Asian Journal of Environment, History and Heritage
June 2022 Vol. 6, Issue. 1, p. 11-26
ISSN 2590-4213 e-ISSN 2590-4310
Published by Malay Arts, Culture and Civilization Research Centre,
Institute of the Malay World and Civilization

MEMAHAMI JENAYAH SIBER DAN KESELAMATAN SIBER DI MALAYSIA: SUATU PEMERHATIAN TERHADAP PANDANGAN SARJANA DAN INTELEKTUAL

(*UNDERSTANDING CYBERCRIME AND CYBERSECURITY IN MALAYSIA: AN OBSERVATION FROM THE PERSPECTIVE OF SCHOLARS AND INTELLECTUALS*)

Nur Sarida Mohd Fuad @ Mohd Daud
& Ahmad Rizal Bin Mohd Yusof

Abstrak

Perkembangan pesat dalam dunia digital telah meningkatkan kebergantungan kepada teknologi maklumat dan komunikasi. Ini telah membuka kepada risiko ancaman baharu iaitu jenayah siber. Jenayah siber memberikan suatu masalah baharu kepada masyarakat dan negara dan ianya menimbulkan kebimbangan kerana memberi kesan kepada pembangunan sosial dan ekonomi yang sangat kritikal. Kelemahan penguatkuasaan undang-undang serta tahap kesedaran masyarakat merupakan antara faktor berlakunya peningkatan jenayah siber. Bagi mengatasi masalah tersebut, kajian ini menggunakan pendekatan awal untuk memahami jenayah dan keselamatan siber berdasarkan kepada penulisan yang telah disumbangkan oleh para sarjana dan intelektual. Dengan menggunakan pendekatan secara kualitatif, setiap penulisan sarjana dan intelektual telah dihuraikan dan dianalisis dengan terperinci bagi melihat dengan lebih jelas jenayah siber serta aspek keselamatan yang diperlukan. Penulisan oleh sarjana dan intelektual yang telah dianalisis serta dibincangkan secara berstruktur ini dapat memudahkan usaha membina suatu kerangka dan mekanisme baharu terutamanya yang melibatkan kerjasama antara pihak kerajaan dan swasta bagi mengurangkan masalah jenayah siber dan meningkatkan aspek keselamatan siber untuk kepentingan bersama. Usaha membanteras jenayah siber perlu dilestarikan setiap masa bagi memastikan masyarakat dan negara dapat menikmati faedah besar daripada dunia digital dan teknologi maklumat.

Kata kunci: Keselamatan siber, jenayah siber, mekanisme penyelarasan, keselamatan negara

Abstract

The rapid development of the digital world has increased its dependence on information and communication technologies. This has unlocked the risk of a new threat, which is cybercrime. Cybercrime has created problems for society and the country and raised concerns because it affected social and economic development in a very critical situation. Weaknesses in law enforcement and the level of public awareness are among the factors contributing to increased cybercrime. To solve the problem, this study used an early approach to broaden and deepen understanding towards cybercrime and cybersecurity based on literature that has been contributed by scholars and intellectuals. Using a

qualitative approach, each scholar and intellectual writing has been discussed and analyzed particularly to observe cybercrime as well as the security aspects required. Scholar and intellectual writings that have been analyzed and discussed can facilitate efforts to create a new framework and mechanism, including cooperation between government and the private sector to reduce the problem of cybercrime and improve cybersecurity aspects in the future. Efforts to combat cybercrime must be sustained at all times to ensure that the community and the country can reap the great benefits of the digital world and information technology.

Keywords: *Cyber crime, cyber security, national security, coordination mechanism*

PENGENALAN

Era moden globalisasi yang muncul setelah era pasca Perang Dingin memperlihatkan ciri-ciri pengaliran bebas merentasi sempadan sama ada manusia, maklumat, idea, barangan, dan sumber dana. Kemunculan internet atau dunia siber sebagai alat komunikasi terkini dalam era globalisasi telah menjanjikan satu wadah penyebaran maklumat, idea, ideologi dan propaganda secara mudah dan pantas tanpa mengira sempadan masa dan geografi. Kesemua maklumat ini boleh dicapai hanya melalui hujung jari. Penggunaan internet secara meluas telah membuka ruang kepada ancaman keselamatan yang lebih besar iaitu ancaman siber. Ancaman siber merupakan masalah yang sering dihadapi oleh para pengguna komputer masa kini memandangkan kebanyakan komputer mempunyai sambungan kepada rangkaian internet yang diketahui bersifat terbuka dan dapat menghubungkan berjuta-juta komputer di seluruh dunia.

Internet kini telah berubah daripada medium komunikasi kepada medium perdagangan serta sumber ekonomi (Holt & Bossler 2016). Kajian penggunaan oleh Jabatan Perangkaan Malaysia mendapati capaian isi rumah kepada internet meningkat kepada 90.1% pada tahun 2019 berbanding 87.0% pada tahun 2018. Selain itu, peratusan penggunaan internet di Malaysia turut meningkat kepada 84.2% bagi tahun 2019 berbanding 81.2% pada tahun 2018 (Jabatan Perangkaan Malaysia 2020). Peratusan capaian telefon bimbit di seluruh Malaysia adalah pada 98.2% bagi tahun 2019 dan ini menunjukkan majoriti masyarakat mempunyai telefon bimbit dengan akses kepada internet.

Oleh yang demikian, dunia siber kini merupakan sebahagian daripada kehidupan manusia moden yang memainkan peranan penting dan banyak mengubah pelbagai aspek kehidupan manusia. Walau bagaimanapun, dunia siber bukan sahaja memberi kesan yang positif, malah boleh membawa kesan yang negatif kepada masyarakat sehingga boleh meningkatkan kadar jenayah. Wall (2007: 219-232) mendapati terdapat hubungan yang signifikan antara penggunaan internet dengan jenayah yang berlaku dewasa ini. Jenayah yang dikenali sebagai jenayah siber ini dilihat mampu memberikan ancaman secara maya kepada masyarakat dan negara. Dalam konteks Malaysia, jenayah siber menyebabkan Malaysia kerugian kira-kira RM1 bilion yang dicatatkan pada tahun 2013. Ia seterusnya meletakkan negara pada tangga keenam dalam senarai negara yang mudah diserang jenayah siber berdasarkan laporan Ancaman Keselamatan Sophos 2013. Saban tahun kegiatan jenayah siber semakin meningkat dan berdasarkan laporan yang dikeluarkan oleh Polis Diraja Malaysia (PDRM), jumlah kerugian yang dicatatkan bagi tahun 2019 meningkat sehingga RM5.8 bilion. Statistik Pasukan Tindakan Kecemasan Komputer Malaysia (MyCERT) juga menunjukkan bahawa jenayah penipuan siber merekodkan jumlah yang tinggi di mana sehingga Mei 2021, sebanyak 3,299 insiden dilaporkan dan bagi tahun 2020 sejumlah 7,593 insiden dilaporkan. Serentak itu, pihak Suruhanjaya Komunikasi Multimedia (SKMM) melaporkan bahawa ketika pelaksanaan Perintah Kawalan Pergerakan (PKP) pada 18 Mac hingga 20 Jun 2020, kes jenayah siber meningkat lebih 80 peratus berbanding tempoh sama pada tahun 2019. Manakala sehingga Mei 2021, sejumlah 4,615 kes jenayah siber dilaporkan. Antara lima jenayah siber tertinggi dilaporkan di Malaysia adalah melibatkan penipuan, pencerobohan, gangguan siber, kod jahat dan insiden berkaitan kandungan.

Peningkatan jenayah siber kini berada dalam keadaan membimbangkan dan ia dikaitkan dengan kekerapan penggunaan internet yang semakin meningkat dan kebergantungan masyarakat terhadap teknologi sehingga mengakibatkan mereka terdedah kepada ancaman siber. Menggodam komputer, mencuri kata laluan untuk perbankan internet, penyalahgunaan kad kredit untuk pembelian atas talian, keganasan siber dan pelbagai kegiatan jenayah era baharu ini dilakukan dengan mudah melalui dunia siber. Kebebasan dunia siber ini menyebabkan isu keruntuhan nilai kemanusiaan dan moral masyarakat kerana terdedah kepada pelbagai bahan-bahan yang tidak bermoral seperti bahan lucah, keganasan dan sebagainya. Tambahan pula, kegiatan jenayah siber ini tidak terhad tempoh masa dan batasan sempadan. Keterbukaan ini secara tidak langsung telah meningkatkan risiko keselamatan dalam kehidupan seharian.

