CHAPTER 5

Future Japan-Australia Pathways to Defence Collaboration: The Australian Perspective

Andrew Davies

Abstract

Australia and Japan share a great many security interests, not least of which the alliances we both have with the United States under the 'hub and spokes' model. As a result, we are in many ways natural partners. However, and for various reasons, we've only recently started to explore the possible mechanisms for defence collaboration. There are several avenues we could explore. In approximate increasing degree of complexity and/or sensitivity, areas for collaborative work can be broadly classified as follows.

Low sensitivity
- Humanitarian and disaster relief capabilities
- 'Second order' security activities, such as anti-piracy patrols and counter terrorism
- Collaboration on cyber defence

Medium sensitivity
- Military exercises
- Collaboration on the development of military capabilities. Examples might include submarine technology and ballistic missile defence

High sensitivity
- Collaboration on foreign intelligence collection
- Development of a shared response to the US 'Air Sea Battle' model
- Collaboration on sensitive 'asymmetric' capabilities, such as cyber warfare and electronic attack

The low sensitivity activities are easy to justify and pursue. The medium sensitivity issues are workable and more can be done in those areas. The high sensitivity activities require more discussion—but the US rebalance in the

Asia Pacific is going to force us to think about them.

Why should we work together?

Australia and Japan are American Allies under the San Francisco system, democracies, OECD members and stakeholders in a stable international order. We have both benefitted greatly from the leadership the United States has demonstrated over the past half century. As a result, we have a shared interest in maintaining the international norms that have allowed our countries to prosper and be secure.

That's largely why Australia and Japan signed a 'Joint Declaration on Security Cooperation' in March 2007. The aim was to create mechanisms by which we could work together 'to respond to new security challenges and threats, as they arise' and 'create a comprehensive framework for the enhancement of security cooperation' between the two countries. Since then, I think it fair to say that the security situation has become more complex—I hesitate to say 'worsened' because the same factors that were in our collective minds then are still present today. Some, such as the threat posed by international terrorism seems to have been reduced. However, the threats posed by the proliferation of WMD remain, and the power balance in the Asia Pacific is shifting in ways that we mightn't like. Cyber security threats have increased exponentially over that time.

In the five years since the Joint Declaration was promulgated, there has been some good progress made in developing a shared idea of how we might work together, but I don't think that either side believes that we have got anywhere near the full potential of the relationship. It's a good time for us to be thinking about the next steps.

Why now?

Perhaps the main reason that Australia and Japan haven't done more together in

security cooperation in the past has been that has been no especially compelling reason for us to do so. While we share the interests noted above, our capitals are separated by 8,000 km, which introduces some practical challenges for routine collaboration. And for the last half of the twentieth century, we have been too busy enjoying an extended period of (mostly) peace and getting on with building our nations. In short, the costs of collaboration outweighed the benefits.

But today we have a number of external drivers that are changing the calculus. They are:

- Demographic trends are causing increased numbers of people living in areas prone to natural disasters, meaning an increased demand for humanitarian and disaster relief operations. The potential impact of climate change in the future will further exacerbate this trend
- Globalisation—distance doesn't mean what it used to mean. In areas of non-traditional security, multinational groups can pose a threat from almost anywhere. In the maritime domain, the world's major trade routes carry import and export traffic from essentially all countries
- (related to the above point) countries that are geographically well separated still share common infrastructure in cyberspace, especially with the convergence of communications and computer systems
- The rising cost and complexity of military systems is driving defence industry companies operating towards mergers, and is also forcing like-minded countries to look for areas where they can share the R&D burden
- Military modernisation in Asia and the resulting proliferation of high-level capabilities, including anti-access and area denial (A2AD) systems
- Countries such as North Korea and Iran are developing nuclear and missile capabilities that can directly threaten their immediate regions and, if exported, have a wider significance
- The rise of China—more than anything else, the shift in power relativities in the western Pacific and the lack of a shared world view between the United States and the PRC

- (related to the previous two points) the United States is developing new strategies for operating in an environment where an adversary is attempting to deny access. The Joint Operational Access Concept and its subordinate AirSea Battle (ASB) concept put a premium on allies providing support in the form of bases and/or military contributions

In short, there are many reasons for Australia and Japan (and other countries with whom our interests are aligned) to develop a greater degree of cooperation on security issues.

