DEFINISI, ANCAMAN DAN MEKANISME KAWALAN POLITIK *CYBERTROOPERS* DI MALAYSIA

NURUL BINTI IWAN

UNIVERSITI PENDIDIKAN SULTAN IDRIS

2024

DEFINISI, ANCAMAN DAN MEKANISME KAWALAN POLITIK *CYBERTROOPERS* DI MALAYSIA

NURUL BINTI IWAN

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

TESIS DIKEMUKAKAN BAGI MEMENUHI SYARAT UNTUK MEMPEROLEH IJAZAH SARJANA SASTERA (PENGAJIAN MALAYSIA) (MOD PENYELIDIKAN)

FAKULTI SAINS KEMANUSIAAN
UNIVERSITI PENDIDIKAN SULTAN IDRIS

2024

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

Sila tanda (√)
Kertas Projek
Sarjana Penyelidikan
Sarjana Penyelidikan dan Kerja Kursus
Doktor Falsafah

INSTITUT PENGAJIAN SISWAZAH

PERAKUAN KEASLIAN PENULISAN

Perakuan ini telah dibuat pada 1 (hari bulan) MEI (bulan) 2024.

i. Perakuan pelajar :

Saya, NURUL BINTI IWAN M20202001439 DAN FAKULTI SAINS KEMANUSIAAN (SILA NYATAKAN NAMA PELAJAR, NO. MATRIK DAN FAKULTI) dengan ini mengaku bahawa disertasi/tesis yang bertajuk DEFINISI, ANCAMAN DAN MEKANISME KAWALAN POLITIK CYBERTROOPERS DI MALAYSIA adalah hasil kerja saya sendiri. Saya tidak memplagiat dan apa-apa penggunaan mana-mana hasil kerja yang mengandungi hak cipta telah dilakukan secara urusan yang wajar dan bagi maksud yang dibenarkan dan apa-apa petikan, ekstrak, rujukan atau pengeluaran semula daripada atau kepada mana-mana hasil kerja yang mengandungi hak cipta telah dinyatakan dengan sejelasnya dan secukupnya

Tandatangan pelajar

ii. Perakuan Penyelia:

Saya, NORHAFIZA BINTI MOHD HED (NAMA PENYELIA) dengan ini mengesahkan bahawa hasil kerja pelajar yang bertajuk DEFINISI, ANCAMAN DAN MEKANISME KAWALAN POLITIK CYBERTROOPERS DI MALAYSIA (TAJUK) dihasilkan oleh pelajar seperti nama di atas, dan telah diserahkan kepada Institut Pengajian Siswazah bagi memenuhi sebahagian/sepenuhnya syarat untuk memperoleh Ijazah IJAZAH SARJANA SASTERA (PENGAJIAN MALAYSIA) (SLA NYATAKAN NAMA IJAZAH).

7 MEI 2024
Tarikh

Tandatangan Penyelia

INSTITUT PENGAJIAN SISWAZAH /
INSTITUTE OF GRADUATE STUDIES

BORANG PENGESAHAN PENYERAHAN TESIS/DISERTASI/LAPORAN KERTAS PROJEK
DECLARATION OF THESIS/DISSERTATION/PROJECT PAPER FORM

Tajuk / *Title*: DEFINISI, ANCAMAN DAN MEKANISME KAWALAN POLITIK CYBERTROOPERS DI MALAYSIA

No. Matrik /*Matric's No.*: M20202001439

Saya / *I* : NURUL BINTI IWAN

(Nama pelajar / *Student's Name*)

mengaku membenarkan Tesis/Disertasi/Laporan Kertas Projek (Kedoktoran/Sarjana)* ini disimpan di Universiti Pendidikan Sultan Idris (Perpustakaan Tuanku Bainun) dengan syarat-syarat kegunaan seperti berikut:-
acknowledged that Universiti Pendidikan Sultan Idris (Tuanku Bainun Library) reserves the right as follows:-

1. Tesis/Disertasi/Laporan Kertas Projek ini adalah hak milik UPSI.
   The thesis is the property of Universiti Pendidikan Sultan Idris
2. Perpustakaan Tuanku Bainun dibenarkan membuat salinan untuk tujuan rujukan dan penyelidikan.
   Tuanku Bainun Library has the right to make copies for the purpose of reference and research.
3. Perpustakaan dibenarkan membuat salinan Tesis/Disertasi ini sebagai bahan pertukaran antara Institusi Pengajian Tinggi.
   The Library has the right to make copies of the thesis for academic exchange.
4. Sila tandakan (√) bagi pilihan kategori di bawah */ Please tick (√) for category below:-*

☐	**SULIT/*CONFIDENTIAL***	Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub dalam Akta Rahsia Rasmi 1972. / *Contains confidential information under the Official Secret Act 1972*
☐	**TERHAD/*RESTRICTED***	Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan ini dijalankan. / *Contains restircted information as specified by the organization where research was done.*
☑	**TIDAK TERHAD / *OPEN ACCESS***	

(Tandatangan Pelajar/ Signature)

(Tandatangan Penyelia / *Signature of Supervisor*)
& (Nama & Cop Rasmi / *Name & Official Stamp*)

Tarikh: 1 MEI 2024

Catatan: Jika Tesis/Disertasi ini **SULIT** @ **TERHAD**, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan ini perlu dikelaskan sebagai **SULIT** dan **TERHAD**.

Notes: If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.

PENGHARGAAN

Terlebih dahulu saya ingin mengucapkan syukur Alhamdulillah ke hadrat Allah S.W.T, kerana di atas limpah dan kurniaNya, maka dapatlah saya menyiapkan tesis ini dengan jayanya walaupun terpaksa menempuhi pelbagai dugaan dan rintangan.

Di kesempatan ini, saya ingin mengucapkan jutaan terima kasih yang tidak terhingga kepada Dr. Norhafiza binti Mohd Hed, selaku penyelia saya di atas kesabaran, sokongan, nasihat dan bimbingan yang diberikan banyak membantu dalam menyiapkan tesis ini. Segala bantuan dan semangat yang diberikan beliau telah banyak mengajar saya untuk menjadi penyelidik dan pendidik yang baik. Tidak dilupakan kepada barisan pensyarah Fakulti Sains Kemanusiaan yang sudi berkongsi ilmu sepanjang pengajian ini. Segala pengalaman yang dilalui tidak akan dilupakan.

Terima kasih kepada pihak penaja iaitu Kementerian Pengajian Tinggi kerana telah memberikan tajaan kepada saya di bawah Fundamental Research Grant Scheme (FRGS) untuk melanjutkan pengajian di peringkat sarjana. Ribuan terima kasih kepada kedua-dua ayahnda dan ibunda yang saya kasihi, yang sentiasa memberi kasih sayang, dorongan, doa, peringatan dan panduan hidup yang amat saya perlukan. Ucapan terima kasih juga turut dititipkan buat suami tercinta yang banyak memberikan idea, cadangan dan semangat. Titipan terima kasih buat adik beradik yang banyak memberi bantuan dan semangat sepanjang proses pengajian ini. Sesungguhnya segala pengorbanan yang telah dilakukan amat saya sanjungi dan akan saya ingati sepanjang hayat ini.

Akhir kata, ucapan terima kasih juga kepada semua yang terlibat secara langsung dan tidak langsung dalam memberikan sumbangan, cadangan dan bantuan dalam menyiapkan tesis ini. Semoga penyelidikan dan tesis ini dapat dijadikan panduan serta wadah ilmu yang berguna untuk tatapan minda generasi yang akan datang.

Sekian, terima kasih.

Nurul binti Iwan

ABSTRAK

Di Malaysia, kemunculan gerakan *cybertroopers* dilihat signifikan pada Pilihan Raya Umum ke-12 dan berkembang pada Pilihan Raya ke-14. Sejajar dengan perkembangan ini, isu *cybertroopers* mula mendapat perhatian ramai sarjana yang mengkaji tentang kewujudan dan peranannya dalam konteks politik di Malaysia. Namun, kajian berkaitan pendefinisian istilah politik *cybertroopers* masih lagi terhad sehingga istilah ini turut disamakan dengan konsep *netizen, keyboard warriors*, dan askar siber. Malah, kajian tentang ancaman kumpulan *cybertroopers* ke atas keselamatan negara juga kurang dibincangkan di Malaysia. Oleh itu, kajian ini menyelidiki konsep dan tipologi yang sesuai bagi menggambarkan *cybertroopers* dalam konteks Malaysia, ancaman yang dibawa oleh *cybertroopers* kepada keselamatan nasional serta mekanisme terbaik bagi mengawai gerakan ini. Kajian ini menggunakan kaedah campuran iaitu gabungan pendekatan kualitatif dan kuantitatif. Bagi kaedah kuantitatif, kajian tinjauan menerusi instrumen soal selidik digunakan dan diedarkan secara rawak kepada seramai 395 belia di Perak dan Selangor. Manakala, bagi kaedah kualitatif, instrumen temu bual bersama 10 informan yang dipilih secara bertujuan daripada golongan akademik, *cybertroopers* dan aktivis politik telah digunakan. Dapatan kajian menunjukkan definisi istilah *cybertroopers* merujuk kepada pihak yang diupah menjadi agen perantara antara pemimpin dengan rakyat untuk menyampaikan sesuatu isu yang boleh mempengaruhi pemikiran masyarakat di media sosial. Dapatan kajian juga mendapati bahawa gerakan *cybertroopers* ini memberi ancaman yang sederhana (min: 2.29, s.p: 0.36) di mana mereka berupaya mengganggu gugat kestabilan politik, tetapi tidak memberi ancaman besar terhadap keselamatan negara. Selain itu, tindakan kerajaan melaksanakan pengawasan dan penapisan siber (min: 2.50, s.p: 0.33), serta penerapan pendidikan keselamatan siber (min: 2.79, s.p: 0.45) kepada masyarakat merupakan mekanisme kawalan yang paling efektif dalam mengawal gerakan ini. Implikasi kajian ini diharap dapat memberi pendefinisan terkini kepada istilah *cybertroopers,* sekali gus membantu kerajaan dalam membangunkan kerangka baharu dalam menangani gerakan *cybertroopers* di Malaysia.

DEFINITION, THREATS AND CONTROL MECHANISMS OF POLITICAL CYBERTROOPERS IN MALAYSIA

ABSTRACT

In Malaysia, the emergence of cybertrooper movements was significantly observed during the 12th General Election and expanded during the 14th General Election. In line with this development, the issue of *cybertroopers* has gained attention from scholars studying their existence and roles in the Malaysian political context. However, studies related to the definition of the term *cybertroopers* are still limited, leading to the term being equated with concepts like netizens, keyboard warriors, and cyber soldiers. Moreover, research on the threats posed by *cybertroopers* to national security is also lacking in Malaysia. Therefore, this study investigates definition and typologies to describe *cybertroopers* in the Malaysian context, the threats they pose to national security, and the control mechanisms to counteract this movement. The study employs a mixed-methods approach, combining qualitative and quantitative methods. For the quantitative method, a survey instrument was used and randomly distributed to 395 youth in Perak and Selangor. Meanwhile, for the qualitative method, interviews were conducted with 10 purposively selected informants from academic, cybertrooper, and political activist. The findings indicate that the definition of the term *cybertroopers* refers to individuals who are hired as intermediaries between leaders and the public to convey issues that can influence public opinion on social media. The research also found that cybertrooper movements pose a moderate threat (min: 2.29, s.d: 0.36), as they can disrupt political stability but do not pose a significant threat to national security. Additionally, government actions such as implementing cyber surveillance and filtering (min: 2.50, s.d: 0.33) and promoting cybersecurity education (min: 2.79, s.d: 0.45) to the public are identified as the most effective control mechanisms against this movement. The implications of this study are expected to provide a contemporary definition of the term *cybertroopers*, thereby assisting the government in developing a new framework to address cybertrooper movements in Malaysia.

