BAB I

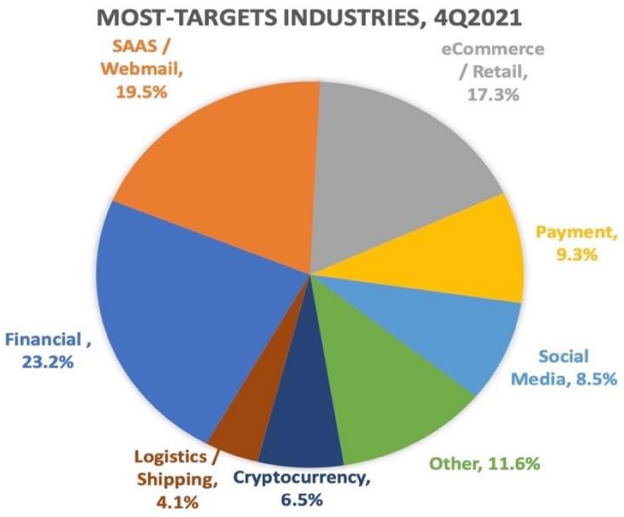
PENDAHULUAN

1.1 Latar Belakang Masalah

Kejahatan siber adalah tindakan kriminal yang dilakukan dengan memanfaatkan teknologi digital untuk mencapai tujuan yang melanggar hukum. Kejahatan siber mencakup berbagai aktivitas ilegal yang dilakukan secara *online*, mulai dari pencurian data hingga peretasan sistem, penyebaran *malware*, dan manipulasi informasi dengan tujuan merugikan individu, organisasi, atau negara (Wall, 2007). Bentuk kejahatan siber bertujuan mendapatkan keuntungan secara ilegal dan berdampak pada kerugian finansial serta reputasi bagi korbannya (Gordon & Ford, 2006). Dengan berkembangnya teknologi digital, jenis-jenis kejahatan siber semakin beragam dan menuntut perhatian khusus dari berbagai pihak untuk menjaga keamanan informasi dan infrastruktur digital.

Salah satu bentuk kejahatan siber yang meningkat adalah *phishing*. *Phishing* adalah tindakan yang berupaya memperoleh informasi sensitif atau rahasia secara elektronik dari pengguna yang biasanya untuk tujuan pencurian dengan membuat situs web replika dari organisasi yang sah (Akinyelu & Adewumi, 2014). *Phishing* adalah metode penipuan siber yang memanfaatkan teknik manipulasi untuk memperoleh informasi sensitif dengan menyamar sebagai entitas yang sah atau tepercaya. Teknik ini mengandalkan pengelabuan untuk menipu individu agar memberikan data pribadi atau informasi keuangan yang berharga, seperti nomor identitas, kata sandi, atau rincian kartu kredit.

Phishing merupakan ancaman yang sulit untuk dicegah karena penyerang sering kali menggunakan kelemahan psikologis manusia untuk mengecoh korban. Menurut Kevin Mitnick, seorang pakar keamanan siber dan mantan peretas terkenal, "*The human factor is truly security's weakest link*", yang menegaskan bahwa serangan *phishing* berhasil karena mengeksploitasi kelemahan manusia dalam mengenali ancaman (Mitnick, 2017). Pelaku dapat dengan mudah membuat email atau situs web yang terlihat sangat meyakinkan dan profesional, sehingga banyak pengguna yang tidak dapat membedakan antara komunikasi yang sah atau yang berbahaya (Hadnagy, 2018b). Selain itu, rendahnya tingkat kesadaran dan pendidikan tentang keamanan siber dimasyarakat dapat memperburuk situasi ini, menjadikan penyerang memiliki target yang lebih mudah untuk menyerang.



Gambar 1. 1 ***Most-Targets Industries in Phishing Attacks 2021***

Sumber: Anti-Phishing Working Group (APWG), 2022

Gambar 1.1 menunjukkan *tren* serangan *phishing* yang menyasar industri keuangan menjadi jenis serangan terbesar dibandingkan dengan yang lainnya. Persentase serangan yang terjadi di industri keuangan mencapai angka yang signifikan, yaitu sebesar 23,2% dari total keseluruhan serangan *phishing* yang terjadi. Hal ini menunjukkan bahwa industri keuangan, menjadi target utama bagi pelaku kejahatan siber dalam menjalankan aksinya. Besarnya persentase tersebut menunjukkan bahwa serangan *phishing* terhadap industri keuangan masih menjadi ancaman yang sangat serius dan perlu mendapatkan perhatian lebih besar, guna meningkatkan sistem keamanan serta kewaspadaan terhadap berbagai modus serangan yang terus berkembang seiring dengan kemajuan teknologi.

Pembobolan bank akibat serangan *phishing* memiliki konsekuensi serius, mulai dari kerugian finansial hingga krisis kepercayaan masyarakat terhadap sistem keuangan digital. Serangan *phishing* bukan hanya menyebabkan kerugian ekonomi, tetapi juga merusak integritas sistem keuangan secara menyeluruh (Revenkov et al., 2021). *Phishing* mengeksploitasi kepercayaan nasabah dengan mereplikasi situs web bank yang meyakinkan, memungkinkan pencurian data sensitif secara masif. Dampak finansial yang ditimbulkan sering kali signifikan, namun lebih berbahaya adalah terganggunya kepercayaan publik terhadap sistem perbankan digital. Kegagalan lembaga keuangan dalam mendeteksi dan merespons *phishing* menunjukkan lemahnya sistem deteksi ancaman yang masih bergantung pada metode konvensional seperti filter statis dan *blacklist* (Seenan et al., 2021). Kondisi ini diperparah oleh rendahnya literasi digital masyarakat dan minimnya koordinasi antarlembaga, yang menciptakan kerentanan sistemik dalam keamanan finansial

digital (Oshmankevich, 2021).

Singapura adalah negara di Asia Tenggara dengan ekonomi digital yang maju dan infrastruktur teknologi yang canggih, menjadikannya pusat keuangan dan inovasi di kawasan Asia Tenggara, dengan sektor industri digital Singapura berkembang pesat (Yong Soon Tan & Jasmine Lim, 2023). Ketergantungan Singapura pada sistem digital juga menimbulkan risiko yang kompleks. Dengan meningkatnya transformasi digital yang semakin berkembang, serangan siber bukan lagi sekedar ancaman teknis melainkan juga mengancam stabilitas ekonomi dan keamanan nasional, terutama karena semakin banyak industri penting yang bergantung pada jaringan *online*. Jika Singapura tidak segera menerapkan strategi keamanan berbasis kecerdasan buatan dan meningkatkan literasi digital, pertahanan sibernya akan tertinggal dari ancaman yang semakin canggih (Andrew Tan & Michelle Lee, 2023).