Some of the factors in the list above are areas where Australia, Japan and other countries already have cooperative programs in place or under development. Examples include multilateral efforts to combat naval piracy, to which Australia and Japan have contributed warships, military exercises to build confidence and experience across regional militaries and humanitarian and disaster relief operations, in which many countries have participated. As well, there are developing relationships in the area of cyber security and network defence. These are all positive developments, and I'm sure we'll see more activity of those sorts. But they are in some ways 'second order' security matters—with the exception of cyber security—and are less challenging to develop than 'first order' security relationships involving the top end military capabilities and the more difficult issues thrown up by the geopolitics of the Asia Pacific region and beyond. Since this paper is about future pathways to deeper cooperation, the remainder of the paper will focus on those areas—noting that they are likely to prove as difficult as they are important.

Having said that, it doesn't necessarily follow that Australia and Japan should be looking for deep cooperation on all security issues. There will be instances where our interests don't coincide to any great degree. In every case, the two governments will balance the costs and benefits (immediate or potential) and make decisions based on judgements of how their national interest is best served. For example, Japan has much less stake in the stability of The Solomon Islands or Timor Leste than does Australia. Similarly, the extent to

which Australia wants to become enmeshed in North Asian security remains a lively topic for national discussion. At the time of the Joint Declaration that the then Australian Opposition Leader (and future Prime Minister), Kevin, Rudd, supported enhanced security co-operation with Japan, but opposed a mutual defence pact, saying that 'to do so at this stage may unnecessarily tie our security interests to the vicissitudes of an unknown security policy future in North East Asia.' And influential Australian thinkers like Hugh White actively advocate an Australian policy line that is more 'neutral' between Washington and Beijing.

The degree of cooperation between Australia, Japan, the United States and other countries will be decided by future governments on all sides, and they will weigh many factors when doing so. For Australia and Japan, one of the most important will be the expectations that the United States has of each of our contributions to the wider security framework it is trying to put in place. And let us be blunt—what we are talking about it the response of the established regional powers to the rise of China. There is already a strategic competition underway between the United States and China. So far it has been benign, but there are signs that it could become more complex and potentially dangerous. The United States has made it clear in public that it would like both Australia and Japan to do more in the sphere of military security. It would be unwise for us to not think about how we might fit into the bigger picture and the stance we might take.

AirSea Battle and America'a allies

For now, one of the major policy challenges for Australia and Japan (and for other countries in the region) is how we should respond—individually and collectively—to the US pivot/rebalancing now underway and the accompanying development of strategic and military concepts. The most important of these is the 'AirSea Battle' (ASB) concept, which has become the most visible sign of efforts by the United States' military to readjust its military doctrine to deal with the growing A2/AD challenge. So far, the debate

in the United States on 'AirSea Battle' has paid relatively little attention to the views and roles of America's Asian allies in this concept. However, as a Center of Strategic and Budgetary Assessment (CSBA) report noted: 'AirSea Battle is not a US-only concept. Allies such as Japan and Australia, and possibly others, must play important enabling roles in a stable military balance.' This raises some important strategic considerations for our defence planning, and it potentially complicates the delicate balancing act between the United States as security ally and China as major trading partner—which is the case for both Australia and Japan.

At least in the public domain, we know relatively little about ASB. But we do know that the American thinking includes a layered approach to defeating A2/AD, and there several aspects that will potentially impinge on Australia and Japan's force structures and/or doctrine development. Alternatively, either or both countries might be forced to decide what we aren't prepared to do. The ASB components of most significance in this respect are:

- the hardening of bases in North Asia (especially ROK, Japan and Guam)
- a 'defence in depth' approach of dispersing US forces across a wider area
- tactics and technologies to disrupt the command, control and ISR capabilities of the PLA
- deep strike capabilities against distant targets
- distant blockade operations against shipping traffic to and from China.

The first two of these activities are relatively easy to implement, and can be done on a bilateral basis with the US. Agreements on the hardening of bases or the hosting of US forces are basically matters for the US and its allies and partners to discuss among themselves. For example, Singapore has agreed to host four USN warships and Australia will host 2,500 USMC personnel and additional port visits by American vessels. But the last three of the dot points above are serious undertakings indeed, and would require a great deal of commitment on behalf of America's allies if we are to participate.