Kegiatan jenayah siber ini bukan sahaja memberi kesan kepada individu tetapi juga kepada negara. Pelaku kegiatan ini mengambil peluang ke atas ruang siber yang terbuka bagi mencapai kekayaan dan kuasa yang diinginkan. Serangan siber boleh berlaku dalam bentuk penghantaran bom e-mel, spam, gangguan, ancaman penggodam, serangan virus, penafian perkhidmatan dan pencerobohan yang akan mengakibatkan kerugian besar serta menyebabkan kehilangan maklumat sulit syarikat mahupun kerajaan. Laporan akhbar saban hari juga melaporkan pelbagai kegiatan jenayah siber yang telah menyebabkan kerugian individu dan juga syarikat. Sebagai contoh, pada 23 Jun 2021 melaporkan seorang kerani kerugian sebanyak RM713,450 disebabkan oleh terpedaya dengan pelaburan mata wang asing palsu melalui aplikasi atas talian yang digunakan semenjak tahun 2017. Berdasarkan laporan, individu tersebut telah membuat 45 kali transaksi ke dalam akaun individu dan satu akaun syarikat dengan jumlah keseluruhan RM713,450 melalui pelaburan dalam nilai dolar Amerika Syarikat (USD) (Mohd Khidir Zakaria 2021). Kes seumpama ini turut dilaporkan pada 17 Mei 2021, di mana seorang wanita berusia 25 tahun telah kerugian RM255,250 berikutan terpedaya dengan pesanan yang diterima melalui aplikasi *WhatsApp* mengatakan individu tersebut memenangi peraduan dari sebuah syarikat produk makanan dan minuman terkenal sebanyak RM3,300. Individu tersebut telah membuat transaksi sebanyak 52 kali ke atas lapan akaun berbeza secara deposit tunai sebelum menyedari bahawa dirinya tertipu dan membuat laporan di Ibu Pejabat Polis Daerah Kota Setar pada 10 Mei 2021 (Adie Sufian Zulkefli 2021).

Selain memberi kesan kepada ekonomi, aspek keselamatan sosial dan kesihatan turut perlu diberi perhatian. Kesan keselamatan sosial yang melibatkan masyarakat ini akan memberi impak yang berpanjangan secara amnya. Sebagai contoh jenayah siber yang berbentuk gangguan akan menyebabkan trauma kepada individu yang menerima gangguan. Dalam era globalisasi kini, masyarakat terdedah dengan pelbagai aplikasi seiring daripada semasa ke semasa. Ini secara tidak langsung membuka ruang jenayah siber berlaku tanpa disedari. Kes penipuan melalui dunia siber yang menyebabkan individu kerugian puluhan sehingga ratusan ribu ringgit secara tidak langsung boleh menyebabkan kemurungan berpanjangan kepada individu terlibat. Begitu juga gangguan siber melalui media sosial boleh menyebabkan mangsa sentiasa berada dalam ketakutan kerana sering rasa diperhatikan. Ketika dunia dilanda pandemik penularan wabak COVID 19, kegiatan jenayah siber semakin menunjukkan peningkatan.

Dalam ucap utama Mesyuarat Menteri-menteri Digital ASEAN Pertama (ADGMIN1) yang diadakan pada 21-22 Januari 2021 di Kuala Lumpur, mantan Perdana Menteri Malaysia YAB Tan Sri Muhyiddin Yassin berkata, cabaran utama yang dihadapi kumpulan serantau dalam bidang siber adalah untuk terus berada di hadapan dalam dua bidang utama iaitu mengekang jenayah siber dan menuju kemajuan ekonomi digital. Selain itu, beliau turut menegaskan bahawa Malaysia menyedari bentuk jenayah siber rentas sempadan dan cabaran untuk membawa penjenayah siber ini ke muka pengadilan memerlukan pendekatan serantau yang selaras dan bersepadu (Pejabat Perdana Menteri 2021). Dengan jumlah kerugian tinggi yang dicatatkan oleh negara disebabkan jenayah siber, kegiatan ini memerlukan usaha semua pihak untuk menanganinya. Pihak kerajaan dan swasta dilihat perlu memainkan peranan lebih pro aktif dalam membanteras jenayah ini. Jenayah siber ini juga merupakan ancaman keselamatan yang boleh merencatkan pembangunan ekonomi negara. Aspek perundangan juga perlu dilihat supaya usaha menangani jenayah siber ini dapat dilaksanakan secara holistik.

Berdasarkan kepada masalah yang telah dijelaskan, timbul suatu minat dan motivasi tinggi untuk memahami dan mendalami masalah jenayah siber dan keselamatan siber di Malaysia. Ia penting bagi meningkatkan lagi pemahaman seterusnya membina suatu kefahaman baharu bagi menangani jenayah siber dan keselamatan siber di Malaysia secara inklusif. Pada masa yang sama, pengkaji juga melihat potensi kajian terhadap jenayah siber ini membuka ruang dan peluang baharu dalam menggabung jalinkan kerjasama antara pihak kerajaan dan swasta bagi memacu kepada suatu usaha bersama dalam membanteras jenayah siber. Secara umumnya makalah ini bertujuan untuk meninjau dan memerhati beberapa penulisan yang telah disumbangkan oleh para sarjana, intelektual dan juga pengkaji sama ada yang berada dalam dunia akademik dan bukan akademik. Ia sangat penting disebabkan melalui pandangan dan kajian yang telah dijalankan, suatu refleksi lengkap dapat dibentuk dan digunakan dalam meneruskan kajian ini di masa akan datang. Bagi memenuhi impian menjadi kenyataan, konsep jenayah siber ini perlu dihuraikan terlebih dahulu sebelum tinjauan dan pemerhatian dilakukan terhadap pandangan sarjana dan intelektual yang telah menjalankan kajian dan penyelidikan yang berkait dengan jenayah siber.

JENAYAH SIBER DAN KESELAMATAN SIBER

Jenayah siber secara umumnya merujuk kepada suatu perbuatan yang dilakukan secara sengaja atau tidak, oleh individu atau kumpulan yang mewakili mana-mana organisasi bagi mendapatkan maklumat secara tidak sah atau pun merosakkan peranti komputer, telefon pintar, dan peralatan lain yang berkait dengan perkakasan, perisian dan rangkaian internet. Teknik untuk memasuki ruang komputer sama ada melalui rangkaian internet, perisian dan perkakasan direka dan dibentuk dengan menggunakan kemahiran dan kreativiti yang tinggi dalam bidang teknologi maklumat dan juga teknologi digital. Ia kadang kala melibatkan pembinaan suatu algoritma umum dengan berbantukan bahasa pengaturcaraan yang asas seperti *C++, Java, Assembly Language* dan sebagainya. Kebanyakan jenayah siber dikenal pasti melalui penipuan e-mel dan internet, penipuan identiti (di mana maklumat peribadi dicuri dan digunakan), kecurian data kewangan atau pembayaran kad, kecurian dan penjualan data korporat, *Cyber extortion* (menuntut wang untuk mengelakkan serangan terancam), serangan perisian tebusan (sejenis pemerasan siber), *Crypto jacking* (penggodam melombong mata wang kripto menggunakan sumber yang tidak mereka miliki) dan *Cyberespionage* (penggodam mengakses data kerajaan atau syarikat). Walaupun peraturan dan undang-undang yang diperkenalkan oleh negara masing-masing untuk menangani masalah jenayah siber, kepintaran para penggodam dan juga ketirisan dalam pembangunan sistem dan juga seni bina aplikasi dapat menjadikan mereka lebih kreatif untuk terus menguji kemahiran masing-masing dalam aspek jenayah siber. Mungkin penjelasan yang diberikan terhadap jenayah siber ini dapat dijadikan sebagai asas dalam memahami jenayah siber dengan lebih terperinci.

Seterusnya keselamatan siber pula merujuk kepada aspek-aspek perlindungan yang digunakan untuk melindungi perisian, perkakasan (peranti mudah alih seperti telefon pintar dan sebagainya) dan rangkaian internet daripada serangan penggodam serta pihak yang tidak bertanggungjawab. Keselamatan siber juga dapat dijelaskan sebagai teknologi, proses dan amalan yang direka bentuk untuk melindungi rangkaian, peranti, program dan data daripada serangan, kerosakan atau akses tanpa kebenaran yang dilakukan oleh pihak yang tidak bertanggungjawab sama ada individu atau organisasi. Keselamatan siber juga dikenali sebagai keselamatan teknologi maklumat. Keselamatan siber sangat penting difokuskan kerana organisasi kerajaan, tentera, korporat, kewangan dan perubatan dalam sesebuah negara sentiasa terlibat dalam aktiviti mengumpul, memproses dan menyimpan jumlah data yang besar pada komputer dan peranti lain. Sebahagian besar data itu boleh menjadi maklumat sensitif, sama ada harta intelek, data kewangan, maklumat peribadi atau jenis data lain yang diakses atau pendedahan tanpa kebenaran boleh membawa kesan negatif. Secara umumnya, institusi atau organisasi menghantar data sensitif merentasi rangkaian ke peranti lain semasa menjalankan perniagaan atau melakukan aktiviti perkongsian maklumat. Dalam hal ini, keselamatan siber menerangkan disiplin yang khusus untuk melindungi maklumat tersebut dan sistem yang digunakan untuk memproses atau menyimpannya. Apabila jumlah dan kecanggihan serangan siber berkembang, syarikat dan organisasi, terutamanya yang ditugaskan untuk melindungi maklumat yang berkaitan dengan keselamatan negara, kesihatan atau rekod kewangan, perlu mengambil langkah untuk melindungi maklumat sensitif perniagaan dan kakitangan mereka. Seawal

Mac 2013, perisikan tertinggi Amerika Syarikat memberi amaran bahawa serangan siber dan pengintipan digital adalah ancaman utama kepada keselamatan negara mengatasi aspek keganasan. Bagi keselamatan siber yang berkesan, institusi atau organisasi perlu memastikan sistem keselamatan yang dimiliki dapat melindungi elemen seperti rangkaian, aplikasi, data, pangkalan data, *cloud* dan *mobile*. Aspek pemulihan juga perlu diperincikan jika proses mengembalikan sistem kepada asal selepas dirosakkan oleh para penjenayah siber.