Kondisi tersebut tercermin dari salah satu kejahatan *cyber phishing* yang berhasil mengecoh banyak korban di Singapura. Dimana, kasus tersebut menimpa nasabah OCBC Bank Singapura yang terjadi pada Desember 2021, dengan puncak serangan berlangsung selama sekitar satu minggu, yaitu dari 23 Desember 2021 hingga 30 Desember 2021. Berdasarkan publikasi oleh *Singapore Police Force* 2023, dalam kasus ini pelaku mengirimkan SMS palsu yang mengaku dari bank, memperingatkan korban tentang upaya akses tidak sah, dan meminta mereka mengeklik tautan untuk verifikasi. Setelah mengklik, korban diarahkan ke situs palsu yang meminta kredensial perbankan serta OTP, yang kemudian digunakan penipu untuk mencuri dana. Mengutip laporan dari berita *Channel New Asia*

(CNA) pada tahun 2022, awalnya 469 nasabah mengalami kerugian sebesar S$8,5 juta atau sekitar 103,78 miliar rupiah, namun jumlah korban terus bertambah hingga mencapai 790 orang dengan total kerugian S$13,7 juta atau sekitar 167,51 miliar rupiah. Dalam rentang waktu yang singkat ini hanya 7 hari tercatat dari 23 Desember hingga 30 Desember 2021 lebih dari 80% total kerugian terjadi, yang menunjukkan efektivitas serangan dan kerentanan sistem keamanan serta rendahnya kewaspadaan nasabah saat masa libur akhir tahun (Channel New Asia, 2022).

Kasus *phishing* yang menimpa OCBC Bank Singapura tidak hanya menyebabkan kerugian finansial langsung bagi 790 nasabah dengan total kerugian mencapai S$13,7 juta, tetapi juga berdampak serius terhadap kepercayaan publik terhadap sistem perbankan digital (Ang, 2022). Dampak terbesar dari serangan ini adalah rusaknya rasa aman digital masyarakat, dimana nasabah merasa rentan terhadap penipuan bahkan dari saluran komunikasi yang terlihat sah (Azam et al., 2023). Selain itu, reputasi OCBC sebagai salah satu bank tertua dan terbesar di Asia Tenggara ikut terguncang, menunjukkan kelemahan institusional dalam mendeteksi dan menangani serangan berbasis rekayasa sosial. Insiden ini juga menimbulkan tekanan terhadap regulator dan lembaga keamanan siber untuk mempercepat reformasi kebijakan perlindungan konsumen dan memperkuat literasi digital sebagai bagian dari ketahanan siber nasional (Tan, 2022).

Kasus *phishing* OCBC Bank Singapura memiliki signifikansi besar terhadap sistem *cybersecurity* nasional karena mengungkap secara nyata kelemahan dalam deteksi, pencegahan, dan mitigasi serangan siber berbasis rekayasa sosial di

industri paling sensitif yaitu keuangan. Serangan ini berhasil mengecoh sistem keamanan bank dan mencuri data serta dana ratusan nasabah melalui metode manipulatif yang tidak terdeteksi oleh perlindungan teknis konvensional. Serangan *phishing* terutama menargetkan psikologi pengguna, menjadikan kesadaran manusia sebagai pertahanan utama (Kumar et al., 2020). Insiden ini memicu perubahan yang penuh ancaman bagi Singapura, termasuk keharusan untuk memperluas kebijakan keamanan siber dari sisi teknologi menuju penguatan kapasitas sosial, edukasi publik, dan peningkatan kesadaran digital secara sistemik.

Cyber Secutity Agency of Singapore (CSA) adalah badan pemerintah yang didirikan pada 1 April 2015 untuk memperkuat keamanan siber nasional dan melindungi infrastuktur informasi kritis dari ancaman digital. CSA berada di bawah Kantor Perdana Menteri dan dikelola oleh Kementerian Pembangunan Digital dan Informasi Singapura, dengan mandat utama untuk mendukung keamanan nasional, stabilitas ekonomi digital, dan ketahanan dunia maya Singapura (CSA, 2025b). CSA berupaya menjaga keamanan dunia maya Singapura untuk mendukung keamanan negara, mendukung ekonomi digital, dan melindungi gaya hidup digital kita. Badan ini mengawasi fungsi keamanan siber nasional, dan bekerja sama dengan para pemimpin sektor untuk melindungi Infrastruktur Informasi Penting Singapura (CSA, 2021c).

Menghadapi ancaman kejahatan *cyber phishing* tersebut, *Cyber Security Agency of Singapore* (CSA) berperan penting dalam menjaga keamanan dunia maya negara Singapura menerapkan kebijakan strategis yang menekankan perlindungan infrastruktur penting, peningkatan kesadaran publik, dan kerja sama

Internasional. Menurut David Koh, Kepala Eksekutif CSA, "Keamanan siber bukan hanya tentang teknologi, tetapi juga bagaimana kita membangun ketahanan nasional dalam menghadapi ancaman yang terus berkembang" (D Koh, 2021). Kebijakan yang dikeluarkan CSA yaitu, Program *Cybersecurity Awareness Campaign* untuk meningkatkan kesadaran publik tentang ancaman siber. Dalam program tersebut meluncurkan kampanye "*Better Cyber Safe than Sorry*", yang menekankan pentingnya literasi digital sebagai pertahanan utama terhadap ancaman siber (CSA, 2021a).

Selain berperan dalam koordinasi keamanan siber, *Cyber Security Agency of Singapore* (CSA) memperoleh dasar hukum yang lebih kuat lewat pengesahan *Cybersecurity Act* 2018. Undang-undang ini disahkan Parlemen pada 5 Februari 2018 dan disetujui Presiden pada 2 Maret 2018, lalu mulai berlaku pada tahun yang sama. Aturan ini mewajibkan CSA untuk melindungi *Critical Information Infrastructure* (CII), mewajibkan pelaporan insiden siber, dan memberi hak kepada *Commissioner of Cybersecurity* untuk memberikan arahan jika terjadi ancaman siber yang signifikan. Dengan adanya undang-undang ini, CSA tidak hanya berperan sebagai koordinator, tetapi juga sebagai lembaga dengan kewenangan hukum untuk menjaga keamanan siber nasional, termasuk dalam menghadapi serangan phishing di sektor keuangan (NCC Group, 2021)

Karena meningkatnya jumlah serangan siber *phishing* terhadap individu dan industri penting di Singapura khususnya industri keuangan, maka CSA melakukan beberapa langkah strategi yang dilakukannya. Salah satu langkah yang dilakukan CSA adalah membentuk Program *Cybersecurity Awareness Campaign*. Program

ini berupaya untuk mengedukasi masyarakat tentang pentingnya menjaga keamanan digital dan mencegah ancaman siber seperti *phishing* melalui kebiasaan siber yang aman. Dari program *Cybersecurity Awareness Campaign* meluncurkan kampanye besar yaitu "*Better Cyber Safe than Sorry*" yang bertujuan mengurangi ancaman siber dengan mengedukasi publik agar lebih waspada terhadap *phishing*, serta memperkuat kebiasaan keamanan digital melalui tindakan preventif seperti password kuat dan 2FA (CSA, 2021a). Program-program tersebut bertujuan untuk menciptakan budaya keamanan siber yang lebih kuat dan mengurangi risiko kejahatan siber, khususnya *phishing* di masyarakat.