KANDUNGAN

BAB 5 KESIMPULAN

SENARAI JADUAL

SENARAI RAJAH

SENARAI SINGKATAN

PRU	Pilihan Raya Umum
AS	Amerika Syarikat
BN	Barisan Nasional
PH	Pakatan Harapan
TPPA	Trans-Perjanjian Perkongsian Pasifik (TPPA)
1MDB	1 Malaysia Development Berhad
CMA	Akta Komunikasi dan Multimedia
SKMM	Suruhanjaya Komunikasi dan Multimedia Malaysia
PDRM	Polis DiRaja Malaysia
KDNK	Keluaran Dalam Negara Kasar
PKP	Perintah Kawalan Pergerakan
ICT	Teknologi Maklumat dan Komunikasi
NIS	Perkhidmatan Maklumat Nasional
PCTA	Philipine Cable Television Association
BSSN	Badan Siber dan Sandi Negara
ID-SIRTII/CC	*Indonesia Security Incident Response Team on Internat and Infrastructure/ Coordination Centre*
SPSS	*Statistical Package Social Sciences*
POS	*Political Opportunity Structure*
TPA	Teori Penentuan Agenda
SPM	Sijil Pelajaran Malaysia
DOSM	Jabatan Perangkaan Malaysia
QSR	*Qualitative Solution and Research*

BAB 1

PENDAHULUAN

1.0 Pengenalan

Kepesatan teknologi pada hari ini telah berjaya mewujudkan 'media sosial' yang dilihat sebagai satu transformasi yang sangat berjaya dalam dunia teknologi. O'Reilly (2005) memperkenalkan istilah web 2.0 pada tahun 2005 di mana beliau mendakwa bahawa web 2.0 menunjukkan perubahan sebenar di mana penghasilan *Google*, *Amazon*, Wikipedia atau *Craiglist* dalam komuniti berhubung antara satu sama lain. O'Reilly & Battelle (2009, p.1) mengakui bahawa istilah ini dicipta untuk mengenal pasti keperluan strategi ekonomi baru syarikat internet selepas krisis 'dot.com' di mana banyak syarikat internet pada ketika itu dilihat gagal untuk berkembang akibat krisis kewangan. Mandiberg (2012) berpendapat bahawa media sosial adalah kandungan media yang menjadi kegunaan syarikat korporat untuk menyampaikan maklumat. Kemunculan laman Web 2.0 ini membolehkan pengguna berinteraksi dan berkolaborasi antara satu sama lain sebagai pencipta kandungan dalam komuniti maya seperti *Facebook*, *YouTube*, *Flickr* dan sebagainya. Ia berbeza dengan generasi pertama laman web 1.0 di mana individu hanya terhad melihat kandungan secara pasif

(Blank & Reisdorf, 2012). Ini menunjukkan bahawa media sosial dari awal penubuhannya adalah satu alat untuk menyampaikan maklumat kepada pengguna internet. Oleh itu, media sosial menjadi mekanisme penting kepada masyarakat khususnya pemimpin politik. Bukan di Malaysia sahaja, malah di seluruh dunia ahli politik menggunakan media sebagai satu platform untuk menyampaikan maklumat dan menarik sokongan masyarakat terutamanya sewaktu pilihan raya. Beberapa contoh fenomena politik seperti kemenangan Barack Obama dalam pilihan raya presiden di Amerika Syarikat (AS) pada tahun 2008 adalah disebabkan oleh keberkesanan kempennya menerusi media siber sebagai mekanisme untuk mendekati rakyat, khususnya belia. Fenomena berkembangnya politik siber di Amerika dapat dilihat apabila Barack Obama menggunakan media sosial dalam pilihan raya pada ketika itu. Menerusi penggunaan siber, ianya dapat menyampaikan manifesto beliau ke seluruh penduduk Amerika, sekali gus, meraih undi daripada mereka. Melalui konsep komunikasi secara media, ianya memudahkan orang awam untuk lebih dekat dan dapats berkomunikasi secara langsung dengan beliau. Hal ini, menyebabkan wujudnya komunikasi dua hala antara rakyat dan pemerintah serta memudahkan proses manifesto berjalan dengan lancar kerana rakyat mendapat maklumat secara terus daripada pemerintah.

Selain itu, revolusi yang melanda Tunisa dan Mesir atau ‘Arab Spring’ adalah senario politik yang menunjukkan peranan penting media siber dalam menggerakkan protes politik yang menjatuhkan regim pemerintah dan membawa gelombang pendemokrasian di dunia Arab. Kemunculan perkhidmatan rangkaian sosial yang ada pada hari ini dilihat sebagai satu revolusi yang mengubah cara pengguna internet bersosial dan berinteraksi di ruang siber. Gerakan protes rakyat di Mesir mula dicetuskan oleh sekumpulan aktivis muda yang menuntut agar proses pembaharuan politik dilaksanakan di negara tersebut. Ianya juga merupakan rentetan kepada krisis

politik yang melanda Tunisia sebelum itu. Seluruh dunia dikejutkan dengan krisis yang melanda Mesir sehingga membawa kepada keputusan pengunduran Presiden Hosni Mubarak. Revolusi di Mesir ini telah merebak ke negara-negara serantau dan mencetuskan pelbagai gerakan anti-kerajaan seperti Algeria, Yemen, Bahrain dan Libya. Hal ini jelas menunjukkan bahawa rangkaian sosial memainkan peranan yang penting dalam membantu golongan aktivis melancarkan propaganda siber mereka dan mempengaruhi persepsi rakyat untuk menentang kerajaan dan menubuhkan satu kerajaan yang baharu. Rangkaian sosial dijadikan platform oleh rakyat Mesir untuk mereka berinteraksi dan berkomunikasi sesama sendiri dan melancarkan gerakan revolusi menentang kerajaan.

Di Malaysia, fenomena yang sama turut berlaku apabila kuasa politik Barisan Nasional (BN) semakin terhakis sehingga mencetuskan 'tsunami politik' pada Pilihan Raya Umum (PRU) 2008[1]. Kegagalan BN untuk mengekalkan dua pertiga majoriti di Parlimen adalah disebabkan oleh pengaruh media baru, khususnya media sosial (web 2.0) seperti *Youtube*, *Facebook*, *Twitter* dan *Myspace.* Media baru ini telah digunakan secara meluas oleh pihak pembangkang untuk menarik sokongan masyarakat. Tun Abdullah Ahmad Badawi yang merupakan Perdana Menteri Malaysia pada waktu itu turut mengakui bahawa kegagalan BN dalam peperangan *online* menyebabkan mereka hilang sebahagian besar sokongan anak muda. Menurut Abdullah (New Straits Times, 2008, Mac 26, 2),

[1]Dalam PRU 2008, kuasa politik BN semakin luntur apabila tercetusnya 'tsunami politik'. Keputusan PRU 2008 memperlihatkan BN hanya memperolehi 50.27% berbanding 63.9% undi pada PRU 2004. Keputusan PRU ini menunjukkan penurunan sokongan generasi muda kepada BN. Antara sebab utama generasi muda memihak kepada pembangkang adalah kerana kegagalan strategi BN untuk menarik sokongan generasi muda. Strategi politik pembangunan yang menjadi asas manifesto BN tidak lagi relevan kepada generasi muda. Golongan ini lebih mementingkan isu-isu demokrasi, tadbir urus yang baik, hak asasi dan kesejagatan. Rujuk kajian Norhafiza (2012) untuk perbincangan lanjut.

> We didn't think it was important. It was a serious misjudgment. We thought that the newspapers, the print media, the television were important but young people were looking at text messages and blogs. (The influence of alternative media) was painful. But it came at the right time, not too late.

Menurut Nadia (2017), masyarakat secara umumnya lebih cenderung untuk menggunakan media sosial bagi membincangkan isu-isu terkini selain mengutarakan pendapat masing-masing tentang sesuatu isu yang berbangkit. Antara media sosial yang sering digunakan masyarakat kini ialah *Facebook*, *Twitter*, *Whatsapp*, *Instagram, Tik Tok* dan lain-lain. Hal ini, ditambah lagi dengan adanya penggunaan teknologi menerusi penggunaan telefon bimbit yang memudahkan masyarakat memperoleh dan berkongsi maklumat sesama mereka. Selain itu, golongan belia juga dilihat sangat aktif menggunakan media sosial sehingga menjadikannya sebagai satu bentuk keperluan dalam hidup mereka. Dahlgren (2007) dan De Vreese (2007) melihat faktor media internet sebagai penjana yang menggerakkan penglibatan belia dalam politik. Melihat kepada senario politik semasa, dunia siber adalah medium yang paling berpengaruh dalam kehidupan golongan muda. Ini kerana dunia siber memberikan lebih ruang kebebasan dan autonomi kepada mereka untuk berdiskusi, mengakses sumber informasi dan mengekspresi pendapat.

Penggunaan media siber ini juga turut memberi impak yang besar terhadap lanskap politik negara apabila buat pertama kali dalam sejarah Malaysia berlakunya pertukaran kerajaan dari kerajaan BN kepada kerajaan Pakatan Harapan (PH) pada PRU ke-14 tahun 2018 dan pada PRU ke-15 pada tahun 2022 disebabkan oleh penggunaan media sosial. Menurut Lee Kuok, Rizal Zamani dan Rafiq (2018), berlaku perubahan ketara dalam penggunaan saluran media baharu daripada emel, SMS, dan

blog kepada *YouTube, Facebook, Tik Tok* dan *Whatsapp.* Penggunaan saluran media baharu ini merupakan satu-satunya pilihan yang PH ada kerana media arus perdana dikawal oleh kerajaan BN. Hal ini memberi kelebihan kepada PH kerana PH telah lama mendominasi dan menggunakan media ini secara maksimum, khususnya dalam menarik sokongan anak muda. Media baharu ini dilihat lebih terbuka dan bebas meskipun ianya boleh mewujudkan polemik politik menerusi penyebaran maklumat palsu.

Ramai sarjana yang menyatakan bahawa parti atau pemimpin politik yang menguasai media akan mempunyai kelebihan untuk memenangi pilihan raya (McCombs & Shaw, 1972; Kahn & Kenney, 1999; Downey & Fenton, 2003). Oleh itu, parti-parti politik mula menumpukan kepada kempen siber atau menggunakan platform media sosial untuk berkomunikasi dan menyalurkan maklumat kepada masyarakat, khususnya pengundi. Aktivisme siber yang meluas ini akhirnya telah memunculkan amalan *political astroturfing* atau lebih dikenali sebagai *cybertroopers* di Malaysia. *Political Astroturfing* bermaksud aktiviti *top-down* di Internet yang dilaksanakan secara palsu dan penipuan oleh aktor politik dengan menggunakan khidmat individu lain (Kovic et al., 2018). Walker (2014) pula mendefinisikan *political astroturfing* sebagai kempen di mana para peserta kelihatan seperti sebahagian dari gerakan atau sentimen akar umbi yang tulen, sedangkan sebenarnya disusun secara terpusat dari atas ke bawah *top-down*. Dari definsi-definisi ini, terdapat lima elemen penting yang ditekankan dalam *political astroturfing*. Pertama, *political astroturfing* berlaku di Internet. Kedua, ia dimulakan oleh aktor politik. Ketiga, ianya palsu dengan menggunakan identiti atau memanipulasi pandangan orang lain. Keempat, ianya bersifat penipuan kerana tujuan *astroturfing* ini adalah untuk mengaburi sasaran, biasanya masyarakat (termasuk dalam kumpulan individu dan kumpulan kecil) untuk mempercayai bahawa aktiviti pembuatan itu nyata. Kelima, ianya adalah aktiviti yang

strategik kerana aktor politik yang terlibat dalam *political astroturfing* ini mengejar tujuan tertentu dalam melakukannya. Persoalannya, adakah istilah *political astroturfing* ini selari dengan istilah politik *cybertroopers*? Walaupun istilah *political astroturfing* tidak digunakan dengan meluas di Malaysia, namun ciri-ciri ini dapat dilihat dalam gerakan politik *cybertroopers* di negara ini, yang menjadi salah satu objektif kajian ini.