Dalam konteks sosiologi, jenayah siber dan keselamatan siber merupakan suatu fenomena sosial yang berlaku di mana-mana tempat di dunia, institusi dan organisasi, kerajaan dan swasta, akademik dan bukan akademik. Ia turut melanda masyarakat dan individu yang menjadi tunjang kepada pembangunan sebuah negara bangsa. Menurut Markey (1926), fenomena sosial merangkumi semua tingkah laku yang mempengaruhi atau dipengaruhi oleh organisma yang hidup dan bertindak balas antara satu sama lain. Ini termasuk pengaruh daripada generasi yang lalu. Perkembangan dalam kajian sosial yang memberikan asas kepada konsep ini ialah aliran tingkah laku dan penekanan kepada sifat objektif kehidupan sosial, kajian kumpulan, dan kehidupan kumpulan, alam sekitar dan kajian ekologi. Kesahihan konsep yang mengehadkan fenomena sosial kepada interaksi manusia sentiasa dipersoalkan disebabkan asas yang luar biasa untuk perbezaan ini adalah asas psikologi yang dipanggil "sedar" atau "kesedaran." Aktiviti sedar, atau kesedaran yang digunakan sebagai istilah umum, tidak terhad kepada organisma manusia dan tidak memberikan asas. Interaksi sedar, dalam erti kata "berfikir" atau aktiviti konseptual, dipersoalkan sebagai asas saintifik untuk batasan sosial tersebut. Mungkin definisi fenomena sosial yang dijelaskan oleh Markey (1926) agak kompleks. Namun demikian, aspek utama yang ingin difokuskan adalah jenayah siber menjadi masalah sejagat yang perlu ditangani secara bersama demi memastikan keselamatan dan perlindungan sentiasa dapat dikekalkan pada masa hadapan.

Berdasarkan kepada penjelasan ringkas ini, definisi terhadap jenayah siber dan keselamatan siber ini dapat dijelaskan dalam konteks asas sebelum pengkaji memfokus kepada kajian dan penyelidikan yang lebih luas, mendalam dan terperinci terhadap pandangan sarjana dan intelektual yang menjalankan kajian dan penyelidikan terhadap jenayah siber. Untuk memudahkan lagi pemahaman, bahagian seterusnya akan membincangkan metodologi yang digunakan bagi merungkai dengan lebih konstruktif terhadap tujuan penulisan artikel ini.

METODOLOGI

Pengkaji menggunakan pendekatan kualitatif secara analisis dokumen untuk memudahkan huraian dan perincian dilakukan terhadap penulisan yang berkait dengan jenayah siber, keselamatan siber dan kerjasama pihak kerajaan dan swasta dalam menangani masalah jenayah siber dan meningkatkan aspek keselamatan siber. Data yang diperoleh adalah melalui buku, jurnal, artikel, bab buku, laporan akhbar dan internet digunakan untuk memudahkan tugas pengkaji. Kajian kepustakaan selama tiga bulan telah dilakukan melalui eksplorasi maklumat di internet, perpustakaan Tun Seri Lanang dan juga sokongan daripada pengkaji lain. Oleh kerana pandemik Covid-19 membataskan pergerakan, pengkaji banyak memfokuskan usaha melalui bahan-bahan yang dimuat turun secara percuma melalui *Google* dan setiap satu daripada bahan yang telah diterbitkan dimasukkan pada bahagian rujukan dalam artikel ini. Bagi memudahkan lagi pemahaman, Jadual 1 menunjukkan ringkasan kepada sumber-sumber yang dimuat turun bersama-sama dengan nama penulis, tahun diterbitkan dan jenis bahan yang diperoleh.

Jadual 1. Penulisan Sarjana dan Intelektual dalam bidang Jenayah dan Keselamatan Siber

	Penulis	**Tahun**	**Bahan Penerbitan**
1	Donn B. Parker	1989	Buku
2	Speer	2000	Artikel
3	Nazura Abdul Manap dan Jasri Jamal	2004	Artikel

4	Broadhurst	2006	Artikel
5	Azeez Nureni Ayofe, Barry Irwin	2010	Artikel
6	Kamini Dashora	2011	Artikel
7	Duryana Mohamed	2013	Artikel
8	Prasad, Roslina dan Azizah	2014	Artikel
9	Asiah Bidin, Shariffah Nuridah Aishah Syed Nong Mohamad dan Akmal Mohamad	2015	Artikel
10	Omar Hamdan dan Abd. Manaf Ismail	2015	Artikel
11	Max Manley	2015	Artikel
12	Tatiana Tropina	2015	Buku
13	Timea Pahi dan Florian Skopik	2016	Artikel
14	Ganesin A/L Supayah dan Jamaludin Ibrahim	2018	Artikel
15	Andrew Futter	2018	Artikel
16	Maslina Daud, Rajah Rasiah, Mary George, David Asirvatham dan Govindamal Thangiah	2018	Artikel
17	Chooi Shi Teoh, Ahmad Kamil Mahmood dan Suhazimah Dzazali	2018	Artikel
18	Nor Shazwina, Muhamad Yusnorizam, Nurhizam, Siti Mariam	2019	Artikel
19	Muhammad Adnan Pitchan dan Siti Zobidah Omar	2019	Artikel
20	Bernardi Pranggono, Abdullah Arabo	2020	Artikel

Jadual 1 merupakan usaha pengkaji untuk mendapatkan bahan-bahan yang berguna bagi meluaskan pemahaman terhadap aspek jenayah dan keselamatan siber. Terdapat 20 bahan kesemuanya yang telah diperoleh dan ianya menjadi suatu garis panduan serta rujukan bagi menjalankan kajian dengan lebih terperinci. Bagi memudahkan lagi pemahaman, bahagian seterusnya akan membincangkan huraian secara ringkas pandangan sarjana dan intelektual melalui penulisan mereka.

PENULISAN SARJANA DAN INTELEKTUAL YANG BERKAIT DENGAN JENAYAH DAN KESELAMATAN SIBER

Penulisan sarjana dan intelektual dalam bidang jenayah dan keselamatan siber dikategorikan kepada tiga bahagian; jenayah siber, keselamatan siber dan kerjasama awam-swasta. Ini penting bagi menghuraikan dengan ringkas pandangan sarjana dan intelektual terhadap ketiga-tiga aspek tersebut.

Jenayah Siber

Terlebih dahulu definisi jenayah siber perlu dikenal pasti sebelum kajian ini dibincangkan dengan lebih lanjut. Ini bertujuan mendapatkan kefahaman yang jelas terhadap maksud jenayah siber. Berdasarkan kajian lepas, definisi yang komprehensif telah dibuat oleh Donn B. Parker (1989) seorang penyelidik mengenai keselamatan dan jenayah komputer untuk Institut Penyelidikan dan Pembangunan Antarabangsa SRI di Menlo Park, California. Beliau menyatakan bahawa jenayah komputer adalah mana-mana perlakuan yang mempunyai niat dan dikaitkan dengan komputer melalui apa-apa cara dan menyebabkan mangsa menderita atau boleh menyebabkan penderitaan, kerugian secara berterusan. Jabatan Kehakiman Amerika Syarikat menguatkan lagi definisi ini dengan menyatakan bahawa jenayah komputer adalah mana-mana aktiviti yang tidak sah di mana pengetahuan mengenai teknologi komputer digunakan untuk merealisasikannya. Namun demikian, harus diakui bahawa terdapat pelbagai takrifan jenayah siber yang berbeza antara negara. Bagi negara-negara Islam, kegiatan judi, pornografi dan pengiklanan seks adalah merupakan satu jenayah tetapi tidak untuk kebanyakan negara barat contohnya di Amerika Syarikat kerana hal-hal sebegini dianggap remeh dan hanya pornografi kanak-kanak saja dikategorikan sebagai jenayah. Mereka lebih memberi tumpuan kepada keselamatan dan perdagangan dengan merangka pelbagai undang-undang yang berkait rapat dengan keselamatan dan perdagangan seperti akta hak cipta, penggodaman, penyebaran virus dan sebagainya. Dengan adanya takrifan yang berbeza ini, ia dilihat sukar untuk penguatkuasaan undang-undang siber secara global dilaksanakan.

