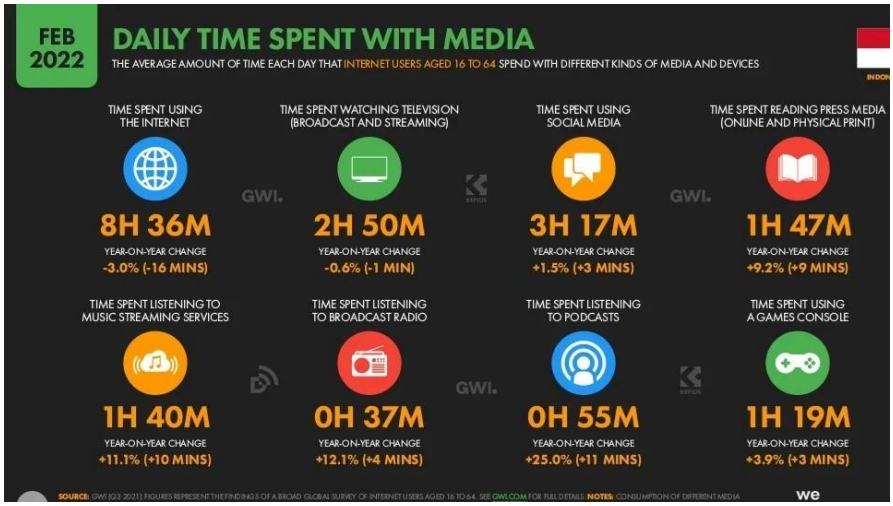
BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Internet sudah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari di seluruh dunia. Bahkan akses terhadap internet sudah merupakan sebuah komoditas yang harus dipenuhi oleh seluruh negara. Dengan akses dan jaringan internet yang sudah menjadi norma, media digital menjadi suatu hal yang terus muncul sebagai suatu bentuk konektivitas di dalam internet tersebut. Media digital sendiri adalah platform konten digital yang dapat ditransmisikan melalui internet atau jaringan komputer. Hal ini juga termasuk teks, audio, video, dan grafik. Ini berarti bahwa berita dari jaringan TV, surat kabar, majalah, dan media literasi lain yang disajikan di situs web atau blog dapat termasuk dalam kategori ini. Sebagian besar media digital didasarkan pada penerjemahan data analog menjadi data digital. Dengan berkembangnya media digital, media sosial juga menjadi salah satu hal yang menjadi suatu kepastian dalam kehidupan modern saat ini. Dimana orang-orang yang tidak menggunakan media sosial saat ini bahkan dianggap tidak praktis dan ketinggalan zaman. Hal ini kembali dibuktikan dengan peristiwa yang menyebabkan seluruh dunia untuk bertumpu kepada media sosial, yaitu pandemi Covid-19 pada tahun 2020. Pandemi Covid-19 membuat media sosial menjadi suatu cara pasti bagi orang-orang untuk berkomunikasi satu sama lain karena batasan pertemuan langsung yang diterapkan pada saat itu.

Indonesia sendiri tidak lepas dari penggunaan masif sosial media, bahkan sebelum pandemi Covid-19. Penggunaan Internet sebagai sumber utama informasi dan pengetahuan pun tidak terelakkan dengan adanya evolusi terhadap gaya hidup masyarakat Indonesia. Hal ini dibuktikan dengan konsumsi internet Indonesia yang



Gambar 1.1 Penggunaan Media Sehari-Hari Masyarakat Indonesia

Sumber: https://www.hootsuite.com/research/social-trends

cukup tinggi. Dimana berdasarkan gambar 1.1 milik Hotsuite 2022, sepertiga hidup netizen Indonesia, yakni 8 jam 36 menit, dihabiskan di layar Internet. Disusul dengan bermain media sosial selama 3 jam 17 menit, lalu menonton televisi, bermain game, dan yang paling sedikit waktunya adalah mendengarkan radio. Saat ini radio menjadi media yang paling sedikit jangkauannya.

Dengan konsumsi internet yang mencakup hampir seluruh bagian masyarakat di Indonesia, ancaman penyalahgunaan fungsi internet pun menjadi semakin nyata. Kejahatan dunia maya, yang memanfaatkan alat-alat digital seperti

komputer dan web, telah mencapai proporsi yang mengerikan. Pornografi, kejahatan komputer, dan bahkan terorisme digital, perang informasi, dan peretas semuanya merupakan dampak buruk yang mengerikan yang ditimbulkan oleh gelombang perkembangan konsumsi internet dan juga perkembangan teknologi. Selain itu, internet memunculkan aktivitas-aktivitas baru yang tidak dapat sepenuhnya diatur oleh peraturan perundang-undangan yang ada karena ciri-ciri internet yang tidak mengenal batas-batas geografis dan berfungsi sepenuhnya secara virtual (Widijowati, 2022). Dapat dikatakakan bahwa berkembangnya internet tidak hanya memberikan harapan baru, tetapi juga ketakutan baru.

Salah satu perkembangan penyalahgunaan intenrnet yang banyak digunakan sekarang adalah operasi pengaruh atau *influece operations*. Pemanfaatan Informasi sebagai alat yang digunakan dalam sebuah perseteruan sebenarnya sudah ada sejak pertama kali peradaban itu sendiri berdiri. namun, munculnya era informasi telah mengakibatkan penyebaran taktik, teknologi, dan ancaman secara eksponensial yang berkaitan dengan seni dan sains yang relatif baru yang disebut *Influence Operations*. Operasi pengaruh adalah upaya bersama yang dilakukan oleh suatu aktor, seperti negara atau kelompok teroris, untuk ikut campur dalam proses pembuatan makna oleh individu atau kelompok di luar kendali hukum mereka melalui alat dan fasilitas pada layanan media sosial yang tersedia untuk umum (Bergh, 2020). Hal ini dilakukan untuk berkontribusi terhadap timbulnya opini dan kesan yang menguntungkan pihak yang melakukan operasi pengaruh dan/atau tidak menguntungkan pihak lain.

Dengan sifat internet yang tidak memiliki batas-batas dalam penyebarannya, tentunya operasi pengaruh ini dapat secara langsung merambah ke Indonesia, baik itu operasi yang dilakukan oleh pihak lokal atau internasional. Secara praktis, operasi pengaruh hanyalah pengeluaran konten, baik otomatis atau manual, ke layanan media sosial. Namun, sama seperti serangan peretasan yang perlu menemukan mekanisme penyampaian yang sesuai, operasi pengaruh juga harus menyebarkan konten di forum yang relevan. Layanan media sosial yang berbeda memiliki karakteristik dan properti yang berbeda pula. Contoh media sosial menunjukkan bahwa blog memberikan interaksi yang lebih lama dan mendalam, umur konten yang lebih lama, namun lebih sedikit berbagi konten. Twitter, di sisi lain, memfasilitasi penyebaran yang cepat, postingan isu tunggal, lebih sedikit waktu untuk terlibat secara kritis dengan konten, dan umur konten yang pendek.

