(Check Against Delivery)

SPEAKING NOTES FOR

ASEAN Regional Forum

Workshop on Measures to Enhance Cyber Security

- Legal & Cultural Aspects

KWA CHONG GUAN

Council For Security Cooperation in the Asia Pacific

Co-Chairs and Participants of this ARF Workshop on Cyber Security,

I would like to thank you all for inviting me to join your meeting to report on the findings and recommendations of a Cyber Security Study Group we convened in 2011. I would like to thank CSCAP-China and the China Institute of International Studies for facilitating my participation in this Workshop.

I have brought some hard copies of our CSCAP Memorandum the Study Group produced on *Ensuring A Safer Cyber Security Environment* and apologise that I may not have brought sufficient copies for everyone. However, the Memorandum is available on the CSCAP website and can be downloaded from there.

I want in the ten minutes assigned to me to outline to you some of the assumptions we made in the drafting of our CSCAP Memorandum. As a concise policy memorandum we could not elaborate on the assumptions upon which we based our recommendations. I would now like to explain some of these assumptions so that you would have a better grasp of what we are recommending in our Memorandum.

The first assumption we made is that the web-based operations and services we are all increasingly dependent upon is extremely vulnerable to a widening spectrum of increasingly complex and sophisticated threats. These threats are not only hostile targeting from state and non-state actors, including cyber criminals, but also natural disasters and accidental events. I assume we are gathered here because we are agreed that the security of our cyber space is of growing concern. We further assumed that the nature of the threat or threats requires a regional or international cooperation to tackle. Like a pandemic, accurate attribution of the source of a computer virus is difficult and requires an international effort to track and monitor. Worse, a computer virus can mutate and spread faster than the H5N1 Avian flu virus.

The second assumption we made is that the extent of regional and wider international cooperation ASEAN and ARF members are prepared to enter into to is largely dependent upon whether they have a cyber security strategy which identifies the cyber threats they may have to confront and how they intend to respond to such potential threats. Some like Singapore are attempting to treat cyber security as a criminal issue, the response to which is then law enforcement. Others may see the protection of their cyber space as a security issue affecting the sovereignty and jurisdiction of the nation state. Cyber security, we in the CSCAP Study Group noted, is ultimately a Domestic Security Issue, but governments must recognize that there are cyber threats which, like pandemics, is beyond the remit of the state to deal with on its own, and need to cooperate with others in the region and internationally to tackle. The CSCAP Study Group thus recommended that governments enact a holistic cyber security strategy that includes cyber security as a regional security issue.

But this recommendation that enacting a holistic cyber security strategy is easier declared than implemented, as the experience of many of us around this table would indicate. In this context, I look forward to hearing from our Australian colleague Mr Tobias Feakin on the emerging agenda for cyber security in Australia. I was given to understand in our CSCAP Study Group that Australia had gone the furthest compared to the US or the UK in thinking through what are the building blocks and how they can be stacked for a holistic cyber security strategy.

What are the prospects for regional cooperation on cyber security within our emerging national cyber security agendas and strategies? Again it is easy to declare that we should be more open and transparent in sharing our experiences, learn from each other and defines what “best practice.” is But we do this on the assumption that we are prepared to trust others with knowledge of capabilities we have or lack and must develop to deal with what cyber security threats. In this context the Australian Strategic Policy Institute paper on the emerging agenda for Australian cyber security is candid in declaring that part of any Australian strategy must be to “determine how to strengthen cyber cooperation with the US” and the need to “develop a strategy on how to engage China on cyber” meaning that China’s cyber capabilities are a potential problem for Australia.

What then are the issues and areas of any holistic cyber security strategy on which stakeholders and actors in any state cyber security strategy and policies must reach out to others and develop some kind of regional engagement strategy?

Embedded in the recommendation to “promote an effective partnership arrangement between government and the private sector” is a reference to the basic vulnerability of our web-based operations and services in our dependence upon industry to provide the platform (both software and hardware) upon which the Internet we depend upon is constructed. In this structure a telecom provider or host server provides the service for its clients to access the world-wide web without the need to personally invest in software and information communications hardware. This reliance upon a main Internet service for access and connection to the world-wide web, for data storage facilities, which is increasing via cloud computing and for software and solutions to data processing results in three security gaps in our computer security:

> The first is that all users, including countries (except for the telecom and internet service providers) do not control the security of their data, access and connections to the world-wide

web or software applications and solutions to their information communications needs, and unable to integrate their security concerns into the system.

The second is that the security of our data and access to the system is as strong, or as weak, as the Host Server's data protection infrastructure and processes,

The third is that all it needs is a Single Point of Failure to threaten not only the service users, but also constitute a risk to the Critical Infrastructures of the State which may also depend upon the internet for its command and control systems.

The crux of the issue of a "Public-Private Partnership" we and others draw attention to as one of our recommendations for action is how the public and private sectors can cooperate to mitigate the risk of a Single Point of Failure which can deny us access to the world-wide web and lose our data in the servers of the telecom providers. Worse is to prevent a system failure. But how to enhance this "Public-Private Partnership" to mitigate the risk of our dependence upon industry for our access to the world-wide web and storage of our date is ultimately a domestic security issue.

The intent of our CSCAP Memorandum's slew of recommendations about the need to develop National Computer Emergency Response Teams (CERTS) and Computer Security Incident Response Teams (CSIRTs) is to respond to a crisis following a breach of the telecoms servers systems, creating a Single Point of Failure, especially when that breach extends to threatening the command and control systems of our Critical Infrastructures, in particular, power grids, transport systems or communications systems.

But the effectiveness of our CERTs and CSIRTs is dependent upon the expertise of their teams. Here then there is scope for regional cooperation in education and training of CERT and CSIRT teams so they can respond more effectively individually, but as a network and team to collectively mitigate cyber threats and vulnerabilities. The ARF is well placed to assist its members build up their cyber security capacity, The ARF is also well placed to facilitate the networking of their CERT teams to facilitate sharing of information and experience about the detection, containment and mitigation of cyber threats.

(8 Sep 2013)