BAB I

PENDAHULUAN

1.1.Latar Belakang Masalah

Penulis akan memfokuskan wacana diskursus terkait kebijakan pemerintah dalam menanggulangi kejahatan siber di Indonesia. Kejahatan siber merupakan salah satu kejahatan yang bersifat digital serta tidak terhalang oleh batas-batas negara dan waktu seluruh *region* di dunia. Kejahatan siber yang terpaut dengan seluruh "*illegal activites*" dan merupakan bentuk dari insinkronisasi implementasi dari adanya keamanan nasional yang harus diterapkan di Indonesia. Dengan adanya fenomena prevalensi/ perilaku masyarakat yang terbiasa dalam menggunakan teknologi digital, maka menjadi celah penujuman atau dengan kata lain celah-celah sugesti untuk para pelaku kejahatan siber dalam mengakses identitas target kejahatan siber tersebut. Terlebih lagi dengan banyak fakta masyarakat modern secara terbuka menyebarluaskan bentuk-bentuk aktivitas sehari hari di sosial media.

Kejahatan siber tidak terhalang oleh batas-batas negara dan waktu seluruh *region* di dunia. Penanganan kejahatan siber notabenenya merupakan hak pemegang kendali keamanan di Indonesia. Pihak pengendali keamanan menemukan beberapa kedok yang dilakukan oleh pelaku kejahatan siber. Pengatasnamaan penegak hukum menjadi sasaran identitas palsu kejahatan siber contohnya polisi, jaksa dan pegawai di badan perpajakan negara. Berbagai tipu muslihat oleh pelaku kejahatan siber telah dipersiapkan dengan matang seperti membuat akun *bank* untuk akses penerimaan arus keuangan (Carvalho et al., 2020). Hasil pemerasan dan penipuan sebagai lembaga penegak hukum dan ultimatum akan dikelola di dalam rekening *bank*. Hal tersebut adalah contoh dari kejahatan siber yang akan meluas menjadi kejahatan terorisme jika penegakan regulasi tidak diterapkan secara maksimal di Indonesia.

Mekanisme pengelolaan jejaring kejahatan siber dapat terhubung dengan adanya koneksi tak terhingga bahkan dari satu benua ke benua lainnya. Jangkauan tak terbatas oleh pelaku kejahatan siber dengan istilah *internet protocol*. Kumpulan jejaring internet dari berbagai belahan dunia membentuk sistem yang dikendalikan oleh para pelaku kejahatan siber dalam naungan *internet protocol*. Namun, perkembangan zaman mendobrak celah-celah geologis

untuk saling memberi manfaat dalam banyak bidang (Ebert, 2020). Beragam kebutuhan dasar manusia seperti kebutuhan sehari-hari dapat terpenuhi dengan akses internet dan piranti komputer. Para petinggi negara juga mampu menjalin kerjasama dengan berbagai negara di dunia dengan adanya kemajuan internet. Koneksi tersebut dapat memberi *insight* perbandingan dalam perimbangan pembuatan kebijakan yang akan diterapkan. Selain itu, pemanfaatan oleh pihak swasta dalam mengembangkan investasi jarak global menambah pendapatan investasi dalam negeri dengan devisa untuk APBN di Indonesia. Jejaring informasi memudahkan akademisi dan ilmuwan yang pakem di berbagai bidang dalam meluapkan pengetahuan yang tersebar dari berbagai portofolio jenjang Pendidikan (Ünal, 2020).

Dalam beberapa penelitian yang terkait dengan kejahatan dunia siber tidak secara rinci menjelaskan tata kelola regulasi kejahatan siber. Ranah kejahatan siber sebagai tindakan preventif pemerintah mengatasi masalah kejahatan siber tidak terlalu diperdalam pembahasannya oleh penelitian sebelumnya. Tindakan utama sebagai tolok ukur pemerintah dalam mengentaskan kejahatan siber haruslah berkembang seiringan dengan kemajuan zaman. Tolok ukur tersebut menjadi bahan implementasi hukum dalam mengentaskan kejahatan siber dan pemantauan kasus-kasus kejahatan siber di Indonesia**.**

Kejahatan siber sangat berkorelasi erat dengan adanya keamanan di dunia virtual. Keamanan siber di dunia virtual haruslah selalu mengalami perkembangan sistem keamanan sehingga dapat menangkal adanya kebocoran sistem keamanan digital. Kejahatan siber yang menyerang jagat maya tanpa terkecuali menghadirkan *insight/*kesadaran para pemangku kebijakan setiap negara untuk berkontribusi mencegah kejahatan siber dapat berujung pada terorisme siber secara universal. Kesadaran tersebut mengarah kepada konsentrasi tema keamanan internasional dalam pertemuan ASEANAPOL ke-23 di Filipina yang turut mengikutsertakan kepolisian Indonesia. Ranah pembahasan keamanan siber yang termaktub dalam kejahatan siber menjadi permasalahan serius yang harus ditanggulangi untuk mencegah adanya keberlangsungan kasus terorisme siber.

Kesadaran pemerintah selaku pemangku kebijakan di seluruh negara-negara di dunia menyadari bahwa kecenderungan untuk tidak dapat membendung seluruh kejahatan siber yang dapat memata-matai kinerja komputer di berbagai bidang. Selain itu, adanya penghilangan jaringan kompuer, pemindahan data yang tidak disertai izin legal dan mengakses komputer untuk kepentingan tertentu mendorong pemerintahan Indonesia untuk mengesahkan sebuah regulasi.

Satu dari rentetan regulasi terkait dengan kejahatan siber yaitu UU No. 11 tahun 2008 terkait dengan ITE (*UU No. 11 Tentang Informasi Dan Transaksi Elektronik*, 2008). Eksistensi dari sebuah regulasi di suatu negara berguna untuk menyelaraskan sikap preventif negara dan saling berkontribusi aktif dengan negara lain dalam membentuk jejaring keamanan internasional.

