Penyelidikan keselamatan siber mantap kunci pertahanan negara

Pada awal kemunculan Revolusi Industri 4.0 (IR4.0), timbul pelbagai persoalan mengenai kesediaan Malaysia untuk mengadaptasi perkembangan itu supaya terus maju seiring dengan negara lain.

Namun, pandemik COVID-19 yang melanda seluruh negara ketika ini secara tidak langsung mewujudkan satu persekitaran norma baharu yang mendokong perkembangan IR4.0, pada masa sama, mempercepatkan lagi agenda transformasi digital di Malaysia.

Ia seterusnya mengubah 100 peratus cara bekerja, belajar malah berkomunikasi antara satu sama lain. Dalam erti kata lain, transformasi yang berlaku ketika ini jauh berbeza berbanding dialami manusia terdahulu.

Perkhidmatan awan, data raya, rantaian blok (blockchain), malah teknologi kecerdasan buatan (AI) kini semakin menampakkan fungsinya, malah turut menjadi pilihan sektor kerajaan dalam menguruskan kecekapan perkhidmatan awam khususnya.

Di saat kita semakin serasi dengan perubahan IR4.0 dan transformasi digital yang berlaku sepanjang pandemik ini, negara dikejutkan pula dengan isu ancaman siber daripada kumpulan penggodam seperti 'Anonymous Malaysia'.

Meskipun keupayaan kumpulan ini belum lagi teruji, ia tetap menjanjikan cabaran yang cukup besar bagi sektor keselamatan siber di Malaysia.

Secara tidak langsung, isu ini wajar ditangani sebaiknya memandangkan ia membabitkan ancaman terhadap maklumat strategik negara yang turut memberi implikasi terhadap keselamatan dan kedaulatan negara.

Dalam konteks ini, kerajaan menerusi Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) memiliki garis panduan keselamatan pelayan (server) untuk kegunaan organisasi kerajaan. Ia memerlukan setiap organisasi mengikuti segala garis panduan yang turut membabitkan aspek operasi dan kewangan.

Ini termasuklah keperluan meningkatkan penguatkuasaan pematuhan teknologi dengan keselamatan maklumat garis panduan atau piawaian antarabangsa, terutama membabitkan proses perolehan dan kewangan memandangkan ia nadi kepada sesebuah perkhidmatan.

Setiap organisasi juga perlu diwajibkan untuk melaksanakan latihan siber dan prosedur keselamatan siber pada peringkat organisasi yang bakal berfungsi sebagai platform untuk mengembangkan kepakaran yang relevan.

Dalam konteks keselamatan sistem, dua perkara asas yang wajib dilaksanakan pada peringkat ini ialah pemasangan sistem pengesanan pencerobohan dan pemantauan serta penguatkuasaan oleh staf yang bertanggungjawab.

Mereka perlu sentiasa peka dan proaktif dalam memantau sistem terbabit, pada masa sama, meningkatkan penggunaan sistem amaran bagi setiap pelayan yang digunakan.

Pendedahan sedemikian secara tidak langsung menyumbang kepada pencegahan tindak balas kejadian keselamatan siber yang sesuai, baik pada peringkat organisasi mahupun nasional.

Tidak dinafikan, inisiatif kesedaran keselamatan siber di Malaysia sedang dijalankan oleh agensi atau organisasi berkaitan menerusi pelbagai pendekatan dan kumpulan sasaran.

Contohnya, kempen CyberSAFE dikendalikan CyberSecurity Malaysia dan kempen 'Klik Dengan Bijak' yang diperkenalkan Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM).

Bank Negara Malaysia (BNM) pula dengan kerjasama Kementerian Perdagangan Dalam Negeri dan Hal Ehwal Pengguna (KPDNHEP) bekerjasama menghasilkan buku kecil mengenai panduan menjalankan perniagaan dan urus niaga elektronik.

Namun, program kesedaran seperti ini hanya berfungsi sebagai 'barisan hadapan' dalam konteks keselamatan siber. Justeru, agenda kesediaan keselamatan siber perlu dipupuk pada peringkat organisasi dan nasional dengan komitmen lebih besar.

Universiti, terutama ahli akademik dan penyelidik perlu memainkan peranan penting dengan menghasilkan inovasi penyelidikan berimpak dalam bidang keselamatan siber yang mampu mempertahankan negara daripada serangan penggodam ini.

Dalam konteks ini, usaha bersepadu dan penguatkuasaan pihak bertanggungjawab, terutama kerajaan dan industri adalah perlu bagi membolehkan penyaluran hasil penyelidikan yang inovatif dapat dimanfaatkan oleh bidang relevan dengan kepentingan negara.