Kampanye *"Better Cyber Safe than Sorry"* merupakan inisiatif nasional yang digagas oleh *Cyber Security Agency of Singapore* (CSA) sebagai bagian dari program luas *Cybersecurity Awareness Campaign*. Kampanye ini dirancang untuk menjangkau seluruh lapisan masyarakat di Singapura dengan tujuan meningkatkan kesadaran mengenai ancaman siber seperti *phishing*, serta mendorong praktik keamanan digital yang baik. Menurut dokumen resmi CSA, kampanye ini diluncurkan sebagai respons terhadap meningkatnya ancaman *phishing* di negara tersebut dan dipromosikan melalui berbagai saluran media, termasuk materi edukasi digital, media sosial, kerja sama dengan sektor perbankan, serta materi publik lainnya (CSA, 2025a). Dengan jangkauan yang luas dan perannya dalam strategi keamanan siber nasional, kampanye ini dapat dikategorikan sebagai upaya besar dalam membangun ketahanan siber masyarakat Singapura.

Sejalan dengan pelaksanaan *kampanye "Better Cyber Safe than Sorry"*, bahwa ancaman *phishing* yang menjadi sasaran program tersebut bukan sekadar persoalan kurangnya pengetahuan masyarakat, melainkan bentuk serangan yang secara sistematis memanfaatkan kelemahan psikologis individu. *Phishing* termasuk dalam kategori *social engineering*, yaitu teknik manipulasi yang mengeksploitasi kepercayaan, kepanikan, maupun rasa urgensi untuk mendorong korban menyerahkan informasi sensitif secara sukarela (Hadnagy, 2018a). Faktor manusia tetap menjadi salah satu elemen dominan dalam insiden pelanggaran data, termasuk pada kasus *phishing* (Verizon, 2023). Kondisi ini menegaskan bahwa celah keamanan tidak hanya berada pada sistem teknologi, tetapi juga pada pola respons dan perilaku pengguna. Oleh karena itu, kampanye kesadaran siber yang dilakukan oleh CSA perlu dianalisis sebagai respons terhadap ancaman *phishing* yang berbasis manipulasi psikologis, sehingga efektivitasnya tidak hanya diukur dari peningkatan pengetahuan, tetapi juga dari kemampuannya membentuk respons perilaku yang lebih waspada.

Kondisi tersebut berkaitan langsung dengan konsep *cyber resilience*, yang menekankan bahwa ketahanan siber tidak hanya bergantung pada penguatan sistem dan regulasi, tetapi juga pada kemampuan individu dan institusi untuk mengenali, merespons, serta beradaptasi terhadap ancaman yang terus berkembang (Torbjørn Haugen & Terry Lou, 2017). Dalam kerangka ini, kampanye kesadaran siber memiliki peran strategis sebagai bagian dari upaya membangun kapasitas masyarakat agar tidak mudah menjadi korban rekayasa sosial. Namun demikian, peningkatan kesadaran keamanan digital tidak selalu secara otomatis menghasilkan

perubahan perilaku yang konsisten dalam praktik sehari-hari (ENISA, 2022). Dengan begitu, terdapat tantangan dalam memastikan bahwa pesan kampanye benar-benar terinternalisasi menjadi kebiasaan digital yang berkelanjutan. Hal inilah yang menjadikan analisis terhadap implementasi kampanye CSA penting untuk dilakukan, khususnya dalam menghadapi peningkatan *phishing* di industri keuangan Singapura.

Penelitian ini menjelaskan bagaimana tantangan dari program ini, karena terdapat peningkatan serangan *phishing* yang meningkat di industri keuangan.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang yang sudah peneliti uraikan di atas, maka rumusan masalah yang peneliti rumuskan adalah:

Bagaimana *Cybersecurity Awareness Campaign* "*Better Cyber Safe than Sorry*" oleh CSA di Singapura ditinjau dari konsep *cyber resilience* dan *social engineering*?

1.3. Tujuan Penelitian

a. Tujuan Utama

Penelitian ini bertujuan untuk menganalisis *Cybersecurity Awareness Campaign "Better Cyber Safe than Sorry"* yang dilaksanakan oleh *Cyber Security Agency of Singapore* (CSA) di Singapura pada tahun 2021, dengan meninjau kampanye tersebut melalui konsep *cyber resilience* dan *social engineering* dalam upaya pencegahan ancaman *phishing*.

b. Tujuan Khusus

Menganalisis faktor-faktor penghambat yang menyebabkan *Cybersecurity Awareness Campaign* "*Better Cyber Safe than Sorry*" yang dikeluarkan CSA belum optimal dalam upaya pencegahan ancaman *phishing* di Singapura.

1.4. Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Penelitian ini memberikan kontribusi terhadap pengembangan kajian Hubungan Internasional dalam isu keamanan non-tradisional, khususnya keamanan siber. Dengan mengangkat kasus *phishing* di industri keuangan, penelitian ini menekankan bahwa serangan digital berbasis manipulasi psikologis seperti *phishing* memerlukan pendekatan keamanan yang lebih adaptif dan multidimensional. Penelitian ini mengangkat peran institusi nasional, yaitu *Cyber Security Agency of Singapore* (CSA). Penelitian ini memperluas pemahaman tentang bagaimana aktor negara dan kawasan dalam merespons ancaman seperti *phishing* yang dapat mengeksploitasi celah psikologis manusia dan kecanggihan teknologi. Selain itu, penelitian ini juga membuka diskusi bahwa keamanan digital tidak cukup dilihat sebagai isu teknis, melainkan persoalan stuktural yang berkaitan dengan literasi digital, akses teknologi, dan kapasitas kelembagaan.

1.4.2 Kegunaan Praktis

Secara praktis, penelitian ini dapat menjadi rujukan kritis bagi pemangku kebijakan, lembaga keamanan siber, dan industri keuangan dalam mengevaluasi kelemahan struktural dan teknis dalam respons terhadap serangan *phishing*.

Penelitian ini menyoroti bahwa pendekatan yang masih reaktif dan bertumpu pada kesadaran individu perlu digantikan dengan strategi berbasis teknologi deteksi dini seperti AI, serta peningkatan literasi digital yang sistematis dan berkelanjutan. Dengan demikian, penelitian ini tidak hanya memberi masukan teknis, tetapi juga mendorong reformasi pendekatan keamanan siber yang lebih strategis, adaptif, dan kolaboratif.