Menurut Speer (2000), jenayah siber adalah merupakan ancaman keselamatan terbaru dalam dunia pada hari ini, dan ia berbeza daripada ancaman lain yang dihadapi dunia. Kajian beliau telah mengaitkan ancaman jenayah siber dengan ancaman keselamatan lain, serta membuktikan bahawa terdapat keunikan dalam ancaman jenayah siber dari segi ancaman kepada negara itu sendiri dan peringkat antarabangsa. Beliau melihat bahawa struktur keselamatan sedia ada perlu ditambah baik untuk mengawal ancaman jenayah siber ini. Menurut beliau, terdapat empat elemen utama jenayah siber yang dikaji iaitu lokasi penjenayah ketika melakukan jenayah, wujudnya mangsa, pesalah dan tindakan untuk menangani ancaman. Langkah ini perlu untuk mengenal pasti sifat jenayah siber sebelum perbandingan dibuat dengan ancaman keselamatan lain. Ini kerana jika dibandingkan dengan ancaman tradisional lain, penjenayah akan berada di lokasi secara fizikal, namun bagi kes melibatkan jenayah siber adalah sukar untuk mengesan lokasi penjenayah yang melakukannya. Menurut pengkaji, usaha untuk menangani jenayah siber harus dipertingkatkan kerana jenayah ini semakin berleluasa. Usaha berterusan diperlukan bagi memahami mengapa penjenayah melakukan jenayah ini dan langkah-langkah yang boleh diambil untuk menghentikannya. Secara keseluruhan, ancaman jenayah siber sangat besar dan akan terus berkembang mengikut arus teknologi. Ancaman ini perlu dibendung sebelum menjadi lebih parah dan peranan kerajaan adalah amat penting dalam usaha menanganinya.

Nazura Abdul Manap dan Jasri Jamal (2003) melalui kajian 'Jenayah Komputer: Perbandingan Menurut Akta Jenayah Komputer 1997 dan Prinsip Undang-Undang Jenayah Islam' mengupas mengenai sejauh mana prinsip undang-undang jenayah Islam yang berlandaskan kepada al-Quran dan al-Sunnah boleh diguna pakai dalam memberi jawapan kepada permasalahan jenayah siber. Berdasarkan kajian tersebut, Kanun Keseksaan merupakan statut induk yang mentadbir kesalahan-kesalahan jenayah yang berlaku di Malaysia. Walaupun tiada peruntukan khusus dalam statut bagi menyelesaikan masalah jenayah alaf baharu ini, beberapa peruntukan undang-undang mungkin boleh diguna pakai. Namun begitu, peruntukan-peruntukan tersebut tidak lengkap malah terdapat beberapa kelemahan yang menyukarkan pengaplikasian peruntukan undang-undang berkenaan kepada permasalahan siber. Ini dapat dilihat menerusi pemakaian beberapa peruntukan seperti seksyen 378 bagi kecurian maklumat atau data dalam sistem komputer, seksyen 415 berkaitan penipuan yang berlaku dalam data komputer menyebabkan kecurian wang melalui pengubahan maklumat, seksyen 463 bagi menyelesaikan kes pemalsuan kata laluan dan seksyen 425 mengenai perbuatan yang menyebabkan kerosakan data komputer. Akta Jenayah Komputer 1997 ini menggariskan beberapa bentuk kesalahan yang boleh disabitkan di bawah peruntukan akta ini. Elemen-elemen yang merupakan prasyarat bagi sabitan kesalahan adalah bersesuaian dengan sifat jenayah komputer itu sendiri. Dengan adanya akta sebegini, sedikit sebanyak membantu

menyelesaikan masalah jenayah komputer atau siber. Oleh kerana peruntukannya digubal khusus bagi menyelesaikan masalah jenayah komputer, maka masalah seperti pengaplikasian elemen-elemen yang sukar dipenuhi dan terdapat dalam Kanun Keseksaan kepada jenayah komputer tidak lagi timbul. Walau bagaimanapun, seperti undang-undang yang lain, Akta Jenayah Komputer 1997 juga tidak lari daripada kelemahan-kelemahan tertentu yang seharusnya ditangani segera.

Broadhurst (2006) pula berpandangan bahawa jenayah siber juga merupakan jenayah tradisional seperti penipuan, pencurian identiti dan pornografi kanak-kanak yang dilakukan dengan pantas terhadap sejumlah besar mangsa dengan menggunakan komputer. Selain itu jenayah ini juga dikaitkan dengan penggodaman komputer secara tidak sah serta kerosakan dan gangguan kepada sistem komputer itu sendiri. Perkara yang paling memudaratkan adalah pengeksploitasian kod yang mengganggu operasi komputer pada skala global sehingga mengancam semua urus niaga secara elektronik. Pengkaji juga melihat perkembangan teknologi ini telah membuka ruang yang lebih dinamik bagi jenayah siber berkembang. Menurut pengkaji, peranan teknologi digital dan maklumat untuk menjana hasil negara mengundang risiko baharu di semua peringkat sama ada nasional, serantau mahu pun antarabangsa. Proses globalisasi yang semakin meningkat juga menunjukkan tindak balas global dalam menangani permasalahan ini masih belum dapat dilaksanakan secara sepenuhnya. Perkembangan dasar dan polisi berkaitan ruang siber amat penting sebagai usaha menangani jenayah siber merupakan fokus pengkaji di samping pencapaian masyarakat antarabangsa terhadap isu ini.

Kamini Dashora (2011) dalam artikel beliau bertajuk '*Cyber Crime in the Society: Problems and Preventions*' mengupas pendekatan berbeza setiap negara dalam menghadapi isu jenayah siber. Beliau juga berpandangan jenayah siber telah muncul sebagai ancaman yang serius menyebabkan agensi penguatkuasaan dan risikan mula mengambil tindakan membendung ancaman rentas sempadan ini. Sebagai contoh di India, pihak polis telah menubuhkan sel siber khas di seluruh negeri dan memberikan pendidikan berkaitan jenayah siber kepada tenaga kerja di sana. Berdasarkan kajian ini, pengkaji mengupas mengenai masalah jenayah siber dalam kalangan masyarakat berdasarkan laporan berita dan media massa. Jenayah siber menurut pandangan pengkaji merupakan suatu bentuk jenayah baharu yang sangat rumit dalam dunia siber masa kini. Ini kerana ancaman secara maya sukar dikesan dan penguatkuasaan undang-undang yang lebih ketat wajar dilaksanakan. Menurut pengkaji juga, sehingga kini masih tiada undang-undang yang dibuat untuk menghapuskan jenayah secara keseluruhan namun penguatkuasaan undang-undang adalah penting bagi mengekang kegiatan jenayah untuk terus berleluasa. Pengkaji juga mengupas setiap jenis jenayah dan langkah-langkah bersesuaian mengatasi jenayah siber ini namun keupayaan minda manusia adalah sangat kompleks dan tidak dapat dibayangkan. Jenayah siber semakin meluas dan penguatkuasaan serta kesedaran masyarakat harus dipertingkatkan.

Artikel '*Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws*' daripada Duryana Mohamed (2013) membincangkan usaha-usaha yang telah diambil oleh kerajaan dalam usaha menangani jenayah siber di Malaysia. Pengkaji melihat peningkatan jenayah siber ini mula mendapat perhatian apabila laman sesawang Parlimen Malaysia dan Universiti Teknologi Mara (UiTM) diserang penggodam pada tahun 2002. Kejadian seperti ini semakin meningkat saban tahun melibatkan pelbagai agensi kerajaan dan swasta sehingga menyebabkan kerugian yang besar. Perkara ini menyebabkan Cyber Security Malaysia di bawah Kementerian Sains dan Teknologi Malaysia (MOSTI) meningkatkan sistem pertahanan bagi menjaga data sulit dan kerahsiaan negara. Pelbagai usaha yang dilaksanakan oleh Cyber Security Malaysia dalam menjaga keselamatan siber negara daripada serangan siber. Selain Cyber Security Malaysia, Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) juga bertanggungjawab dalam menggubal dasar berkaitan keselamatan siber. Namun, menurut pengkaji, Malaysia masih tidak mempunyai perundangan keselamatan siber yang khusus seperti undang-undang anti-spam berbanding beberapa negara lain. Penguatkuasaan undang-undang berkaitan jenayah siber ini wajar diperhalusi bagi membolehkan pesalah dikenakan hukuman yang setimpal. Ini kerana sehingga kini, undang-undang sedia ada memerlukan ruang penambahbaikan seiring peredaran zaman. Teknologi masa kini semakin bergerak pantas sekali gus membuka ruang jenayah siber berleluasa tanpa mengira mangsa.

Justeru, undang-undang yang lebih tegas perlu dikuatkuasakan bagi mengekang jenayah siber ini terus berleluasa.