Cybertroopers merupakan istilah yang digunakan di Malaysia bagi menerangkan kegiatan yang dilakukan oleh seseorang yang diupah oleh kerajaan atau parti poitik untuk menyebarkan propaganda politik di internet, terutamanya media sosial (Farid, 2019, 2 November). Golongan *cybertroopers* diupah dan dibayar gaji oleh golongan politik atau pihak berkepentingan untuk membuat serangan sesuatu isu kepada pihak lawan yang bermotifkan untuk menjatuhkan kreadibiliti pihak lawan. Golongan ini juga bergerak secara individu dan secara berkumpulan seperti yang dilakukan sewaktu pilihan raya (Farid, 2019, 2 November). *Cybertroopers* merupakan pengulas yang dibayar oleh parti-parti politik sama ada pihak kerajaan atau pembangkang untuk menyerang lawan mereka dan golongan ini sangat aktif semasa berlangsungnya proses pengundian (Freedom House, 2014). Tiada istilah yang tepat untuk menggambarkan siapakah golongan *cybertroopers* kerana ramai sarjana memberikan tafsiran yang berbeza-beza mengikut konteks atau keadaan semasa. Golongan *cybertroopers* kebanyakannya diupah dan diberi bayaran oleh pihak yang mengupah untuk menyebarkan maklumat, dan adakalanya membuat serangan isu kepada pihak lawan bermotifkan untuk menjatuhkan kreadibiliti pihak lawan. Golongan ini juga ada yang bergerak secara individu, bebas dan secara berkumpulan seperti yang dilakukan pada waktu pilihan raya. Menurut laporan dari Freedom House (2014), *cybertroopers* merupakan pengulas politik yang dibayar oleh parti-parti politik sama ada di pihak kerajaan atau pembangkang untuk menyerang lawan mereka. Kumpulan

ini sangat aktif khususnya semasa berlangsungnya proses pengundian dan pilihan raya. Hujah ini disokong melalui kenyataan yang diberikan oleh jentera siber yang dikenali sebagai Bob (dalam Haspaizi & Yasmin, 2019, 24 Mac) di mana kumpulan jentera siber ini dibayar lumayan mencecah ribuan ringgit bagi mempromosi, menangkis serangan dan menyerang individu atau pihak tertentu di media sosial terutamanya apabila menjelang PRU. Kumpulan ini memainkan peranan sangat penting dan amat diperlukan oleh parti politik bagi menguasai siber, sekali gus membentuk persepsi rakyat.

Kebangkitan politik *cybertroopers* tidak hanya berlaku di Malaysia sahaja, tetapi ianya adalah suatu fenomena global, termasuklah negara-negara maju. Di negara-negara maju, amalan *cybertroopers* ini dikenali sebagai *political astroturfing, political bots,* atau *political sock puppets. Political bots* ialah, aplikasi atau perisian yang menjalankan tugas automotik dan menjalankan interaksi dengan pengguna melalui internet dan ia digunakan untuk mempengaruhi pendapat umum. Misalnya, aplikasi atau perisian digunakan untuk melaksanakan fungsi seperti menghantar suapan berita atau mesej secara automatik di laman sosial secara pukal serta seringkali melakukan *spam* kepada pengguna sosial mengenai sesuatu perkara yang berkaitan. Manakala, *political sock puppets* pula menggambarkan tentang penggunaan identiti dalam talian yang mengelirukan seperti penggunaan akaun palsu dalam media sosial (Hart & Klink, 2017). Kehadiran *sock puppets* di media sosial juga ada kalanya dilihat seperti menyokong, mempertahankan dan memperjuangkan sesebuah organisasi atau individu. Selain itu, mereka juga sering memanipulasi pendapat umum dan menyamar sebagai pihak ketiga serta sering kali tidak mengakui diri mereka sebagai pemilik asal akaun tersebut. Kehadiran *sock puppets* di media sosial mewujudkan kebimbangan bukan sahaja kepada parti politik malah orang awam. Misalnya, *Twitter* telah mengenal pasti seramai 1.4 juta pengguna yang

berpengkalan di Amerika telah berkomunikasi dengan akaun *sock puppet* iaitu akaun palsu yang digunakan untuk tujuan penipuan pada waktu pilihan raya Presiden 2016. Disebabkan oleh kempen yang meluas dari *political astroturfing* pada pilihan raya tersebut, Amerika terpaksa mewujudkan unit ketenteraan untuk mempertahankan diri daripada ancaman tersebut (Hart & Klink, 2017).

Selain itu, ancaman *political astroturfing* juga berlaku di negara lain seperti dalam pilihan raya Perancis 2017 (Ferrara, 2017).[2] Kejadian sama turut berlaku di Perancis di mana saluran *Twitter* antara 27 April hingga 7 Mei 2017 menunjukkan perbincangan hangat tentang pilihan raya. *Twitter* berjaya mengumpulkan data besar yang mengandungi hampir 17 juta *tweet* berkaitan dengan pilihan raya presiden Perancis 2017. Jumlah ini menunjukkan bahawa pengguna media berminat untuk membincangkan secara terbuka tentang pemimpin yang bertanding dan pilihan raya presiden di media sosial. Kebanyakan pengguna *Twitter* yang terlibat ialah warga asing yang tidak terlibat secara langsung dalam pengundian presiden di Perancis. Hal ini menyebabkan wujudnya kekeliruan dan persaingan hebat antara bakal presiden kesan dari kewujudan *political astroturfing.* Selain itu, kewujudan *political astroturfing* ini juga boleh menggugat kepercayaan rakyat terhadap berita atau informasi yang dimanipulasi.

Pilihan raya Brexit 2016 di United Kingdom (UK) juga menunjukkan penglibatan menonjol *political astroturfing*. Misalnya, hasil kajian Bastos dan Mercea (2017) mendapati bahawa pilihan raya Brexit yang berlangsung di UK lebih kurang sama

[2]Media sosial dieksploitasi secara sistematik untuk memanipulasi dan mengubah pendapat umum. Beberapa kempen disinformasi telah diselaraskan melalui bot,akaun media sosial yang dikawal oleh skrip komputer yang cuba menyamar sebagai pengguna manusia yang sah. Dalam kajian ini, satu operasi sedemikian berlaku menjelang pilihan raya presiden Perancis 2017. Rujuk kajian Ferrara (2017) untuk perbincangan lanjut.

dengan apa yang berlaku di Perancis. Kehadiran *sock puppet* di media sosial digunakan untuk menyuarakan pendapat dan memanipulasi pendapat umum dengan menggunakan akaun palsu. Sebanyak 13,493 akaun *Twitter* direkodkan telah menghantar *tweet* mengenai referendum keahlian Kesatuan Eropah sepanjang proses pilihan raya ini berjalan. Sejurus selesai pilihan raya ini, semua akuan tersebut tidak aktif dan hanya dibuka untuk tujuan sementara sahaja. Hal ini jelas menunjukkan bahawa pilihan raya di Eropah turut mengalami gangguan daripada golongan *sock puppet* yang cuba untuk memanipulasi sesuatu berita atau memberi sokongan atau menyatakan ketidakpuasan hati mereka kepada kepimpinan politik.

Manakala, di China juga turut mengalami situasi yang sama apabila media sosial digunakan sangat meluas oleh penduduknya yang ramai. China mempunyai hampir 1300 syarikat media sosial dan tapak web serta berjuta-juta ciapan yang ditulis setiap hari oleh pengguna media di negara tersebut (King et al., 2017). Walau bagaimanapun, kerajaan China mengenakan kawalan yang meluas ke atas semua sistem yang digunakan. Hasil kajian King et al. (2017) menunjukkan bahawa *cybertroopers* di China menggunakan media sosial untuk mengelak daripada perdebatan hangat tentang isu sensitif atau kontroversi oleh parti politik dan kerajaan. Malah, mereka juga ditubuhkan bermatlamat untuk mengalih perhatian orang ramai daripada membincangkan topik perbualan yang sensitif dalam media sosial. Merujuk kepada kajian-kajian kes di atas, walaupun pelbagai istilah yang digunakan untuk merujuk kepada kegiatan dalam talian yang digerakkan bagi tujuan politik, khususnya untuk mempengaruhi perbincangan atau pendapat politik, namun setiap istilah ini mempunyai konsep dan bentuk yang berbeza bergantung kepada fungsi masing-masing.

1.1 Latar Belakang Kajian

Di Malaysia, sejarah awal kemunculan gerakan *cybertroopers* tidak dapat diketahui dengan jelas, namun ianya dilihat berkembang sekitar pada PRU tahun 2008. Semasa PRU-12 yang lalu, parti Barisan Nasional (BN) buat pertama kali mengalami pencapaian merosot sepanjang sejarah PRU di negara ini. BN hanya memenangi 140 kerusi parlimen daripada 222 kerusi yang ditandinginya. Manakala, di peringkat DUN, BN hanya memenangi 307 kerusi daripada 505 kerusi yang ditandinginya (Norhafiza, 2012). Parti-parti lawan seperti Pakatan Rakyat (PR) yang terdiri daripada Parti Keadilan Rakyat (PKR), PAS dan Parti Tindakan Rakyat (PKR) menunjukkan pencapaian lebih baik pada pilihan raya ini. Kemersotoan pencapaian BN pada pilihan raya ini dipengaruhi oleh pelbagai faktor dalaman dan luaran. Antara faktor-faktornya ialah BN meletakkan wajah-wajah baharu dalam kepimpinan. Malah beberapa calon yang dilantik terlibat dalam pelbagai kes mahkamah seperti rasuah, jenayah, penyalahgunaan kuasa dan pemilikan harta yang berlebihan.

Antara faktor luaran yang mempengaruhi penolakan Masyarakat terhadap BN pada ketika itu ialah kegagalan manifesto BN dan peranan media massa semasa kempen pilihan raya sedang berjalan. BN, dalam kempennya pada waktu itu, gagal untuk menghormati hak asasi dan kebebasan politik rakyat. Ini kerana kerajaan masih lagi memonopoli dan mengawal ketat media arus perdana sehinggakan berita yang dilaporkan oleh media arus perdana haruslah sealiran dengan aspirasi kerajaan. Keadaan berat sebelah ini menunjukkan kerajaan tidak memberi keadilan sepenuhnya kepada parti-parti lain untuk mendekati rakyat menerusi media arus perdana. Hal ini menyebabkan orang awam kehilangan kepercayaan terhadap BN, sekali gus menolak mereka pada pilihan raya ini. Pada pilihan raya ini, media sosial menjadi platform alternatif termasuk media sosial yang digunakan oleh pembangkang dalam usaha

memobilisasi sokongan masyarakat dan menentang kerajaan. Penggunaan media sosial pada PRU 2008 ini dilihat berhasil kepada pembangkang apabila berjaya menafikan kemenangan dua pertiga majoriti BN dalam Parlimen yang telah dikuasai selama lebih 53 tahun, dan memonopoli lima buah negeri termasuk Kelantan. Berbanding era reformasi 1998, penggunaan media alternatif pada PRU12 ini adalah lebih tinggi, meluas dan komprehensif. Ini kerana isu-isu utama yang didedahkan oleh media alternatif seperti skandal rasuah, penyalahgunaan kuasa, salah laku pemimpin lebih mendapat perhatian masyarakat, khususnya belia, sekali gus membentuk pandangan mereka sebelum mengundi dalam pilihan raya. Kebanyakan provokasi-provokasi politik ini digerakkan oleh para *cybertroopers* dari parti-parti politik.