Operasi pengaruh juga dapat dilakukan secara manual, seperti me-retweet pesan Twitter atau menautkan ke berita, atau mungkin juga terotomatisasi. Algoritma adalah dimensi penting di semua media sosial. Sebagian besar situs berita dan media sosial mengandalkan algoritma ini untuk secara otomatis memilih konten yang dianggap relevan atau diinginkan oleh pengguna media sosial tersebut (Bergh, 2020). Faktor penting lainnya dari operasi pengaruh adalah bagaimana terdapat ketidakjelasan identitas pengirim dan konteks konten dari media sosial itu sendiri. Kemampuan untuk menganonimkan siapa yang berada di balik operasi pengaruh dari audiens target menyulitkan pengguna dan moderator untuk memblokir pengguna untuk menghindari berita palsu, misalnya. Yang lebih penting lagi, nama samaran memungkinkan mereka yang memposting konten untuk

mengklaim keahlian/pengetahuan yang tidak mereka miliki mengenai topik tertentu, atau, dengan menggunakan beberapa identitas online yang dipalsukan, mereka dapat membuat pernyataan pendukung untuk meningkatkan kepercayaan terhadap informasi yang disajikan (Bradshaw, 2020).

Gambar 1.2 Contoh Operasi Pengaruh Di Media Sosial Twitter

Sumber: Twitter

Mengenai konten, kurangnya konteks di media sosial berarti konten yang diposting oleh pengguna lain dapat dibingkai ulang. Hal ini dapat dilakukan melalui ketidakjujuran, sarkasme halus, atau dengan tidak merujuk pada konteks dunia nyata untuk membuat konten tersebut seolah-olah mendukung tujuan operator

pengaruh. Format seperti teks pendek, video, gambar, dan konten campura yang digunakan layanan media sosial juga berpengaruh. Misalnya, meningkatnya informasi visual berarti bahwa pihak yang menyerang dapat menghindari kebutuhan akan keterampilan berbahasa dan dapat membuat konten yang langsung menarik emosi sehingga mengabaikan pekerjaan/analisis kognitif apa pun (Bergh, 2020) misalnya gambar anak-anak sekarat atau hukuman mati yang tidak adil.

Gambar 1.3 Contoh Operasi Di Media Sosial Instagram

Sumber: Instagram

Contoh nyata dari operasi pengaruh yang terjadi di media sosial dapat dilihat melalui gambar 1.2 yang diambil peneliti dari media sosial Twitter. Tweet itu

sendiri mengindikasikan, melalui video dan pernyataan yang sudah di kirim, bahwa Islam merupakan agama yang buruk dan bagaimana Indonesia merupakan negara yang lebih baik sebelum terjadinya islamisasi. Kemudian contoh lain dapat dilihat melalui gambar 1.3 yang diambil peneliti dari media sosial Instagram. Konten ini sendiri mengindikasikan bahwa masyarakat Indonesia perlu menegakkan khilafah pada tahun 2024 yang disertakan dengan bukti video dan kutipan diluar konteks dari ustadz-ustadz yang mendukung pernyataan tersebut.

Efek yang dihasilkan dari operasi pengaruh ini sendiri memiliki banyak contoh yang berbahaya bagi keamanan nasional. Dimana operasi pengaruh ini dapat menyebabkan pergeseran keyakinan dan perilaku politik, meningkatnya sentimen xenofobia atau diskriminatif, dan meningkatnya skeptisisme dan ketidakpastian (Bateman et al., 2021). Di Indonesia sendiri ancaman nyata yang datang dari operasi pengaruh ini sendiri berhubungan dengan ekstremisme berbasis kekerasan yang mengarah pada terorisme. Contohnya yaitu dalam bidang rekrutmen dan pembangunan komunitas ekstremis berbasis kekerasan serta *lone wolf* terorisme yang datang dari ideologi ekstremisme. Hal ini juga didukung dengan sifat operasi pengaruh yang memfasilitasi tumbuhnya perilaku antisosial dan ilegal yang sebelumnya tidak terpikirkan (Bergh, 2020).

Indonesia sebagai suatu negara semestinya bertindak terkait ancaman nyata yang terus terjadi dari tahun ke tahun ini. Dalam studi Hubungan Internasional sendiri, sekuritisasi merupakan salah satu langkah yang dilakukan suatu negara apabila ingin mengatasi suatu isu yang mengancam eksistensi dari negara tersebut. Dimana dapat kita lihat bahwa ruang digital Indonesia masih belum aman dari

operasi pengaruh ekstremisme berbasis kekerasan yang mengarah pada terorisme. Dengan isu yang mengancam ini, peneliti tertarik untuk menganalisis apa upaya sekuritisasi yang dilakukan oleh pemerintah Indonesia dalam menanggulangi operasi pengaruh ekstremisme berbasis kekerasan yang mengarah pada terorisme.

Kemudian terkait perspektif yang digunakan oleh peneliti dalam isu operasi pengaruh ini, peneliti berupaya melihat sekuritisasi pemerintah Indonesia dari sisi keamanan siber sosial. Dimana untuk menghasilkan ruang digital yang aman dari ekstremisme berbasis kekerasan yang mengarah pada terorisme di Indonesia, keamanan siber sosial menawarkan aspek-aspek terkait apa yang dapat dilakukan dan teori-teori teknis dari operasi pengaruh yang dilakukan oleh berbagai entitas ini. Keamanan siber sosial ini sendiri merupakan suatu bentuk studi yang relatif baru sehingga dapat dipastikan akan memberikan perspektif baru terhadap isu operasi pengaruh yang sedang dihadapi Indonesia saat ini.

1.2 Rumusan Masalah

Internet merujuk pada Mark Zuckeberg pada pidatonya di Universitas Virginia (2015) adalah *the fifth estate* yang memungkinkan setiap penggunanya memiliki kuasa baru untuk memproduksi pesan dalam skala lebih besar. Pendek kata, teknologi baru ini menjadikan kuasa informasi tak lagi hanya milik elite dan media massa konvensional. Namun, penggunaan media sosial yang tinggi ini menyimpan riak yang dapat menjadi gelombang dari dalam. Media sosial adalah

ruang terbuka, sehingga siapapun dapat membagikan ide atau pemikirannya secara bebas, dan seringkali tanpa filter.