Prasad, Roslina dan Azizah (2014) pula telah menjalankan kajian mengenai jenayah siber di Malaysia dengan melihat kepada aspek dan jenis jenayah, statistik jenayah, undang-undang berkaitan serta peranan Malaysia dalam menangani isu ini. Pengkaji turut mencadangkan supaya kajian lebih terperinci dibuat dengan melihat secara khusus kepada definisi mengenai jenayah siber itu sendiri supaya penguatkuasaan undang-undang yang seragam dapat dilaksanakan. Walaupun telah ramai yang menjadi mangsa jenayah siber namun, masih banyak isu mengenai jenayah siber belum difahami sepenuhnya. Justeru, adalah penting untuk memahami pelbagai aspek jenayah siber supaya keputusan dan tindakan yang lebih bijak diambil. Berdasarkan kajian, pengkaji menyatakan bahawa pada tahun 2012, laporan daripada Norton Cybercrime melaporkan 556 juta pengguna telah menjadi mangsa jenayah siber dengan purata sebanyak 1.5 juta setiap hari dan 18 mangsa dalam tempoh satu saat di seluruh dunia. Kerugian sebanyak RM2.75 bilion dicatatkan oleh Malaysia dalam tempoh lima tahun (2008 hingga 2013) disebabkan oleh jenayah siber dan ini dilaporkan sendiri oleh Cyber Security Malaysia. Secara keseluruhannya, pengkaji juga mengakui bahawa jenayah siber berkembang dengan pesat berbanding jenayah lain dan ia boleh mengancam keselamatan negara. Pengkaji telah melihat kepada definisi jenayah siber sedia ada dan mendapati masih terdapat kekurangan dalam menjelaskan definisi sebenar jenayah siber.

Asiah Bidin, Shariffah Nuridah Aishah Syed Nong Mohamad dan Akmal Mohamad (2015) mengupas berkaitan jenayah intipan siber yang diklasifikasikan sebagai jenayah baharu dewasa kini. Menerusi artikel bertajuk 'Intipan Siber: Jenayah Baru dalam Masyarakat Kontemporari', pengkaji membincangkan bagaimana penggunaan laman rangkaian sosial meningkatkan risiko terhadap jenayah intipan siber (*cyber stalking*). Artikel ini turut membincangkan bagaimana jenayah ini berlaku serta persoalan sama ada perundangan sedia ada memadai dalam usaha menangani jenayah siber. Berdasarkan artikel ini, pengkaji membincangkan bagaimana laman rangkaian sosial dijadikan medium perantara untuk menjalankan modus operandi jenayah intipan siber. Jenayah ini memberi kesan terhadap mangsa sehingga menimbulkan rasa takut dan trauma berpanjangan. Kita sedia maklum, laman rangkaian sosial seperti *Facebook, Friendster, Twitter* merupakan antara yang tertinggi digunakan oleh pengguna. Secara tidak sedar pengguna telah mendedahkan maklumat peribadi dan kerahsiaan melalui aplikasi tersebut sekali gus membuka ruang kepada pelaku jenayah untuk mengganggu mangsa. Pelaku ini mengintip mangsa berdasarkan maklumat yang didedahkan melalui aplikasi rangkaian sosial sehingga menimbulkan rasa takut terhadap mangsa yang diganggu. Perlakuan ini walaupun tidak secara fizikal tetapi boleh memberi kesan yang mendalam terhadap menangani jenayah ini. Menurut pengkaji, beberapa negara telah mewujudkan undang-undang khusus bagi menangani kes berkaitan jenayah intipan siber. Namun, Malaysia masih memerlukan masa untuk menyelesaikan jenayah siber secara efektif.

Keselamatan Siber

Azeez Nureni Ayofe dan Barry Irwin (2010) dalam artikel '*Cyber Security: Challenges and the way forward*' mengupas berkaitan jenayah siber yang semakin serius telah menimbulkan kebimbangan kerana ia merupakan ancaman keselamatan siber. Pengkaji melihat fenomena ancaman ini semakin canggih dan memerlukan tindak balas yang pantas dalam menyediakan perundangan bagi melindungi ruang siber dan pengguna. Kajian ini menerangkan mengenai cabaran dalam keselamatan siber serta bagaimana ruang siber digunakan oleh penjenayah sehingga menyebabkan ramai menjadi mangsa sekali gus mengancam keselamatan negara. Pengkaji melihat keselamatan siber dalam tiga aspek iaitu jenayah siber dalam kalangan individu, harta dan kerajaan. Jenayah siber dan keselamatan siber telah menjadi subjek perhatian seluruh dunia kerana evolusi jenayah ini berkembang dengan begitu pantas. Dari segi perundangan, pengkaji juga merumuskan walaupun pencapaian sesebuah negara semakin maju, namun negara-negara tersebut masih menggunakan undang-undang '*terresstrial standard*' untuk mendakwa jenayah siber di mana undang-undang ini telah wujud sebelum kedatangan ruang siber lagi. Keselamatan siber dilihat sukar dibendung dan persekitaran serta ruang siber yang selamat tidak akan dapat dicapai selagi ancaman maya terus berlaku.

An Overview of Cyber Security in Malaysia merupakan artikel yang ditulis oleh Ganesin A/L Supayah dan Jamaludin Ibrahim (2016) mengupas berkaitan keselamatan siber yang memfokuskan kepada tiga faktor utama perbincangan iaitu teknologi, organisasi dan manusia yang merujuk kepada pengguna. Berdasarkan kajian, pengkaji menyatakan Malaysia merupakan antara negara yang menjadi sasaran jenayah siber berleluasa. Laporan yang dikeluarkan oleh Cyber Security Malaysia merekodkan peningkatan kes yang dilaporkan daripada 3,564 pada tahun 2009 kepada 8,009 pada tahun 2010 melibatkan 127% dalam tempoh satu tahun sahaja. Kerugian yang dilaporkan pada tahun 2009 melibatkan RM22.3 juta dan sekiranya dibiarkan tanpa penguatkuasaan yang lebih tegas akan menyebabkan kerugian yang lebih besar buat negara. Penggunaan teknologi yang kian meluas menjadikan pelaku jenayah siber juga semakin berevolusi dalam menjalankan kegiatan mereka. Kerajaan Malaysia dilihat mengambil perhatian serius dalam menangani jenayah siber melalui Cyber Security Malaysia. Namun, pengkaji melihat penguatkuasaan undang-undang yang lebih tegas dan usaha berterusan agensi kerajaan perlu dipertingkatkan dalam menangani jenayah siber. Faktor kelemahan kesedaran pengguna dalam melayari laman sesawang dan rangkaian sosial juga harus dipertingkatkan bagi mengurangkan risiko menjadi mangsa jenayah siber.

Kajian Andrew Futter (2018) bertajuk '*Cyber' semantics: why we should retire the latest buzzword in security studies*' pula mengupas berkaitan perdebatan penggunaan perkataan siber dalam aspek pengajian keselamatan. Ini kerana terdapat beberapa kajian yang dilihat gagal menyentuh isu 'siber' dalam beberapa perkara, malah didapati segelintir ahli politik gagal menggunakan istilah tersebut ketika memperkatakan bagaimana ia menjadi ancaman yang kritikal kepada negara. Kajian ini mengupas kekeliruan dan salah faham penggunaan perkataan siber dalam pengajian keselamatan, kajian strategik, pertahanan serta pembuatan dasar dan ini adalah tidak bersesuaian apabila membicarakan mengenai cabaran berkaitan rangkaian dan sistem komputer. Pengkaji juga berpandangan terma siber wajar dikeluarkan daripada istilah akademik dan wacana perbahasan seterusnya dibiarkan kembali pada fiksyen sains. Justeru, kajian ini ingin melihat bagaimana perbezaan pandangan pengkaji dengan realiti keselamatan siber yang berlaku sekarang.

Nor Shazwina, Muhamad Yusnorizam, Nurhizam dan Siti Mariam (2019) melalui artikel *CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries* mengupas berkaitan isu keselamatan siber dalam kalangan negara ASEAN. Keselamatan siber telah menjadi isu besar pada peringkat global sekali gus menyebabkan ASEAN meningkatkan langkah untuk mengatasi isu ini. Kajian ini telah mengkaji kes-kes berkaitan keselamatan siber yang berlaku dalam kalangan negara-negara ASEAN dari tahun 2014 sehingga tahun 2019. Secara amnya tiada negara yang terlepas daripada ancaman keselamatan siber dalam arus globalisasi yang semakin berkembang. Beberapa kes insiden siber yang kritikal melibatkan negara ASEAN antara Januari 2017 sehingga Mei 2019 telah dilaporkan. Sebagai contoh, pada bulan Julai 2018, Singapura menghadapi serangan siber yang besar apabila penggodam berjaya menggodam sistem teknologi maklumat institusi SingHealth dan mencuri data 1.5 juta rekod pesakit. Perkara ini dilaporkan sendiri oleh Perdana Menteri Singapura dalam artikel yang diterbitkan TODAY. Di Malaysia, sejumlah 45 insiden serangan *ransomeware* yang menyerang pelbagai sektor dan industri telah menjejaskan beberapa organisasi dilaporkan pada tahun 2018. Secara keseluruhannya, kajian ini mendapati masih terdapat ruang lingkup keselamatan siber yang perlu diperincikan merangkumi sektor swasta, dasar perlindungan dan infrastruktur bersesuaian untuk masyarakat. Dalam usaha menangani isu keselamatan siber ini juga, negara anggota ASEAN perlu berganding bahu dan bekerjasama secara holistik.

Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang merupakan artikel yang ditulis oleh Muhammad Adnan Pitchan dan Siti Zobidah Omar (2019) mengupas mengenai tahap kesedaran masyarakat yang menjadi antara penyumbang kepada peningkatan isu keselamatan siber. Pengkaji menyatakan bahawa netizen atau warga net sangat mudah terdedah kepada ancaman siber tanpa mereka sedari. Netizen dengan mudah berkongsi maklumat peribadi di platform media sosial dan sebagainya tanpa memikirkan keselamatan diri. Malah menurut pengkaji, mereka tidak merasakan tindakan tersebut mengundang bahaya ancaman siber. Selain itu, penguatkuasaan undang-undang juga penting dalam menangani isu keselamatan siber dan berdasarkan kajian, didapati tahap kesedaran yang lemah serta kurangnya pengetahuan berkaitan penguatkuasaan undang-undang siber telah memberi kesan ke atas kes jenayah siber di

Malaysia. Muhammad Adnan et al. (2017) berpendapat faktor kurangnya ilmu kefahaman tentang undang-undang siber turut menyumbang kepada peningkatan statistik jenayah siber. Terdapat pelbagai akta dan perundangan di Malaysia yang telah diwartakan untuk kegunaan bagi kesalahan dalam talian namun menurut Anita (2004) masih terdapat golongan netizen yang tidak menyedari kewujudan akta-akta tersebut malah menyalahgunakan kemudahan internet yang diberikan oleh kerajaan.

Bernardi Pranggono dan Abdullah Arabo (2020) mengupas berkaitan cabaran keselamatan siber dalam tempoh pandemik yang melanda dunia. Ini kerana terdapat peningkatan isu keselamatan siber walaupun dalam keadaan dunia dilanda penularan wabak COVID-19. Pandemik yang melanda telah menimbulkan kegusaran, ketidakpastian dan perubahan besar dalam kehidupan seharian manusia. Organisasi juga perlu menyesuaikan keadaan sekarang dan membuat rombakan terhadap cara kerja apabila pekerja perlu bekerja dari rumah. Namun, terdapat kebanyakan organisasi yang tidak bersedia dengan perubahan ini malah perancangan yang sewajarnya juga tidak disediakan. Situasi ini menyebabkan organisasi terdedah kepada ancaman serangan siber. Penjenayah siber mula mengambil kesempatan menyebabkan kegiatan jenayah siber meningkat. Antara serangan siber yang meningkat menurut pengkaji dalam tempoh pandemik ialah penipuan, pancingan data (*phishing*) dan sebaran penolakan perkhidmatan (DDoS) di mana mereka menyerang organisasi dan individu berhubung maklumat berkaitan vaksin COVID-19. Mereka mengeksploitasi data dan maklumat yang ada untuk mengaut keuntungan lumayan. Sektor kesihatan turut menjadi sasaran serangan siber apabila maklumat pesakit, perubatan dan penyelidikan digodam oleh penjenayah siber. Keadaan ini membimbangkan dan membuatkan kerajaan perlu mengambil langkah dengan lebih berkesan untuk menangani masalah tersebut. Sekiranya sektor kesihatan diserang pastinya menimbulkan lebih banyak masalah dan kerugian yang besar buat negara. Justeru, sektor kesihatan juga perlu meningkatkan kesiapsiagaan dalam menghadapi ancaman keselamatan siber.

Kerjasama Awam – Swasta

Ancaman keselamatan internet sebagai isu utama negara: Isu-isu kontemporari, pendekatan dan penyelesaian daripada Oemar Hamdan dan Abd. Manaf Ismail (2015) mengupas perbincangan berkaitan isu keselamatan siber yang semakin menjadi ancaman kepada negara. Isu ini mendapat perhatian global kerana memberi kesan yang membimbangkan bukan sahaja kepada pengguna tetapi juga negara. Kerjasama semua pihak termasuklah individu, masyarakat, agensi kerajaan, agensi swasta adalah perlu dalam usaha menangani ancaman keselamatan siber yang semakin meruncing. Dasar yang digubal bertujuan melindungi semua pihak supaya tidak terjebak dengan salah laku internet. Pengkaji menyatakan berdasarkan kajian bahawa ancaman siber semakin berleluasa berikutan kebanyakan syarikat dan agensi masih mengamalkan dasar keselamatan yang lemah, malah ada yang tidak mempunyai dasar dan polisi keselamatan siber di agensi mereka. Kakitangan dan individu pengguna juga kebanyakan tidak mengamalkan etika penggunaan siber yang selamat menyebabkan terdedah menjadi mangsa ancaman keselamatan siber. Menurut pengkaji, menyedari kepentingan keselamatan teknologi maklumat, Malaysia telah menubuhkan agensi pemantauan iaitu Pusat Respons Kecemasan dan Keselamatan ICT Kebangsaan (NISER) pada tahun 2001 dengan tujuan menangani masalah insiden keselamatan ICT negara. Agensi ini bertindak menjalinkan kerjasama dengan pelbagai agensi lain dalam memberikan perkhidmatan penilaian teknologi, insurans keselamatan dan pelbagai lagi. Terdapat juga agensi lain yang berperanan dalam memberikan perkhidmatan teknologi maklumat. Justeru, agensi kerajaan, swasta dan pengguna seharusnya bekerjasama dalam memastikan ancaman keselamatan siber dapat ditangani dengan baik.

Max Manley (2015) dalam kajian bertajuk '*Cyberspace's Dynamic Duo: Forging Cybersecurity Public-Private Partnership*' memerihalkan keberkesanan kerjasama awam – swasta harus didasari dengan empat elemen iaitu kepercayaan, panduan undang-undang yang jelas, pendekatan daripada bawah ke atas dan penglibatan masyarakat secara menyeluruh. Secara amnya, kerjasama awam dan swasta terus meningkat di seluruh dunia dan ia memberi kelebihan dalam menjalankan urusan dengan lebih berkesan. Menurut Osborne (2000), kerjasama awam dan swasta merupakan elemen penting dalam merangka dasar di seluruh dunia dan sekiranya jaringan kerjasama yang terbina berdasarkan kerangka kerja yang efektif, ia akan dapat membuahkan hasil positif terhadap pelaksanaan projek

yang dijalankan. Namun begitu, kepercayaan dan keyakinan tinggi harus diletakkan bagi membolehkan kerjasama berjalan dengan baik. Dalam konteks kajian ini, peranan agensi kerajaan dan swasta adalah sama penting untuk merangka usaha bersesuaian menangani isu keselamatan siber. Malaysia mempunyai pelbagai agensi berkaitan keselamatan siber seperti Cyber Security Malaysia, Suruhanjaya Komunikasi dan Multimedia (SKMM), Polis Diraja Malaysia (PDRM) dan lain-lain. Namun, jenayah siber terus meningkat dan peranan agensi sedia ada harus ditingkatkan untuk menangani masalah ini.

Kajian bertajuk '*Public-Private Collaboration: Cybercrime, Cybersecurity and National Security*' oleh Tatiana Tropina (2015: 1-41) mengupas pendekatan isu keselamatan siber dan juga perlindungan maklumat kritikal memerlukan kolaborasi awam dan swasta bagi mewujudkan persekitaran rangkaian maklumat yang selamat. Namun, apabila keselamatan siber diletakkan sebagai agenda utama dalam pembuatan dasar, terdapat pihak kerajaan dan sarjana akademik yang melihat kegagalan tersebut adalah disebabkan oleh pihak swasta tidak dapat menjamin tahap keselamatan yang dikehendaki. Secara tidak langsung, peralihan konsep ini membawa kepada cadangan untuk menetapkan tatacara yang lebih berkesan dari segi perkongsian maklumat dan prosedur pematuhan. Kajian ini melihat isu kolaborasi awam dan swasta dari perspektif yang luas dan memfokuskan kepada pelbagai bentuk bidang kerjasama termasuklah menangani masalah jenayah siber, perlindungan maklumat kritikal infrastruktur dan keselamatan negara. Bagi tujuan analisis ini, pengkaji melihat jenayah siber tidak hanya kepada isu kerahsiaan, integriti tetapi juga merangkumi jenayah lain seperti kandungan gambar keganasan penderaan kanak-kanak dan jenayah atas talian. Skop kerjasama awam dan swasta di sini dikaitkan dengan 'domain keadilan jenayah' termasuk pendakwaan, penyiasatan dan pengesanan awal gangguan jenayah yang dilakukan dalam talian dan ia adalah berdasarkan udang-undang dan prosedur jenayah. Kedua adalah bidang kerjasama yang melibatkan penglibatan sektor swasta dalam keselamatan negara dan ini merujuk kepada kerjasama antara industri dan kerajaan menangani ancaman keselamatan seperti pengintipan ekonomi dan ancaman keselamatan politik. Manakala bidang ketiga kerjasama adalah pakatan antara pihak berkepentingan swasta dan pengawal selia mengenai ketahanan siber dan perlindungan infrastruktur maklumat. Justeru, kerjasama awam dan swasta ini perlu diperhalusi sebaik mungkin bagi memberi manfaat kepada kedua-dua pihak sekali gus dapat menjamin keselamatan negara.