1.5. Kerangka Pemikiran

1.5.1. *Literature Review*

Terdapat empat penelitian terdahulu yang menjadi acuan penulis dalam penelitian ini. Salah satu penelitian yang menjadi rujukan penelitian ini adalah "*Cyber Capabilities and National Power: Volume Two – Singapore*" oleh *The International Institute for Strategic Studies* (IISS), yang diterbitkan pada tahun 2023. Penelitian ini memberikan penilaian terhadap kapabilitas siber nasional Singapura. Singapura dianggap memiliki institusional yang kuat melalui pembentukan lembaga seperti *Cyber Security Agency of Singapore* (CSA) dan integrasi keamanan digital ke dalam struktur pertahanan negara melalui pembentukan *Digital and Intelligence Service* (DIS). Namun, penelitian ini secara kritis menyoroti bahwa meskipun kekuatan keamanan siber Singapura bergantung pada kerangka kebijakan yang normatif dan keberhasilan diplomatik, negara itu masih memiliki keterbatasan dalam hal kapasitas teknis dan operasionalnya. Dalam penelitian ini nanti, temuan ini menekankan perlunya CSA untuk tidak hanya berfokus pada pengembangan kebijakan, tetapi juga untuk mendorong inovasi lokal dan pengembangan sumber daya manusia yang berkelanjutan (IISS, 2023).

Penelitian kedua yang menjadi referensi penelitian ini adalah *"Phishing Schemes in the Banking Sector: Recommendations to Internet Users on Protection and Development of Regulatory Tasks"* yang ditulis oleh Pavel V. Revenkov, Kseniya R. Oshmankevich, dan Aleksandr A. Berdyugin pada tahun 2021 (Revenkov et al., 2021). Penelitian yang ditulis menganalisis skema *phishing* di sektor perbankan dan mengungkap bagaimana *cybercriminal* secara canggih memanipulasi kepercayaan pengguna internet dengan meniru situs web resmi lembaga keuangan, seperti bank palsu dan perusahaan asuransi palsu, yang dirancang untuk mencuri data sensitif pengguna. Para peneliti menemukan korelasi signifikan antara jumlah kejahatan komputer dan jumlah lembaga perbankan di Rusia yang mengindikasikan bahwa pengurangan bank "penyedot uang" justru berkorelasi dengan peningkatan keamanan sistem perbankan. Sementara itu, para peneliti menemukan bahwa faktor utama yang menyebabkan pengguna rentan terhadap serangan *phishing* adalah tingkat literasi siber yang rendah. Temuan ini menunjukkan bahwa untuk mengurangi kerentanan terhadap serangan *phishing*, perlu ada pendekatan yang lebih holistik yang melibatkan pendidikan formal, kampanye kesadaran publik, dan kolaborasi antara sektor publik dan swasta (Revenkov et al., 2021).

Selanjutnya, terdapat penelitian dengan judul *"Advanced Phishing Detection Techniques in Financial Services: Lessons from ASEAN Banking Sector"* yang ditulis oleh S. Seenan, J. Abawajy, dan T. H. Kim pada tahun 2021 (Seenan et al., 2021). Dalam penelitian ini secara kritis mengevaluasi kegagalan pendekatan konvensional dalam mendeteksi serangan *phishing* di sektor keuangan ASEAN dan

menunjukkan bahwa, meskipun teknologi deteksi canggih seperti *machine learning, natural language processing, dan threat intelligence* telah diperkenalkan, penerapannya masih jauh dari kata optimal. Penelitian ini menekankan bahwa banyak bank di wilayah ASEAN masih menggunakan sistem berbasis *blacklist* dan filter heuristik statis, yang sangat mudah dilewati oleh skema *phishing* yang berkembang dan semakin kontekstual. Salah satu masalah paling menonjol adalah kurangnya investasi pada kemampuan lembaga keuangan sendiri untuk mendeteksi secara internal. Temuan ini mendorong perlunya investasi yang lebih besar dalam teknologi deteksi yang inovatif dan pengembangan sistem berbagi informasi ancaman yang lebih efektif di antara lembaga keuangan (Seenan et al., 2021).

Penelitian terakhir yang digunakan sebagai rujukan penelitian ini adalah *"ASEAN Cooperation to Combat Transnational Crime: Progress, Perlis, and Prospects"* yang ditulis oleh Pushpanathan Sundram pada tahun 2024. Penelitian ini menyoroti bagaimana dinamika kejahatan lintas negara (*transnational crime*) di kawasan Asia Tenggara berkembang semakin kompleks dan menantang di tengah ketidakmerataan kapasitas negara-negara anggota ASEAN. Kejahatan siber tidak hanya menuntut respons nasional, tetapi juga kolaborasi lintas batas yang cepat, terkoordinasi, dan berkelanjutan. Dalam konteks kejahatan siber, pendekatan kolektif ASEAN mulai diarahkan melalui inisiatif seperti ASEAN CERT *Incident Drill* (ACID)**,** yang merupakan upaya regional untuk mensimulasikan respons terhadap insiden siber. Namun, ACID masih menghadapi tantangan serius dalam hal efektivitas karena belum dibarengi dengan sistem koordinasi *real-time*, standar prosedur yang seragam, serta mekanisme tindak lanjut yang mengikat. Dengan

begitu, penelitian ini mengusulkan perlunya reformasi dalam kerangka kerja sama ASEAN untuk menciptakan mekanisme yang lebih responsif dan terintegrasi, termasuk pengembangan standar operasional yang seragam dan sistem koordinasi *real-time* (Sundram, 2024).

Berdasarkan beberapa tinjauan pustaka tersebut dapat dilihat bahwa adanya *gap* atau kebaruan dari penelitian ini yang terletak pada isi penelitian yang memiliki fokus untuk menganalisis apa saja tantangan yang dihadapi CSA dalam menjalankan *Cybersecurity Awareness Campaign "Better Cyber Safe than Sorry"* untuk mencegah ancaman *phishing* di Singapura. Program ini juga dibentuk karena meningkatnya serangan *phishing* yang terjadi.

1.5.2. *Human Security Concept*

Konsep *Human Security* diperkenalkan oleh *United Nations Development Programme* (UNDP) dalam *Human Development report* tahun 1994. UNDP menekankan bahwa keamanan tidak hanya dipahami sebagai keamanan negara (*state security*), melainkan harus berorientasi pada keamanan manusia sebagai individu (*people-centered security*). UNDP menjelaskan bahwa *human security* merupakan upaya perlindungan terhadap manusia dari berbagai ancaman yang dapat mengganggu kehidupan dan kesejahteraan, termasuk ancaman ekonomi, kesehatan, lingkungan, sosial, maupun ancaman berbasis kriminalitas (UNDP, 1994). Dalam kerangka tersebut, UNDP membagi *human security* ke dalam beberapa dimensi, salah satunya adalah *personal security*, yaitu perlindungan individu dari ancaman kekerasan dan tindakan kriminal yang dapat mengancam keselamatan manusia dalam kehidupan sehari-hari (UNDP, 1994).