Gerakan *cybertroopers* ini semakin berkembang pada PRU 2013, digunakan dengan meluas pada PRU 2018, dan semakin aktif pada PRU 2022. Kejatuhan Barisan Nasional (BN) pada PRU ke-14, salah satunya adalah berpunca daripada 'perang siber' yang digerakkan oleh *cybertroopers* di media sosial. Perang siber adalah penggunaan teknologi komputer dan internet untuk melakukan perang di dunia maya. Pelaku perang siber saling bersaing untuk menguasai dan memanfaatkan sumber daya teknologi dan informasi yang ada di dalamnya untuk menyerang, menghancurkan, menyesatkan, mempengaruhi, mengalihkan, mengganggu, atau menghentikan komunikasi, arus informasi dan isinya serta pelbagai tindakan lain yang mengakibatkan kerugian dan melemahkan lawan (Salomon, 2021). Menurut Zahid Hamidi (dalam Haspaizi & Yasmin, 2019, 24 Mac), 93.4% *cybertroopers* di negara ini adalah pro-PH yang menjadi pembangkang pada waktu itu, manakala selebihnya adalah penyokong kerajaan BN.

Gerakan politik *cybertroopers* ini memberi impak yang besar bukan hanya kepada keputusan pilihan raya, malah terhadap pola pengundian Masyarakat.

Misalnya, pada ketiga-tiga PRU13, PRU14 dan PRU15 ini menyaksikan perubahan pola undi popular yang menunjukkan graf populariti setiap gabungan parti politik turun naik secara signifikan. Ini kerana terdapat kumpulan yang lebih tertumpu untuk membuat perbandingan secara alam maya tetapi tidak turun untuk terlibat secara langsung dalam pengundian. Impak dari keadaan tersebut, ia dikaitkan dengan faktor penolakan parti atau calon tertentu selain didorong oleh sentimen yang dimainkan sepanjang tempoh berkempen. Banyak parti politik atau pemimpin politik secara individu menggunakan khidmat *cybertroopers* dalam memastikan matlamat politik mereka tercapai, terutamanya sewaktu menjelangnya pilihan raya umum. Pemimpin politik sanggup mengeluarkan kos kewangan yang banyak untuk mengupah *cybertroopers* sama ada bergerak secara solo atau berkumpulan. Terdapat *cybertroopers* ini yang bergerak bebas tanpa terikat atau diupah oleh organisasi atau pemimpin politik, namun jumlah mereka adalah sangat sedikit atau minoriti. Kebanyakan *cybertroopers* di Malaysia ini adalah mereka yang diupah atau dibayar oleh organisasi politik atau pemimpin sendiri. Malah, ada dalam kalangan *cybertroopers* yang menjadikan kegiatan ini sebagai satu kerjaya untuk mencari rezeki kerana gaji yang ditawarkan adalah sangat lumayan sehingga boleh mencecah puluhan ribu. Antara tugas yang perlu dilakukan oleh *cybertroopers* ini adalah mempromosi, menangkis serangan dan menyerang pihak atau individu tertentu di media sosial (Haspaizi & Yasmin, 2019, 24 Mac). Menurut Tariq Banday dan Mattoo (2013), terdapat empat kategori media sosial yang menjadi medium tumpuan kebanyakan *cybertroopers* iaitu rangkaian media sosial seperti *Facebook, Twitter, Instagram* dan *Linkedln.* Gerakan *cybertroopers* ini menggunakan saluran-saluran ini kerana ianya mempunyai jumlah pengguna yang paling tinggi, capaian yang mudah dan efektif untuk berkongsi informasi. Walaupun platform yang digunakan oleh gerakan *cybertroopers* ini adalah platform umum yang digunakan oleh kebanyakan masyarakat, namun gerakan atau individu yang diupah sebagai *cybertroopers* ini sukar

di kenal pasti. Identiti mereka tidak boleh dikenal pasti dan kabur kerana mereka selalunya menggunakan foto dan akaun palsu. Penggunaan identiti dan akaun palsu menyukarkan pihak berkuasa untuk mengesan aktor utama yang menggerakkan kegiatan *cybertroopers* ini, sekali gus tiada tindakan yang boleh dilakukan bagi menghalang *modus operandi* gerakan politik *cybertroopers* ini.

Gerakan *cybertroopers* ini mempunyai kebaikan dan keburukannya dalam konteks politik di Malaysia. Dari satu sisi, gerakan *cybertroopers* ini merancakkan ruangan siber dengan pelbagai informasi politik secara terus kepada masyarakat. Keadaan ini dilihat sangat baik di mana ia dapat meningkatkan pengetahuan politik masyarakat di samping dapat mengurangkan kos apabila kempen-kempen secara bersemuka dapat dilakukan secara virtual atau dalam talian. Namun, dari sisi lain, kewujudan gerakan ini memberi ancaman kepada keselamatan negara dan mampu menganggu gugat keharmonian masyarakat terutamanya apabila melibatkan isu berkaitan perkauman dan agama. Menurut Teo (dalam Mohd Azlim, 2019, November 11), keharmonian kaum di negara ini sering diganggu gugat oleh beberapa faktor, antaranya ialah sikap ahli politik yang sering memainkan sentimen perkauman dan agama dalam media sosial. Penyalahgunaan media sosial oleh *cybertroopers* ini akan memberi impak yang serius ke atas keharmonian masyarakat yang pelbagai. Oleh itu, bagi menjamin keselamatan negara dan kestabilan masyarakat, kerajaan telah mengambil langkah drastik dengan mengenakan pengawasan dan penapisan siber ke atas akaun dan kandungan media sosial individu yang boleh menggugat sensitiviti politik, kaum dan agama di Malaysia di bawah akta-akta seperti Akta Hasutan (1948)[3],

[3]Akta Hasutan 1948, merupakan suatu akta undang-undang di Malaysia yang digubal untuk menghalang perbincangan yang dikatakan sebagai menghasut. Akta ini sebenarnya digubal oleh penjajah British pada tahun 1948. Akta ini menjadikan ucapan yang mempunyai kecenderungan menghasut sebagai suatu kesalahan jenayah. Akta Hasutan bertujuan untuk menghalang sebarang bentuk hasutan, fitnah dan penghinaan terhadap raja dan kerajaan sehingga boleh menganggu gugat keselamatan negara.

Akta Rahsia Rasmi (1972)[4] dan Akta Komunikasi dan Multimedia (1988)[5]. Namun, penguatkuasaan undang-undang drakonian ini dilihat seperti melanggar hak dan kebebasan berpolitik masyarakat sehingga para sarjana seperti Zakaria Ahmad (1989), Crouch (1996) dan Case (2002) melabelkan Malaysia sebagai negara quasi-demokrasi, semi-demokrasi atau demokrasi autoritarian. Sehubungan dengan kenyataan di atas, tesis ini menyelidiki definisi dan tipologi *cybertroopers* dalam konteks Malaysia serta ancaman kepada keselamatan negara yang mungkin wujud disebabkan oleh gerakan *cybertroopers* ini, sekali gus mengkaji mekanisme terbaik bagi mengawal gerakan ini. Kajian ini menghujahkan bahawa ketiadaan definisi dan tipologi yang sesuai bagi menggambarkan *cybertroopers* di Malaysia ini menyebabkan penguatkuasaan akta, penapisan siber dan pengawasan ke atas akaun-akaun media sosial tidak dapat dilaksanakan dengan baik bagi mengekang gerakan *cybertroopers* ini. Oleh itu, dapatan kajian ini dilihat sangat signifikan untuk dijadikan panduan bagi badan kerajaan dan bukan kerajaan untuk mengawal gerakan ini bagi mengekalkan keharmonian dan menjaga keselamatan negara.

[4]Akta Rahsia Rasmi 1972, digubal pada tahun 1972 sebagai suatu akta yang menyekat penyebaran maklumat berkenaan dengan kedaulatan negara dan keselamatan bagi memelihara rahsia kerajaan dari bocor kepada negara lain.

[5]Akta Komunikasi dan Multimedia 1998 mengandungi sejumlah 282 seksyen ini turut memperuntukkan dua seksyen yang berkaitan dengan keselamatan siber iaitu seksyen 211 dan seksyen 233. Berdasarkan seksyen 211(1) seseorang individu atau pemberi perkhidmatan aplikasi kandungan tidak boleh memberikan kandungan yang berunsurkan sumbang, lucah, palsu, mengancam atau bersifat jelik untuk tujuan dan niat menganggu, mengacau, mendera atau mengugut mana-mana orang.

1.2 Permasalahan Kajian

Jika dilihat fenomena di Malaysia pada era globalisasi kini, semua informasi diletakkan dihujung jari hingga menyebabkan kebergantungan manusia kepada internet meningkat. Hal ini jelas terbukti apabila kadar penggunaan internet meningkat dari 0.1% pada tahun 1995 sehingga mencecah 87.4% pada tahun 2018. (Suruhanjaya Komunikasi dan Multimedia Malaysia, 2020). Berdasarkan statistik dari Laporan Data Reportal (2023), peratusan penggunaan media sosial di Malaysia tanpa mengira umur dan jantina adalah seramai 30.2 juta pengguna bersamaan dengan 91.7 peratus jumlah populasi sebenar. Antara platform yang banyak digunakan oleh masyarakat Malaysia ialah aplikasi *YouTube* sebanyak 93.2 peratus diikuti dengan *Facebook* sebanyak 84.8 peratus, *Instagram* sebanyak 74.3 peratus dan *Tik tok* sebanyak 59.9 peratus pengguna. Manakala, bagi masa yang dihabiskan oleh masyarakat Malaysia untuk melayari media sosial ialah sekitar 8 jam sehari. Penggunaan media sosial yang tinggi di Malaysia menunjukkan bahawa negara ini mempunyai ekosistem dan fasiliti internet yang baik, sekali gus memberikan peluang kepada masyarakat untuk mengakses maklumat dengan cepat. Namun, dalam masa yang sama, masyarakat juga terdedah kepada ancaman siber termasuk jenayah dan pemalsuan maklumat oleh gerakan *cybertroopers.*

Penggunaan meluas media siber ini menyumbang kepada perkembangan dan perubahan dalam gerakan *cybertroopers* di Malaysia. Meskipun kajian berkaitan *cybertroopers* ini semakin berkembang, namun kajian-kajian ini hanya menumpukan kepada peranan dan medium yang digunakan oleh politik *cybertroopers* dalam menggerakkan aktiviti mereka (Tan, 2022; Hopkins, 2014; Tapsell, 2013; Mastura, Siti Zobidah & Krauss, 2020). Terdapat sarjana yang menyelidiki pendefinisian *cybertroopers* di Malaysia, namun ianya masih lagi terhad. Misalnya, kajian Hopkins

(2014) mendefinisikan *cybertroopers* sebagai blogger, *tweeters* atau pengguna yang memberi komen dan maklum balas kepada ciapan dalam talian. Tapsell (2013) pula mendefinisikan politik *cybertroopers* sebagai jentera yang diupah oleh orang-orang secara persendirian sama ada blok kerajaan atau pembangkang untuk memfitnah ahli-ahli politik dan ini adalah bentuk kempen dalam rangkaian media sosial. Namun, pendefinisian yang diberikan oleh sarjana-sarjana ini masih kabur dan tidak bersandar kepada data empirikal yang jelas sehingga menyebabkan istilah *cybertroopers* ini sering disalah erti dan dikaitkan dengan *netizen*, *keyboard warrior*, *makcik bawang* dan sebagainya. Berbeza dengan kajian di negara-negara luar, pendefinisian istilah dan bentuk-bentuk *political astroturfing* telah banyak dan meluas dilakukan oleh sarjana. Pendefinisian yang jelas tentang *political astroturfing* ini memberi kelebihan kepada sarjana dan kerajaan untuk melaksanakan langkah kawalan bagi mengurangkan risiko dan impak gerakan ini terhadap kestabilan politik negara mereka. Merujuk kepada definisi *political astroturfing* di atas, maka bagaimana pula definisi istilah *cybertroopers* yang paling sesuai untuk diaplikasikan dalam konteks Malaysia? Dan apakah kerangka yang paling sesuai untuk mengukur ciri-ciri atau bentuk *politik cybertroopers* di Malaysia? Tesis ini berhujah definisi dan tipologi politik *cybertroopers* adalah sesuai mengikut definisi *political astroturfing* yang dikemukakan oleh Kovic et al. (2018) iaitu *political astrotufing* sebagai aktiviti *top-down* di internet yang dilaksanakan secara palsu dan penipuan oleh aktor politik dengan menggunakan khidmat individu lain.