Adanya regulasi sebagai bentuk upaya pemerintah di berbagai negara menjadikan beberapa instrumen kenegaraan dalam mencegah adanya kejahatan siber, yaitu adanya aksi nyata dari sebuah regulasi yang diadakan oleh beberapa negara (Cotteleer et al., 2021). Negara tersebut adalah Amerika Serikat yang menyebut aksi ketahanan keamanan virual yaitu *Federal Legislation: Update April United States Code*, negara Malaysia yang ikut serta dengan mengadakan *Computer Crime Act*, dan juga Australia dengan tema *The Cyber Crime Act.*

1.2.Rumusan Masalah

Penulis menjabarkan perumusan masalah seperti berikut ini;

1) "Mengapa kebijakan pemerintah Indonesia dalam menghadapi ancaman kejahatan siber belum efektif?"

1.3.Tujuan Riset

Penulis merangkum tujuan penelitan yang ada dalam tesis ini berupa;

1) Mendalami proses *cyber crime* yang terjadi di Indonesia;
2) Mendalami berbagai tindakan solutif yang digagas oleh pemerintah sebagai upaya untuk menanggulangi *cyber crime* yang ada di Indonesia.

1.4.Kontribusi Riset

Penulis menerapkan kontribusi riset yang ada dalam tesis yaitu;

a. Dalam ranah akademis riset yang penulis perdalam akan memperkaya horizon pengetahuan akademisi baik untuk mahasiswa yang mendalami pakem bidang ilmu lainnya dan terkhusus mahasiswa Hubungan Internasional;
b. Dalam ranah praktis riset yang penulis perdalam diharapkan mampu menjadi bahan perimbangan untuk para pembuat regulasi terkait dengan penanggulangan serta pencegahan atas kasus-kasus kejahatan siber
   yang ada di Indonesia.

1.5.Tinjauan Pustaka

Penulis mencoba mengklasifikasi beberapa penelitian sebelumnya terkait dengan tema yang bersangkutan dengan kejahatan siber. Di sisi lain, penulis menelaah titik perbedaan konkret sebagai faktor yang mengakibatkan kejahatan siber terus berlanjut jika regulasi di kubu pemerintahan Indonesia tidak efektif (Ramadhan, 2020). Dalam buku yang ditulis oleh Maskun "Kejahatan siber (*cyber crime)*" menyertakan rententan permasalahan kejahatan siber berdasarkan *timeline* atau kronologi kejahatan siber. Buku tersebut juga mengulik dengan sistematis perihal faktor-faktor yang mengacu pada terjadinya rantai kejahatan siber yang tak kunjung bisa musnah (Maskun, 2013).

Dasar regulasi yang penulis cermati di dalam buku ini sangatlah *fundament.* Tindakan preventif untuk menindak kejahatan siber yang ada di Indonesia pada tahun 2008 yaitu UU ITE (Undang-undang Informasi dan teknologi). Dalam regulasi tersebut memuat hal-hal mendasar yang diakui secara internasional dengan melampirkan "*Transnational Dimension Cyber Crime*". Regulasi yang fundamen dan krusial merupakan acuan negara di dunia sebagai acuan konvensi hukum untuk mengatasi kejahatan siber/ *cyber law of cyber crime.* Negara di seluruh dunia berupaya secara hukum dengan segelintir aturan-aturan mengikat yang berpengaruh terhadap kelangsungan keamanan di seluruh dunia. Masyarakat internasional tidak hanya berhadapan dengan kejahatan yang bersifat konkret, namun juga turut berkecimpung sebagai korban dalam ranah para penjahat digital atau penjahat siber (Setiawan, 2020).

Penulis juga menyertakan penelitian komprehensif tindakan kriminalisasi kejahatan siber yang memiliki karakteristik tertentu. Ada strategi yang berguna untuk memberantas kejahatan siber dalam penelitian bertajuk "Memerangi *cyber crime* / Karakteristik, Motivasi dan Strategi Penanganan dalam perspektif Kriminologi" (Widodo, 2015). Penelitian tersebut mengeksplisitkan analisis berdasarkan perspektif dunia kriminologi. Widodo mendeskripsikan bahwa refleksi pemahaman aspek kriminologis bersifat bukti konkret dan motif yang mendasari pelaku kejahatan siber dalam terorisme siber (Widodo, 2015). Simplifikasi tindakan koneksitas penyelesaian kejahatan siber memerlukan kontribusi pihak yuridis dalam menangani perkara kejahatan siber.

Kejahatan siber merupakan serangkaian kejahatan yang tidak bisa diungkap dengan metode pendataan kasus kejahatan regular. Kejahatan regular seperti yang terjadi di sekitar kehidupan manusia seperti perampokan, pembunuhan invidual maupun pembunuhan masal serta

pencurian yang sifatnya konkret (Dlamini & Mbambo, 2019). Jejaring barang bukti yang tidak hanya bisa diungkap dengan hasil visum atau barang bukti berupa barang memerlukan pelacakan alamat *IP Adreess.* Alamat digital membantu pelacak kejahatan siber untuk memblokir/*hack* jejaring kejahatan siber. Jejak rekam yang telah dilakukan oleh pelaku kejahatan siber dapat terekam secara detail dan presisi sehingga bukti *valid* kasus kejahatan siber dapat ditemukan.