Boas Simanjuntak dari SAFENet yang juga aktivis pengamat isu terorisme juga melihat fenomena operasi penyebaran ideologi ekstremisme berbasis kekerasan yang mengarah pada terorisme di platform media sosial masih relevan dan perlu diperhatikan (Guritno & Rastika, 2021). baik penyebaran yang dilakukan secara terbuka, misalnya melalui Facebook dan Instagram, maupun secara inklusif melalui platform percakapan Telegram. Operasi pengaruh di ruang digital sendiri sebenarnya sudah ditandai sebagai permasalahan potensial seiring perkembangan teknologi digital sejak 2013. Dimana hal ini menunjukkan bahwa sudah lebih dari 10 tahun pemerintah Indonesia berhadapan dengan isu ini.

Komitmen pemerintah Indonesia sendiri dalam melindungi warganya dari operasi pengaruh ideologi ekstremisme berbasis kekerasan yang mengarah pada terorisme di ruang digital pun menjadi penting, karena jika operasi pengaruh ini dibiarkan berjalan ideologi-ideologi ini akan mempengaruhi masyarakat awam dan meningkatkan aktivitas-aktivitas terorisme seperti pembangunan komunitas, rekrutmen, dan bibit-bibit terorisme *lone wolf*. Dalam menanggulangi isu ini, keamanan siber sosial menjadi sebuah konsep yang sangat relevan. Selain karena keamanan sosial di ruang digital yang memang menjadi tujuan dari pemerintah Indonesia, keamanan siber sosial merupakan sebuah konsep yang sudah tidak asing lagi dengan operasi pengaruh serta manuver-manuver informasi yang terjadi di ruang digital.

Peneliti kemudian tertarik untuk mengkaji bagaimana upaya sekuritisasi pemerintah indonesia untuk menciptakan ruang digital yang aman dari ekstremisme berbasis kekerasan yang mengarah pada terorisme dengan menggunakan konsep keamanan siber sosial.

1.3 Tujuan Penelitian

Mengetahui dan mendeskripsikan upaya sekuritisasi pemerintah Indonesia untuk menciptakan ruang digital yang aman dari ekstremisme berbasis kekerasan yang mengarah pada terorisme dengan menggunakan konsep keamanan siber sosial.

1.4 Manfaat Penelitian

Penelitian ini diharapkan akan dapat memberikan manfaat penelitian :

1.4.1 Manfaat Akademis

Penelitian ini diharapkan mampu berkontribusi menambahkan konteks ke-Indonesiaan pada teori sekuritisasi dan konsep keamanan siber sosial tentang upaya pemerintah untuk menciptakan ruang digital yang aman dari ekstremisme berbasis kekerasan yang mengarah pada terorisme.

1.4.2 Manfaat Praktis

Penelitian ini diharapkan bermanfaat bagi para fasilitator dan pihak berwenang untuk menimalisir penyebaran ideologi ekstremisme berbasis kekerasan yang mengarah pada terorisme di ruang digital.

1.4.3 Manfaat Sosial

Penelitian ini diharapkan mampu berkontribusi untuk meningkatkan kesadaran masyarakat atas operasi pengaruh terkait ekstremisme berbasis kekerasan yang mengarah pada terorisme di Indonesia. Manfaat lainnya adalah untuk para peneliti teori dan konsep dalam hubungan internasional, dimana penelitian ini diharapkan dapat membantu memberikan peta permasalahan yang lebih jernih terkait upaya suatu pemerintah dalam melakukan sekuritisasi terhadap isu operasi pengaruh terkait ekstremisme berbasis kekerasan yang mengarah pada terorisme di ruang digital.

1.5 Kerangka Konsep

1.5.1 Tinjauan Pustaka

Dengan perhatian yang tinggi terhadap internet dan nilai-nilai ekstremisme berbasis kekerasan yang diwaspadai semua orang, terdapat beberapa penelitian yang membahas topik yang serupa.

Penelitian terkini pertama yang dirujuk adalah artikel jurnal milik Vyan Tashwirul Afkar dan Miftakhul Indi Mas'ud berjudul "Sekuritisasi Isu Radikalisme Islam di Indonesia Tahun 2014 - 2019" (2023). Penelitian ini sendiri berisi

membahas tentang langkah- langkah Pemerintah dalam membangun persepsi bahwa radikalisme adalah ancaman yang harus diselesaikan secara gawat darurat berdasarkan teori sekuritisasi Buzzan (1998). Penelitian ini sendiri menemukan bahwa Langkah sekuritisasi yang dilakukan oleh pemerintah Indonesia antara lain terlihat dari pernyataan Presiden, informasi BIN dan BNPT, kanal media kementerian dan lembaga, pembentukan BPIP, sampai pembubaran HTI (Afkar & Mas'ud, 2023). Walaupun begitu, penelitian ini menyimpulkan bahwa sekuritisasi yang dilakukan oleh pemerintah Indonesia ini tidak berhasil membangun keseragaman persepsi karena pemerintah tidak secara gamblang memberikan kriteria dan parameter kelompok radikal yang dimaksud sebagai ancaman eksistensial (Afkar & Mas'ud, 2023). Persamaan dari penelitian ini sendiri terletak pada topik yang diangkat oleh penulis mengenai bagaimana upaya sekuritisasi pemerintah Indonesia dalam menghadapi ekstremisme berbasis kekerasan. Perbedaan terletak pada bagaimana penelitian ini lebih fokus kepada sekuritisasi dari aksi ekstremisme itu sendiri dan bukan penyebaran ideologi ekstremisme di ruang digital.

Kemudian penelitian berikutnya adalah penelitian milik Ihsanul Religy Utami & Gonda Yumitro di tahun 2023, berjudul "Strategi Pemerintah Indonesia Dalam Mengatasi Pengaruh Ideologi Transnasional Radikal di Media Sosial" (2023). Jurnal ini berusaha meneliti bagaimana strategi pemerintah Indonesia dalam mengatasi pengaruh ideologi transnasional radikal di media sosial. Penelitian ini sendiri menemukan bahwa dalam mengatasi pengaruh ideologi transnasional radikal di media sosial, pemerintah Indonesia melakukan tiga strateg. Pertama,

Cyber Security Strategy sebagai upaya mengambil kebijakan, sebagai instrument, sebagai shock terapy, dan penyelesaian sengketa. Kemudian Strategi yang kedua yakni Strategi Edukasi dengan cara memberikan edukasi kepada publik akan bahaya radikalisme dengan konten positif maupun penyebaran narasi damai melalui media sosial. Lalu yang ketiga adalah Strategi Penegakan Hukum UU ITE NO 19 Tahun 2016 Atas Tindak Pidana radikalisme siber (Utami & Yumitro, 2023). Persamaan dari penelitian ini sendiri terletak pada topik penelitian yang sama-sama meneliti upaya pemerintah Indonesia dalam menghadapi isu radikalisme di media digital. Kemudian perbedaan terletak pada sumber dan spesifikasi dari penelitian ini, dimana penelitian ini dilakukan dengan cara mengumpulkan data dari berbagai sumber kredibel berbentuk jurnal, artikel ilmiah, surat kabar online, dan sumber kredibel lainnya dari situs terpercaya serta laman berita yang relevan dengan topik. Kemudian penelitian ini juga lebih fokus kepada strategi pemerintah Indonesia secara keseluruhan dalam menghadapi radikalisme di media digital.

