**PEMBERITAHUAN PERTANYAAN DEWAN RAKYAT**
**MESYUARAT KEDUA, PENGGAL KEDUA**
**PARLIMEN KEEMPAT BELAS**

---

**PERTANYAAN : JAWAB LISAN**

**DARIPADA : TUAN MOHD SHAHAR BIN ABDULLAH [ PAYA BESAR ]**

**TARIKH : 9 JULAI 2019 (SELASA)**

**SOALAN : 43**

**Tuan Mohd Shahar bin Abdullah [ Paya Besar ]** minta **MENTERI KOMUNIKASI DAN MULTIMEDIA** menyatakan :-

a) apakah dasar Kementerian kepada syarikat-syarikat telekomunikasi dalam melaksanakan strategi penguatkuasaan bagi mengsifarkan jenayah siber dalam semua kategori yang semakin membimbangkan di negara kita; dan

b) apakah usaha yang telah dan akan dilaksanakan Kementerian dalam menjamin Jaringan Komunikasi Atas Talian Negara tidak dapat diceroboh dan digodam supaya rakyat Malaysia dapat melakukan sebarang urusan harian atas talian dengan selamat.

**JAWAPAN**

Tuan Yang Dipertua,

**Soalan (a)**

1. Untuk makluman Ahli Yang Berhormat, tindakan membanteras jenayah siber merupakan suatu usaha kolektif yang melibatkan pelbagai Kementerian dan Agensi. Secara khusus bagi pihak penyedia perkhidmatan komunikasi, pihak tersebut telah diarahkan untuk mengemaskini pangkalan data pelanggan talian telefon prabayar bagi

mengelakkan ianya disalahguna untuk tujuan penipuan dan seumpamanya. Sehingga Mei 2019, sebanyak **1,128,385** talian prabayar yang didaftar secara meragukan telah dikesan. Daripada jumlah tersebut, sebanyak **67%** talian telah ditamatkan perkhidmatannya dan baki **33%** telah dikemaskini dengan maklumat yang sah.

2. Selain itu, Kementerian juga menggalakkan para pengguna Internet mengamalkan kaedah kawalan kendiri. Contohnya, kerjasama Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan Penyedia Perkhidmatan Internet (*Internet Service Provider*) di Malaysia seperti Celcom, UMobile, Digi, Maxis, Telekom Malaysia (TM), TIME, Tune Talk dan sebagainya, telah melancarkan inisiatif aplikasi kawalan ibu bapa (*Parental Control Tools*) bagi mengawalselia aktiviti anak-anak mereka di alam maya sekaligus melindungi keluarga mereka daripada terdedah kepada risiko-risiko dan anasir yang negatif.

**Soalan (b)**

1. Tahap keselamatan siber negara sentiasa berada dalam ranking terbaik dunia dan diiktiraf oleh badan global dengan kedudukan ke-tiga (3) terbaik telah direkodkan dalam Global Cybersecurity Index 2017 yang dikeluarkan oleh *Telecommunication Union (ITU) dan ABI Research.* Mahupun demikian, Kerajaan masih tetap terus berusaha memperbaiki dan memastikan tahap keselamatan siber negara sentiasa berada dalam keadaan yang baik dan terkawal.

2. Pihak Kementerian melalui SKMM, menjadi peneraju utama bagi sektor “informasi dan komunikasi” yang merupakan salah satu sektor kritikal di bawah *Critical National Infrastructure;* CNII. SKMM adalah salah satu agensi yang terlibat di dalam inisiatif NC4 di mana SKMM memainkan peranan khusus di dalam memantau dan seterusnya melindungi infrastruktur kritikal komunikasi dan maklumat negara.

3. Pusat Keselamatan Rangkaian SKMM juga bertindak sebagai pusat setempat pengurusan ancaman makro siber, serta pusat koordinasi dan kerjasama sektor awam dan pihak swasta bagi sektor informasi dan komunikasi.

4. Selain itu, Kerajaan juga telah menetapkan keperluan dengan izin *baseline*, keselamatan siber yang perlu kepada agensi-agensi infrastruktur maklumat kritikal melalui pelaksanaan pensijilan MS ISO/IEC 27001 Sistem Pengurusan Keselamatan Maklumat dengan izin, Information Security Management System (ISMS).

5. Melalui CyberSecurity Malaysia (CSM) pula, Kementerian telah memberi tumpuan kepada 4 aspek utama iaitu dari segi keupayaan ramalan (*predictive*), keupayaan pencegahan (*preventive*), keupayaan tindak balas (*responsive*) dan keupayaan pembetulan (*corrective*) bagi menjamin keselamatan siber dan jaringan komunikasi dalam talian tidak dapat diceroboh dan digodam.

6. Di antara langkah yang diambil oleh CSM adalah dengan membangunkan aplikasi *big data analytics* (BDA) yang berupaya meramalkan trend ancaman siber dari semasa ke semasa. CSM turut terlibat dalam program kesedaran dan latihan kepada pengguna internet mengenai aspek keselamatan siber melalui penganjuran program CyberSAFE (*Cyber Security Awareness for Everyone*).

7. CSM turut menyediakan Perkhidmatan Amaran Awal Siber (Cyber999) yang berperanan sebagai pusat koordinasi setempat bagi membolehkan pengguna Internet menghubungi Pusat Bantuan Cyber999 untuk melaporkan insiden-insiden keselamatan siber seperti pencerobohan siber, kecurian identiti, pembulian siber, penipuan siber dan sebagainya.

8. Selain itu, jika serangan siber telah berlaku CSM turut melaksanakan perkhidmatan CyberDEF yang bertujuan untuk mengesanan, membasmi dan menyediakan penyiasatan forensik bagi pencurian data atau serangan siber.