But we should at least think through the capabilities that would be required for us to do so—even if we subsequently decide that they are steps too far. And the way in which the issues will need to be discussed won't be the same for our countries, although they are likely to be controversial in both. Australia has long been involved in expeditionary military operations—including participation in many wars—in support of its major power allies. So to some extent participation in ASB would be consistent with previous Australian policy. But, as noted above, Australia is currently debating where on the spectrum of cooperation with the United States we want to sit, and to what extent we want to avoid confrontation with China—in short, how we balance our security and economic interests. Japan faces the same issue, as well as unresolved territorial disputes, but any participation in ASB is likely to be further complicated by Article 9 considerations. For example, it seems unlikely to me that Japan would consider the development of deep strike capabilities.

And it's also not clear that all of the elements in AirSea Battle are things we would want to support. For example, extensive disruption of the command and control and ISR networks of a nuclear power during a serious confrontation doesn't help in managing escalation—which will be one of the major concerns in any future conflict. These are serious issues, and it is to be hoped that the United States will share more details of its thinking as the concept develops.

Nonetheless, there are things that Australia and Japan could do that are short of full participation but would allow a tiered engagement—which we could adjust in either direction in the future should circumstances require it—as well as supporting and enabling the American concepts. Two broad classes of activity are the development of naval forces that are interoperable with the USN and cooperation on the development of capabilities for computer network operations. Neither would commit Australia or Japan to ASB, but both are likely to be welcomed by the United States as adding depth to their own capabilities and both would give us the option of participation in American activities at various levels of commitment.

Submarines—an area for Australia/Japan cooperation?

Australia and Japan both have sophisticated naval capabilities and both employ American-sourced systems such as the P-3 Orion, Aegis combat system and Seahawk helicopters. Both navies exercise with the USN and both have a good degree of interoperability with the USN. There is not much we have to do to be able to work with the Americans at sea. However, there is one current opportunity for collaboration between Japan, Australia and the United States which would further the cause of interoperability—Australia's future submarine (FSM) project.

The FSM has been the subject of much discussion in Australia, and we are in the process of gathering information in order to decide on the best way ahead. There are four options on the table (all diesel-electric), but the stated requirement is for a long range submarine with high endurance and a substantial payload. As well, interoperability with the USN and the desire to have the best capabilities possible mean that the American combat system and weapons in the Collins class will likely be retained. The current Collins class has many of the desired properties, but has suffered from reliability problems, especially concerned with its propulsion system. Given that, there are strong indications that the way ahead will be one of two possibilities:

- an evolution of the current Collins class submarine, retaining the combat system and weapons—or their next generation counterparts—but with a substantially new propulsion system (diesel engines, generators, electric motors and batteries)
- a new design submarine that draws on the conventional submarine design skills in Australia and elsewhere and incorporates American combat and weapon systems.

Of course, Japan builds very successful large conventional submarines that are suited to operations in the Pacific region, something that isn't necessarily true of European submarines designed for operations in the smaller and colder oceans of northern Europe. Japanese submarine systems are likely to be of

great interest to Australia and there have been some discussions between the FSM project managers and Japanese representatives—I am not entirely sure who, but I know that the MoD has taken an interest in potential collaboration.

It remains to be seen what can be achieved but, as a minimum, I would think that Australia would be very interested in Japanese propulsion technology as an option for either of the submarine approaches described above. I have been told informally that a licence build of a Japanese design in Australia is very unlikely. Similarly, I don't think that Australia would seek to have submarines built for it in Japan. In both cases there are industrial issues to be managed. And, in any case, given Australia's preference for an American combat system and weapons, the result is almost certainly going to be a hybrid of European and American technologies in the hull and operating systems.

The Australian government has committed to developing a submarine propulsion testbed facility. It would be very helpful if one of the systems tested had significant Japanese input. To be honest, Japan's submarines seem to be more reliable than Australia's and I think there is much you can teach us.

Network operations

The final section of this paper will discuss the potential for Australia and Japan to contribute to a wider allied effort on computer network operations. For the purpose of discussion, these can be broken into three types, again in increasing order of sensitivity and complexity:

- computer network defence—keeping our own data and networks secure, and developing an understanding of the nature of the threats against them in order to deploy successful countermeasures
- computer espionage—the use of network exploitation techniques in order to gather information
- offensive cyber operations—either by the deployment of 'cyber weapons' similar to the Stuxnet worm, or by network infiltration and disruption (either

by degrading or disabling network performance) or by techniques such as inserting false data or corrupting stored information.