Selain alamat surel yang berifat digital, pelacak kejahatan siber menyertakan bukti *devices* untuk dapat dilacak di kemudian hari. Penyelidikan yang berhasil dilakukan oleh pelacak kejahatan siber akan menghubungkan *smartphone*/gawai milik pelaku dengan komputer. Multifaset/beraneka segi alasan yang dipergunakan oleh kejahatan siber berupa modus operandi. Modus operandi yaitu kejahatan yang dilaksanakan oleh perorangan atau memiliki korelasi dengan sindikat siber lainnya. Penyelidikan kasus yang sifatnya sporadis, yang bermakna bahwa pihak pelacak mendapati bahwa penjahat siber melakukan *dual identity* yaitu identitas ganda bahkan lebih dalam berbagai bukti perangkat dalam menjalankan kasus kejahatan siber tersebut.

Terdapat banyak retropeksi/kilas balik perihal berbagai motif kejahatan siber yang interkoneksi di satu bidang dan bidang lainnya. Motif yang berupa kasus SARA yang sedang meruyak, membombardir kultus individu seseorang yaitu untuk dicemarkan, adanya kompetifitas dalam perpolitikan perekonomian yang menimbulkan kejahatan siber. Beberapa motif tersebut saling menjatuhkan sehingga mengakibatkan tindakan saling balas dendam antar berbagai pihak. Penelitian lain yang bertajuk "Internet dan Terorisme: Menguatnya Aksi Global *Cyber-Terrorism* melalui *New Media*" oleh Sarinastiti mengungkapkan pendiversifikasian antara media yang berkutat pada perkembangan teknologi masa kini serta propaganda kejahatan siber dalam menyajikan berita yang bersifat komersialisasi. Seperti halnya tindakan preseden/tindakan yang telah menjadi kronologi peristiwa kejahatan siber ini menjadikan beberapa pola kejahatan siber seperti:

1. Kenihilan dari tindakan kekerasan atau ancaman eksesif bukan merupakan kejahatan siber. Hal tersebut serupa dengan pemberontakan masal seperti lonjakan pajak serta *peace demonstration* dalam bentuk demonstrasi digital untuk mendulang kuantitas masa tidaklah dikungkungkan sebagai kejahatan siber.
2. Konsep apriori dasar pelaku kejahatan siber menyeruakkan psikologi masyarakat dengan propaganda kegelisahan untuk melancarkan aksi kejahatan siber terkait tujuan tertentu secara

digital.

3. Tema-tema perpolitikan seperti rezim pemerintahan yang akan digulingkan, tidak tercapainya keputusan suara dalam narasi eksplisit/diskusi terbuka untuk kebijakan sosial/perpolitikan menghadirkan wacana kejahatan siber sebagai solusi terbaik untuk mencapai tujuan oleh oknum berkepentingan.

Kejahatan digital yang tidak terjangkau batas adalah cara yang paling memungkinkan untuk kelancaran aksi kejahatan siber. Penyebaran dari kejahatan siber yang ada di dunia digital meruyak ke dalam media elektronik seperti halnya radio ataupun televisi. Namun, penggunaan *new media* yang bisa berupa audiovisual serta tulisan dapat menjadi cara untuk para pelaku kejahatan siber dalam menyebarluaskan dokumentasi video. Media tersebut berupa propaganda *online game*, media sosial, *website*, serta majalah *online*.

Penelitian lain terkait dengan kejahatan siber yaitu Terorisme dan *Cyberspace*: Fenomena *Cyber-Terrorism* sebagai Kejahatan Transnasional oleh Maskun (Kadir et al., 2019). Keamanan negara atas kejahatan internasional tidak dapat tercapai jika tidak terdapat keadaaan kontemplatif/kondusif dengan kriteria kejahatan seperti :

1. Korupsi

   Fenomena korupsi yang marak terjadi di Indonesia menjadi aspirasi publik dari penggiat anti korupsi dunia digital dan menghasilkan "Gerakan aktivis anti-korupsi". Masyarakat yang menjadi sasaran kejahatan digital memperkokoh konsolidasi organisasi aktivis anti korupsi (*ICMLG 2017 5th International Conference on Management Leadership and Governance*, 2017). Advokasi perlindungan terhadap gerakan siber ini juga merupakan tindakan preventif untuk mencegah adanya aksi yang semakin merajalela di Indonesia. Penyuaraan pemenuhan hak asasi di era modern seperti saat ini mencakup adanya hak asasi dalam lini digital. Oleh karenanya, pemenuhan hak keselamatan fisik maupun mental para aktivis dalam menyuarakan anti korupsi sangat diprioritaskan. Upaya "*public opinion control*" yang menjadikan negara sebagai aktor utama kejahatan siber menghasilkan *digital authorities*. *Digital Authorities* yakni berupa kontrol pemerintah terhadap kebijakan atas suara rakyat yang diberikan kepada pihak-pihak tertentu dalam ranah represi digital. Represi digital yang ditandai dengan kungkuggan untuk tidak beraspirasi secara transparansi, padahal transparansi sangat dibutuhkan untuk

menguatkan jejaring benteng keamanan siber antara pemerintah dan masyarakat luas (*Times* Indonesia, 2022)

Ketimpang tindihan pemenuhan hak asasi digital merupakan kebalikan dari pengimplikasian UU KPK No. 19 tahun 2019 (*Undang-Undang Republik Indonesia Nomor 19 Tahun 2019*). Undang-undang tersebut menerapkan ketegasan pemberantasan korupsi yang dikaitkan dengan adanya kemudahan akses bagi para koruptor mengikuti perkembangan digital yang mumpuni. Penyelewengan kemajuan digital berkedok kejahatan siber mampu membungkam suara pihak-pihak penyuara kebenaran (Kurnia, 2021). Pegiat anti terorisme siber di komunitas akademisi turut merespon kebijakan pemerintah yang tidak menampakkan kefektifan regulasi yang terkait dengan kejahatan siber apalagi di era serba digital seperti saat ini (Wijayanto et al., 2021).