Dalam konteks perkembangan ancaman keamanan kontemporer, ancaman terhadap individu tidak hanya berbentuk kekerasan fisik, tetapi juga berkembang dalam bentuk ancaman non-tradisional melalui ruang digital (UNDP, 2025). Salah satu ancaman tersebut adalah *cyber phishing*, yaitu bentuk kejahatan siber berbasis manipulasi sosial (*social engineering*) yang menargetkan individu untuk memperoleh data pribadi, akses akun, maupun informasi finansial korban. Hal ini sejalan dengan pemikiran *Commission on Human Security* yang menekankan bahwa *human security* berfokus pada perlindungan individu dari ancaman yang bersifat luas dan semakin kompleks, sehingga memerlukan upaya pencegahan berbasis perlindungan masyarakat (Commission on Human Security, 2003). Oleh karena itu, fenomena *phishing* dapat dipahami sebagai ancaman keamanan non-tradisional yang memiliki implikasi terhadap dimensi *personal security*, khususnya terkait perlindungan identitas serta rasa aman individu dalam aktivitas digital.

Dalam penelitian ini, konsep *human security* khususnya *personal security* digunakan untuk menjelaskan bahwa *Cybersecurity Awareness Campaign "Better Cyber Safe than Sorry"* oleh *Cyber Security Agency of Singapore* (CSA) merupakan bentuk upaya negara dalam melindungi masyarakat dari ancaman *phishing* melalui pendekatan edukasi dan peningkatan kesadaran publik.

1.5.3 *Cyber Resilience Concept*

Cyber resilience adalah kemampuan suatu organisasi untuk tetap berfungsi secara efektif meskipun mengalami serangan siber atau gangguan signifikan (Torbjørn Haugen & Terry Lou, 2017). Konsep ini mencakup kesiapan untuk merespons ancaman dan memulihkan sistem dengan cepat untuk mengurangi

dampak terhadap operasional, bukan hanya fokus pada pencegahan. Selain itu, *cyber resilience* menekankan pentingnya kontinuitas operasional, di mana organisasi dapat tetap beroperasi meskipun serangan terjadi, serta memastikan kerugian yang ditimbulkan dapat diminimalkan

Dalam penelitian ini, konsep *cyber resilience* digunakan untuk menjelaskan bagaimana suatu negara dapat mempertahankan kontinuitas operasional sistem digitalnya meskipun menghadapi serangan siber, seperti yang terjadi pada kasus *phishing* OCBC Bank. Dengan begitu, program *Cybersecurity Awareness Campaign: "Better Cyber than Sorry"* yang dilaksanakan oleh *Cyber Security Agency of Singapore* (CSA) merupakan bentuk implementasi dari pendekatan *cyber resilience*, dengan tujuan membangun ketahanan sosial melalui peningkatan kesadaran publik. Melalui edukasi yang masif, kampanye ini memperkuat kesiapsiagaan masyarakat sebagai garda terdepan dalam menghadapi ancaman *phishing*, yang tidak hanya mengganggu sistem, tetapi juga kepercayaan publik terhadap layanan digital.

Konsep *cyber resilience* terdiri dari lima komponen utama yang saling mendukung untuk menciptakan ketahanan digital yang tangguh. Komponen tersebut mencakup: *asset identification* (identifikasi asset), yaitu mengidentifikasi dan mengklasifikasi aset digital yang penting untuk dilindungi; *protection* (perlindungan), yaitu penerapan kebijakan dan teknologi untuk melindungi aset dari potensi ancaman; *detection* (deteksi), yakni kemampuan untuk mengenali serangan atau insiden keamanan secara cepat; *response* (respons), yaitu penyusunan prosedur dan rencana tindakan segera ketika insiden terjadi; serta *recovery* (pemulihan),

yakni strategi untuk mengembalikan fungsi sistem dan layanan utama dengan cepat setelah insiden siber (Andhika, 2023). Kelima komponen ini sangat penting untuk membangun sistem yang tidak hanya tahan terhadap serangan, tetapi juga mampu pulih dan beradaptasi dengan cepat terhadap ancaman siber yang terus berkembang

Dalam penelitian ini, konsep *cyber resilience* tercermin dalam langkah strategis yang diambil oleh CSA, khususnya melalui program *Cybersecurity Awareness Campaign* kampanye "*Better Cyber Safe than Sorry*" sebagai pendekatan edukatif dan preventif dalam menghadapi ancaman *phishing*. *Cyber resilience* mencakup lima elemen utama. Pertama, *identification*, yaitu kemampuan untuk mengenali aset digital yang penting serta memahami bentuk ancaman yang berpotensi muncul. Kedua, *protection*, yaitu upaya perlindungan untuk mengurangi peluang keberhasilan serangan melalui peningkatan kesadaran, penguatan perilaku aman, serta penerapan kebiasaan *cyber hygiene*. Ketiga, *detection*, yaitu kemampuan mendeteksi tanda-tanda serangan *phishing* secara dini agar risiko dapat diminimalkan sebelum menimbulkan dampak yang lebih besar.

Selanjutnya yang keempat, *response,* yaitu kemampuan mengambil tindakan cepat dan tepat ketika ancaman teridentifikasi, termasuk pelaporan serta langkah mitigasi untuk menekan kerugian. Kelima, *recovery,* yaitu proses pemulihan setelah insiden terjadi melalui perbaikan sistem, pengamanan ulang akun, serta penguatan kebijakan agar serangan serupa tidak terulang. Dengan demikian, *cyber resilience* menjadi alat analisis penting dalam menilai sejauh mana efektivitas kebijakan CSA melalui kampanye *"Better Cyber Safe than Sorry"*

dalam membangun ketahanan masyarakat terhadap ancaman *phishing* dan menjaga stabilitas keamanan digital Singapura.

1.5.4 *Social Engineering Concept*

Social engineering atau rekayasa sosial merupakan salah satu bentuk kejahatan siber yang paling berbahaya dan sering digunakan. Christopher Hadnagy (2018) mendefinisikan *social engineering* sebagai penggunaan manipulasi psikologis untuk mempengaruhi individu agar melakukan tindakan tertentu atau mengungkapkan informasi sensitif yang seharusnya tetap dirahasiakan. Dalam definisi ini, Hadnagy menekankan bahwa serangan *social engineering* bukan hanya mengandalkan kelemahan teknis sistem, melainkan lebih pada pemahaman terhadap perilaku dan psikologi manusia yang dapat dimanfaatkan untuk mendapatkan akses ke data pribadi atau sistem yang terlindungi (Hadnagy, 2018a). Pelaku serangan menggunakan teknik seperti *phishing* untuk menipu korban, dengan memanfaatkan kepercayaan, rasa takut, atau rasa urgensi yang tidak berdasar, sehingga korban tanpa sadar menyerahkan informasi yang sangat berharga. Oleh karena itu, konsep *social engineering* mengkritisi pendekatan keamanan siber yang terlalu menitikberatkan pada teknologi, dengan menegaskan bahwa celah terbesar seringkali terletak pada ketidaksiapan manusia dalam menghadapi manipulasi sosial.

Christopher Hadnagy menegaskan bahwa informasi pribadi merupakan aset paling berharga dalam kejahatan rekayasa sosial, karena siapa pun yang memilikinya dapat mengendalikan keputusan targetnya. Pernyataan ini menempatkan data pribadi sebagai sasaran utama dalam strategi manipulatif

berbasis psikologis. Konsep ini relevan dalam menganalisis serangan *phishing* yang menimpa nasabah OCBC Bank Singapura. Dalam kasus tersebut, pelaku memanipulasi korban melalui pesan palsu yang meniru komunikasi resmi bank dan mendorong korban mengungkapkan data pribadi. Keberhasilan serangan ini menunjukkan bahwa meskipun sistem keamanan digital canggih, celah terbesar ada pada ketidaksiapan individu dalam mengidentifikasi pesan yang mencurigakan atau memahami tanda-tanda manipulasi sosial, seperti rasa urgensi yang tidak berdasar atau permintaan informasi pribadi melalui saluran yang tidak biasa. Berdasarkan konsep ini, serangan *phishing* dapat dianalisis tidak hanya dari sisi teknologi, tetapi juga dari aspek individu. Hal ini sejalan dengan fokus penelitian saya yang menyoroti pentingnya program *Cybersecurity Awareness Campaign* dalam kampanye *"Better Cyber Safe than Sorry"*, yang bertujuan untuk meningkatkan literasi keamanan digital dan kesadaran nasabah terhadap ancaman *social engineering*, guna mengurangi kerentanannya terhadap serangan *phishing*.

1.6. Operasionalisasi Konsep

1.6.1. Definisi Konseptual

1.6.1.1 *Human Security Concept*

Human security merupakan konsep keamanan yang menempatkan manusia sebagai fokus utama, dengan menekankan perlindungan individu dari berbagai ancaman yang dapat mengganggu keselamatan dan kesejahteraan hidupnya. Seiring dengan perkembangan dinamika global, khususnya memasuki era 2000-an, dimana ancaman keamanan tidak lagi didominasi oleh

konflik militer antarnegara, melainkan berkembang ke arah ancaman non-tradisional seperti kemiskinan, penyakit, terorisme, hingga kejahatan siber yang secara langsung memengaruhi individu (UNDP, 2025).

UNDP dalam *Human Development Report* 1994 menjelaskan bahwa *human security* mencakup upaya untuk menciptakan kondisi *freedom from fear* dan *freedom from want*, serta meliputi berbagai dimensi keamanan seperti ekonomi, kesehatan, politik, hingga keamanan personal (UNDP, 1994). Salah satu dimensi penting dalam *human security* adalah *personal security*, yaitu perlindungan individu dari ancaman kekerasan maupun tindakan kriminal yang dapat merusak rasa aman dalam kehidupan sehari-hari (UNDP, 1994). Sejalan dengan hal tersebut, *Commission on Human Security* menegaskan bahwa *human security* bertujuan melindungi "vital core" kehidupan manusia dari ancaman yang semakin luas dan kompleks melalui strategi perlindungan (*protection*) dan pemberdayaan (*empowerment*) masyarakat (Commission on Human Security, 2003).

1.6.1.2. *Cyber Resilience Concept*

Cyber resilience, menurut konsep yang dicetuskan oleh Paul D. White (2018) , merujuk pada kemampuan sistem atau organisasi untuk terus berfungsi dan pulih dengan cepat dari gangguan atau ancaman siber, seperti serangan siber atau kerusakan sistem. Konsep

ini menekankan pentingnya bukan hanya perlindungan terhadap ancaman atau serangan yang dapat merusak sistem informasi, tetapi juga kesiapan untuk merespons, memitigasi, dan memulihkan kembali operasional dengan minimal gangguan. *Cyber resilience* tidak hanya berfokus pada pencegahan tetapi juga pada kemampuan untuk beradaptasi dan bertahan dalam menghadapi dinamika ancaman yang terus berkembang, serta memastikan kelangsungan layanan dan pemulihan yang cepat setelah insiden (Alhidaifi, 2024). Dengan kata lain, *cyber resilience* menggabungkan elemen identifikasi, perlindungan, deteksi, respons, dan pemulihan untuk memastikan ketahanan sistem terhadap ancaman siber secara menyeluruh.

1.6.1.3 *Social Engineering Concept*

Konsep *Social Engineering* merujuk pada teknik manipulasi psikologis yang digunakan oleh penyerang untuk mengeksploitasi kelemahan manusia dalam sistem keamanan. Dalam konteks ini, *social engineering* berfokus pada aspek psikologis dan sosial individu untuk memperoleh akses atau informasi sensitif yang seharusnya dilindungi. Menurut Kevin Mitnick, seorang tokoh yang dikenal dalam dunia keamanan siber, dalam bukunya *The Art of Deception* (2002), *social engineering* melibatkan penyerang yang memanipulasi korban agar mengambil tindakan yang diinginkan, seperti memberikan data pribadi, membuka akses sistem, atau

mengklik tautan berbahaya, dengan cara meyakinkan atau menipu mereka. *Social engineering* sering kali digunakan untuk menyerang kelemahan terbesar dalam sistem keamanan manusia itu sendiri, bukan perangkat keras atau perangkat lunak. Penyerang bisa menggunakan berbagai teknik, seperti *pretexting*, *phishing*, atau *baiting*, untuk menipu korban agar melakukan tindakan yang menguntungkan penyerang.

1.6.2. Definisi Operasional

1.6.2.1. *Human Security Concept*

Dalam penelitian ini, *human securitry concept* khususnya dimensi *personal security* dioperasionalisasikan sebagai upaya perlindungan individu dari ancaman kekerasan maupun kriminalitas yang dapat menganggu keselamatan, keamanan identitas, serta rasa aman dalam kehidupan sehari-hari (UNDP, 1994). *Personal security* dapat dinilai melalui beberapa indikator keselamatan inidvidu, seperti tingkat ancaman kriminalitas, risiko individu menjadi korban, serta tingkat rasa aman masyarakat terhadap ancaman yang berkembang (Koundouri, 2023). Oleh karena itu, penelitian ini menilai *personal security* melalui implementasi *Cybersecurity Awareness Campaign "Better Cyber Safe than Sorry"* oleh CSA, dengan ukuran keberhasilan berupa sejauh mana kampanye tersebut mampu meningkatkan kesadaran publik (*cybersecurity awareness*), mendorong perubahan perilaku aman pengguna (*safe online*

behaviour), serta memperkuat kemampuan individu dalam mengenali dan menghindari teknik *phishing* melalui peningkatan literasi digital sebagai bentuk pengurangan risiko masyarakat menjadi korban.

1.6.2.2. *Cyber Resilience Concept*

Cyber resilience dalam penelitian ini dioperasionalkan sebagai kemampuan sistem dan masyarakat untuk bertahan serta pulih dari gangguan siber, dengan penekanan khusus pada respons negara seperti Singapura melalui *Cyber Security Agency* (CSA). Untuk mengoperasionalisasikan konsep ini, penelitian ini mengamati bagaimana kebijakan dalam sebuah program seperti *Cybersecurity Awareness Campaign* dalam kampanye *"Better Cyber Safe than Sorry"* dilakukan untuk meningkatkan pemahaman publik tentang ancaman siber dan bagaimana kampanye tersebut memotivasi perubahan perilaku masyarakat. Ukuran keberhasilan dapat dilihat dari tingkat partisipasi dalam program edukasi ini, serta dampaknya pada kesadaran dan kesiapsiagaan masyarakat terhadap serangan *phishing* (Bellini et al., 2025). Penelitian ini menilai sejauh mana CSA dan programnya berhasil membangun ketahanan yang tidak hanya bersifat teknis, tetapi juga sosial, melalui peningkatan kapasitas adaptif individu dan organisasi dalam menghadapi ancaman siber.