Selain pendefinisian istilah, kajian ini juga bertujuan untuk menyelidiki ancaman gerakan politik *cybertroopers* ini kepada keselamatan negara. Kewujudan politik *cybertroopers* ini memberi impak positif dan negatif ke atas politik nasional dan masyarakat. Dari satu sisi, politik *cybertroopers* ini dilihat signifikan kerana gerakan ini memainkan peranan sebagai agen penyebaran maklumat yang berupaya

meningkatkan kesedaran dan pengetahuan politik masyarakat. Gerakan *cybertroopers* ini dilihat semakin penting dalam kempen pilihan raya bagi membantu parti menyebarkan maklumat dalam rangkaian media sosial (Junaidi et al., 2014). Dari sis yang lain, terdapat sarjana yang melihat penubuhan *cybertroopers* ini dari sisi negatif di mana ianya berupaya mengancam keselamatan negara menerusi penyebaran maklumat palsu yang mampu mengganggu gugat sensitiviti masyarakat, khususnya sewaktu pilihan raya (Mohd Azlim, 2019, November 11). Misalnya, terdapat beberapa isu yang berkait dengan *cybertroopers* di Malaysia yang berupaya memberi ancaman kepada kestabilan politik.

Antaranya ialah isu mantan isteri Perdana Menteri, Rosmah Mansor yang dikatakan telah menubuhkan sebuah pasukan *cybertroopers* pada tahun 2012. Pasukan *cybertroopers* ini telah dibayar dengan bayaran yang lumayan dan bertanggungjawab memantau kandungan media sosial termasuklah kritikan negatif yang dilemparkan kepada beliau seperti isu beg tangan mahal, isu penggunaan jet kerajaan dan isu kepentingan kewangan dalam projek kerajaan (Astro Awani, 2020, 9 September). Penubuhan pasukan *cybertroopers* ini walaupun tidak memberi ancaman besar terhadap keselamatan negara, namun ianya mampu mewaujudkan politik kebencian dalam kalangan masyarakat. Selain itu, seorang bekas *cybertroopers* yang juga merupakan bekas Ketua Penerangan Wanita PKR, Syarul Ema Rena Abu Samah telah didakwa atas tuduhan dengan sengaja menggunakan aplikasi rangkaian media sosial, melalui profil *Facebook* ‘Ratu Naga’ untuk membuat dan memulakan penyebaran komen negatif terhadap Najib berhubung Trans-Perjanjian Perkongsian Pasifik (TPPA). Selain itu, Syarul Ema juga pernah membuat pengakuan bahawa beliau pernah menghasilkan sebuah video yang membangkitkan isu perkauman hingga mencetuskan kemarahan orang Melayu terhadap DAP. Hal ini telah

membangkitkan sentimen perkauman dalam kalangan pengguna internet terutamanya masyarakat umum yang mempercayai berita palsu di media sosial.

Isu yang dimainkan oleh politik *cybertroopers* ini tidak hanya menjejaskan masyarakat, namun pemimpin politik dan pegawai kerajaan juga turut terkesan dengan serangan *cybertroopers* ini. Misalnya, peguam negara, Mohamed Apandi Ali mengakui bahawa beliau sangat tertekan dengan serangan *cybertroopers* yang dibayar oleh bekas Perdana Menteri, Dato' Sri Najib bin Tun Razak berhubung dengan skandal 1Malaysia Development Berhad (1MDB) (Malaysiakini, 2020, 7 Julai). Selain itu, pertukaran kerajaan dari BN ke PH buat pertama kalinya dalam sejarah Malaysia berlaku disebabkan oleh serangan besar-besaran *cybertroopers* dalam menjatuhkan pimpinan Najib Tun Razak melalui 'perang siber' (Lee Kuok, Rizal Zamani & Rafiq, 2018). Antara kritikan negatif utama yang digunakan oleh *cybertroopers* ke atas Najib ialah isu rasuah, penyalahgunaan kuasa khususnya isu IMDB.

Selain PRU, politik *cybertroopers* juga bergerak aktif pada pilihan raya negeri. Misalnya, pilihan raya negeri Sabah pada tahun 2020, parti Warisan didakwa telah mengupah seramai lima orang *cybertroopers* yang dibawa khas dari Semenanjung bertujuan untuk menyebarkan propaganda berkaitan Warisan bagi meraih sokongan rakyat Sabah (Sabah Gazette, 2020, 25 September). Dalam pilihan raya ini juga, kebanyakan ahli politik Sabah saling tuduh menuduh antara satu sama lain menggunakan *cybertroopers* dalam kempen memburukkan pihak lawan (Loh & Zhang, 2020). Isu politik yang giat diperdebatkan di ruang digital ini meskipun ada kalanya bersifat *non-partisan* atau tidak memihak kepada mana-mana blok politik, namun jika tidak terkawal akan mengancam kestabilan politik. Contoh kes-kes di atas jelas menunjukkan bahawa gerakan *cybertroopers* politik ini berupaya memberi ancaman

kepada keselamatan negara. Oleh itu, kajian ini akan mengenal pasti ancaman dalaman dan luaran kepada keselamatan negara yang berupaya dilakukan oleh gerakan *cybertroopers*.

Jika gerakan politik *cybertroopers* di Malaysia berupaya memberi ancaman terhadap kestabilan politik dan keselamatan negara, maka muncul persoalan terakhir dalam tesis ini iaitu apakah mekanisme terbaik bagi mengawal kegiatan *cybertroopers* di Malaysia? Adakah kerajaan telah melaksanakan inisiatif bagi mengekang gerakan politik *cybertroopers*? Jika ya, apakah tindakan yang telah dilakukan kerajaan? Jika dilihat, kerajaan telah mengambil pelbagai tindakan bagi tujuan menjaga keselamatan negara dan ketenteraman awam seperti menguatkuasakan Akta Anti-Berita Tidak Benar 2018 (Anti-Fake News At 2018), Akta Komunikasi dan Multimedia (CMA) 1998, iaitu seksyen 233 (1) dan Akta Hasutan 1948, Akta Rahsia Rasmi 1972, Akta Kesalahan Keselamatan (Langkah-langkah Khas) 2012 atau SOSMA. Misalnya, dalam alam siber, kawalan yang dilakukan ialah dengan menguatkuasakan Akta Anti-Berita Tidak Benar 2018. Akta ini telah dibentangkan pada 27 Mac 2018 dan diwartakan pada 11 April 2018. Secara umumnya, dalam seksyen 4 (1), akta ini melarang mana-mana individu membuat, menawarkan, menerbitkan, mencetak atau menyebarkan berita palsu. Namun, seseorang hanya akan didakwa sekiranya perbuatan ini dilakukan dengan niat. Sekiranya seseorang tidak mengetahui atau tidak menyedari maklumat dikongsi dalam talian adalah palsu, maka dia tidak melakukan kesalahan di bawah seksyen 4 ini. Selain itu, akta Komunikasi dan Multimedia (CMA) 1998, iaitu seksyen 233 (1) pula mengenai seseorang yang menggunakan internet atau telefon untuk menyebar berita palsu boleh dikenakan tindakan undang-undang. Jika didapati bersalah mereka boleh dedenda RM 50,000 atau dipenjarakan selama tempoh tidak melebihi satu tahun atau kedua-duanya sekali. Akta Hasutan 1948 pula berkaitan dengan undang-undang yang melarang wacana yang disifatkan sebagai

hasutan. Akta ini digubal oleh pihak berkuasa British Malaya pada tahun 1948 untuk membendung pemberontakan komunis tempatan. Perbuatan seperti ucapan dengan kecenderungan menghasut, termasuk hasutan yang membawa kebencian, penghinaan atau menimbulkan rasa tidak puas hati terhadap kerajaan atau menimbulkan perasaan niat jahat dan permusuhan antara kaum akan dikenakan tindakan di bawah akta ini. Akta ini dipinda pada tahun 2015 dengan memasukkan larangan media dalam talian. Pindaan ini dibuat untuk mengelakkan individu menggunakan internet bagi perbuatan menghasut dan menyebabkan perpecahan kaum.

Namun begitu, mekanisme kawalan yang diambil oleh kerajaan dilihat kurang berkesan dalam membendung ancaman politik *cybertroopers* yang dilihat semakin aktif. Buktinya, jumlah *cybertroopers* di negara ini semakin meningkat dari masa ke semasa. Menurut Leong (2015), jumlah *cybertroopers* terlatih yang diupah oleh BN sahaja adalah seramai 2000 orang pada tahun 2015, dan akan meningkat pada masa akan datang. Pertambahan jumlah politik *cybertroopers* ini menunjukkan gerakan ini semakin bergiat aktif terutamanya sewaktu pilihan raya. Loh dan Sarah (2023) menghujahkan bahawa politik *cybertroopers* diwujudkan bukan untuk mengubah pandangan politik tetapi untuk memperkukuhkan pandangan dan mereka akan menimbulkan keraguan terhadap pandangan politik yang betul sehingga menutup debat atau merosakkannya. Contohnya, dalam pertarungan siber antara *cybertroopers* PH, BN dan Perikatan Nasional (PN), setiap pihak berkeras menyatakan pihak mereka tidak bersalah dan tuduhan yang dibuat adalah tidak benar. Kesannya, kewujudan *cybertroopers* yang aktif berkembang ini menjadikan pemilih Malaysia semakin terpolarisasi dan terpecah mengikut pandangan politik masing-masing. Malah, terdapat juga pemilih yang menjadi apati kerana dipengaruhi oleh propaganda yang dimainkan oleh politik *cybertroopers* ini.