2. Kejahatan lingkungan

Kejahatan siber kerap menyangkut partisipasi aktif yang menitikberatkan kepada istilah "*neighborhood watch group*". Organisasi tersebut bekerja sama mengawasi kejahatan siber di Indonesia. Penerapan asas kekeluargaan yang menjadikan solidaritas masyarakat yang kuat sehingga tidak menyisikan celah bagi taktik modus operandi pelaku kejahatan siber untuk mengakses data-data masyarakat (Moneva et al., 2022). Data personal seperti *chat room* yang berisikan data pribadi dapat menjadi celah untuk para pelaku kejahatan siber. *Chat Room* menjadi medium kejahatan siber yang meruyak, apalagi terkait dengan informasi yang berkaitan dengan pemerintahan stabilitas keamanan negara untuk diretas demi merusak lingkungan keamanan negara (Bambang & Fitriana, 2009).

Implikasi dari kejahatan siber adalah fasilitas *google earth* dan *google map* yang digunakan dalam menyebarluaskan aksi teror. Bentuk teror berupa teror fisikal maupun teror digital yang akan mengarahkan aksi kejahatan menuju ruang lingkup teror fisikal. Fenomena kemajuan teknologi tentunya seperti pisau bermata dua, yaitu kedua sisinya memiliki keunggulan dan kelemahan yang bersamaan terjadi. Dengan kata lain, dua sisi berkebalikan tersebut adalah "paradoks kemajuan teknologi". Pelaku kejahatan siber mengakses data-data privasi target secara mudah dan tidak dikenakan tarif. Adanya keleluasaan penyalahgunaan data pribadi tidak memiliki hambatan untuk menyebarluaskan aktifitas sehari-hari. Stigma masyarakat modern yang selalu

menyebarluaskan aktivitas sehari-hari seperti foto dan video yang memperlihatkan anggota keluarga secara utuh. Selain itu, data-data pribadi seperti data kependudukan, aset, rumah, pekerjaan secara detail dapat dikumpulkan dan menjadi sasaran empuk pelaku kejahatan siber (Barrio, 2022).

Pelaku kejahatan siber melalui akun-akun pribadi menyebarluaskan video-video bertajuk kekerasan sebagai usaha untuk "*brainwash*". Upaya *brainswash* tersebut yang menjadikan dogma masyarakat untuk terbiasa melihat aksi yang memuat kekerasan dalam *video broadcast*. Tindakan reaksionar tersebut juga bertujuan agar masyarakat luas menangkap hal tersebut sebagai komprehensifitas cara kerja kejahatan siber yang pada akhirnya akan menjadi sorotan banyak pihak.

Seluruh rangkaian kegiatan kejahatan siber sifatnya dikategorikan sebagai kegiatan yang *counter productive*. Kegiatan tersebut mengacuhkan norma kehidupan sosial seperti pengenkripsian *file-file* rahasia kegiatan kejahatan siber dapat disebarkan melalui email milik target para teroris siber. Kejahatan siber yang berdampak kepada lingkungan masyarakat mengandung pola dalam jejaring internet seperti:

1. *Dissemination Pattern* (Pola Diseminasi) yaitu pola tindakan kejahatan siber yang menitikberatkan bombardir rasa ketakutan dan kegelisahan yang ada di masyarakat melalui diversifikasi atau ragam kecanggihan media di internet.
2. *Threat and Violence Pattern* (Pola Ancaman dan Kekerasan) yakni pola tindakan kejahatan siber yang menggunakan piranti/alat persenjataan bersifat fisik untuk menambah riuh keadaan kejahatan siber yang sifatnya digital.
3. *Real Time Pattern* (Pola Kejadian Terkini) yaitu pola pelaksanaan untuk mengawasi pengendalian aksi kejahatan siber yang harus terjamin keberhasilannya dikarenakan serangkaian kegiatan siber merupakan konsorsio/ hasil pembiayaan banyak pihak dalam mewujudkannya.

Multifaset upaya pelaku kejahatan siber untuk menunjukkan eksistensi kejahatan siber merupakan *incoming alert* untuk seluruh lapisan masyarakat dalam menghadapi gelombang kejahatan siber. Para pelaku kejahatan siber merangkai pelatihan kejahatan secara digital atau *online terrorism recruitment* seperti halnya pembuatan bom yang harus dipandu oleh para pelaku terorisme siber. Sumber pemasukan dalam kegiatan yang pelaku terorisme siber lakukan adalah dalam bentuk mata uang elektronik. Mata uang

eletronik seperti *bitcoin* yang saat ini sedang marak dipergunakan menjadi mata uang digital di seluruh dunia. Kejahatan siber tidak hanya berkedok politik saja, namun terselip juga agenda memporak-porandakan keamanan negara berbasis Islam dengan "*cyber jihad*".

Pratinjau penegak hukum di Indonesia diperlukan dalam upaya menegaskan regulasi *cyber operation* yang berakhir pada *cyber attack*. Terdapat juga tindakan *cyber surveillance* yaitu pengawasan kegiatan operasi kejahatan siber yang menggiring adanya penyerangan siber. *Cyber Counter Crime* yang merupakan upaya menginvestigasi kegiatan kejahatan siber yang sesuai dengan *rule of law* di Indonesia. Aktor negara yang menangani kasus kejahatan siber yaitu BIN (Badan Intelijen Negara), Polri (Kepolisian Republik Indonesia), TNI (Tentara Nasional Indonesia) serta BNPT (Badan Nasional Penanggulangan Terorisme). Upaya investigasi kejahatan siber akan bermuara dengan dilanjutkannya tindakan pemblokiran situs kejahatan siber oleh Kemenkominfo (Kementerian Komunikasi dan Informatika).