Timea Pahi dan Florian Skopik (2016) menerusi kajian '*A Public-Private-Partnership Model for National Cyber Situational Awareness*' mengupas berkaitan kemajuan era globalisasi telah menghubungkan pelbagai infrastruktur daripada kedua-dua sektor awam dan swasta seperti teknologi maklumat, komunikasi, perbankan, bekalan tenaga dan lain-lain. Oleh itu, perlindungan sistem ini adalah penting bagi mencapai kemakmuran dan kesejahteraan ekonomi bersama. Pengkaji memperkenalkan model *public-private-partnership cyber situational awareness* (P3CSA) sebagai kerangka kerja yang membolehkan kerjasama lebih erat dilaksanakan. Kerangka kerja ini menawarkan konsep dan metodologi pengumpulan data pelbagai peringkat dengan lebih pantas yang membolehkan peringatan awal terhadap situasi keselamatan siber dapat diambil tindakan sewajarnya. Pengkaji merumuskan bahawa pelaksanaan struktur kerangka P3CSA yang berkesan memerlukan keupayaan dan pelaporan insiden yang efektif pada semua peringkat dan organisasi bagi melindungi infrastruktur kritikal sekali gus menjamin keselamatan nasional.

Artikel '*Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations?*' daripada Maslina Daud, Rajah Rasiah, Mary George, David Asirvatham dan Govindamal Thangiah (2018) mengupas perbincangan berkaitan bagaimana pematuhan terhadap keselamatan siber dapat membantu meningkatkan kerjasama dalam organisasi. Perbincangan ini melihat kepada pengendalian organisasi dalam mematuhi prosedur keselamatan siber bagi mengelakkan kehilangan data sulit dan juga kerahsiaan sesebuah organisasi. Kerjasama semua pihak daripada pengurusan tertinggi sehingga kakitangan atau pengguna adalah perlu bagi menjaga pematuhan keselamatan siber. Agensi awam dan swasta perlu meningkatkan kerjasama bagi memastikan keselamatan siber organisasi dapat dijaga sekali gus membantu mengelakkan penyalahgunaan teknologi yang menyebabkan jenayah siber berleluasa.

Chooi Shi Teoh, Ahmad Kamil Mahmood dan Suhazimah Dzazali (2018) menerusi kajian '*Cyber Security Challenges in Organisations: A Case Study in Malaysia*' mengupas berkaitan cabaran keselamatan siber pada peringkat organisasi. Kajian ini memfokuskan kepada tiga faktor yang dikenal pasti iaitu teknologi, proses dan manusia. Faktor teknologi merujuk kepada perkembangan teknologi yang semakin pesat seiring peredaran zaman. Proses dalam kajian ini merujuk kepada cabaran dalam melaksanakan pelan yang telah digubal, manakala faktor manusia merujuk kepada cabaran dari segi kemahiran. Justeru, kajian ini mengupas bagaimana sesebuah organisasi mendepani cabaran keselamatan siber berdasarkan tiga faktor ini. Berdasarkan kajian, pengkaji juga melihat kerjasama semua pihak adalah perlu bagi menjaga keselamatan siber sesebuah organisasi.

ANALISIS DAN PERBINCANGAN

Daripada 20 bahan penerbitan tersebut, pengkaji sebenarnya dapat memerhatikan dengan jelas sumbangan yang telah diberikan oleh para sarjana dan intelektual yang telah menerbitkan penulisan masing-masing dalam buku dan juga artikel akademik. Pengkaji tidak berhasrat untuk menganalisis dan membincangkan satu persatu bahan-bahan tersebut yang telah pun dijadikan sebagai penulisan literatur untuk menyiapkan tesis sarjana. Secara umumnya, penulisan yang berasaskan kepada kajian dan penyelidikan yang telah dijalankan oleh para sarjana dan intelektual ini lebih terfokus kepada isu teknikal seperti rangkaian, struktur rangkaian, komunikasi atas talian, penggunaan perisian, perkakasan dan peranti serta dasar dan polisi yang dapat diangkat menjadi undang-undang yang mampu memberi perlindungan kepada pengguna dalam penggunaan aplikasi, peranti dan rangkaian dalam dunia siber. Jika dilihat sepintas lalu, kajian dan juga penyelidikan yang telah disumbangkan oleh sarjana dan intelektual melalui buku dan artikel tersebut dapat memberikan suatu gambaran yang umum tentang punca berlakunya jenayah siber, meningkatkan lagi aspek keselamatan siber dan kerjasama antara institusi kerajaan dan swasta dalam memacu kepada perlindungan secara total.

Jika diperhatikan kepada jenayah siber, penulisan yang menjustifikasi konsep tersebut lebih terfokus kepada isu-isu teknikal yang ditemui serta eksplorasi yang dilakukan terhadap punca kepada masalah tersebut. Kebanyakan definisi yang dijelaskan oleh para sarjana dan intelektual berasaskan kepada kajian dan penyelidikan mereka dan ini sebenarnya menjadi panduan dan motivasi kepada pengkaji sendiri untuk memudahkan kajian dijalankan seterusnya menjadi pelengkap kepada usaha berterusan dalam memantau perkembangan jenayah siber di Malaysia. Kebanyakan sarjana dan intelektual di luar negara menjustifikasi jenayah siber dalam konteks yang sangat terperinci. Setiap satu definisi yang dinyatakan disertakan dengan contoh serta faktor lain yang menjadi penyumbang kepada berlakunya jenayah siber ini. Selain itu, sebahagian mereka seperti Parker (1989) dan Speer (2000) juga terlibat dalam usaha pihak kerajaan Amerika Syarikat untuk bersama-sama membantu memantapkan lagi langkah berwaspada dalam menangani jenayah siber. Penulisan sarjana dan intelektual tempatan pula lebih tertumpu kepada pendekatan yang digunakan untuk mengatasi masalah jenayah siber ini melalui pendekatan Islam sebagai contoh. Penyelidik seperti Nazura Abdul Manap dan Jasri Jamal (2003) memfokuskan kepada pendekatan Islam secara inklusif bagi mengekang penularan jenayah siber sekali gus mengurangkan kadar jenayah siber. Hal ini disebabkan tiadanya peraturan dan perundangan tertentu di Malaysia yang dapat digunakan bagi menghukum pesalah yang terlibat dalam jenayah siber. Ada banyak contoh yang dapat diperhatikan terhadap masalah yang dijelaskan oleh kedua-dua pengkaji ini. Oleh kerana isu politik tempatan di Malaysia merupakan suatu topik perbincangan yang hangat sama ada dalam ruang akademik dan bukan akademik, penularan jenayah siber berkait dengan isu politik sangat membimbangkan dan ianya perlu dibendung bagi memastikan kemajuan negara dapat dilestari untuk suatu jangka masa yang panjang.

Dalam konteks keselamatan siber, pengkaji memfokuskan kepada usaha yang dilakukan oleh para penyelidik, ahli akademik, sarjana dan intelektual dalam melihat penulisan berkaitan bidang tersebut. Secara umumnya, kebanyakan penulisan yang disumbangkan oleh sarjana dan intelektual tempatan lebih tertumpu kepada usaha dan komitmen yang boleh dilakukan bagi mengatasi masalah siber. Pengkaji tempatan lebih berminat untuk menyelesaikan tersebut berdasarkan kepada faktor-faktor teknikal, sumber manusia dan aspek kewangan yang mampu dimiliki oleh para institusi, organisasi mahupun individu bagi memberi perlindungan secara menyeluruh terhadap jenayah siber.

Ada juga pengkaji seperti Muhammad Adnan Pitchan dan Siti Zobidah Omar (2019) yang memberi penekanan terhadap kesedaran masyarakat terutamanya netizen di media sosial yang sangat terdedah kepada jenayah siber. Pengkaji berpandangan langkah ini merupakan suatu usaha terbaik yang dapat dilakukan bagi memaklumkan kepada masyarakat tentang bahayanya jenayah siber. Walaupun usaha ini memerlukan komitmen daripada semua pihak, pengkaji dapat melihat usaha ini telah pun dijalankan oleh beberapa pihak tertentu yang terlibat dalam penyediaan rangkaian internet kepada masyarakat seperti Telekom Malaysia, Celcom, Maxis, U-Mobile dan sebagainya. Selain itu, pihak kerajaan melalui Suruhanjaya Komunikasi dan Multimedia atau ringkasnya SKMM turut sama-sama membantu dalam mengurangkan jenayah siber seterusnya memantapkan aspek keselamatan siber.

Penulisan yang berkait dengan kerjasama awam-swasta pula memberikan impak yang sangat positif dalam rangka memudahkan pemahaman terhadap kajian yang dijalankan ini. Kebanyakan sarjana dan intelektual, dalam dan luar negara banyak menumpukan aspek kerjasama yang kukuh antara agensi kerajaan dan swasta kerana melalui usaha ini, aspek keselamatan dapat ditingkatkan ke suatu peringkat yang lebih tinggi. Apabila adanya kerjasama seperti ini, usaha memerangi jenayah siber akan menjadi lebih mudah dan untuk negara membangun seperti Malaysia, perancangan yang mantap pada masa hadapan bagi memperkenalkan undang-undang baharu untuk menghukum penggodam yang terlibat dapat dilakukan dengan mudah. Pengkaji juga tertarik dengan suatu model yang diperkenalkan oleh Timea Pahi dan Florian Skopik (2016) yang dikenali sebagai P3CSA. Model ini sebenarnya boleh dijadikan sebagai panduan bagi kerajaan Malaysia untuk memudahkan lagi mekanisme kerjasama antara pihak kerajaan dan swasta bagi mengurangkan jenayah siber dan meningkatkan keselamatan siber. Hal ini sangat penting bagi melindungi masyarakat dan mampu menjadi pemacu kepada kejayaan dalam bidang teknologi maklumat dan digital.

