2006 ASEAN REGIONAL FORUM STATEMENT ON COOPERATION IN FIGHTING CYBER ATTACK AND TERRORIST MISUSE OF CYBER SPACE

Issued in Kuala Lumpur, Malaysia, on 28 July 2006

The Chairman of the ASEAN Regional Forum (ARF), on behalf of the participating states and organization, issues the following statement:

Strongly condemning all acts of terrorism regardless of their motivations, whenever and by whomsoever committed, as one of the most serious threats to international peace and security;

Reaffirming the imperative to combat terrorism in all its forms and manifestations;

Rejecting any attempt to associate terrorism with any religion, nationality, race, or culture;

Ensuring that all measures to combat terrorism are in accordance with the United Nations Charter and other applicable principles of international law, including humanitarian and human rights law;

Acknowledging that terrorist misuse of cyber space is a destructive and devastating form and manifestation of global terrorism whose magnitude and rapid spread would be exacerbated by the increasing cyber interconnectivity of countries in the region;

Recognizing the serious ramifications of an attack via cyber space to critical infrastructure on the security of the people and on the economic and physical well-being of countries in the region;

Recognizing the detrimental impact of fear which can be enhanced by the terrorists in conjunction with attacks in physical space;

Further recognizing that terrorist misuse of cyber space is a form of cyber crime and a criminal misuse of information technologies;

Acknowledging that the proceeds from cyber crime may be laundered and/or used to fund terrorist activities;

Emphasizing the importance of ARF countries acting cooperatively to prevent the exploitation of technology, communications, and resources, including Internet, to incite support for and/or commit criminal or terrorist acts, including the use by terrorists of the internet for recruitment and training purposes.

Recalling the ARF Statement on Strengthening Transport Security against International Terrorism of 2 July 2004, which mentions, in particular, that ARF countries will endeavor to cooperate to ensure that terrorists are prevented from using information technology and its applications to disrupt and sabotage the operation of transportation systems;

Stressing the need for cooperation between governments and the private sector in identifying, preventing, and mitigating cyber-attacks and terrorist misuse of cyber-space;

Believing that an effective fight against cyber-attacks and terrorist misuse of cyber space requires increased, rapid and well-functioning legal and other forms of cooperation.

1. ARF participating states and organization endeavor to enact, if they have not yet done so, and implement cyber crime and cyber security laws in accordance with their national conditions and by referring to relevant international instruments and recommendations/guidelines for the prevention, detection, reduction, and mitigation of attacks to which they are party, including the ten recommendations in the UN General Assembly Resolution 55/63 on Combating the Criminal Misuse of Information Technologies.

2. ARF participating countries and organization acknowledge the importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyber space and encourage the formulation of such a framework that may include the following proposed courses of action:

- Identify national cyber security units and increase coordination among national agencies;
- Develop national watch, warning, and incident response capabilities;
- Collaborate/cooperate with international and regional agencies for cyber investigation and collection and sharing of cyber evidence and, effective management of resources for mutually beneficial partnerships that foster international cooperation, interoperability, and coordination in fighting criminal and terrorist misuse of cyber space;
- Conduct training/ technology transfer and counter-measures, especially digital forensics;
- Reinforce capabilities to protect and recover critical infrastructure, minimize loss, track and trace the sabotage activities on such infrastructure;
- Encourage private sector partnership with the government in the field of information security and fighting cyber crime, including the protection of critical infrastructure;
- Increase public awareness on cyber security and cyber ethics with emphasis on safety and security, best practices, the responsibilities of using information networks and negative consequences from misuse of networks.

3. ARF participating states and organization agree to work together to improve their capabilities to adequately address cyber crime, including the terrorist misuse of cyber space by:

- Endeavoring to identify national cyber security units and joining and participating in established networks of cooperation;
- Endeavoring to establish an ARF-wide network of Computer Security Incident Response Teams (CSIRT) concerning cyber- crime to facilitate the real time exchange of threat and vulnerability assessment and issuance of required warnings and patches and which would join existing cyber and incident warning and response networks;
- Leveraging on existing cooperation among different CSIRT networks and collaborating with other international and regional organizations with similar concerns;
- Providing, where and when possible, technical assistance and capacity-building programs to countries that request help in developing laws, extending training (in forensics, law enforcement, legal and technical matters), and when and where possible, providing hardware and software;
- Within the framework of applicable data protection regulation, information and intelligence sharing between law enforcement, partners, and regional agencies, and community;
- Enhancing efforts towards training and awareness among the masses to bring about a culture of cyber security.

4. The ARF participating countries and organization also commit to continue working together in the fight against cyber crime, including terrorist misuse of cyber space, through activities aimed at enhancing confidence among different national CSIRTs, as well as formulating advocacy and public awareness programs.

5. ARF participating countries and organization commit themselves to adopting such measures as may be appropriate and in accordance with their obligations under international law to prohibit by law incitement to commit a terrorist act or acts, including through computer networks.

6. The ARF participating countries and organization decide to annually review the progress of these and other efforts to combat cyber attack and the terrorist misuse of cyber space at subsequent ARF Ministerial Meetings.

28 July 2006

Kuala Lumpur