Tindakan sigap atau *straight forward* dalam kejahatan siber haruslah diterapkan karena kejahatan siber tidak dapat diketahui secara pasti tempat pelaksanaannya. Di sisi lain, proses bagaimana pelaku kejahatan siber dalam melancarkan aksinya, dan waktu pelaksanaan rencana yang juga tidak dapat diprediksi. Teknik yang diimplikasikan oleh para sindikat kejahatan siber adalah dengan menerapkan sistem *dead drop*. Teknik tersebut menyembunyikan identitas teroris siber seperti menyebarkan *chat* sesama pelaku kejahatan siber untuk melancarkan serangan siber. (Kementerian Komunikasi dan Informatika, 2021b).

3. Terorisme Siber

Dalam buku "Media Sosial sebagai Strategi Perekrutan Terorisme di Indonesia" penulis memahami aspek psikologis yang mendukung adanya perilaku kejahatan siber. Aspek psikologis masyarakat yang terdampak oleh kejahatan siber yang harus diperhatikan seperti pemenuhan hak kesejahteraan, kebahagiaan dan rasa tenang pada masyarakat (Yunos & Hafidz, 2011). Medium dari perilaku kejahatan siber yang dilancarkan seperti penyebarluasan propaganda yang dilakukan tidak terpaku oleh batas-batas wilayah. Medium seperti konten yang ada di majalah, kaset, buku, dan video di media sosial dan aplikasi perpesanan yaitu *WhatsApp, Instagram, Facebook,* dan *Twitter*.

Pelaku kejahatan siber tidak membuang-buang tempo untuk menyebarkan postingan negatif dalam perekrutan anggota kejahatan siber. Pengoptimalan ruang gerak oleh para kejahatan siber di *social media* diibaratkan seperti sebuah *echo room* (Nadjib & Cangara, 2017). *Echo room* disebut ruang bergema sebagai pola ekstrimisme dalam perekrutan calon anggota pelaku kejahatan siber. Tujuan teroris siber adalah mencapai perekrutan jumlah teroris siber yang maksimal.

Penulis menelaah bahwa terkait dengan adanya pengaruh terhadap keadaan psikologi yang ada di masyarakat luas menjadi sasasran empuk bagi para pelaku siber. Istilah yang kerap dikaitkan dengan adanya pengaruh untuk mendominasi cara pikir yang disebut juga dengan "*brainwashing"*. *Brainwashing* yang mengaitkan segala unsur kebencian berkaitan dengan penegakan hukum seperti hukum Islam yang terbelenggu, postingan yang beredar luas di *social media* masyarakat, pendoktrinan kekerasan yang berbalut ideologi, dan spekulasi negatif untuk menghujat penggunaan produk yang dihasilkan oleh negara-negara Barat melalui *social media* masyarakat berkedok keagamaan (Rajawat, 2022).

Medium kejahatan siber melancarkan stigma "*De-Culturated*" yaitu cara kejahatan siber untuk mengembangkan Islam dengan paradigma Islam yang patuh terhadap aturan beragama maupun hidup bermasyarakat dengan nuansa kedamaian. Hal tersebut dapat digambarkan lewat situs Islam yaitu *www.salafipublications.com.* Situs tersebut menghubungkan calon pelaku kejahatan siber bertukar pengalaman tanpa mengenal batas waktu dan jarak. Hal tersebut akan mengarahkan pemikiran untuk mendobrak aturan Islam di Indonesia. Peran berbagai negara yang juga mendominasi pemikiran kejahatan siber dari berbagai negara dari penjuru dunia (Saleem et al., 2022).

Para perekrut generasi pelaku kejahatan siber menargetkan usia-usia transisi untuk dapat bergabung lebih mudah. Kondisi psikologi di masa remaja yang sangat rentan juga menjadi faktor dalam memfilter berbagai informasi. Banyak informasi yang memiliki tujuan terselubung oleh para pelaku kejahatan siber. Daya serap dan adaptasi remaja pada masa-masa transisi lebih mudah untuk menerima hal-hal yang sifatnya radikal dan kontradiktif. Remaja yang terjebak tindakan kontroversial dan radikal berada pada masa pengenalan adaptasi pemikiran yaitu dikenal dengan "*cognitive opening*". Pada masa *cognitive opening* tentunya remaja akan lebih riskan menerima semua

paradigma yang seakan-akan merupakan gerakan mendobrak yang penuh dengan perubahan suatu tatanan (Pratama & Bamatraf, 2021). Namun, hal tersebut merupakan fatamorgana keyakinan yang mengarah pada kekerasan dan bahkan perekrutan kejahatan siber. Dengan demikian, termaktub di dalamnya sejumlah gebrakan wacana baru dalam mengikuti perkembangan zaman untuk bergerak aktif secara digital.

Perekrut pelaku kejahatan siber mendalami trik-trik yang disertai fundamen mendasar pada ranah emosional calon rekrutmen. Ranah emosional seperti rasa ketidakpuasan terhadap ekspektasi kehidupan yang ditandai dengan rasa mudah tersulut emosi atas keadaan sekitar. Dengan keadaan psikologi sosial yang sedemikian rupa, sangat mudah untuk para rekruter kejahatan siber untuk melancarkan aksi propaganda. Aksi propaganda yang dilakukan seperti menyalahkan kinerja pemerintah yang tidak sesuai dengan ekspektasi pelaku kejahatan siber dengan mengatasnamakan kepentingan bersama (Arab, 2020).

Pada dasarnya, tidak semua kinerja program pemerintah dapat memenuhi ekspektasi masyarakat yang ada di suatu negara. Hal tersebut dikarenakan kendala seperti keterbatasan jangkauan pemerintah, contohnya dalam ranah otonomi daerah di bawah pimpinan regional. Dengan keadaan geologi negara yang luas, pemerintah juga memerlukan kemaksimalan pemenuhan sarana-prasarana dan saling sinergi dalam pembangunan negara dengan jejaring perangkat hukum serta pemangku kebijakan lainnya. Asas pengubahan pemenuhan keinginan untuk mengubah tatanan negara dengan falsafah hukum kemajemukan dengan sistem pemerintahan terpusat secara syariat Islam adalah salah satu kedok keagamaan oleh pelaku *cyber crime* dalam perwujudan kejahatan siber (Cahyani & Agustin, 2020).