Ini juga bertepatan hala tuju Malaysia kini yang memfokuskan kepada perkembangan sains industri berasaskan teknologi dan inovasi (STI) yang mana ia memerlukan teknologi yang mampan dan berdaya tahan.

Dalam memenuhi keperluan ini, fungsi merentas domain keselamatan, tahap keselamatan, ketahanan, kepercayaan, privasi, hubungan, interoperabiliti serta dinamik komposisi adalah keperluan yang cukup mendesak.

Dari sudut akademik pula, ada keperluan memperkasakan keselamatan siber menerusi kursus diajar di bawah program Teknologi Maklumat dan Komunikasi (ICT) serta Program Kejuruteraan Komputer.

Sebagai contoh, keperluan keselamatan siber perlu dijadikan kurikulum dalam kursus berkaitan, antaranya pengaturcaraan perisian (pengekodan selamat), perisian dan kitaran pembangunan sistem, pangkalan data, sistem operasi, sistem rangkaian serta pembangunan platform aplikasi lintas.

Pada peringkat Universiti Malaysia Perlis (UniMAP), kurikulum berasaskan siber sekuriti diperkenalkan dalam beberapa subjek Ijazah Sarjana Muda Teknologi Kejuruteraan Elektronik bagi program (Rekabentuk Rangkaian Elektrik).

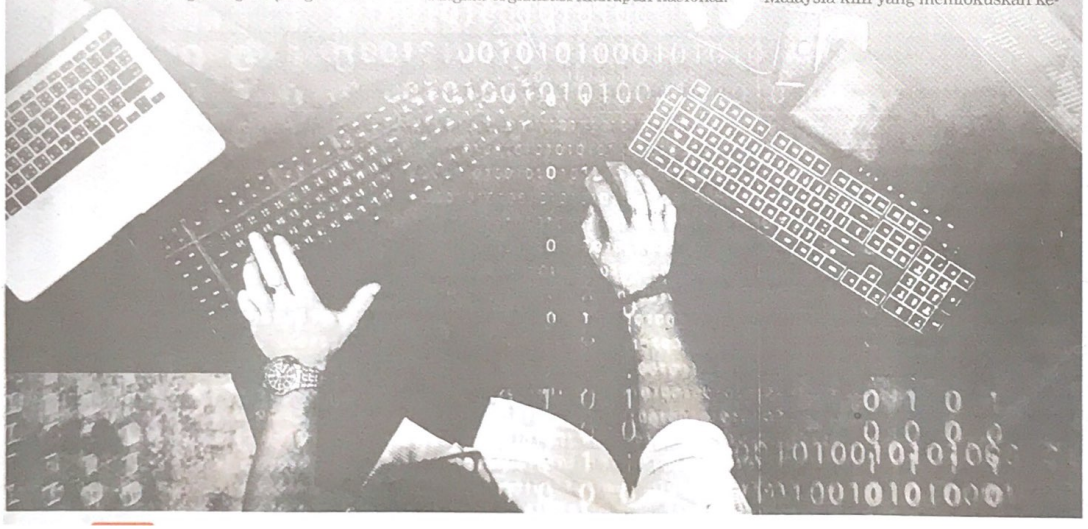
Pada masa sama, beberapa kerjasama pintar dijalankan dengan agensi pendidikan lainnya dalam mewujudkan hala tuju pekerjaan dalam bidang keselamatan siber di Malaysia.

Ini termasuklah dengan Cisco Academy yang membolehkan pelajar UniMAP mengambil sijil profesional Aviatrix Certified Engineer (ACE) dan Certificate in Cyber Security – Ethical Hacking.

Namun, kepentingan akademik dan penyelidikan tidak boleh berjaya tanpa sokongan dan kerjasama jitu daripada kerajaan serta industri. Pendanaan dalam bentuk insentif seperti geran sepadan misalnya, wajar diperbanyakkan bagi mengembangkan inovasi penyelidikan.

Pada masa sama, inisiatif tertentu bagi membolehkan graduan mendapat persijilan profesional keselamatan siber juga harus ditingkatkan bagi memastikan hasrat negara memiliki sekitar 12,000 tenaga kerja dalam bidang siber sekuriti tercapai.

Pengakhiran diimpikan ialah masa depan negara dan atas dasar itu, pelaburan sewajarnya perlu dimulakan sekarang.



***Dr R Badlishah** adalah Naib Canselor Universiti Malaysia Perlis (UniMAP), manakala **Suhizaz** adalah Penasihat Sistem Pengurusan Keselamatan Maklumat (ISMS) dan Pensyarah Kanan UniMAP*