Computer network defence is an easy activity to justify—it is a perfectly reasonable response to hostile activity such as espionage or sabotage aimed at exploiting our critical systems. Given that many of the threats to Australian and Japanese (and other countries) systems originate from the same sources, it makes a lot of sense to cooperate on cyber defence. Some of that is already happening. Probably the biggest impediment to effective collaboration is the organisational arrangements put in place by different governments. In Australia, and I suspect Japan, the perfect solution that allows the right policy settings across the spectrum of cyber threats—from criminal risks to individuals and businesses through to the protection of top secret government data—is yet to be found. Yet successful cyber defence needs to be 'joined up' to avoid weaknesses in one sector being exploited to gain access to others. For example, government departments that are connected to the MoD might allow access to systems that are in turn connected to the JSDF. The people who use those systems are also potential vulnerabilities. As a result of all of these factors, coordinating cyber security actions across one government is difficult. Trying to do it between two different countries is harder still. Nonetheless, this is likely to be a growth area in cooperation—we have an international problem and need an international solution.

Moving up the spectrum of cyber activity, the conduct of computer espionage is an increasingly important part of intelligence operations for virtually every country. Australia and Japan—and each of us with the United States—already have certain intelligence sharing and coordination arrangements in place. It stands to reason that at least some of the data collected via network exploitation would also be shared. But, unlike other forms of intelligence such as imagery or signals intelligence, network exploitation is not a passive activity—it necessarily intrudes into the infrastructure of the target. That extra complication means that operational procedures need to be designed with legal and political considerations in mind. There is no in-principle reason that

precludes cooperative activities, but working across jurisdictions requires the alignment of those activities with two sets of domestic law and with international law.

Offensive cyber operations are more problematic still. All of the same legal difficulties apply, but there is yet another layer of organisational complexity. Australia has opted to set up its cyber operations centre under the auspices of its signals intelligence organisation—which sits in the Department of Defence, but is not within the Australian Defence Force. The United States has opted to set up a Cyber Command subordinate to its armed forces Strategic Command, with components sitting within Army, Navy and Air Force command structures.

Japan, if I understand recent announcements correctly, has opted for a model that looks a little more like the US model, being situated under the Defense Ministry, and as an arm of the JSDF. Unlike Australia, there doesn't seem to be any explicit linkage to intelligence. The need for cooperation with allies has been publically stated—press reports stress the importance of being able to 'take joint action with the United States.' It would make sense for Australia to be able to cooperate with both parties.

For all of the reasons discussed above, it will be difficult—but not impossible—to develop a seamless approach to network operations across the three countries. And there are incentives for us to takes steps in that direction. Some early steps that should be possible with running into too many technical, organisational or legal problems include tabletop planning exercises and 'war gaming' defensive responses to hostile cyber activity. These activities would allow the parties involved to understand each other's doctrine and let the partners share their insights into the nature of cyber threats and the options for dealing with them.

Moving beyond planning and gaming exercises, sharing information on target networks and their characteristics, including defensive measures and potential vulnerabilities, would allow for a certain amount of 'burden sharing'

in cyber space. Each participating country would get a better coverage of the 'landscape' and activity in cyber space than it would be able to gather through its own resources. It would also potentially provide a 'surge capability' against targets that suddenly increase in priority. This is a similar model to existing arrangements between allied countries in other areas of intelligence work, such as signals intelligence.

Finally, software development of 'cyber weapons' (think Stuxnet style software packages) is an area of potential cooperation—if not the production of joint software, at least by sharing knowledge of network vulnerabilities. This would be one potential outgrowth activity of the 'target development' work described in the previous paragraph.

Conclusion

The Asia-Pacific security landscape is changing in ways that make it more complex—and in some ways more dangerous, as strategic competition between the established major powers and the rising power of the PRC deepens. The American response to the challenge being posed is in many ways still a 'work in progress' and some of the more aggressive notions entering the public domain might be put aside as a more nuanced approach to the 'Asian Century' emerges.

Nonetheless, as two of America's close allies in the region, Australia and Japan need to think hard about the expectations that the United States might have of us. We need to decide how we can work together to support our ally—and we need to decide what we are prepared to do in support of their strategy. This paper discusses a range of possible ways that Australia and Japan could cooperate to develop capabilities that will allow us to play a part in securing the region for the benefit of all. Some of the options described here are 'easy'—they can readily be justified and don't have too much downside risk. Others would increase the stakes and certainly won't be appreciated in Beijing. The trick for us will be to weigh the costs and benefits and decide which we want to pursue.