THE REGIONALIST
INSTITUTE FOR REGIONAL SECURITY

CYBER 'KONFRONTASI'

Thomas Paterson

Key customers: Department of Defence (Australian Signals Directorate, International Policy Division, Strategic Policy Division); Department of Home Affairs (Cyber Security Division); Department of Foreign Affairs and Trade (Indonesia Branch, National Security Strategy, Cyber & Intelligence Branch & Ambassador for Cyber Affairs); Department of Prime Minister and Cabinet (National Security Division, International Policy).

Indonesia's economic growth means it is on track to becoming the world's fourth largest economy in purchasing power parity terms by 2050. As a result Indonesia has the opportunity to become a major power in Asia in the coming decades. This would offer Australia significant economic opportunity but potentially create a strategic problem. Indonesia's economic growth would enable it to generate greater strategic capacity, which would include cyber capabilities. If Australia and Indonesia experience a major disagreement or develop significantly divergent national interests in the future, cyber capabilities would represent an attractive means for Indonesia to protect those interests. Australia must continue increasing strategic engagement with Indonesia to further enable the type of close relationship that best ensures Indonesia remain a strategic partner. A closer cyberspace partnership would help strengthen the relationship and disincentivise future cyber aggression.

INCREASING CYBER CAPABILITY

The Indo-Pacific region is witnessing significant changes in the balance of power with the rise of China, which has significant implications for Indonesia. Although it has always liked to hedge in its relationships with other states, Indonesia's strategic threat perception is being challenged by its experience of tensions with China over the Natuna Islands. Strategic threats for Indonesia also emanate from cyberspace, largely because Indonesia is one of the world's most cyber vulnerable states; it was ranked of 70th of 193 countries in the International Telecommunications Union's 'Global Cybersecurity Index' 2017. In 2013, Indonesia even became for a short period the world's largest source of cyber attack traffic.

Cyberspace presents not only strategic risks but also strategic opportunities for Indonesia. As a domain, cyberspace presents as an attractive area of strategic investment for the Indonesian military, because the barrier to entry and cost threshold is low relative to expensive traditional military platforms. Cyberspace also opens up participation in the military for people who would otherwise have not been interested or capable of joining. These benefits represent an opportunity for the Indonesian government to build an effective offensive and defensive cyber capability. Investment in cyber capabilities is also attractive because cyber technologies can have a dual use benefit in addressing the various non-military cyber security issues Indonesia faces, including disinformation and cyber crime.

The Indonesian government has been trying to improve cyber security to reduce vulnerability and increase capability, although they remain some-way off achieving full cyber maturity. Current reform efforts include the State Code Authority (Lemsaneg) being subsumed into the national cyber coordination authority – the Badan Siber dan Sandi Negara (BSSN). Problematically, budget constraints have hampered Indonesia's ability to more quickly develop its cyber capabilities. Indonesia is thus unlikely to currently possess an offensive cyber capability that could threaten Australia.

Although this threat is likely to remain low during the next decade, the trajectory of Indonesian economic growth and the strategic capability dividends this growth could produce, gives Indonesia the potential to become a great power. Increased capabilities could in future include a capacity to launch offensive cyber attacks. This could represent a security risk for Australia, particularly if Indonesia is willing to use this capability against Australia to protect its interests.

DIVERGENT INTERESTS – TERRITORIAL INTEGRITY

Indonesia is likely to eventually develop mature offensive cyber capabilities, as its asymmetric benefits are attractive to states like Indonesia that have small defence budgets and instead direct spending toward health, education and infrastructure. If Indonesia and Australia were to experience a major disagreement over territory or maritime boundaries, there may exist an incentive to strike using cyber weapons. Cyber weapons are attractive because they offer states the ability to deliberately operate below the threshold of armed conflict to gain an advantage. Any offensive cyber exchange would be damaging to both states, but Indonesia would enjoy greater resolve due to the importance of territorial integrity. One of the potential flashpoints is West Papua. Forty-five per cent of Indonesia's copper reserves and 41m hectares of productive forest are located in West Papua, and this greatly contributes to Indonesia's resolve to retain this territory in particular. Indonesia also fears a separatist movement domino effect, where the loss of West Papua would galvanise unrest in other areas like Aceh (North Sumatra), Maluku Islands, Minahasa (North Sulawesi), Riau (Eastern Sumatra) and Kalimantan.

