force in military cyber affairs. Singapore, whose agreement would be required, could perceive this collaboration as a prime opportunity, given that Singapore is currently manoeuvring itself into a strategic position in the widening diplomatic gap between the US and China.

Stage 3: Request limited observer status to the pre-existing Indonesia-China cyber security cooperation program

The Indonesia-China program appears to be more oriented towards government responses to cyber war as opposed to military-military cooperation so this would still leave room for further 'cooperation escalation'. There seems to be some confusion in public domain over whether this program includes cyber war simulation cooperation. If indeed cyber war games are not currently included in the program, then Australia could push to add them to the agenda. This move would display strong Australian diplomatic initiative to Asia-Pacific cyber statecraft and could be received by China as a positive signal. A further escalation of this spiral could be Australia's accession as a third full member, making it a tri-lateral program.

Stage 4: Implement a cyber war games initiative

With mutual cooperation better embedded, Australia should seek to implement a definitive cooperative initiative, such as a re-occurring IWD-SSF cyber warfare simulation program – Sino-Australian war games being something that has occurred previously. In addition to warfare simulations, such a program could include cyber war mitigations and cyber crisis management. A key feature of these war games should be a focus on understanding the operational disparity in both nations' conceptions of Active Defence. Another important feature would be a focus on developing cyber war de-escalation doctrine, which the PLA currently lacks. Australia and China could hold high-level military and diplomatic talks alongside the cyber war game to attempt to agree on and delineate red lines regarding state-based cyber attacks on targets like critical infrastructure.