Kemudian pada tahun 2022 lalu terdapat penelitian Yusep Ginanjar berjudul "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara" (2022). Jurnal ini sendiri bertujuan untuk mengetahui Tujuan dari penelitian ini adalah untuk mengetahui bagaimana strategi indonesia dalam membangun keamanan siber untuk menghadapi ancaman kejahatan siber melalui Badan Siber dan Sandi Negara. Penelitian ini sendiri menemukan bahwa BSSN dapat mewujudkan stabilitas keamanan nasional di ruang siber adalah dengan beberapa strategi berikut. Yang pertama yaitu penguatan pengamanan infrastruktur siber. Kedua yaitu

pembangunan dan penguatan Computer Emergency Response Team (CERT). Kemudian yang ketiga adalah pencegahan kejahatan siber dan peningkatan kerjasama internasional bidang siber. Lalu strategi keempat adalah penguatan kapasitas sumber daya manusia keamanan siber. Kemudian yang terakhir penyelesaian kejahatan siber melalui peningkatan *clearance rate* tindak pidana siber (Ginanjar, 2022). Persamaan dari penelitian ini sendiri terletak pada topik penelitian yang sama-sama meneliti upaya pemerintah Indonesia dalam isu keamanan siber Indonesia untuk menanggulangi radikalisme di media digital. Kemudian perbedaan terletak pada konsep dan teori dari penelitian ini, dimana penelitian ini menggunakan konsep diplomasi siber dan teori institusional. Penilitian ini juga lebih spesifik kepada strategi dari satu intansi pemerintah saja yaitu Badan Siber dan Sandi Negara.

1.5.2 Konsep

1.5.2.1 Sekuritisasi

Teori sekuritisasi pada studi hubungan Internasional sendiri diawali ketika perang dingin berakhir. Dimana hal tersebut memicu perdebatan mengenai gagasan keamanan. di satu sisi penganut teori-teori tradisional prihatin dengan keamanan negara dan sering kali berfokus pada analisis stabilitas militer dan politik. Di sisi lain, penganut teori-teori progresif berusaha memasukkan jenis ancaman lain yang tidak bersifat militer dan lebih berdampak pada masyarakat dibandingkan negara. Hal ini memperluas agenda keamanan dengan memasukkan konsep-konsep seperti keamanan manusia dan keamanan regional bersama dengan gagasan budaya dan identitas. Terlepas dari apakah seseorang setuju dengan pandangan tradisional atau progresif, akhir Perang Dingin menunjukkan bahwa keamanan pada dasarnya

merupakan konsep yang diperdebatkan saat itu. Dengan menunjuk pada sifat keamanan yang pada dasarnya diperdebatkan, pendekatan kritis terhadap keamanan berargumen bahwa "keamanan" tidak selalu bersifat positif atau universal, namun bergantung pada konteks dan subjek, dan bahkan terkadang bersifat negatif (Eroukhmanoff, 2018).

Teori sekuritisasi menunjukkan kepada kita bahwa kebijakan keamanan nasional bukanlah suatu hal yang alamiah, melainkan dirancang secara hati-hati oleh para politisi dan pengambil keputusan. Menurut teori sekuritisasi, isu-isu politik dianggap sebagai isu-isu keamanan ekstrem yang harus segera ditangani ketika isu-isu tersebut telah diberi label sebagai "berbahaya", "mengancam"', "mengkhawatirkan" dan sebagainya oleh aktor sekuritisasi yang memiliki kekuatan sosial dan institusional untuk memindahkan isu ini di luar ranah politik (Buzan et al., 1998). Jadi, permasalahan keamanan tidak hanya sekedar muncul namun harus diartikulasikan sebagai masalah oleh aktor-aktor yang melakukan sekuritisasi. Teori sekuritisasi menantang pendekatan tradisional terhadap keamanan di dalam studi hubungan internasional dan menegaskan bahwa isu-isu tersebut pada dasarnya tidak mengancam dengan sendirinya. sebaliknya, dengan menyebutnya sebagai masalah keamanan maka masalah tersebut menjadi masalah keamanan.

Penjelasan diatas menunjukkan pilihan peneliti untuk menggunakan teori sekuritisasi milik Barry Buzan, Ole waever dan Jaap De Wilde dari Mahzab Kopenhagen. Dimana Inti dari teori tersebut menunjukkan struktur retoris para pengambil keputusan ketika membingkai suatu isu dan berusaha meyakinkan khalayak untuk mengangkat isu tersebut di atas isu politik. Inilah yang kita sebut

dengan tindak tutur atau *speech act* (Buzan et al., 1998). Mengkonseptualisasikan sekuritisasi dalam bentuk *speech act* menjadi penting karena menunjukkan bahwa kata-kata tidak sekadar menggambarkan realitas, namun merupakan realitas, yang pada gilirannya memicu respons tertentu. Oleh karena itu, ancaman bukan sekedar ancaman secara alami, tetapi dikonstruksikan sebagai ancaman melalui bahasa.

Isu keamanan apa pun dapat disajikan dalam spektrum mulai dari yang tidak dipolitisasi (masalah tersebut belum menjadi perdebatan publik) hingga yang dipolitisasi (masalah tersebut telah menimbulkan kekhawatiran publik dan masuk dalam agenda) hingga sekuritisasi (masalah tersebut telah dibingkai sebagai ancaman eksistensial) (Filimon, 2016). Ketika suatu isu disekuritisasi, tindakan sering kali dilegitimasi dengan menggunakan bahasa yang bersifat mendesak dan ancaman yang ada, serta merupakan tindakan yang mungkin dianggap tidak demokratis dalam situasi normal.

