NO. SOALAN: 496

PEMBERITAHUAN PERTANYAAN DEWAN RAKYAT

PERTANYAAN	:	**BUKAN LISAN**
DARIPADA	:	**DR. TAN SENG GIAW**
		[KEPONG – DAP]
NO. SOALAN	:	**496**

Dr. Tan Seng Giaw [Kepong] minta **PERDANA MENTERI** menyatakan keadaan keselamatan siber dan langkah memeliharanya.

JAWAPAN: **YB. DATO' SERI DR. SHAHIDAN BIN KASSIM**
MENTERI DI JABATAN PERDANA MENTERI

Tuan Yang Di-Pertua,

Landskap dan situasi keselamatan siber di negara kita secara umumnya adalah terkawal. Risiko keselamatan siber negara dinilai dari semasa ke semasa berdasarkan ancaman dan kelemahan yang dihadapi dalam persekitaran siber. Sifat dimensi ruang siber yang luas, tanpa sempadan dan berciri ketanpanamaan (anonymous) memberi cabaran kepada agensi keselamatan negara dalam mengurus ancaman ini memandangkan ianya boleh dieksploitasi oleh sesiapa sahaja yang mahu melaksanakan agenda-agenda berniat jahat kepada masyarakat dan negara.

Dengan penemuan serta kemajuan teknologi pada masa kini, trend ancaman keselamatan siber menjadi semakin rumit dan sukar diramal. Ancaman siber yang wujud ketika ini melibatkan boleh dikategorikan seperti berikut:

a) penggunaan internet, media sosial atau sebarang media siber baharu untuk mempengaruhi pemikiran masyarakat yang mampu menggugat kestabilan dan keselamatan negara, melanggar undang-undang negara serta menjejaskan nilai dan identiti nasional;
b) penggunaan internet, media sosial dan sebarang media siber baharu oleh sindiket, gerakan jenayah terancang, ekstremis dan pengganas;

c) Kegiatan *cyber espionage*, menceroboh dan mencuri maklumat rasmi Kerajaan;
d) Serangan berskala besar ke atas infrastruktur dan sistem kritikal Negara;
e) Penipuan dalam talian; dan
f) Penyalahgunaan teknologi.

Justeru, pengurusan keselamatan siber yang bersepadu dan terselaras telah dilaksanakan memandangkan ancaman yang melibatkan keselamatan siber dijangka akan terus meningkat berikutan daripada tahap kebergantungan yang tinggi negara dan masyarakat terhadap teknologi ini dalam kehidupan seharian.

Di atas kesedaran ini juga, Dasar Keselamatan Negara yang telah dilancarkan baru-baru ini telah menetapkan 'mengukuhkan keselamatan dan ketahanan siber bagi mencapai keadaan persekitaran siber yang selamat dan berdaya tahan' sebagai salah satu strategi utama dasar.

Selain itu, Kerajaan juga telah mengambil langkah proaktif dan perlindungan kepada agensi-agensi Infrastruktur Maklumat Kritikal Negara (Critical National Information Infrastructure – CNII) daripada ancaman dan serangan siber melalui inisiatif di bawah Dasar Keselamatan Siber Negara (National Cyber Security Policy - NCSP) dan Pelan Pengurusan Keselamatan Siber Negara (National Cyber Crisis Management Plan - NCCMP). Pelan ini yang dibangunkan berdasarkan kepada rangka kerja pengurusan risiko yang menggariskan strategi bagi mengurangkan kesan serangan siber dan tindakbalas yang perlu dilaksanakan oleh agensi-agensi CNII yang terdiri daripada agensi awam dan swasta.

Selain itu, Kerajaan juga telah menetapkan keperluan dan *baseline* keselamatan siber yang perlu kepada agensi-agensi CNII melalui pelaksanaan Pensijilan MS ISO/IEC 27001 Sistem Pengurusan Keselamatan Maklumat (*Information Security Management System* - ISMS). Pensijilan ini menetapkan keperluan pematuhan melalui satu pendekatan yang sistematik dalam pengurusan maklumat bagi menjamin keselamatan maklumat termasuk polisi, proses, prosedur dan fungsi perkakasan dan perisian berkaitan.

Kerajaan juga telah membangunkan Pusat Kawalan dan Penyelarasan Siber Negara (National Cyber Coordination and Command Centre - NC4) di bawah Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara (MKN) bagi melaksanakan tugas pemantauan, pengeluaran amaran dan *advisories* berkaitan langkah pencegahan dan perlindungan bagi menangani ancaman siber kepada semua agensi-agensi CNII.

Sekian, terima kasih.