4. Pembajakan Pesawat

Penjahat yang menjalankan aksi untuk memiliki hasil rampasan berupa uang *cash* lazimnya diproyeksikan dengan cara yang marak dilakukan seperti halnya menipu target dengan kepalsuan kepemilikan surat berharga, menculik ataupun merampok target yang dilakukan beriringan hingga mencuri kendaraaan baik beroda dua maupun lebih. Deretan kejahatan lainnya seperti kartu kredit yang menjadi celah untuk kebanyakan masyarakat dan menjadi animo masyarakat luas untuk tertarik memilikinya merupakan celah

kejahatan siber. Hal tersebut menyebabkan motif kejahatan siber yang semakin beraneka ragam sehingga pelaku kejahatan memiliki banyak modus penipuan. Hal serupa juga terjadi dalam kasus DVD bajakan yang melingkupi pengatasnamaan kekayaan intelektual seseorang atau agensi tertentu (Paterson, 2022).

Sejalan dengan adanya arus teknologi yang semakin erat dengan kehidupan manusia, memunculkan celah untuk kejahatan yang semakin luas di bidang siber. Dalam bidang pembajakan udara juga melibatkan pelaku aksi teror bajak udara yang melakukan aksinya sesuai dengan perkembangan pembajakan digital yang menggantikan pembajakan fisik di udara. Terdapat banyak cara yang dilakukan untuk meruntuhkan kinerja pesawat dengan cara *fly by wire* (Schneier, 2003). Hal pertama yang dilakukan oleh para peretas kejahatan siber via kontrol pernavigasian dengan memutarbalikkan arah pesawat hingga menuju arah yang tidak sesuai dengan landasan pacu terbang pesawat. Teknologi *cyber* menggunakan komunikasi dan interaksi tanpa batas. Kontrol yang didominasi dengan sistem *fly by wire* menjadikan sistem kejahatan peretasan yang dilakukan melalui sistem pernavigasian. Arah pernavigasian yang menjadi kontrol pesawat akan disesuaikan oleh kehendak peretas siber. Fenomena kejahatan ini merupakan pertanda menggunakan medium komunikasi siber (Gurtov et al., 2018).

Terdapat pendalamaan pengunaan komunikasi siber dalam indoktrinasi siber yang diimplementasikan oleh jejaring teroris ISIS atau dengan kata lain (*Islamic State of Iraq and Syria*). Destinasi utama ISIS yang terus dipropagandakan berada di Suriah terus menggaungkan metode komunikasi siber untuk saling bermigrasi menyerang titik-titik lemah target region yaitu salah satunya dengan adanya *illegal fundraising*. *Illegal fundraising* merupakan salah satu teknik yang digunakan untuk melancarkan propaganda kejahatan siber (Kim et al., 2019). Peningkatan propaganda kejahatan siber tersebut bisa meruyak ke dalam jenis *cyber crime* lainnya dan terproyeksikan ke dalam *cyber terrorism*. Adanya ketidakstabilan sekuritisasi yang ada di suatu tatanan kenegaraan juga dapat mempengaruhi keamanan suatu negara terlebih lagi dalam keamanan siber.

5. *Cyber Narcoterrorism*

Stabilitas keamanan yang ada di negara Indonesia haruslah diawasi dengan serangkaian pasukan penjaga keamanan teritorial maupun digital . Pasukan (Pérez, 2022)pertahanan yang menjadi garda terdepan di Indonesia yaitu Tentara Nasional Indonesia. Hal tersebut dikarenakan adanya penyebaran dari kejahatan siber yang tidak hanya berkutat pada keamanan teritorial kenegaraan. Hilir dari penyebaran kejahatan siber tersebut akan berdampak padas ketidakamanan Indonesia secara menyeluruh (Chaidar, 2017). Kebijakan yang ada di dalam rangkaian tata perundang-undangan tentang penyalahgunaan obat-obatan terlarang juga merupakan bentuk dari tindakan solutif sekaligus tindakan preventif dari pemerintah terkait dengan kejahatan siber di bidang obat-obatan terlarang (M. C. Ünal, 2019). Regulasi tersebut akan menjadi langkah preventif untuk mengintimidasi para pelaku kejahatan siber dalam melakukan penyebaran kejahatan siber. Sistematika dari regulasi tersebut berdampak pada tindakan penegasan untuk perwujudan pasal-pasal terkait (Björnehed, 2006).

Segelintir usaha yang dipacu oleh para pelaku kejahatan siber dalam obat-obatan terlarang mengandung banyak upaya kekerasan didalamnya (Gaffney, 2018). Hal tersebut d ilakukan karena banyaknya keuntungan yang didapatkan oleh para sindikat narkoba untuk meraup keuntungan dengan terus bergulirnya profit narkotika yang notabenenya diperlukan oleh banyak pihak di dunia (Reeves, 2013). Tujuan lain dari aktifitas ilegal tersebut untuk membiayai operasional teroris siber. Pendanaan yang dilakukan melalui bisnis terlarang ini akan menjadikan tingkat perekrutan yang dibutuhkan dalam jejaring narkotika akan menjadi ter-*update* (Aggrawal, 2015). Pendanaan yang sangat mendukung akan terus membuat kemampuan operasional teroris siber dalam hal narkotika menjadi mumpuni (Ken-dror Feldman & Gross, 2020).