Untuk menampilkan hipotesis keamanan sebagai speech act dan ancaman keamanan, Mahzab Kopenhagen menciptakan konsep "sekuritisasi". Dimana terkait konsep tersebut Wæver menyatakan bahwa "Tidak ada hal alam di luar sana yang menjadi ancaman keamanan dan lainnya yang tidak. Kita sebagai komunitas, secara politis, terkadang memilih untuk menangani berbagai hal dengan cara tertentu. Kami menamakan hal-hal tertentu sebagai "masalah keamanan" dan ketika kami melakukannya, sesuatu terjadi pada masalah tersebut dan interaksi kami di sekitarnya. [...] Hal ini di luar batas normal aturan politik. [...] Sekuritisasi adalah situasi di mana objek referensi menggambarkan ancaman eksistensial dan membenarkan penggunaan tindakan luar biasa bagi khalayak yang relevan"

(Filimon, 2016). Objek referensi disini atau *referent object* merupakan suatu objek (negara atau masyarakat) yang dipandang secara eksistensial terancam dan harus diamankan oleh aktor sekuritisasi (Buzan et al., 1998).

Sebagai alat penelitian, sekuritisasi memungkinkan seseorang untuk mengikuti contoh ketika suatu objek memasuki wilayah ancaman keamanan dan lebih jauh lagi, bergerak dari "bidang politik normal ke dalam wilayah politik darurat dimana hal tersebut dapat ditangani dengan cepat dan tanpa perlu peraturan dan regulasi pembuatan kebijakan yang normal (demokratis)" Dalam hal performativitas, Mahzab Kopenhagen mengusulkan pandangan tentang keamanan yang menjadi performatif melalui tindakan sekuritisasi dalam arti bahwa suatu isu menjadi sekuritisasi hanya ketika "aktor sekuritisasi yang memiliki kekuatan yang sesuai" mengidentifikasinya dan menyatakannya sebagai ancaman keamanan (Williams, 2008). Karena teori sekuritisasi berakar pada *speech act*, maka tindakan sekuritisasi bergantung pada kapasitas aktor sekuritisasi untuk menetapkan apa yang digambarkan oleh Williams sebagai "klaim yang efektif secara sosial tentang ancaman, melalui bentuk di mana klaim tersebut dapat dibuat untuk diakui dan diterima sebagai hal yang meyakinkan oleh audiens yang relevan" (Williams, 2008). Mengenai tindak tutur keamanan, Buzan, Wæver dan de Wilde berpendapat bahwa: "[...] tindak tutur keamanan tidak didefinisikan dengan mengucapkan kata keamanan. Yang penting adalah penunjukan ancaman nyata yang memerlukan tindakan darurat atau tindakan khusus dan penerimaan penunjukan tersebut oleh khalayak yang signifikan" (Buzan et al., 1998).

1.5.2.2 Keamanan Non-Tradisional

Dengan bentuk dunia global yang semakin terhubung satu sama lain, studi keamanan "non-tradisional" atau non-traditional security studies menjadi suatu pembicaraan yang hangat bagi para akademisi, pengamat keamanan, dan masyarakat umum di seluruh dunia. Secara tradisional, ancaman keamanan dilihat dari sudut pandang kelangsungan hidup negara dan dipahami terutama dalam konteks konflik militer antarnegara. Sementara keamanan non-tradisional yang sebagian besar bersifat transnasional, merupakan suatu jenis studi yang memperhatikan ancaman-ancaman seperti terorisme, degradasi lingkungan dan perubahan iklim, penyakit menular, kejahatan transnasional, dan migrasi ilegal. Ancaman ini sendiri dianggap melintasi batas negara dan beroperasi di luar lingkup tindakan negara konvensional yang tidak serta merta dianggap mengancam keberadaan negara secara langsung, namun menantang kapasitas nyata atau persepsi negara dalam melindungi masyarakat yang terdampak (Hameiri & Jones, 2013).

Jika kita melihat kembali kepada teori sekuritisasi, dalam sub-bidang studi Keamanan hubungan internasional, teori sekuritisasi mengacu pada kumpulan literatur yang beragam dan komprehensif. Kumpulan literatur ini pun mengalami banyak perkembangan pasca perang dingin. Perkembangan ini pada akhirnya menyebabkan perluasan teori yang melampaui studi sekuritisasi generasi pertama, dimana perluasan tersebut diwakili oleh Mazhab Kopenhagen atau Copenhagen School (Filimon, 2016). Pendekatan mereka sendiri tentunya dikembangkan dalam konteks seruan pasca-Perang Dingin, dengan tujuan memperluas definisi keamanan

yang berupaya memasukkan serangkaian permasalahan mendesak dan sampai sekarang terabaikan seperti perubahan lingkungan, kemiskinan dan hak asasi manusia ke dalam agenda keamanan negara. Mazhab Kopenhagen secara bersamaan berkontribusi pada seruan untuk memperluas konsep tersebut dan berupaya memberikan batasan analitis terhadap konsep tersebut. Penganutnya belum berupaya mengembangkan kerangka kerja mengenai bagaimana keamanan harus didefinisikan atau bagaimana aktor-aktor kunci harus melakukan pendekatan terhadap dinamika atau krisis keamanan eksternal. Sebaliknya, Mazhab Kopenhagen berfokus pada bagaimana keamanan itu sendiri diberi makna melalui proses intersubjektif dan dampak politik apa yang ditimbulkan oleh konstruksi keamanan tersebut (Williams, 2008).

Mazhab Kopenhagen umumnya dikaitkan dengan Copenhagen Peace Research Institute (COPRI), yang didirikan pada tahun 1985 oleh Parlemen Denmark (Filimon, 2016). Mahzab ini sendiri berpusat di sekitar karya Barry Buzan dan Ole Wæver. Sejak awal tahun 1990-an, berbagai penulis mengembangkan serangkaian pengamatan dan argumen tentang cara kerja keamanan di Eropa. Kerja kolaboratif ini mencapai puncaknya pada tahun 1998 dengan munculnya karya berjudul “Security: A New Framework for Analysis”, yang ditulis oleh Barry Buzan, Ole Wæver dan Jaap de Wilde (Buzan et al., 1998). Ciri utama dari aliran pemikiran ini adalah bagaimana aliran ini akan beroperasi dengan konsep keamanan yang dianggap dibangun secara sosial (dan dapat dibangun). Mazhab Kopenhagen sendiri memiliki objek studi tentang keamanan dan implikasinya terhadap kehidupan individu. Sebelum munculnya analisis Mazhab Kopenhagen,