KESIMPULAN

Jenayah siber, keselamatan siber dan kerjasama awam-swasta merupakan asas penting dalam menggambarkan secara umum fokus kepada kajian ini. Penulisan yang telah disumbangkan oleh sarjana dan intelektual, dalam dan luar negara, menjadi motivasi dan panduan berguna untuk pengkaji bagi memastikan suatu kefahaman yang menyeluruh dapat dibina seterusnya menjalankan kajian ini dengan lebih tersusun dan sistematik. Huraian dan penjelasan yang diberikan sebelum ini juga dapat memudahkan kajian ini menyumbangkan suatu mekanisme yang inklusif dalam menentukan hala tuju negara untuk mengurangkan jenayah siber, meningkatkan keselamatan siber dan akhirnya memberi tumpuan penuh kepada usaha kerajaan dalam menjadikan bidang teknologi komunikasi maklumat serta teknologi digital sentiasa dipelihara dan dipastikan keberkesanannya dalam memacu ekonomi negara dan memastikan masyarakat sentiasa selamat dalam menempuhi perkembangan dunia siber yang semakin kompleks dan berdaya saing. Walaupun terdapat pelbagai halangan dalam usaha murni ini, jika tidak dipecahkan ruyung, manakan dapat sagunya. Jika tidak dilakukan usaha berterusan, manakan dapat kejayaannya. Begitu juga dengan hasrat menggunung tinggi pengkaji melalui kajian yang dimulakan dengan tapak yang kecil tetapi dengan langkah yang besar. Melalui kajian ini, usaha untuk meningkatkan lagi minat masyarakat terutamanya dalam pembangunan ekonomi dan sara hidup berterusan melalui dunia siber dapat dilestarikan untuk suatu jangka masa yang panjang dan hal ini turut memberi keuntungan besar kepada negara dalam rangka membina masyarakat digital dengan nilai murni serta moral yang tinggi.

RUJUKAN

Adie Sufian Zulkefli. 2021. Kerani rugi lebih RM255,000 ditipu menang peraduan. *BERNAMA*, 17 Mei 2021.

Anita, A. R. & Nazura, A. M. 2004. *Jenayah Berkaitan dengan Komputer: Perspektif Undang-Undang Malaysia*. Kuala Lumpur: Dewan Bahasa dan Pustaka.

Andrew Futter. 2018. 'Cyber' semantics: why we should retire the latest buzzword in security studies. *Journal of Cyber Policy* 3(3):1-16.

Asiah Bidin, Shariffah Nuridah Aishah Nong Mohamad & Akmal Mohamad. 2015. Intipan Siber: Jenayah Baru dalam Masyarakat Kontemporari. *Jurnal Islam dan Masyarakat Kontemporari* 11(3): 10-21.

Azeez Nureni Ayofe & Barry Irwin. 2010. Cyber security: Challenges and the way forward. *Computer Science and Telecommunications* 29(6): 66-69.

Broadhurst, R.G. 2006. Developments in the global law enforcement of cyber-crime. *Policing*: *An International Journal of Police Strategies and Management* 29(3): 408-433.

Cyber Security Malaysia. 2021. MyCERT Incidents Statistic. https://www.mycert.org.my/statistics/2021 [10 Mei 2021].

Dashora, K. 2011. Cybercrime in the society. *Journal of Alternative Perspectives in the Social Sciences* 3(1): 240-259.

Donn B. Parker. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. United States of America: John Wiley & Sons Inc.

D.S. Wall. 2007. *Cybercrimes: The Transformation of Crime in the Information Age Cambridge*. United Kingdom: Polity Press.

Ganesin A/L Supayah & Jamaludin Ibrahim. 2016. An Overview of Cyber Security in Malaysia. *Kuwait Chapter of Arabian Journal of Business and Management Review* 6(4):12-20.

Jabatan Perangkaan Malaysia. 2020. Laporan Survei Penggunaan dan Capaian ICT oleh Individu dan Isi Rumah 2019. 10 April 2020.

John Markey. 1926. A Redefinition of Social Phenomena: giving A Basis for Comparative Sociology. *American Journal of Sociology* 31: 733-743.

Maslina Daud, Rajah Rasiah, Mary George, David Asirvatham & Govindamal Thangiah. 2018. Bridging the Gap Between Organisational Practices and Cyber Security Compliance: Can Cooperation Promote Compliance Organisations? *International Journal of Business and Society* 19(1): 161-180.

Max Manley. 2015. Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership. *Journal of Strategic Security* 8(3): 85-98.

Mohamed, D. 2013. Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review* 29(1): 66–76.

Muhammad Adnan Pitchan & Siti Zobidah Omar. 2019. Dasar Keselamatan Siber Malaysia: Tinjauan terhadap kesedaran netizen dan undang-undang. *Jurnal Komunikasi* 35(1): 103-119.

Mohd Khidir Zakaria. 2021. Kerani rugi RM700,000 kena perdaya. https://www.bharian.com.my/berita/kes/2021/06/831234/kerani-rugi-rm700000-kena-perdaya, *Berita Harian* [23 Jun 2021].

Mohd Shamir bin Hashim. 2011. Malaysia's National Cyber Security Policy: The country's cyber defence initiatives. *Second Worlwide Cybersecurity Summit (WCS)*.

Muhammad Adnan Pitchan, Siti Zobidah Omar, Jusang Bolong & Akmar Hayati. 2017. Analisis Keselamatan Siber dari Perspektif Persekitaran Sosial: Kajian Terhadap Pengguna Internet di Lembah Klang. *Journal of Social Sciences and Humanities* 12(2): 016-029.

Nazura Abdul Manap & Jasri Jamal. 2003. Jenayah Komputer: Perbandingan Menurut Akta Jenayah Komputer 1997 dan Prinsip Undang-undang Jenayah Islam. *Jurnal Undang-undang dan Masyarakat* 7: 15-36.

Nor Shizwana Mohamed Mizan, Muhamad Yusnorizam Ma'arif, Nurhizam Safie Mohd Satar & Siti Mariam Shahar. 2019. CNDS-Cybersecurity: Issues and challenges in ASEAN countries. *International Journalof Advanced Trendsin Computer Science and Engineering* 8(14): 113-119.

Oemar Hamdan & Abd Manaf Ismail. 2015. Ancaman Keselamatan Internet sebagai isu utama Negara: Isu-isu Kontemporari, Pendekatan dan Penyelesaian. *Majalah Ilmiah UNIKOM* 13(2).

Osborne, S.P. 2000. *Public Private Partnerships: Theory and Practice in International Perspective*. London: Routledge.

Pranggono, B. & Arabo, A. 2021. Covid-19 Pandemic Cybersecurity issues. *Internet Technology Letters* 4(2): e247.

Parker, Donn B., *Criminal Justice Resource Manual on Computer Crime*, US Department of Justice, 1980, reprinted 1989.

Pejabat Perdana Menteri. 2021. https://www.pmo.gov.my/2021/01/keynote-address-at-the-first-asean-digital-ministers-meeting/ [10 Mei 2021].

Prasad Jayabalan, Roslina Ibrahim & Azizah Abd Manap. 2014. Understanding cybercrime in Malaysia: an overview. *Sains Humanika* 2(2): 109-115.

Speer, D.L. 2000. Redefining borders: The challenges of cybercrime. *Crime, Law and Social Change* 34: 259-273.

Teoh, C. S, Mahmood, A.K & Dzazali, S. 2018. Cybersecurity Challenges in organisations: A case study in Malaysia. *International Conference on Computer and Information Sciences (ICCOINS).* 13-14 August 2018.

Thomas J. Holt1 & Adam M. Bossler. 2016. Technology and Violence. *The Wiley Handbook on the Psychology of Violence*: 588-603.

Timea Pahi, Florian Skopik. 2016. A Apublic-Private-Partnership Model for National Cyber Situational Awareness. *International Journal on Cyber Situational Awareness* 1(1): 31-53.

Tropina, T. 2015. *Public-Private Collaboration: Cybercrime, Cybersecurity and National Security.* Self and Co-regulation in Cybercrime, Cybersecurity and National Security.

Nur Sarida Binti Mohd Fuad@Mohd Daud
Pelajar Sarjana
Pusat Kajian Sejarah, Politik & Hal Ehwal Antarabangsa
Fakulti Sains Sosial dan Kemanusiaan
Universiti Kebangsaan Malaysia
43600 UKM Bangi
Selangor Darul Ehsan
E-mel: p106667@siswa.ukm.edu.my

Ahmad Rizal Mohd Yusof, (Ph.D)
Felo Penyelidik
Institut Kajian Etnik
Universiti Kebangsaan Malaysia
43600 UKM Bangi
Selangor Darul Ehsan
E-mel: army@ukm.edu.my

Diserahkan: 19 Disember 2021
Diterima: 16 Februari 2022
Diterbitkan: 30 Jun 2022