PERANG SIBER HANYA ILUSI MAYA?

China, Rusia dan Korea Utara didakwa mempunyai keupayaan tentera siber yang mampu melumpuhkan prasarana kritikal maklumat sesebuah negara.

Oleh Redy Jeffry Mohamad Ramli dan Nadia Salwa Mohamad

Ketika Amerika Syarikat meraikan ulang tahun kemerdekaannya pada 4 Julai lalu, satu siri serangan siber berupa serangan *denial-of-service* (DDoS) telah dilancarkan ke atas rangkaian Internet di Amerika Syarikat dan Korea Selatan yang menyaksikan kira-kira 25 laman web agensi kerajaan dan syarikat termasuk Rumah Putih, Jabatan Perbendaharaan, Jabatan Pengangkutan, Suruhanjaya Perdagangan Persekutuan, Jabatan Pertahanan, Agensi Keselamatan Nasional, Jabatan Keselamatan Dalam Negeri, Bursa Saham Nasdaq dan New York serta akhbar The Washington Post mengalami gangguan.

Di Korea Selatan siri serangan tersebut berlarutan sehingga 8 Julai yang menyaksikan 11 organisasi termasuk Pejabat Presiden yang dikenali sebagai Blue House dan Kementerian Pertahanan serta salah sebuah bank terbesar di Korea Selatan, akhbar utama dan agensi perisikannya menjadi sasaran serangan yang mengakibatkan laman web organisasi berkenaan lumpuh atau sukar diakses.

Menurut laporan media, serangan siber ke atas Amerika Syarikat dan Korea Selatan itu didakwa dilakukan oleh Korea Utara.

Jika disoroti insiden serangan siber yang serupa seperti yang dialami oleh Amerika Syarikat dan Korea Selatan baru-baru ini, ia bukanlah kejadian pertama

yang berlaku. Estonia (2007), Georgia (2008) dan Kyrgyzstan (Januari 2009) pernah mengalami serangan siber dan yang dituduh menjadi dalang serangan ke atas ketiga-tiga negara itu ialah Rusia.

Persoalannya, apakah benar Korea Utara dan Rusia bertanggungjawab melancarkan perang siber atau ia sekadar hipotesis pihak media dan penganalisis?

Dalam insiden serangan siber ke atas Estonia, Georgia, Kyrgyzstan dan baru-baru ini ke atas Amerika Syarikat dan Korea Selatan, tiada bukti kukuh pembabitan Rusia dan Korea Utara dalam serangan tersebut.

Jika analisis dan hipotesis penganalisis diambil kira, China, Rusia dan Korea Utara adalah antara negara yang mempunyai kekuatan tentera yang terkuat di alam siber.

Rusia dan China adalah dua buah negara yang sering memperagakan keupayaan ketenteraan mereka di alam siber berdasarkan beberapa insiden serangan siber yang didakwa oleh penganalisis-penganalisis keselamatan siber dilancarkan oleh kedua-dua negara berkenaan.

Rusia didakwa memiliki militia siber yang mengawal botnet terbesar di dunia iaitu antara 150 hingga 180 juta nod. Kebiasaannya, serangan siber berupa DDoS boleh dilancarkan menerusi nod tersebut walaupun nod tersebut tidak berada di negara yang melancarkan serangan.

Namun sehingga kini, belum ada bukti kukuh untuk mengaitkan serangan ke atas Estonia, Georgia dan Kyrgyzstan itu dilancarkan oleh militia siber Rusia.

China bukan sahaja merupakan negara yang mempunyai jumlah tentera yang teramai yakni 2.3 juta orang malah di alam siber kekuatan ketenteraan China sering mendapat perhatian kuasa besar dunia seperti Amerika Syarikat dan Britain.

Dalam tahun 2007, ketika serangan siber ke atas Australia dan New Zealand tercetus, China didakwa menjadi dalang serangan tersebut. Malah dilaporkan China mempunyai bala tentera siber yang terdiri daripada Tentera Pembebasan Rakyat (PLA) yang sering menceroboh rangkaian komputer di Amerika Syarikat, Kanada, Jerman dan Jepun bagi mengumpul maklumat dan mencuri data penting negara-negara berkenaan. Namun sehingga ke hari ini, tiada bukti kukuh atas dakwaan tersebut.

Korea Utara yang menyertai China dan Rusia dalam senarai negara yang memiliki tentera siber yang besar didakwa telah bertahun-tahun memiliki sepasukan tentera yang dianggotai oleh kira-kira 100 penggodam yang kebanyakannya adalah graduan akademi tentera di Pyongyang yang bertanggungjawab mengumpul maklumat dan mengganggu jaringan komputer di Korea Selatan dan Amerika Syarikat.

Malah sumber perisikan Korea Selatan pernah mendedahkan bahawa Korea Utara mempunyai ‘Unit 121’ iaitu satu organisasi ketenteraan yang dianggotai

oleh 500-1000 penggodam mahir yang pernah menggodam jabatan pertahanan Korea Selatan dan Amerika Syarikat.

Seperti dalam kes Rusia, segala dakwaan ke atas Korea Utara hanyalah hipotesis penganalisis. Malah menurut seorang penyelidik botnet, berdasarkan analisis yang dibuat ke atas kod perisian berbahaya (*malware*) yang digunakan dalam serangan ke atas Amerika Syarikat dan Korea Selatan, tiada penunjuk yang membuktikan serangan tersebut dilakukan atau didalangi oleh Korea Utara.