6. Perdagangan Organ Tubuh

Regulasi yang menanggulangi kasus perdangangan organ tubuh termaktub dalam Persatuan Bangsa-bangsa Pasal 6 (c). Regulasi tersebut berisikan “Kejahatan yang dilakukan terhadap kemanusiaan dapat dianggap seperti tindakan yang dikategorikan

sebagai kejahatan dalam rangka kegiatan deportasi (pengasingan dan pengiriman penduduk ke negara asal), perbudakan, dan pembunuhan. Tindakan yang menyalahi hukum terhadap penduduk sipil baik dalam jangka waktu penganiayaan maupun peperangan disertai dengan alasan keagamaan, rasial serta adanya ketegangan politik yang diselenggarakan oleh mahkamah yuridikasi" (Cherry, 2017). Berdasarkan hukum yang telah disepakati oleh masyarakat internasional, maka dapat ditarik konklusi bahwa praktik perdagangan terhadap organ merupakan wujud dari tindakan eksploitasi yang tidak berkeperimanusiaan. Pihak-pihak yang turut andil dalam memberikan akses untuk perdagangan organ tubuh manusia juga merupakan bagian dari pihak yang melakukan perbuatan *illegal* (Paminto, 2017).

7. Pencurian Kekayaan Intelektual

Fundamen dari regulasi pengambilan hak atas kekayaan intelektual milik seseorang termaktub dalam Pasal No. 19 UU tahun 2016 terkait Transaksi Elektronik dan Informasi. Bunyi dari Undang-Undang tersebut adalah sebagai berikut : "*Dokumen yang sifatnya elektronik dan Informasi Elektronik dipatenkan sebagai kekayaan intelektual baik yang tersebar di Internet maupun secara fisik merupakan Hak Kekayaan Intelektual berkaitan dengan Peraturan Perundang-undangan*". Regulasi tersebut menaungi hak atas cipta karya yang tentunya sudah diakui keabsahannya dalam daftar kepemilikan kekayaan intelektual. Terkait dengan adanya pelanggaran oleh pencaplokan hak milik, dijatuhi pasal sebagai tindakan pembobolan oleh *electronic system* meskipun tidak tercantum dengan detail penjatuhan hukuman di pasal tersebut (Cotteleer et al., 2021). Pembajakan kekayaan intelektual adalah seperti *internet piracy* yang terdiri dari *carding*, *hacking*, dan *cracking* (Nations, 2000).

Tabel 1. Studi Pustaka

No	Penelitian Terdahulu	Temuan Penelitian
1	Maskun, 2013 Judul Buku: Kejahatan	Penelitian dalam buku ini menelaah titik perbedaan signifikan terpaut dengan

	siber *(cyber crime)*	pengaruh regulasi yang bersifat konkret terkait dengan kejahatan siber. Signifikansi tersebut dapat menjadi tolok ukur apakah faktor efisiensi regulasi memegang pengaruh yang sangat besar terkait dengan kasus kejahatan siber. Dalam buku ini terdapat rententan permasalahan kejahatan siber berdasarkan *timeline* atau kronologi kejahatan siber. Kronologi kasus tersebut sangatlah diperlukan karena regulasi yang seharusnya mampu mencegah adanya rentetan kejadian serupa haruslah teratasi terkait dengan kejahatan siber.
2	Abraham D. Sofaer, Gregory D. Grove, George Wilson, 2001 Judul Buku: *Draft International convention to Enhance Protection from Cyber Crime and Terrorism*	Buku ini mengangkat wacana tentang infrastruktur teknologi yang telah menjadikan keamanan teknologi semakin rentan. Kerentanan adanya informasi yang berkembang begitu pesat akan mempengaruhi banyaknya kegagalan menjaga keamanan data sehingga menimbulkan banyak kerugian di banyak

		bidang. Beberapa bidang yang terkena imbas adalah di bidang infrastruktur akibat adanya pemblokiran oleh para peretas dan berujung pada peledakan. Pada bidang krusial lainnya, seperti adanya perekonomian yang merosot turun dalam bidang peningkatan pendapatan dikarenakan adanya kejahatan siber yang sifatnya digital sehingga para pemblokir dapat meretas situs kementerian vital yang ada di negara seperti kementerian keuangan, kementerian keamanan dan kementerian perdagangan.
3	Widodo, 2015 Judul: Memerangi *cyber crime* / Karakteristik, Motivasi dan Strategi Penanganan dalam Perspektif Kriminologi	Penelitian yang disadur dalam buku ini melampirkan adanya komprehensitifitas dari kejahatan siber yang memiliki karakteristik tertentu. Komprehensifitas tersebut harus dibarengi dengan strategi yang melibatkan adanya analisis berdasarkan ruang lingkup khusus untuk mengatasi kejahatan siber, yaitu dari sudut pandang kriminologi. Meskipun para

		kriminolog mampu memberikan sudut pandang terkait dengan adanya penyelesaian masalah kejahatan siber, tentu diperlukan kontribusi aktif dari pihak yuridis untuk saling bersinergi membentuk jejaring keamanan digital. Hal tersebut sangat diperlukan karena kejahatan siber bukanlah sama halnya dengan kasus kejahatan reguler.
4	Sarinastiti, 2017 Judul: Internet Dan Terorisme Menguatnya Aksi Global *Cyber-Terrorism* melalui *New Media*	Penulis mendalami penelitian terkait dengan kejahatan siber yang menyatakan adanya diversifikasi media dan perkembangan teknologi yang berkaitan erat dengan kejahatan digital seperti kejahatan siber. Adanya penyajian berita yang sifatnya menguntungkan secara komersial mampu menjadi bahan perimbangan para teroris siber untuk menyuplai dana kegiatan terorisme siber dengan beberapa pola. Pola-pola kegiatan yang tidak mengandung kekerasan bukan