This resolve would be heightened in a future where Indonesia has more economic weight, which has allowed it to develop its conventional capabilities and improve its force posture. Also the US would not necessarily back Australia, like it did during the East Timor intervention, for fear of pushing Indonesia into the arms of China. The strategic challenge from China means the US now has a much greater perception of Indonesia's value as a partner in the Indo-Pacific. As a result, the US would be unlikely to take sides in any major disagreement between Indonesia and Australia - significantly decreasing Australia's resolve and increasing Indonesia's strategic confidence.

DIVERGENT INTERESTS – AUTHORITARIANISM 2.0

If Indonesia becomes a far more powerful state in South East Asia and the US surrenders its dominant position in the Indo-Pacific, Australia would become much more vulnerable. An Indonesian government willing to deploy cyber power against Australia could exploit this vulnerability. The willingness to do so would be heightened if Indonesia were to revert to authoritarianism. While Indonesia is a democracy the likelihood of conflict is low, but if Indonesia were to revert to being an authoritarian state headed by a belligerent leader, this could change. Ideological motivations combined with a lack democratic checks and balances could result in a situation where Indonesia is willing to use cyber power against Australia.

Although the trade losses and economic damage that could result from Indonesia deploying cyber power against Australia would be significant, this

might not deter an authoritarian regime. Australia was worth $2.5 bn dollars to Indonesia as an export market and Australian tourists also contributed $3.1 bn to the Indonesian economy in 2017. Even though Indonesian aggression towards Australia would risk two-way trade of more than $16.5 bn, an authoritarian regime not as beholden to voters could more easily choose to sacrifice this trade in pursuit of other interests. The willingness to incur economic costs would also be more likely if Indonesia's economy was bigger and it could more easily absorb losses. Where Indonesia has also developed greater strategic capabilities off the back of major economic growth, the willingness to project power against Australia would be even more distinct.

Increasing conservative Islamism in Indonesian society and politics is becoming more conspicuous, indicating the possibility that Indonesia could also become an authoritarian Islamic state. One particularly alarming development that indicates the pervasiveness of conservative Islamism in Indonesian institutions is the release of an Indonesian intelligence (Badan Intelijen Negara) document that lists 1,300 senior civil service, university, military and police members as belonging to the hardliner pan-Islamist group Hizb ut-Tahrir Indonesia (HTI). This includes 10-15 per cent of Indonesia's junior army officers.

Indonesia is currently suffering from a widespread apathy towards democracy and democratic institutions amongst the ruling elite from across the political spectrum, which has resulted in an appetite for strong populist leaders. Indonesia's recent history with authoritarianism also contributes to the potential for democratic retreat. Indonesian political figures advocating for a rolling back of key democratic reforms further increase the potential for this to occur. The proposed legal revisions and policies currently being pursued by the Indonesian government, demonstrate an illiberal turn that increases the potential for a backsliding towards authoritarianism. A seemingly well-executed election does not preclude this, as the underlying causes are much more deep-seated.

The deployment of cyber power against Australia would be even more likely if a belligerent leader came to power in an authoritarian Indonesia. Because authoritarian leaders are not as beholden to voters they can act more arbitrarily, which can include engaging in acts of aggression towards other states. Cyber power is an attractive measure to authoritarian leaders because it allows for aggressive actions to be perpetrated with less risk of attribution or decisive pushback. An authoritarian Indonesian leader with greater strategic capabilities may choose to project cyber power against Australia as a deterrent, or as a 'below the threshold'

measure in an attempt to achieve escalation dominance. This could occur in response to a disagreement over West Papua, maritime boundaries in the Timor Sea or even prior to any action to re-take Timor-Leste. In a future where Indonesia is far more powerful and the US might not support Australia in a disagreement with Indonesia, an authoritarian Indonesian leader may choose to take strong actions based off a strategic calculation that Australia does not have the resolve to respond.

POLICY RECOMMENDATIONS

Australia needs to position itself to avoid these potential outcomes. As Indonesia does not currently present as a conceivable threat to Australia, now is the time to be building a relationship that means Indonesia is irrevocably aligned with Australia. The recently announced Comprehensive Strategic Partnership and subsequent MoU on Cyber Cooperation is a positive step in the right direction, but more needs to be done. Further increasing strategic engagement would not only create better economic opportunities but also create the necessary pre-conditions for a potential alliance agreement in the future. Australia should conduct its relations with Indonesia in a manner that keeps open the option of a future alliance agreement, especially if the US was to become increasingly isolationist and accept Chinese regional dominance in East and Southeast Asia. Further strategic engagement should particularly focus on cyberspace, which could help to further bolster the relationship.