Persoalannya, mengapakah kawalan menerusi tindakan undang-undang ini tidak berkesan untuk menyekat gerakan politik *cybertroopers* ini? Walaupun kawalan undang-undang yang dikuatkuasakan oleh kerajaan adalah baik, namun kesukaran kerajaan untuk mengenal pasti identiti sebenar *cybertroopers* menyebabkan kegiatan mereka sukar untuk dikawal. Ini kerana *cybertroopers* kini menggunakan foto palsu pada profil mereka dan menyebarkan propaganda dengan kandungan politik yang lebih asli melalui akaun yang lebih meyakinkan (Harris, 2020). Oleh itu, kebanyakkan identiti *cybertroopers* ini sukar untuk dikenal pasti kerana mereka menggunakan profil palsu dan akaun yang sukar untuk dibuktikan ketidaksahihannya. Kesannya, kemampuan untuk mengetahui identiti disebalik akaun adalah sangat terhad bagi kerajaan, apatah lagi masyarakat umum. Jika mekanisme kawalan sedia ada tidak berjaya untuk menyekat dan mengawal gerakan politik *cybertroopers* ini, adakah terdapat mekanisme lain yang lebih efektif? Oleh itu, tesis ini akan menganalisis solusi atau mekanisme terbaik yang boleh dilakukan bagi mengawal gerakan politik *cybertroopers* di Malaysia.

Oleh itu, kajian ini bertujuan untuk mengisi kelompangan yang sedia ada dalam kajian sebelum ini dengan menumpukan perhatian kepada perkembangan politik *cybertroopers* di Malaysia dari konteks pendefinisian istilah dan tipologi politik *cybertroopers,* ancaman gerakan ini ke atas keselamatan negara serta menyelidiki mekanisme yang paling efektif bagi mengawal gerakan politik *cybertroopers* di Malaysia. Sesuai dengan fokusnya, maka andaian yang dibangun dalam tesis ini adalah politik *cybertroopers* di Malaysia yang berupaya memberi ancaman kepada ketenteraman awam ini boleh dikawal menerusi tindakan pengawasan dan penapisan siber oleh kerajaan.

1.3 Persoalan Kajian

Secara lebih khusus, seperti dihuraikan sebelumnya, terdapat tiga persoalan penelitian yang diselidiki dalam tesis ini, iaitu:

i. Apakah definisi dan tipologi politik *cybertroopers* dalam konteks Malaysia?

ii. Adakah politik *cybertroopers* memberi ancaman terhadap keselamatan siber dan keselamatan negara?

iii. Apakah mekanisme kawalan terbaik yang berupaya mengawal gerakan *cybertroopers* di Malaysia?

Kesemua persoalan di atas berpaksi pada sebuah andaian bahawa kerajaan berupaya mengawal gerakan *cybertroopers* di Malaysia sekiranya istilah dan tipologi *cybertroopers* didefinisikan dan dijelaskan dengan baik dan mekanisme yang digunakan juga adalah tepat. Maka, tujuan kajian ini adalah seperti berikut:

1.4 Objektif Kajian

1. Mengenalpasti definisi dan tipologi *cybertroopers* dalam konteks Malaysia
2. Menganalisis ancaman *cybertroopers* terhadap keselamatan negara.
3. Menilai mekanisme kawalan yang terbaik untuk menyekat gerakan *cybertroopers* di Malaysia.

1.5 Kepentingan Kajian

Tesis ini menyelidiki tentang perkembangan politik *cybertroopers* di Malaysia dengan menganalisis definisi dan tipologi *cybertroopers*, ancaman kepada keselamatan negara dan mekanisme terbaik untuk mengawal gerakan ini. Terdapat beberapa kepentingan dan sumbangan kajian ini khususnya kepada teori yang dikaji, metodologi serta sumbangan kepada masyarakat dan organisasi. Secara khususnya, kajian ini memberi implikasi besar dalam mencadangkan penyelesaian bagi sesuatu fenomena sosial yang dikaji.

Kepentingan pertama, penambahbaikan terhadap kajian-kajian lepas yang kurang menyentuh secara terperinci mengenai *cybertroopers*, kajian mereka tidak menganalisis aspek-aspek lain dengan lebih terperinci seperti apakah definisi sebenar politik *cybertroopers*. Siapakah *cybertroopers*? Apakah bentuk-bentuk *cybertroopers*, apakah perubahan yang berlaku dalam gerakan *cybertroopers* dan kesan gerakan ini terhadap keselamatan siber? Dan sejauhmana gerakan ini boleh dikawal oleh kerajaan? Oleh itu, kajian ini akan memberi pengetahuan baharu yang disokog oleh data empirikal mengenai beberapa perkara yang belum sempat dikupas oleh sarjana-sarjana lepas.

Kedua, memberi pendedahan kepada masyarakat mengenai kewujudan politik *cybertroopers* di Malaysia supaya masyarakat awam lebih jelas dengan peranan dan impak gerakan *cybertroopers* ini. Selain itu, memastikan masyarakat mendapat bukti yang tepat dan sahih melalui data empirikal kajian ini kerana kajian ini dilakukan secara *neutral* dan bersifat *non partisan*. Akhir sekali ialah kajian ini juga diharapkan dapat menjelaskan perkaitan isu-isu yang dikaji agar dimanfaatkan oleh semua pihak

termasuk penyelidik bagi kepentingan perkembangan penyelidikan dan akademik negara yang merupakan salah satu aset penting selain membantu pihak kerajaan dalam menangani isu siber di dalam negara.

Ketiga, menjadi sumber rujukan kepada badan kerajaan dan bukan kerajaan. Dengan kajian yang dijalankan ini akan membantu pihak kerajaan untuk mengenal pasti ciri-ciri golongan politik *cybertroopers* dalam kalangan belia di samping dapat melakukan penapisan dan pengawasan siber secara lebih mendalam. Badan bukan kerajaan dapat membantu pihak badan kerajaan dalam melakukan penapisan dan pengawasan melalui aplikasi ataupun sistem yang diperkenalkan bagi membendung gejala ini dari berleluasa.

Keempat, kajian ini menyumbang dalam mengaplikasikan gabungan teori yang berbeza iaitu teori Struktur Peluang Politik dan teori Penentuan Agenda dalam membincangkan mengenai politik *cybertroopers* di Malaysia. Gabungan antara dua teori ini membentuk satu teori yang baru dalam kajian yang dijalankan oleh penyelidik. Secara tidak langsung kajian ini dapat menyokong teori yang dikemukakan oleh penyelidik dan sarjana sebelumnya serta menjadi rujukan kepada penyelidik akan datang.

Akhir sekali, sarjana lepas hanya menggunakan satu kaedah kajian dalam menjalankan penyelidikan sama ada menggunakan kaedah kualitatif atau kaedah kuantitatif. Oleh yang demikian, kajian ini menggunakan pendekatan *mixed-method* untuk melihat keselarasan hasil dapatan di antara dua instrumen yang digunapakai

iaitu soal selidik dan temu bual. Justeru, penggunaan pendekatan *mixed-method* akan memberi dimensi baharu yang lebih jelas berkaitan politik *cybertroopers* di Malaysia.

1.6 Skop Kajian

Skop kajian ini terarah kepada bidang keselamatan siber. Ini kerana keselamatan siber merupakan isu yang hangat diperkatakan melibatkan keselamatan negara dan merupakan satu bentuk ancaman moden alaf baru. Keselamatan siber perlu di teliti lebih mendalam terutamanya berkaitan dengan ancaman keselamatan siber dan pendidikan keselamatan siber kepada masyarakat. Tanggungjawab memberi pendidikan keselamatan siber ini tidak hanya disandarkan kepada kerajaan sahaja. Sebaliknya semua pihak, terutamanya badan bukan kerajaan dan penyelidik perlu berganding bahu untuk mengatasi masalah siber dalam negara agar kegiatan jenayah siber terutama dalam kalangan belia dapat diatasi.

Walaupun kajian ini menyelidiki perkembangan politik *cybertroopers* di Malaysia secara komprehensif, namun, kawasan kajian ini hanya memfokuskan kepada dua negeri yang mempunyai populasi golongan belia yang tinggi di Malaysia iaitu Selangor dan Perak. Pemilihan kedua-dua lokasi kajian ini adalah berdasarkan populasi bilangan belia yang paling banyak di Semenanjung Malaysia serta melihat pandangan belia dari konteks yang berbeza iaitu belia bandar dan belia luar bandar. Kajian ini dijalankan ke atas golongan belia yang berumur 15 hingga 30 tahun sama ada bekerja atau tidak bekerja, terlibat dalam apa-apa sektor, baik kakitangan kerajaan atau swasta atau persendirian tanpa mengira bangsa. Kajian ini turut mengambil kira ciri-ciri demografi seperti jantina, etnik dan beberapa faktor lain seperti pendapatan individu dan tahap pendidikan mereka. Selain itu, kajian ini juga turut melaksanakan

instrumen temu bual dengan 10 informan yang terdiri daripada aktivis yang terlibat secara langsung dalam kegiatan *cybertrooper* di Malaysia, ahli akademik dan pembuat dasar dalam bidang ini yang dipilih secara bertujuan.

Negeri pertama yang dipilih sebagai lokasi kajian ialah negeri Perak Darul Ridzuan. Negeri Perak merupakan negeri yang kedua terbesar di Semenanjung Malaysia selepas Pahang, dan keempat terbesar di Malaysia. Perak bersempadanan dengan negeri-negeri seperti Kedah, Pulau Pinang di sebelah Barat, Kelantan di sebelah Timur Laut, Pahang di Timur, dan Tenggara, Selangor di Selatan dan Selat Melaka di Barat. Negeri kedua iaitu negeri Selangor Darul Ehsan terletak di tengah-tengah Semenanjung Malaysia di Pantai Barat dan mengelilingi Wilayah Persekutuan Kuala Lumpur dan Putrajaya. Negeri ini juga bersempadan dengan negeri Perak di Utara, Pahang di Timur, Negeri Sembilan di Selatan dan Selat Melaka di sebelah Barat. Selangor juga merupakan negeri yang paling kaya di Malaysia berdasarkan Keluaran Dalam Negeri Kasar (KDNK) per kapita. Negeri ini juga merupakan negeri yang paling maju di Malaysia. Hal ini kerana dengan adanya infrastruktur yang terbaik seperti lebuh raya dan pengangkutan awam yang menghubungkan bandar-bandar di Selangor dengan ibu negeri Malaysia, Kuala Lumpur, pusat pemerintahan kerajaan pusat, Wilayah Persekutuan Putrajaya dan Cyberjaya. Bilangan penduduk di negeri ini juga merupakan yang paling ramai di Malaysia dengan taraf hidup yang sangat tinggi dan kadar kemiskinan di negeri ini adalah yang paling rendah di Malaysia.

Kajian ini memfokuskan kepada golongan belia Malaysia terutama sekali mereka yang berusia 15 hingga 30 tahun (berdasarkan pindaan Akta Pertubuhan Belia dan Pembangunan Belia 2007) yang dipilih sebagai fokus utama kajian ini

berdasarkan justifikasi berikut. Pertama, belia ialah pengguna internet yang paling aktif jika dibandingkan dengan generasi yang lebih tua. Kedua, peningkatan penggunaan media sosial yang aktif mendedahkan mereka kepada risiko atau bahaya kesan geran politik *cybertroopers*. Selain itu, golongan belia adalah sasaran utama kebanyakan parti-parti politik untuk mendapatkan sokongan kerana belia merupakan kelompok pengundi yang paling tinggi berbanding dengan kumpulan lain, terutamanya setelah pindaan had umur mengundi dari 21 tahun ke 18 tahun telah dikuatkuasakan.

Dari segi batasan kajian, kajian ini dilaksanakan sewaktu negara dilanda ancaman keselamatan kesihatan iaitu pandemik COVID-19. Pandemik ini dilihat melambatkan proses pengumpulan data kerana penyelidik sukar untuk bergerak ke kawasan kajian bagi mendapatkan data primer dan sekunder. Seterusnya, proses mengenalpasti informan dan responden dalam kajian ini juga mengambil masa yang lama. Isu Perintah Kawalan Pergerakan (PKP) mengehadkan pergerakan penyelidik dengan hanya membenarkan radius pergerakan 10KM daripada kediaman.