		berarti tidak memiliki keterkaitan dengan kejahatan siber. Adanya media seperti *peace demonstration* menjadi bahan kajian untuk ditelaah apakah ada indikasi pergolakan di balik tindakan yang notabenenya tidak menimbulkan aksi kekerasan. Kemudian berlanjut dengan pola lainnya yang terkait, teroris tidak luput dari memporak-porandakan sisi psikologis masyarakat di suatu negara untuk merasa tidak *secure* hingga adanya sikap menyalahkan pihak pemerintah untuk tidak bisa menangani kasus kejahatan siber.
5	Kadir, 2019 Judul: Terorisme dan *Cyberspace*: Fenomena *Cyber-Terrorism* sebagai Kejahatan Transnasional	Penelitian ini merujuk pada keberhasilan suatu negara untuk mencapai adanya keamanan yang stabil menangani kejahatan internasional. Beberapa kriteria kejahatan yang saling berkaitan erat dengan adanya kejahatan siber merupakan fenomena yang tidak boleh dielakkan untuk ditinjau regulasi keamanannya yaitu: korupsi,

		kejahatan lingkungan, pembajakan pesawat. Selain itu, juga terdapat beberapa kejahatan yang bisa menjadi landasan pemerintah untuk terus memperbarui regulasi untuk menampik bahaya dari kejahatan siber dalam hal sumber pendanaan dari perdagangan organ tubuh serta adanya pencurian kekayaan intelektual.

1.6. Kerangka Teori

Penulis menjabarkan kerangka teori yang merupakan pedoman dalam sebuah penelitian berupa model serta teori yang signifikan dan dapat diaplikasikan secara efektif dalam tesis yang sedang penulis teliti. Kerangka teori yang digunakan dalam penelitian ini adalah terkait dengan adanya acuan untuk mensimplikasi fenomena kejahatan siber yang ada di Indonesia. Terkait dengan beberapa konsep yang akan diperdalam oleh penulis dalam penelitian ini, maka teori yang dipaparkan dalam melihat fenomena kejahatan siber adalah teori sekuritisasi (Beech & Bishop). Pemrakarsa dari teori sekuritisasi adalah Jaap de Wilde, Ole Waefer dan Barry Buzan yang mendalami suatu kasus yang berkaitan erat dengan adanya pertahanan di Indonesia dengan ruang lingkup nasional. Hal tersebut juga menjadi kajian mendalam oleh penulis bahwa fenomena kejahatan siber ini memiliki ruang lingkup global. Teori sekuritisasi juga diperdalam dengan adanya konsep *national security* untuk menganalisis strategi yang harus diterapkan oleh pemerintah Indonesia dalam mengefektifkan regulasi yang berguna untuk mencegah adanya kejahatan siber berkelanjutan di Indonesia.

1.6.1. Keamanan Nasional (*National Security*)

Penulis menjabarkan konsep keamanan nasional sebagai diversifikasi atas penjabaran makna. Makna secara terminologi dalam konsep keamanan nasional terbagi atas fungsi dari keamanan nasional serta penggambaran suatu kondisi dari fenomena yang terjadi. Runut konsep keamanan nasional sebagai suatu fungsi untuk menciptakan adanya perasaan aman,

nyaman dan penuh ketertiban. Hal tersebut sangatlah fundamen mengingat masyarakat yang notabenenya memerlukan adanya rasa tentram untuk menjalani hidup bermasyarakat dan bernegara. Keamanan nasional tidak akan dapat tercapai dalam suatu wadah kenegaraan jika pemerintah tidak menerapkan strategi yang diperlukan untuk membentuk sistem keamanan yang utuh (Ramadhan, 2020). Oleh karena itu, sangat dibutuhkan adanya peninjauan ulang terkait dengan adanya penataan strategi yang digunakan untuk mencapai keamanan nasional di Indonesia mengingat bahwa kemajuan zaman yang memberikan banyak keuntungan dengan adanya globalisasi, akan tetapi tetap mampu mengancam sistem keamanan nasional baik secara teritorial maupun digital.

Pengelompokan atas adanya pihak-pihak yang berhak mendapatkan jaminan keamanan adalah dalam ruang lingkup sebuah negara, sebuah organisasi/kelompok bahkan setiap individu (Arifah, 2011). Tentunya hal ini menjadi penanda bahwa sebuah keamanan yang sifatnya merupakan hak menyeluruh untuk setiap insan di sebuah negara tidak serta merta dapat dikuasai ataupun dikontrol oleh negara, keamanan nasional juga merupakan hak masyarakat sipil yang dapat dinilai keefektifan sistemnya (Setiawan, 2020). Dalam penelitian ini, penulis memperdalam kajian terkait dengan adanya interpretasi keamanan nasional yang mengerucut di bidang keamanan digital.

Konsep keamanan digital atau dengan kata lain keamanan dunia siber merupakan peyelarasan interaksi masyarakat di dunia nyata dan *virtual* yang dihubungkan dengan perkembangan teknologi. Teknologi yang bisa mempersatukan komunikasi jarak jauh mampu menjadi sebuah ancaman untuk keamanan nasional di suatu negara (Villacampa, 2022). Keamanan nasional yang melingkupi ranah swasta, pemerintahan dan infrastruktur publik menjadi konsen dari lingkup keamanan yang harus diperdalam di bidang *virtual*. Kondisi yang mengharuskan adanya proteksi tingkat tinggi dengan menggunakan sistem keamanan berupa sandi atau *password* merupakan cara yang bisa menjadi tindakan solutif untuk mencegah adanya kebocoran data-data *internal* yang bersifat rahasia dengan sistem keamanan yang tidak bisa ditembus oleh para peretas dunia siber untuk tujuan tertentu.

1.6.2. Strategi Keamanan

Konsep strategi keamanan yang diprakarsai oleh John P. