Development of the ARF work plan on cyber security

Presentation to the ARF workshop on measures to enhance cyber security – legal and cultural aspects, 11-12 September, Beijing

Henry Fox
Department of Foreign Affairs and Trade
Canberra

Excellencies, ladies and gentlemen.

Many I begin by thanking our host, the governments of China and Malaysia, for taking the initiative to mount this workshop.

I have been asked to update colleagues on the development of the ARF work plan on cyber security, an important regional security initiative, on which Australia is leading, in cooperation with our fellow co-leads on cybersecurity in the ARF, Malaysia and the Russian Federation. I have circulated a paper on the work plan which sets out the input received to date from colleagues. I will be referring to that paper.

It is useful to begin by recalling that when the ARF was established in 1994, it was a result of coordinated efforts to develop a security dialogue between states in the region. The distinguishing elements of this dialogue were confidence building and preventive diplomacy and eventually a conflict resolution capacity.

We have a history of cooperative work on cyber security, in particular on dealing with criminal and terrorist use of the internet. We are entering into a new phase of work

In July 2012 ARF Foreign Ministers adopted the Statement on Cooperation to Enhance Cyber Security. This provides us with the mandate for our work.

Ministers asked officials to "develop an ARF work plan on security in the use of ICTs focused on practical cooperation on confidence building measures."

We should remind ourselves, why are we doing this work?

To date, our work on cybersecurity has focussed on non-state actors. There is a growing realisation that cyberspace is a sphere where states have interests and that these interests are growing. Espionage is in the news everyday. Interest by militaries in using cyber to support their operations is growing.

In this situation and given the specific characteristics of cyberspace – we cannot see tanks or armies in cyberspace - there are issues of misperception, miscalculation and potential escalation in cyberspace that need to be addressed with a view to preventing possible tension or conflict.

It is prudent for us to think about measures that may help prevent escalation and conflict. We have a common interest in seeking to prevent problems occurring between ARF members.

So our aim in developing the work plan is to address this new constellation of issues.

What measures and activities can we put in place that will help prevent problems of a security nature occurring between states in cyberspace?

We have had input from many ARF members and this is summarised in the paper which has been circulated and which is contained in your folders.

In terms of aims and objectives, we have proposed three aims: (1) preventing conflict in cyberspace between states through practical measures; (2) raising awareness of the security dimensions of cyberspace, and (3) enhancing practical cooperation between members to help each other develop strong government ICT networks and to protect their critical infrastructure.

All ARF members generally support these aims.

One member suggested that we need to continue to cooperate on non-state threats, in particular on criminal and terrorist use of the internet.

In terms of objectives, all members support the proposed objectives: confidence building and transparency measures; and capacity building.

So there is wide unanimity on our aims and objectives in relation to the work plan. One colleague has asked for the inclusion of norms development under both aims and objectives and I will return to this shortly.

In terms of possible activities that could be undertaken, colleagues have excelled themselves in making many suggestions - which are set out in detail in the paper. They take into account the recommendations made at the September 2012 seminar, hosted by the ROK and Malaysia in Seoul, on cyber confidence building measures.

A number of issues are raised by these suggestions. We need to prioritise and to think about practicalities

We have identified a program of work that will take many years to deliver.

Given the nature of the ARF – the limited resources of the Secretariat, our reliance on members to host activities, and the difficulties in sustaining momentum for a multi-year program of work - what can we do that will deliver a positive result for regional security? Some proposals are more direct in their impact on security than others. Perhaps this is a criterion we could use.

How does this work connect to the dialogue on norms and the interest of some in including this in the work plan? As I mentioned at the outset the ARF has a particular mandate in confidence building and in preventive diplomacy. Ministers have provided a specific mandate on confidence building measures. How does this suggestion relate to the mandate given to us by Ministers? Is there a need to go back to Ministers on this? The development of norms is a long-term project. How does this mesh with the practical, problem-oriented focus many of us want the ARF to pursue?

What can we do that is practicable?

One possible idea is to develop a regional list of cyber CBMs and then seek to elaborate the list – so each proposal can be fleshed out in more detail.

A recurring theme is for workshops of various kinds. Another theme is the need for databases – or a mechanism by which the ARF can accumulate information and knowledge. Another is for communications networks, an idea that the workshop on cyber CBMs that Australia and Malaysia will be hosting early next year and which I hope all will participate in. Some are interested in work on definitions and concepts.

There is an issue on how we take our work forward

Should we be thinking of an ARF study group on cyber CBMs, dedicated to this work, which could take this work forward?

I would welcome feedback on these issues both now and subsequently. In the paper we have circulated there are two email addresses at which you can reach me (cyberpolicy@dfat.gov.au or peter.higgins@dfat.gov.au).

In terms of the timetable, we are proposing to have the work plan endorsed by Ministers at their meeting in mid 2014. Before then the drafts will be considered by working level officials at the Inter-Sessional Group meetings in Myanmar at the end of this year and in the first half of 2014, as well as by other cyber workshops that may be held. The plan will then go to Senior Officials and to Ministers.