Kajian ini dijalankan sepanjang tempoh pandemik *Covid-19* iaitu bermula pada tahun 2021 sehingga 2022. Namun begitu, bagi mendapatkan penjelasan yang lebih terperinci mengenai kajian ini, pengkaji mengumpulkan data dari tahun 2014 sehingga kini kerana dalam tempoh tersebut perkembangan politik *cybertroopers* sangat meluas di Malaysia dan ianya telah terbukti dalam kempen-kempen PRU-14 dan 15.

1.7 Definisi Operasional

1.7.1 *Cybertroopers*

Menurut Freedom House (2014) *cybertroopers* atau pasukan siber merupakan pengulas yang dibayar oleh parti politik baik pihak kerajaan mahupun pembangkang untuk menyerang pihak lawan. Keadaan ini terjadi sebelum proses pengundian berlangsung. Manakala Bradshaw dan Howard (2019) mendefinisikan *cybertroopers* sebagai individu yang diupah oleh parti politik untuk memanipulasikan pendapat awam secara dalam talian. Ini bermaksud individu yang diupah ini akan menyebarkan propaganda yang berunsur politik di laman sosial untuk memburukkan sebelah pihak. Menurut Johns & Cheong (2019), *cybertroopers* ialah kegiatan yang berbayar untuk memanipulasikan perbincangan politik di media sosial yang mana ianya akan menimbulkan ketidakpastian dan kekeliruan kepada orang awam ataupun masyarakat. Keadaan ini berlaku sewaktu proses pilihan raya di sesebuah negara. Di Malaysia sendiri, pergerakan golongan ini sangat aktif terutamanya dalam menyampaikan propaganda politik dan memanipulasikan berita untuk menjatuhkan kreadibiliti pihak lawan. Jika dilihat, definisi istilah *cybertroopers* yang diberikan sarjana di atas masih kabur. Oleh itu, tesis ini menggunakan konsep *political astroturfing* untuk memahami dengan lebih jelas tentang *cybertroopers.*

Selain *cybertroopers,* istilah ini juga turut disamakan dengan konsep *political astroturfing*. Menurut Kovic et al. (2018), *political astrotufing* ialah aktiviti *top-down* di internet yang dilaksanakan secara palsu dan penipuan oleh aktor politik dengan menggunakan khidmat individu lain. Penggunaan media sosial sebagai medium untuk menyebarkan fahaman dan ideologi ahli politik ketika berlakunya pilihan raya. Schoch

et al. (2022) pula mendefinisikan *political astroturfing* sebagai kempen maklumat palsu yang diselaraskan secara berpusat menerusi penyamaran identiti. Walker (2014) juga merujuk *political astroturfing* sebagai kempen di mana para peserta kelihatan seperti sebahagian dari gerakan atau sentimen akar umbi yang tulen, sedangkan sebenarnya disusun secara terpusat dari atas ke bawah (*top-down*). Parti-parti politik mula menumpukan kepada kempen siber atau menggunakan platform media sosial untuk berkomunikasi dan menyalurkan maklumat kepada masyarakat, khususnya pengundi. Oleh kerana istilah *cybertroopers* tidak didefinisikan dengan jelas oleh sarjana, maka dalam tesis ini, istilah *cybertroopers* akan menggunakan konsep *political astroturfing* yang diperkenalkan oleh Kovic et al. (2018), Schoch et al. (2022) dan Walker (2014).

1.7.2 Pengawasan siber

Wan Amizah (2008) mentakrifkan pengawasan media sebagai kaedah yang digunakan secara sengaja untuk menyekat, memantau, membatalkan dan mengharamkan sebarang maklumat yang ingin disampaikan oleh sesuatu organisasi media kepada orang ramai. Namun, Chomsky (2002) melihat kawalan media ini diperlukan oleh pihak kerajaan memerintah kerana kerajaan akan memastikan media dikawal sedemikian rupa bagi mempengaruhi pendapat, pemikiran dan persepsi rakyat agar sealiran dengan prinsip dan tindakan mereka.

Grasso dan Bessant (2018) menggunakan model Panoptican dalam mendefinisikan istilah pengawasan di mana ia memerlukan ‘set teknik dan juga institusi untuk mengukur, mengawasi dan membetulkan sesuatu yang tidak normal dengan menggunakan mekanisme tatatertib atau disiplin yang menimbulkan ketakutan terhadap pelaku. Pengawasan siber yang digunakan oleh kebanyakan kerajaan adalah bertepatan dengan model Panopticon kerana ini merupakan cara

disiplin yang berkesan untuk mengawasi orang ramai. Namun begitu, pengawasan bukan hanya melibatkan 'pemerhatian terhadap orang awam', tetapi ia juga merangkumi semuanya termasuk pemantauan elektronik, pemerhatian visual melalui CCTV, pengecaman wajah, data instagram dan sebagainya. Oleh sebab itu, langkah pengawasan yang diambil kerajaan menjadi ancaman kepada rakyat.

Menurut pandangan Zurawski (2005), pengawasan merupakan satu aspek yang penting untuk dinilai dan dipantau terutamanya apabila seseorang individu menggunakan sesuatu teknologi. Pengawasan menggunakan teknologi boleh mengawal pelbagai aktiviti, mendapat maklumat serta menilai aktiviti seseorang individu pada masa kini. Pemantauan ini boleh dibuat dengan memerhatikan akaun-akaun media sosial milik masyarakat. Manakala, Fuchs (2012) menyatakan wujudnya konsep pengawasan apabila pengguna saling berhubungan antara satu sama lain melalui aplikasi secara dalam talian, seperti aplikasi media sosial. Oleh itu, sebarang maklumat yang dikongsikan di media sosial mudah untuk dipantau oleh pihak ketiga dan ini memberi kesan buruk apabila masyarakat terdedah kepada pencerobohan atau penyalahgunaan maklumat peribadi oleh pihak yang tidak bertanggungjawab.

Berdasarkan definisi yang diutarakan oleh para sarjana mengenai pengawasan siber, tesis ini akan menggunakan definisi yang telah diberikan oleh Grasso dan Bessant (2018) iaitu pengawasan siber merupakan satu bentuk sekatan yang dilakukan oleh pihak kerajaan dengan memantau akaun-akaun media sosial atau ciapan yang dikongsikan oleh masyarakat dalam talian. Ia bertujuan untuk menjaga ketenteraman awam dan keselamatan negara.

1.7.3 Penapisan siber

Aceto and Pescapè (2015) mentakrifkan penapisan internet sebagai usaha terancang kerajaan untuk merosakkan atau menyekat akses kepada laman sesawang atau kandungan tertentu yang mendatangkan keburukan. Kebiasaannya, penapisan ini dilakukan dengan menapis dan menyaring kandungan internet yang dikongsikan oleh masyarakat. Perkara ini dilakukan untuk melindungi keselamatan negara, menjaga ketenteraman sosial dan melindungi keluarga serta individu. Sebaliknya, menurut Shukla dan Moosavi (2013), penapisan internet membawa maksud kawalan dan/atau tindakan menyekat sesuatu yang boleh dinilai, dilihat dan diterbitkan di internet yang sebahagian besarnya dilakukan oleh kerajaan dan boleh juga dilakukan oleh organisasi swasta atau individu tertentu atas alasan moral, keagamaan dan etika.

Antara usaha kerajaan dalam melakukan penapisan di alam siber ialah dengan mengenakan akta-akta kawalan ke atas media termasuk media siber. Misalnya, Akta Komunikasi dan Multimedia 1998 (AKM 1998) dan Akta Suruhanjaya Komunikasi dan Multimedia 1998 (ASKM 1998) bagi mengawal media baru dan media sosial digunakan untuk melarang penyampaian isi kandungan yang tidak bersesuaian, iaitu kandungan-kandungan yang boleh menyinggung perasaan (offensive) dan boleh dibantah (objectionable) dalam konteks nilai sosial negara ini (Adibah, 2020). Dari satu sisi, penapisan ini dapat mengelakkan penerimaan maklumat yang tidak sesuai. Namun, dari sisi lain, akta kawalan ini dilihat boleh disalahgunakan apabila kerajaan mula menapis isi kandungan yang dilihat tidak mendatangkan faedah kepada mereka (Lee, 2014). Di alam siber, kerajaan telah membentuk sebuah agensi pemantauan keselamatan berkaitan teknologi maklumat dan komunikasi (ICT) bagi menangani masalah insiden-insiden keselamatan ICT negara (Hamdan & Ismail, 2015).

Penggunaan sistem ini bertujuan untuk mewujudkan satu persekitaran penggunaan sumber internet yang bersih.

Kawalan media dalam konteks Malaysia dilaksanakan menerusi cara penapisan kandungan media sama ada media konvensional atau media siber. Ia adalah salah satu cara untuk mencegah segala bentuk penularan berita atau informasi yang kurang tepat kepada masyarakat dan menghindari daripada berita yang dimanipulasi untuk kepentingan sesetengah pihak. Oleh itu, Wan Amizah (2008) mentakrifkan kawalan media dalam bentuk penapisan sebagai kaedah yang digunakan secara sengaja untuk menyekat, menapis, membatalkan dan mengharamkan sebarang maklumat yang ingin disampaikan oleh sesuatu organisasi media kepada orang ramai. Menurut Wan Amizah & Muhammad Adnan (2017), kawalan dalam media terdiri daripada beberapa teknik: 1) Penapisan di mana membenarkan bahagian-bahagian tertentu dan blok bahagian-bahagian tertentu; 2) *Gatekeepers* biasa digunakan dalam penentuan berita. Kawalan ini berlaku dalam semua struktur media; 3) Sekatan akses seperti tembok api atau *firewall* juga digunakan supaya sesuatu maklumat tidak dapat dilayari oleh pengguna menerusi internet dengan memblok terus terhadap sesuatu laman web. Justeru itu, kawalan siber menerusi penapisan sangat penting dilakukan kepada masyarakat untuk menapis sesuatu maklumat yang dilihat mampu mengancam keselamatan dan kebimbangan dalam masyarakat sebelum disiarkan.

Secara umumnya, tesis ini mendefinisikan penapisan siber seperti tafsiran yang diberikan oleh Wan Amizah (2008) iaitu penapisan sebagai kaedah yang digunakan secara sengaja untuk menyekat, menapis, membatalkan dan mengharamkan sebarang maklumat yang ingin disampaikan oleh sesuatu organisasi

media kepada orang ramai. Dalam konteks ini, penapisan ialah tindakan kerajaan untuk menapis semua kandungan maklumat media yang dilihat kurang tepat atau berlawanan dengan aspirasi kerajaan daripada disebarkan kepada masyarakat umum. Penapisan ini dilakukan kerana mengambil kira faktor keselamatan, keamanan serta perpaduan dalam kalangan masyarakat yang pelbagai di negara ini. Penapisan siber sememangnya amat penting dilakukan bagi mengekang serta mengelakkan perkara yang tidak baik timbul dalam dunia alam maya yang boleh mengganggu gugat keamanan negara. Dalam kajian ini, kewujudan golongan *cybertroopers* khususnya dalam politik pada hari ini amat membimbangkan dan memberi impak besar kepada masyarakat.