aliran tradisional mempelajari keamanan utamanya dari sudut pandang militer, hal baru yang dibawa oleh para ahli teori aliran ini yaitu membagi analisis keamanan ke dalam berbagai dimensi. Hal ini diakui pada tahun 1991 di Roma ketika NATO secara resmi menetapkan bahwa keamanan, sesuai pengertian klasik Mahzab Kopenhagen, memiliki lima sektor: militer, politik, kemasyarakatan, ekonomi dan lingkungan hidup (Buzan et al., 1998). Mahzab Kopenhagen sendiri dan konsep-konsep sentralnya pun berkembang seiring berjalannya waktu dan bukan lagi sebagai proyek khusus untuk studi keamanan, melainkan sebagai serangkaian intervensi terhadap konsep dan kasus yang berbeda. Di sisi lain, dalam menanggapi tuduhan yang dilontarkan oleh kaum tradisionalis yang menyatakan bahwa model baru ini tidak koheren, perwakilan Mahzab Kopenhagen menawarkan metode operasional konstruktivis yang melibatkan penggabungan prinsip-prinsip tradisional sekaligus menghilangkan batasan artifisial antara model keamanan dan ekonomi serta mengusulkan cara-cara baru untuk mempelajari bidang-bidang kehidupan sosial yang saling terkait (Hartono, 2023). Pada aliran ini keamanan didefinisikan dengan bergantung pada persepsi ancaman yang nyata bagi keberadaan objek referensi yang sangat dihargai. Sumber ancaman itu sendiri dapat diidentifikasi dari negara-negara yang agresif, tren sosial yang negatif, atau keragaman budaya. Konsekuensinya, dalam konsepsi Mazhab Kopenhagen, ancaman dapat diwujudkan dalam berbagai konteks politik atau bidang kehidupan. Dalam Mahzab ini, Keamanan juga dipandang sebagai tindakan berbicara atau “act of speech” yang kompleks, khususnya dalam mengeksplorasi implikasi problematis terkait keamanan (Buzan et al., 1998). Aliran sekuritisasi ini memiliki keuntungan

dalam menghindari serangkaian masalah yang tidak diinginkan, yang bersifat politis, yang melibatkan beberapa masalah keamanan (jika dilihat dalam pandangan tradisional). Hal ini menghindari penyalahgunaan larangan pembicaraan sederhana tentang masalah keamanan untuk mengubahnya menjadi tujuan yang membutuhkan kesetiaan mutlak (Hartono, 2023).

1.5.2.3 *Social Cyber Security*

Keamanan siber sering kali diperlakukan sebagai masalah keamanan nasional karena respons terhadap serangan yang dilakukan oleh militer dan badan intelijen menciptakan ketergantungan yang menyebabkan ketegangan antara sektor swasta dan pemerintah terus berlanjut. Di banyak negara badan militer dan intelijen mempunyai peran penting dalam keamanan siber. Pendekatan keamanan siber yang dipimpin oleh militer dan badan intelijen tersebar luas dan memiliki beberapa konsekuensi negatif dalam menghadapi ancaman keamanan siber (Burton & Lain, 2020). Keamanan nasional di abad ke-21 sendiri memerlukan investasi dalam keamanan siber sosial yang memadai dalam melibatkan penelitian dasar mengenai interaksi manusia antara teknologi dan perilaku serta keyakinan sosial (K. Carley & Beskow, 2019). Burton dan Lain (2020) mengatasi permasalahan ini dengan mengusulkan pergerakan menuju pendekatan teori dan kebijakan siber berbasis keamanan sosial. Mereka berargumen bahwa konsep keamanan masyarakat, yang pertama kali muncul setelah Perang Dingin, lebih cocok secara teoritis untuk masalah keamanan siber dibandingkan model keamanan nasional tradisional, dan bahwa sebagian besar aktivitas siber berbahaya selama dekade terakhir, termasuk spionase siber, pemaksaan dunia maya, perang dunia maya dan informasi, serta

subversi media sosial, telah menjadi sasaran, dan disebabkan oleh, ketegangan masyarakat (Burton & Lain, 2020).

Pada masa dimana internet menjadi suatu komoditas, keyakinan, opini, dan sikap terbentuk saat orang berinteraksi dengan orang lain melalui media sosial. Informasi dari sumber-sumber berita terpercaya dan temuan-temuan dari ilmu pengetahuan selalu ditantang oleh para aktor yang secara aktif terlibat dalam praktik keilmuan di internet. Baik individu dan mesin propaganda besar, keduanya mengganggu wacana sipil, menimbulkan perselisihan, dan menyebarkan disinformasi. Bot, cyborg, troll, sock-puppets, deep fakes, dan meme hanyalah beberapa dari teknologi yang digunakan dalam rekayasa sosial yang bertujuan untuk melemahkan masyarakat sipil dan mendukung agenda permusuhan atau bisnis (K. M. Carley, 2020). Dengan perkembangan yang pesat dari internet sekarang, saat ini para ilmuwan dari berbagai disiplin ilmu bekerja secara kolaboratif untuk mengembangkan alat dan teori-teori baru. Dimana pengembangan yang dilakukan telah mendorong munculnya bidang ilmu baru yaitu keamanan siber sosial.

Keamanan siber sosial merupakan sebuah bidang ilmiah dan rekayasa baru yang datang dari ilmu sosial komputasi dengan pengaruh besar di bidang penelitian terapan. Temuan dan metode dari ilmu ini relevan bagi pembuat kebijakan, akademisi, dan perusahaan. Keamanan siber sosial menggunakan teknik ilmu sosial komputasi untuk mengidentifikasi, melawan, dan mengukur (atau menilai) dampak tujuan komunikasi. Metode dan temuan di bidang ini juga sangat relevan bagi praktik komunikasi, jurnalisme, dan diplomasi siber (Goolsby, 2020). Keamanan

siber sosial juga dibangun berdasarkan analisis jaringan berdimensi tinggi, ilmu data, pembelajaran mesin, pemrosesan bahasa alami, dan simulasi berbasis agen (K. M. Carley, 2020). Dalam aplikasinya Keamanan siber sosial digunakan untuk memberikan bukti tentang siapa yang memanipulasi media sosial dan internet demi tujuan spesifik, metode apa yang digunakan, dan bagaimana metode manipulasi sosial ini dapat dilawan.

Dengan keamanan siber sosial sebagai bidang yang berkembang dari berbagai sektor ilmiah. Di dalam bidangnya sendiri, terdapat tujuh bidang penelitian inti.

1. *Social Cyber Forensics*: Forensik siber sosial berkaitan dengan identifikasi siapa yang melakukan serangan keamanan siber sosial (K. M. Carley, 2020). Seringkali yang menjadi perhatian adalah pada tipe faktornya dan bukan pada pelaku spesifiknya. Lebih lanjut, hal ini dapat melibatkan penilaian lintas platform dengan kebutuhan untuk melacak sumber informasi. Diperlukan cara-cara baru untuk melacak dan membangun hubungan dalam skala besar.