1.6.2.3. *Social Engineering Concept*

Social engineering dalam penelitian ini dioperasionalkan sebagai serangan yang memanfaatkan kecenderungan psikologis manusia, seperti kepercayaan, rasa aman, atau emosi korban untuk menipu mereka mengungkapkan data sensitif. Untuk mengoperasionalisasikan konsep ini, penelitian ini fokus pada studi kasus serangan *phishing* OCBC Bank yang menggunakan teknik manipulasi psikologis untuk menipu korban. Cara mengoperasionalisasikannya dalam penelitian ini adalah dengan menilai bagaimana individu di masyarakat merespons ancaman tersebut dan bagaimana lembaga keuangan serta pihak berwenang merespons laporan dari korban. Keberhasilan penanggulangan serangan ini dapat dilihat dari kemampuan masyarakat untuk mengenali dan menghindari teknik manipulasi, serta kesiapan lembaga keuangan untuk memberikan edukasi serta mendeteksi potensi penipuan lebih cepat (Junger & Bullée, 2020). Penelitian ini juga menekankan pentingnya mengintegrasikan pendekatan berbasis manusia dalam kebijakan keamanan siber, dengan menilai bagaimana kesadaran psikologis masyarakat dapat menjadi bagian penting dari strategi mitigasi risiko.

1.7. Argumen Penelitian

Serangan *phishing* di Singapura pada tahun 2021 tidak secara eksplisit dapat dikategorikan dalam definisi *social engineering* yang tradisional, seperti penipuan tatap muka atau penyamatan langsung oleh pelaku. Dalam penelitian ini, serangan tetap patut dimasukkan dalam kerangka *social engineering*, mengingat serangan *phishing* memanfaatkan teknik manipulasi psikologis terhadap korban. Walaupun melalui saluran digital, teknik ini tetap mengandalkan emosi, rasa percaya, dan urgensi yang mempengaruhi perilaku individu untuk melakukan tindakan berisiko, seperti mengklik tautan atau memberikan informasi sensitif. Hal ini menunjukkan bahwa serangan *phishing* bukan hanya masalah teknis semata, tetapi juga masalah psikologis yang terkait dengan kerentanannya manusia. Tantangannya dalam penelitian ini adalah lebih mudah memanipulasi individu untuk melakukan tindakan berisiko daripada untuk mempengaruhi mereka agar meningkatkan kewaspadaan dan mengubah perilaku mereka dalam hal keamanan siber.

Dalam kerangka *cyber resilience* yang diterapkan oleh CSA Singapura, tantangan utamanya terletak pada bagaimana mengatasi dimensi psikologis dan perilaku manusia yang berhubungan langsung dengan ancaman *phishing.* Meskipun CSA telah mengembangkan berbagai teknologi keamanan seperti autentikasi dua faktor dan enkripsi untuk memitigasi serangan siber, teknologi saja tidak cukup untuk menangani kerentanannya terhadap manipulasi psikologis yang terjadi dalam serangan *phishing*. Pendekatan yang digunakan CSA melalui kampanye kesadaran dan pelatihan seringkali terbatas karena mengubah perilaku individu untuk lebih

peduli terhadap ancaman siber memerlukan usaha yang lebih besar dibandingkan sekadar menerapkan solusi teknologi.

1.8. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah kualitatif. Metode ini berfokus pada pengumpulan data analisis non-numerik untuk memahami makna, pengalaman, dan dinamika sosial politik secara mendalam. Metode ini cocok digunakan ketika penelitian ingin menjelaskan realitas yang tidak bisa dijabarkan secara statitik atau kuantitatif, melainkan melalui narasi, dokumen, atau pernyataan aktor yang relevan (Patton, 2015). Pendekatan kualitatif digunakan ketika peneliti ingin memahami konteks sosial, ekonomi, dan politik yang saling terkait serta menangkap makna dari tindakan dan proses sosial secara komprehensif (Creswell, 2013). Oleh karena itu, tujuan utama penelitian ini adalah untuk menyajikan pemahaman yang mendalam mengenai tantangan *Cyber Security Agency of Singapore* (CSA) dalam menjalankan *Cybersecurity Awareness Campaign* "*Better Cyber Safe than Sorry*" dalam upaya pencegahan ancaman *phishing* di Singapura.

1.8.1. Tipe Penelitian

Penelitian ini menggunakan pendekatan penelitian deskriptif. Penelitian deskriptif adalah suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran, atau suatu kelas peristiwa pada masa sekarang (Nazir, 2014). Tujuan penelitian deskriptif adalah untuk membuat deskripsi, gambaran, atau lukisan secara sistematis, faktual, dan akurat mengenai fakta-fakta, sifat serta hubungan

antar fenomena yang diselidiki (Sugiyono, 2013). Pendekatan deskriptif ini dipilih karena memungkinkan peneliti untuk mengeksplorasi kompleksitas dinamika kelembagaan dan kebijakan tanpa mengintervensi variabel-variabel yang diteliti. Melalui pendekatan deskriptif, penelitian ini dapat memetakan sejauh mana strategi CSA yang telah dibentuk mampu menjawab tantangan nyata di lapangan, serta mengungkap celah-celah struktural yang masih luput dari perhatian aktor kebijakan.

1.8.2. Situs Penelitian

Penelitian ini menggunakan situs penelitian sebagai sumber data dalam menjawab rumusan masalah, dengan fokus pada industri keuangan negara Singapura. Pengumpulan informasi dilakukan melalui data primer dan data sekunder yang relevan dan kredibel. Data primer diperoleh melalui penelusuran langsung pada situs resmi *Cyber Security Agency of Singapore* (CSA) dan wawancara dengan BSSN sebagai pihak yang menjadi penghubung dalam penyampaian informasi terkait koordinasi keamanan siber di tingkat regional, termasuk pelaksanaan kampanye literasi digital oleh *Cyber Security Agency of Singapore* (CSA). Data sekunder diperoleh melalui studi literatur dari berbagai sumber, termasuk jurnal ilmiah, laporan lembaga internasional, situs resmi pemerintah Singapura, laporan media berita, dokumen kebijakan, serta publikasi dari organisasi regional dan internasional yang berkaitan dengan keamanan siber. Secara khusus, penelitian ini merujuk pada laporan dari *Cyber Security Agency of Singapore* (CSA).