Cyber Exercises

Indonesia struggles with institution building, at which Australia excels. Australia could positively contribute further to Indonesian development of a mature and friendly cyber capability across multiple departments. DFAT has been engaging with the BSSN in capacity building exercises but more could be done. The Australian Government should look to secure agreement from Indonesia to hold tri-annual Indonesia–Australia cyber conferences and crisis management exercises. This forum would be helpful for further enabling a closer cyber relationship by involving stakeholders from across government and industry from both nations. The forum should include scenario-based cyber exercises for the purpose of war-gaming responses to cyber crisis situations. Such an activity could provide a platform to develop closer department-to-department relationships through exercises, such as between the TNI's cyber unit(s) and the ADF's Information Warfare Division. This platform would promote the exchange of ideas on how to better respond to cyber incidents, as well as build stronger people-to-people links and institutional relationships. Such a program would help Indonesian's cyber-related institutions increase their cyber maturity and also give Australia

another platform from which to monitor and influence Indonesia's cyber development.

Educational Links

An emphasis on education would also be prudent. The MoU includes clauses referring to long-term awards such as masters and PhD scholarships. Because the MoU does not provide further detail, the government should publically clarify this aspect to enable greater public understanding of the related benefits to further garner public support. The government should also make a large number of Australia Awards scholarships available for Indonesian students to study cyber courses, particularly cyber policy related courses, at Australian universities. This access would give the next generation of Indonesian cyber security practitioners and leaders exposure to Australia. It would not only stimulate important cross-cultural people-to-people links, but also ensure a certain level of positive influence on how those future leaders think about Australia and cyber policy issues. This education would help promote the 'free and open' internet model to the next generation of Indonesian cyber policy leaders.

Official Exchange Program

In order to foster closer cyber relations in step with the broader defence relationship, a personnel exchange program should be developed with the BSSN. DFAT has been engaging the BSSN alongside other Indonesian cyber security related government departments in short duration programs, but a longer-term government two-way exchange program would be beneficial. An ASD or DFAT personnel exchange program with the BSSN, where cyber policy analysts spend time working together over a longer period, would be highly beneficial to both states. This exchange would be mutually beneficial because it would also help increase closer personal and institutional links. It would help promote further cyber cooperation and capacity improvement, while acting as a confidence building measure to strengthen and reinforce the official relationship. The program would also help increase cooperation against common threats to both nations such as cybercrime, and act as another mechanism to positively influence the development of Indonesian cyber capability.

POTENTIAL RISKS

An official exchange program would present a significant security risk. This risk is heightened by the fact that the BSSN and ASD are both signals intelligence agencies that deal in highly sensitive classified information. While acute, this risk can be mitigated with comprehensive security and program management procedures. Even in the face of a certain level of security risk, a personnel exchange program would be exceedingly beneficial. The relationship dividend of a

consistent and longer-term personnel exchange program would outweigh the potential security risk.

Another broader risk in developing a closer strategic relationship with Indonesia would be if Indonesia engages in behaviour that damages its international image, thus reflecting badly on Australia by extension. In this scenario Australia might have to choose between its close and vital relationship with Indonesia, and being seen as a good global actor that upholds and diligently reinforces United Nations norms. Indonesia could act in ways that are judged as contravening human rights standards or as mistreatment of its own citizens. For example, Indonesia's military could act improperly in areas of unrest, such as West Papua, or Indonesia could further increase online censorship and reduce civil freedoms through draconian legislative revisions. Closer engagement between both states, and Australia consistently encouraging Indonesia to increase transparency, strengthen democratic institutions and closely abide by international norms, would help mitigate this risk.

Thomas Paterson is a freelance writer covering national security and cyber policy issues. He holds a Master of Strategic Studies from the Strategic and Defence Studies Centre (SDSC) at the Australian National University (ANU). Thomas was an ANU research intern with the International Cyber Policy Centre (ICPC) at the Australian Strategic Policy Institute (ASPI) in 2018. He Tweets @1homaspaterson.