1.7.4 Belia

Definisi umur belia adalah berbeza-beza mengikut negara. Misalnya, di Indonesia, belia ditakrifkan sebagai seseorang yang berumur daripada 16 hingga 30 tahun. Jika dilihat peringkat umur belia merupakan peringkat perubahan dari seseorang yang bersifat '*dependent*' kepada '*independent*'. Di Malaysia, belia didefinisikan sebagai individu yang berumur di antara 15 hingga 30 tahun (pindaan Akta Pertubuhan Belia dan Pembangunan Belia 2007). Namun begitu, dari segi pelaksanaan program dan orientasi aktiviti tumpuan kepada individu yang berumur di antara 18 hingga 25 tahun mengikut Dasar Pembangunan Belia Negara 1997. Selain itu, Pertubuhan Bangsa-Bangsa Bersatu mendefinisikan belia iaitu mereka yang berumur antara 15 hingga 24 tahun (United Nations, 2008) dan Pertubuhan Komanwel menyatakan bahawa belia adalah mereka yang berumur antara 15 hingga 29 tahun (The Commonwealth, t.t).

Golongan belia yang bermula dari peringkat umur 15 hingga 30 tahun merupakan golongan yang sering terdedah kepada pelbagai jenis informasi baik

secara digital mahupun fizikal. Misalnya, penglibatan golongan belia dalam bidang politik semasa berada diperingkat universiti menerusi Pilihan Raya Kampus adalah pendedahan awal kepada yang berfungsi sebagai pengalaman yang bermanfaat untuk hidup sebagai warganegara yang matang (Mohd Fuad et al., 2009). Hal ini menunjukkan penglibatan belia semasa proses pilihan raya kampus sudah membuktikan bahawa golongan belia ini merupakan golongan yang boleh mengubah lanskap politik dengan kuasa yang diberikan dengan mereka iaitu kuasa memilih.

Menurut Muhammad Ismail (2007), belia boleh didefinisikan dalam lima kelompok seperti berikut:

i. Golongan belia remaja. Rata-rata kumpulan ini masih di bangku sekolah. Antara beberapa perkara yang perlu ditekankan dalam kumpulan ini adalah mendidik nilai, memupuk jati diri di samping mendedahkan mereka dengan senario yang berubah dan impaknya ke atas mereka.
ii. Golongan belia institusi pengajian tinggi atau penuntut (18 hingga 25 tahun) golongan ini terdiri daripada penuntut yang berada di institusi pengajian tinggi dan lepasan sekolah menengah. Mereka mula memasuki alam lebih bebas daripada kawalan ibu bapa, mahupun peraturan sekolah. Pada peringkat ini, mereka perlu ditekankan dengan moral yang tinggi dan memupuk hubungan sihat apabila bergaul.
iii. Golongan awal pekerjaan (18 hingga 23 tahun). Golongan ini perlu didedahkan dengan pelbagai peluang memajukan diri dalam bidang yang mereka ceburi, galakkan belajar dan menimba pengalaman perlu diutamakan. Di samping itu, program yang dapat meningkatkan kesedaran sosial yang sihat perlu diusahakan dan dilaksanakan.

iv. Golongan belia industri (20 hingga 30 tahun). Sektor industri kini menyediakan peluang kerja yang tinggi di Selangor. Belia perlu diberi peluang meningkatkan diri dalam hal yang berkaitan dengan keperluan kemahiran bekerja dan membangunkan insan.

v. Golongan belia veteran (30 hingga 40 tahun). Biasanya golongan ini sudah berumah tangga dan lebih menumpukan usaha mengukuhkan pendapatan keluarga serta mendidik anak-anak. Mereka ini lebih matang dan ada tanggungjawab yang lebih tinggi pada keluarga.

Manakala, Tuan Pah Rokiah (dalam Nor Anita, 2017) mengklasifikasikan belia sebagai mereka yang berada dalam lingkungan umur 15 hingga 30 tahun iaitu sama dengan kategori umur ini yang didefinisikan oleh Kementerian Belia dan Sukan. Menurut (Mohd Mahadee dalam Nor Anita, 2017), kumpulan umur belia yang berada dalam lingkungan umur 15 hingga 24 merupakan kumpulan belia remaja terbesar di Malaysia. Jumlah populasi terbesar negara juga adalah dalam kalangan kelompok belia dengan jumlah 18 juta orang (Nor Anita, 2017). Jika dilihat kepada semua pandangan sarjana di atas, golongan belia berada pada tahap umur dewasa di mana pada tahap ini pemikiran golongan belia sangat terbuka luas dan mudah terdedah dengan dunia luar baik, baik yang berada di luar bandar mahupun bandar.

Oleh itu, tesis ini mendefinisikan belia sebagai individu yang berumur dari 15 hingga 30 tahun sejajar dengan definisi belia yang diberikan oleh Akta Pertubuhan Belia dan Pembangunan Belia (Pindaan) 2019. Oleh itu, belia yang berumur kurang dari 15 tahun atau lebih daripada 30 tahun akan dikecualikan dari kajian ini. Ini kerana kategori umur ini adalah kelompok belia yang matang di mana pada tahap ini belia telah mempunyai tahap pendidikan formal di peringkat menengah tinggi dan

mempunyai pengetahuan asas tentang politik. Selain itu, kebanyakan kelompok belia ini adalah pengguna aktif internet, terutamanya mereka yang mempunyai akaun media sosial.

1.7.5 Keselamatan Siber

Muhammad Adnan et al. (2017) menjelaskan bahawa keselamatan siber merujuk kepada bagaimana pengguna Internet menggunakan medium Internet secara positif dan selamat serta melindungi diri mereka daripada ancaman siber. Walau bagaimanapun, keberkesanan keselamatan siber pengguna Internet bergantung kepada faktor persekitaran sosial. Keselamatan siber dilindungi oleh sistem yang tersambung ke internet, termasuk perkakasan, perisian dan data, dari serangan siber. Dalam konteks pengkomputeran, keselamatan merangkumi keselamatan siber dan keselamatan fizikal. Kedua-duanya digunakan oleh perusahaan untuk melindungi daripada akses yang tidak dibenarkan ke pusat data dan sistem berkomputer lain. Keselamatan yang dirancang Suntuk menjaga kerahsiaan, integriti dan ketersediaan data adalah sebahagian daripada keselamatan siber.

Keselamatan siber adalah amalan melindungi sistem, rangkaian, perisian dan pelbagai jenis data yang berkaitan dengan internet dari serangan siber. Serangan siber ini biasanya bertujuan untuk mengakses, mengubah, atau memusnahkan maklumat sensitif, memeras wang dari pengguna, atau mengganggu proses perniagaan tradisional. Pelaksanaan langkah-langkah keselamatan siber yang berkesan sangat sukar pada masa kini kerana terdapat banyak peranti daripada individu, dan penyerang yang semakin inovatif mengikut arus kepesatan teknologi kini.

Che (2006), siber membawa maksud penggunaan teknologi komputer. Manakala, pada pandangan Nate Lord (2017), keselamatan siber merujuk kepada teknologi, proses dan amalan melindungi rangkaian, peranti atau data daripada serangan atau kerosakan disebabkan oleh penjenayah. Hal ini jelas menunjukkan bahawa keselamatan siber berkait rapat dengan penggunaan teknologi di mana pada masa kini dunia berada di hujung jari segala maklumat mudah diakses walaupun terdapat kawalan yang ketat. Misalnya, pencerobohan data, penggodaman, jenayah siber, *scammer* dan beberapa lagi aktiviti lain yang mendatangkan risiko dan bahaya kepada individu mahupun pihak sewajarnya sangat memerlukan keselamatan siber. Keadaan ini, membimbangkan pelbagai pihak jika keselamatan siber diambil remeh serta tidak diperketatkan dan dilakukan pemantauan dari setiap masa oleh pihak yang bertanggungjawab.

Keselamatan siber merujuk kepada aspek-aspek perlindungan yang digunakan untuk melindungi perisian, perkakasan dan rangkaian internet daripada serangan penggodaman dari pihak yang tidak bertanggungjawab. Keselamatan siber juga merujuk kepada 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 baik secara individu ataupun kumpulan. Keselamatan siber juga turut berfungsi sebagai keselamatan teknologi maklumat. Justeru itu, keselamatan siber menjelaskan mengenai disiplin untuk melindungi sesuatu maklumat dan sistem yang digunakan untuk memproses dan menyimpan. Keselamatan siber amat penting bagi membendung masalah jenayah siber semakin berleluasa dalam negara. Justeru itu, pelbagai inisiatif yang telah dijalankan oleh pihak kerajaan dan bukan kerajaan untuk membendung gejala siber yang kurang sihat dalam masyarakat.

Selain itu, keselamatan siber juga merupakan satu perbuatan yang melindungi keselamatan maklumat dan ruang siber daripada ancaman anasir luar (George, 2017). Hal ini kerana, kesemua maklumat dan data rakyat individu dilindungi dengan keselamatan siber. Setiap negara bertanggungjawab akan maklumat yang mereka perolehi daripada rakyat yang mana maklumat tersebut sangat sulit kerana dalam data tersebut terkandung segala maklumat-maklumat penting misalnya hal yang berkaitan dengan kewangan, keluarga serta kesihatan. Berdasarkan kepada semua definisi di atas, maka tesis ini mendefinsikan keselamatan siber sebagai amalan atau tindakan pengguna internet untuk melindungi diri dari ancaman atau serangan siber ketika melayari atau menggunakan internet, seperti yang dijelaskan oleh Muhammad Adnan et al. (2017). Oleh itu, kajian ini sekali gus melihat sama ada golongan politik *cybertroopers* ini memberi ancaman keselamatan siber kepada masyarakat atau negara.

1.8 Organisasi Bab

Bagi memastikan tesis ini diorganisasi dengan baik dan tersusun, maka tesis ini dibahagikan kepada lima bab. Bab 1 memperincikan latar belakang kajian, permasalahan kajian, persoalan kajian dan objektif kajian. Penerangan setiap bab juga diterangkan dalam bab ini iaitu organisasi kajian.

Bab 2, merupakan hasil kajian ilmiah terdahulu atau ulasan-ulasan literatur dan kajian yang berkaitan dengan pendefinisian *cybertroopers* dalam konteks Malaysia. Bab ini juga turut menjelaskan secara lebih terperinci mengenai kerangka teoretikal seperti teori Struktur Peluang Politik, teori Penentuan Agenda dan teori Keselamatan, khususnya keselamatan siber. Huraian mengenai teori-teori ini adalah penting bagi memandu penghujahan tesis ini.

Bab 3, menghuraikan tentang aspek metodologi kajian yang di adaptasikan oleh penyelidik dalam kajian ini. Metodologi kajian menerangkan tentang pendekatan dan langkah-langkah yang diambil dalam mendapatkan maklumat yang berkaitan kajian ini seperti reka bentuk kajian, pendekatan, sampel kajian dan instrumen kajian. Pengumpulan data merupakan satu perkara yang penting dan pengkaji perlu menganalisis dengan sebaik mungkin data yang diperolehi agar mencapai objektif yang ditetapkan. Oleh itu, dalam kajian ini pengkaji telah menggunakan pendekatan campuran iaitu gabungan kaedah kuantitatif dan kualitatif.

Bab 4 membahaskan dapatan kajian secara konkrit tentang golongan *cybertroopers* serta mekanisme yang dijalankan oleh kerajaan dalam menyekat aktiviti

golongan ini. Kesemua dapatan objektif kajian tesis ini akan dibincangkan dalam bab ini secara terperinci.

Bab 5, yang merupakan bab terakhir dalam kajian ini yang membuat kesimpulan penemuan utama kajian ini. Dalam bab ini juga, akan dilakukan rumusan tentang definisi dan tipologi politik *cybertroopers*, ancaman yang dibawa mereka dan mekanisme efektif yang boleh dilakukan kerajaan dalam membendung kegiatan golongan politik *cybertroopers*. Sumbangan dan cadangan kajian lanjutan juga turut dibincangkan dalam bab ini.