1.8.3. Subjek Penelitian

Subjek penelitian merupakan pihak, kelompok, atau institusi yang menjadi fokus utama dalam pengumpulan dan analisis data karena memiliki hubungan langsung dengan masalah yang diteliti. Dalam penelitian ini, subjek difokuskan pada satu aktor institusional, yaitu *Cyber Security Agency of Singapore* (CSA). Pemilihan CSA sebagai subjek didasarkan pada perannya sebagai lembaga utama dalam penanganan keamanan siber nasional Singapura, khususnya melalui implementasi program *Cybersecurity Awareness Campaign* dalam merespons meningkatnya ancaman *phishing* di Singapura. Dengan menjadikan institusi ini sebagai subjek, penelitian ini bertujuan untuk memahami bagaimana interaksi kebijakan nasional dapat membentuk ketahanan siber yang adaptif dalam menghadapi ancaman *phishing.*

1.8.4. Jenis Data

Penelitian ini menggunakan dua jenis data yaitu primer dan sekunder. Data primer merupakan data yang dikumpulkan secara langsung oleh peneliti di lapangan untuk menjawab pertanyaan penelitian. Sedangkan, data sekunder merupakan data yang telah dikumpulkan dan diolah oleh institusi lain, yang dapat dimanfaatkan kembali oleh peneliti untuk menjawab permasalahan yang berbeda (Kuncoro, 2003). Dalam penelitian ini, data primer diperoleh dari dokumen yang tersedia pada situs resmi *Cyber Security Agency of Singapore* (CSA) dan juga wawancara dengan BSSN sebagai pihak yang menjadi penghubung dalam penyampaian

informasi terkait koordinasi keamanan siber ke *Cyber Security Agency of Singapore* (CSA), sedangkan data sekunder diperoleh dari dokumen resmi dan laporan resmi, serta artikel ilmiah dan media yang kredibel. Penggabungan kedua tipe data dapat memperkaya keberagaman data dalam upaya penelitian ini.

1.8.5. Sumber Data

Sumber data untuk penelitian ini adalah data primer dan data sekunder. Data primer diperoleh dari penelusuran langsung pada situs resmi *Cyber Security Agency of Singapore* (CSA) dan wawancara derngan BSSN sebagai pihak yang menjadi penghubung dalam penyampaian informasi terkait koordinasi keamanan siber di tingkat regional, termasuk pelaksanaan kampanye literasi digital oleh *Cyber Security Agency of Singapore* (CSA), sedangkan data sekunder diperoleh dari berbagai dokumen resmi, buku, laporan lembaga, jurnal ilmiah, artikel ilmiah, serta media kredibel yang membahas kasus *phishing* di Singapura. Data-data tersebut dikumpulkan dari publikasi yang telah tersedia untuk memberikan gambaran yang komprehensif mengenai kebijakan dan langkah-langkah penanganan kasus *phishing* di wilayah tersebut. Semua data primer dan data sekunder yang telah dikumpulkan kemudian dianalisis secara kritis dan disajikan dalam bentuk narasi sebagai dasar untuk menjawab rumusan masalah penelitian ini.

1.8.6. Teknik Pengumpulan Data

Penelitian ini menggunakan teknik pengumpulan data studi kepustakaan dan wawancara. Studi kepustakaan merupakan metode pengumpulan data yang dilakukan dengan mengakses dan menelaah informasi dari sumber-sumber yang telah tersedia, seperti laporan, publikasi ilmiah, dokumen resmi, serta data yang diperoleh secara daring (Kumar, 2011). Selanjutnya teknik pengumpulan data melalui studi kepustakaaan dengan menggunakan data primer berupa dokumen resmi yang diperoleh langsung dari situs lembaga pemerintah, yaitu *Cyber Security Agency of Singapore* (CSA). Meskipun tidak dilakukan interaksi langsung dengan responden data tersebut tetap dapat dikategorikan sebagai data primer karena berasal langsung dari sumber utama yang mempublikasikan informasi tersebut secara resmi dan otoritatif. Selain itu, metode yang dipilih untuk pengumpulan yaitu melibatkan wawancara dengan narasumber terkait. Dengan memanfaatkan literatur dan data terkemuka yang ditemukan di sumber primer dan sekunder, penelitian ini dapat secara efektif melakukan perbandingan dan analisis terhadap kebijakan keamanan siber dalam menangani ancaman serangan siber, khususnya yang berkaitan dengan isu *phishing*.

1.8.7. Analisis dan Interpretasi Data

Analisis data dalam penelitian ini bersifat kualitatif. Analisis data kualitatif adalah proses kerja sistematis terhadap data yang telah dikumpulkan untuk menemukan pola, tema, dan makna mendalam dari

fenomena sosial atau kebijakan (Bogdan & Biklen, 2007). Data dianalisis melalui proses reduksi, klasifikasi, dan pengorganisasian agar dapat membangun pemahaman utuh terhadap permasalahan yang diteliti, yaitu kebijakan keamanan siber dalam upaya pencegahan ancaman *phishing*. Menurut Creswell, analisis kualitatif meliputi pengodean, pembangunan tema, serta pengaitan data dengan kerangka teori (Creswell, 2014). Sehingga dalam penelitian ini data primer dan sekunder dibandingkan dan dianalisis dalam konteks pendekatan *social engineering*, *cyber resilience dan human security.*

Interpretasi data dilakukan untuk menafsirkan makna dan pola yang muncul dari hasil analisis secara lebih mendalam. Interpretasi data adalah perumusan pemikiran yang menggambarkan penemuan dominan terkait fenomena yang sedang diteliti, dengan mengaitkannya pada konsep atau teori yang relevan (Bogdan & Biklen, 2007). Dalam penelitian ini, interpretasi diarahkan untuk memahami dinamika kebijakan dalam menghadapi kejahatan siber berbasis *phishing*, serta menghubungkan temuan empiris. Proses ini menjadi landasan dalam penarikan kesimpulan dan memberikan kontribusi bagi pengembangan studi Hubungan Internasional, terutama pada bidang keamanan non-tradisional.

1.8.8. Kualitas Data (*goodness criteria*)

Penelitian ini memiliki kualitas data (*goodness criteria)* yang terjaga dengan baik karena menggunakan sumber primer data sekunder yang kredibel dan relevan, berupa wawancara dengan narasumber terkait,

dokumen resmi, laporan, artikel ilmiah, serta publikasi dari lembaga yang berkompeten di bidang keamanan siber dan kerja sama kawasan. Penggunaan data primer dan sekunder yang valid dan terpercaya memungkinkan penelitian ini menghasilkan data empiris dan teoritis yang kuat dalam menganalisis kebijakan dalam menghadapi ancaman *phishing*. Selain itu, penelitian ini juga menerapkan teknik triangulasi data dengan membandingkan berbagai sumber primer dan sekunder, sehingga meningkatkan keakuratan, konsistensi, dan kedalaman analisis, yang sangat penting untuk memperkuat validitas temuan dalam kajian Hubungan Internasional dan keamanan non-tradisional. Dengan demikian, penelitian ini mencapai kualitas data empiris dan teoritis yang penting untuk menjelaskan beragam tantangan yang dihadapi individu, khususnya nasabah layanan keuangan digital, yang menjadikan mereka rentan menjadi korban serangan *phishing*.