Jadi, apakah benar Rusia, China dan Korea Utara mampu melancarkan perang siber ke atas musuh mereka seperti yang dilaporkan oleh media barat atau ia sebahagian daripada propaganda politik Amerika Syarikat dalam meneruskan hegemoninya?

Dari satu sudut, memang tidak mustahil negara seperti Rusia, China dan Korea Utara mampu melancarkan perang siber ke atas mana-mana negara yang dimusuhi mereka.

Malah Amerika Syarikat juga mampu melakukannya kerana adalah mustahil sebuah negara maju seperti Amerika Syarikat yang memiliki teknologi dan pakar dalam teknologi maklumat tidak memiliki tentera sibernya sendiri.

Namun ada sesetengah penganalisis insiden serangan siber berpendapat, ada kemungkinan kerajaan atau tentera Rusia, China dan Korea Utara tidak terbabit langsung dalam serangan siber tersebut sebaliknya ia dilakukan oleh

penggodam yang mahu menguji kemahiran mereka atau yang bersimpati dan pro negara-negara berkenaan.

Dalam kes insiden di Estonia, Georgia, Kyrgyzstan, Amerika Syarikat dan Korea Selatan, jelas ketegangan geopolitik baik di dalam negara berkenaan mahupun di peringkat antarabangsa dikatakan menjadi punca serangan.

Oleh yang demikian adalah tidak mustahil penggodam yang simpati atau pro pada pihak yang ditekan melancarkan serangan siber terhadap pihak yang menekan atas dasar simpati atau protes.

Ini terbukti dalam insiden serangan siber antara Israel-Palestin yang tercetus pada penghujung 2008 dan awal 2009 di mana isu serangan Israel ke atas Palestin ketika itu mengundang rasa simpati penggodam yang akhirnya menyaksikan kira-kira 12,862 laman web dan 72 pelayan Israel berjaya digodam.

Di Iran, ketika pilihan raya presiden pada pertengahan Jun 2009, 12 laman web prokerajaan telah menjadi mangsa serangan siber oleh penyokong parti pembangkang, antaranya laman blog rasmi Mahmoud Ahmadinejad, Pejabat Pemerintah Agung Ayatollah Ali Khamenei, Kementerian Dalam Negeri, Polis Kebangsaan, Kementerian Keadilan dan Iranian Press TV.

Insiden serangan siber tersebut berlaku berikutan ketidakpuasan hati penyokong parti pembangkang dengan pemilihan semula Mahmoud Ahmadinejad sebagai presiden. Penyokong pembangkang menggunakan Twitter sebagai alat

komunikasi dan penyebaran maklumat mengenai kaedah untuk menyerang laman web prokerajaan.

Walaupun perang siber masih merupakan hipotesis para penganalisis, insiden serangan siber bukanlah sesuatu yang asing terutama ketika era masa kini yang menyaksikan kebergantungan tinggi manusia terhadap komputer dan Internet.

Bagi segelintir daripada kita, kebergantungan terhadap komputer (termasuk telefon bimbit) pada hari ini telah mencapai satu tahap di mana jika tidak mengakses komputer sama ada dengan atau tanpa Internet, kita akan merasa gelisah sepanjang hari.

Daripada urusan pejabat sehingga urusan peribadi dan untuk bersosial, komputer atau telefon bimbit menjadi satu alat yang amat penting bagi mengerjakan segala urusan.

Sesetengah pakar di negara maju berpendapat, kebergantungan yang amat tinggi terhadap komputer (Internet) untuk melakukan apa saja urusan penting boleh mencetuskan ‘cybergeddon’ yakni situasi di mana pengguna mengalami kesulitan yang boleh mengancam keselamatan apabila komputer atau jaringan Internet mengalami serangan siber.

Serangan siber bukan sahaja boleh mendatangkan kerugian yang besar kepada pengguna Internet malah jika dilancarkan pada skala besar boleh melumpuhkan prasarana kritikal maklumat negara seperti jabatan kerajaan, perbankan, kewangan dan pengangkutan.

Amerika Syarikat sendiri telah mengklasifikasikan serangan siber sebagai ancaman terbesar mereka selepas perang nuklear dan senjata pemusnahan besar-besaran.

Oleh yang demikian, persoalan mengenai sejauh mana serangan siber itu boleh dianggap sebagai satu bentuk perang yang dilancarkan oleh sesebuah negara sebenarnya bergantung pada persepsi penganalisis atau pihak media yang melaporkannya.

Sama ada perang siber akan menjadi satu realiti suatu hari nanti atau kekal sekadar ilusi yang dicipta oleh kuasa besar seperti Amerika Syarikat dalam mengimbangi kebangkitan negara seperti China dan Korea Utara di pentas politik antarabangsa, yang penting insiden serangan siber tidak mustahil akan menjadi senjata perang pada masa akan datang.

Malaysia sebagai sebuah negara yang semakin bergantung pada teknologi maklumat juga harus bersiap siaga untuk mendepani serangan siber.

Redy Jeffry Mohamad Ramli dan Nadia Salwa Mohamad ialah Penyelidik Media Siber di Bahagian Keselamatan Siber dan Polisi, CyberSecurity Malaysia. *Kenyataan dan pandangan yang terdapat di dalam artikel ini adalah pandangan peribadi penulis.*