2. *Information Maneuvers*: Kuncinya di sini adalah memahami strategi yang digunakan untuk melakukan serangan dan maksud dari strategi tersebut (K. M. Carley, 2020). Diperlukan peningkatan kemampuan untuk mendeteksi manuver, dan memberikan peringatan dini bahwa serangan akan dimulai, khususnya lintas platform.

3. *Motive Identification*: Tujuannya di sini adalah untuk memahami apa motif pelakunya. Mengapa serangan itu dilakukan? Berbagai macam motif telah terlihat. Hal ini termasuk melakukan kampanye pengaruh: untuk bersenang-senang, untuk menciptakan kekacauan, untuk mempolarisasi masyarakat, untuk mengurangi kebosanan, demi uang, untuk

mempolarisasi masyarakat, untuk memasarkan barang atau jasa, untuk mendapatkan pengaruh pribadi, dan untuk membangun komunitas (K. M. Carley, 2020). Dimana tentunya banyak kemungkinan ada alasan lain juga.

4. *Diffusion*: Dalam bidang ini tujuannya adalah untuk menelusuri, dan bahkan memprediksi, penyebaran kampanye pengaruh (K. M. Carley, 2020). Dimana melacak penyerang dan menganalisis dampak serangan di berbagai media sosial adalah hal utama yang ingin dicapai.

5. *Effectiveness of Information Campaigns*: Tujuan dari bidang ini adalah untuk mengukur efektivitas serangan keamanan siber sosial, dimana hal ini mencakup dampak jangka pendek dan jangka panjang. Hal ini juga melibatkan pembuatan ukuran dampak yang lebih baik – seperti polarisasi atau histeria massal – bukan hanya ukuran jangkauan tradisional seperti jumlah pengikut, jumlah suka, dan rekomendasi (K. M. Carley, 2020).

6. *Mitigation*: Ada dua tujuan yang terkait di sini. Pertama adalah memahami bagaimana serangan keamanan siber sosial dapat dilawan atau dimitigasi dan yang kedua adalah memahami bagaimana masyarakat bisa menjadi lebih tahan terhadap serangan (K. Carley & Beskow, 2019). Banyak jalur penelitian berbeda yang dapat dilakukan di sini. Beberapa contohnya adalah penggunaan model berbasis agen untuk menilai dampak intervensi yang relevan, teknik terukur untuk mengajarkan pemikiran kritis di media sosial, dan penelitian dasar tentang karakteristik komunitas yang berketahanan (K. M. Carley, 2020).

7. *Governance*: Tujuannya adalah untuk memahami kebijakan dan undang-undang apa yang diperlukan agar masyarakat dapat terus menggunakan internet tanpa takut akan pengaruh yang tidak semestinya, sehingga demokrasi yang terinformasi dapat bertahan (K. M. Carley, 2020).

1.6 Operasionalisasi Konsep

1.6.1 Sekuritisasi

Argumen utama teori sekuritisasi adalah bahwa dalam hubungan internasional suatu isu menjadi isu keamanan bukan karena sesuatu tersebut merupakan ancaman obyektif terhadap negara (atau *referent object* lainnya), namun karena aktor telah mendefinisikan sesuatu sebagai ancaman eksistensial atau *existential threat* terhadap kelangsungan hidup suatu objek. Dengan melakukan hal tersebut, aktor telah mengklaim hak untuk menangani masalah tersebut melalui cara yang luar biasa atau *extraordinary measures* untuk menjamin kelangsungan hidup *referent object*. Oleh karena itu, keamanan merupakan praktik referensial mandiri: sebuah isu menjadi sebuah isu keamanan hanya jika diberi label sebagai sebuah isu. Namun, fakta bahwa keamanan merupakan konstruksi sosial dan intersubjektif tidak berarti bahwa segala sesuatu dapat dengan mudah diamankan. Agar berhasil melakukan sekuritisasi suatu isu, aktor sekuritisasi harus melakukan tindakan sekuritisasi (menghadirkan sesuatu sebagai *existential threat* terhadap *referent object*) yang harus diterima oleh audiens yang ditargetkan. Hanya dengan mendapatkan penerimaan dari masyarakat, permasalahan ini dapat dipindahkan ke ranah politik normal, sehingga memungkinkan para elit untuk melanggar prosedur dan aturan normal serta menerapkan tindakan darurat.

1.6.2 Keamanan non-tradisional

Isu keamanan non-tradisional adalah tantangan terhadap kehidupan dan kesejahteraan masyarakat serta negara yang muncul dari sumber-sumber non-

militer, seperti perubahan iklim, penyakit menular, kelangkaan sumber daya, bencana alam, isu migrasi, kekurangan pangan, penyelundupan manusia, dan kejahatan transnasional. Bahaya-bahaya ini sering kali bersifat transnasional, tidak dapat diatasi secara sepihak dan memerlukan respons yang komprehensif bahkan penggunaan kekuatan militer. Dalam skripsi ini peneliti akan menggunakan konsep keamanan non-tradisional berdasarkan Mahzab Kopenhagen. Mahzab ini merupakan sebuah pendekatan dalam studi keamanan yang berupaya untuk menerapkan pemahaman yang lebih luas tentang konsep keamanan. Berbeda dengan pendekatan tradisional yang didasarkan pada pertimbangan material dan menggunakan kerangka penelitian positivis, dengan lebih memilih model penjelasan, Mahzab Kopenhagen menambahkan dan beroperasi dengan isu-isu keamanan non-tradisional, di samping isu-isu keamanan yang lebih tradisional. Dimana isu-isu tersebut terbagi dalam lima sektor:

1. Sektor militer
2. Sektor ekonomi
3. Sektor Politik
4. Sektor sosial
5. Sektor lingkungan

1.6.3 *Social Cyber Security*

Keamanan siber sosial merupakan suatu bidang ilmiah yang berbeda dengan keamanan siber. Keamanan siber berfokus pada mesin, dan bagaimana komputer dan database dapat dinegosiasikan. Dalam perbedaannya, keamanan siber sosial berfokus pada manusia dan bagaimana manusia dapat dikompromikan, diubah, dan didegradasi ke hal-hal yang tidak penting. Dimana pakar keamanan siber

diharapkan memahami teknologi, ilmu komputer, dan teknik; pakar keamanan siber sosial diharapkan memahami komunikasi sosial dan pembangunan komunitas, statistik, jaringan sosial, dan pembelajaran mesin (Muller & Burrell, 2022). Pada konsep ini peneliti akan menggunakan konsep dasar-dasar dari keamanan sober sosial menurut Carley (2020) yang dibagi menjadi 7 bagian yaitu:

1. *Social Cyber Forensics*
2. *Information Maneuvers*
3. *Motive Identification*
4. *Diffusion*
5. *Effectiveness of Information Campaigns*
6. *Mitigation*
7. *Governance*

1.7 Asumsi Penelitian

Negara semestinya menjamin hak digital warga negara, khususnya hak mendapatkan perlindungan dari konten-konten negatif termasuk operasi pengaruh di ruang digital yang masuk dalam bentuk narasi intoleransi. Namun dengan semakin massif dan terbukanya platform media sosial, seperti instagram, twitter, dan tik tok menunjukkan bahwa pemerintah masih perlu meningkatkan keamanan siber sosial di Indonesia. Oleh karena itu peneliti berargumen bahwa pemerintah Indonesia sudah melakukan upaya sekuritisasi yang sesuai dengan konsep keamanan siber sosial, walaupun hasil yang didapat masih belum maksimal. Hal ini terbukti dengan masih banyaknya jaringan terorisme dan kejadian terorisme *lone*

wolf yang merupakan hasil dari operasi pengaruh terkait ekstremisme berbasis kekerasan yang mengarah pada terorisme di ruang digital Indonesia.

1.8 Metode Penelitian

1.8.1 Tipe Penelitian

Penelitian "Upaya Sekuritisasi Pemerintah Indonesia Untuk Menciptakan Ruang Digital Yang Aman Dari Ekstremisme Berbasis Kekerasan Yang Mengarah Pada Terorisme Dengan Menggunakan Konsep Keamanan Siber Sosial" ini dilakukan dengan menggunakan perspektif penelitian kualitatif. Penelitian dengan perspektif kualitatif menempatkan peneliti sebagai individu yang sarat nilai, dimana nilai-nilai tersebut mendasari keseluruhan proses penelitian, sejak dari perumusan masalah, tujuan penelitian, sampai pada metode yang digunakan (Alhasbi, 2023).

Penelitian ini sendiri akan melihat bagaimana upaya sekuritisasi yang dilakukan pemerintah dalam membangun ruang digital yang aman dari ekstremisme berbasis kekerasan yang mengarah pada terorisme.Metode analisis yang dilakukan adalah analisis deskriptif-eksploratif.

1.8.2 Subjek Penelitian

Subjek Penelitian dalam hal ini adalah lembaga negara yang terlibat dalam upaya sekuritisasi dalam membangun ruang digital yang aman dari ekstremisme berbasis kekerasan yang mengarah pada terorisme, yakni dari sisi legislatif dan eksekutif serta penegakan hukum, seperti DPR, Kominfo, Kementerian Pertahanan, BSSN, BNPT, Polri dan TNI.

1.8.3 Sumber Data

1.8.3.1 Sumber Data Primer

Sumber data primer dari penelitian ini adalah hasil dari wawancara mendalam dengan seluruh stakeholder terkait pembangunan ruang digital yang aman, khususnya dalam menangani operasi pengaruh terkait ekstremisme berbasis kekerasan yang mengarah pada terorisme. Adapun sumber informasi yang diharapkan adalah perwakilan pemerintah dari pihak eksekutif, legislatif dan yudikatif. Hal ini diperlukan agar dapat memberikan pemahaman komprehensif tentang upaya sekuritisasi yang dilakukan oleh pemerintyah Indonesia.

1.8.3.2 Sumber Data Sekunder

Sumber data sekunder dari penelitian ini adalah studi kepustakaan, buku-buku, dokumen, dan gambar-gambar terkait isu ekstremisme berbasis kekerasan yang mengarah pada terorisme dan ruang digital.

1.8.4 Teknik Pengumpulan Data

1.8.4.1 Wawancara Mendalam

Wawancara mendalam ditujukan untuk menggali informasi terkait upaya strategis apa yang dilakukan seperti program, pedoman, kerjasama internasional dan arsitektur keamanan siber, dalam hal ini DPR diwakili oleh Komisi 1, Kominfo diwakili Dirjen Aptika, Kementerian Pertahanan pada divisi Pusat Pertahanan Siber, BSSN pada divisi Direktorat Keamanan Siber dan Sandi, BNPT pada divisi

Direktorat Penindakan, Polri pada divisi Dittipid Siber dan Densus 88-AT dan TNI dalam divisi Satuan Siber.

1.8.4.2 Observasi

Observasi dilakukan dengan mengamati *event* pemerintah terkait pembangunan ruang digital yang aman dari ekstremisme berbasis kekerasan yang mengarah pada terorisme di Indonesia seperti Rapat Antar Kementerian, Rapat Pembahasan Rencana Aksi Nasional, dan Kampanye Duta Damai.

1.8.4.3 Studi Pustaka

Studi Pustaka dilakukan dengan mengkaji penelitian terdahulu yang relevan dan dokumen-dokumen yang dapat menjelaskan upaya negara dalam menjaga ruang digital dari ideologi ekstremis berbasis kekerasan yang mengarah pada terorisme, seperti Undang-Undang, Peraturan Pemerintah dan Peraturan Presiden dan Keputusan Menteri yang relevan.

1.8.4.4 Analisis dan Interpretasi Data

Metode analisis yang digunakan adalah metode analisis kualitatif, yakni bertujuan tidak hanya membongkar pesan-pesan yang eksplisit tapi juga sekaligus pesan implisit dari data-data yang didapatkan. Dengan menggunakan analisis isi kualitatif, diharapkan dapat mengkaji upaya dan arsitektur pemerintah Indonesia dalam membangun ruang digital yang aman dari ekstremisme berbasis kekerasan yang mengarah pada terorisme. Adapun tahapan penelitian adalah dengan melakukan

kategorisasi, mengklasifikasi data yang tersedia, melakukan wawancara, dan melakukan analisis secara kualitatif

1.8.5 Kualitas Data

Untuk uji keabsahan data dalam penelitian ini, peneliti menggunakan uji kredibilitas (validitas internal) dan dependability (reliabilitas). Uji kredibilitas data dilakukan melalui diskusi ilmiah dengan pakar dan rekan peneliti. Untuk menjamin reliabilitas peneliti juga melakukan uji dependability (reliabilitas) kategori dengan cara melakukan audit (pemeriksaan) terhadap keseluruhan proses penelitian. Akan ada pihak lain yang menjadi audit keseluruhan aktivitas penelitian dan penilaian peneliti dalam mengkaji upaya pemerintah dalam menyiapkan keamanan siber dalam menghadapi radikalisme di media digital.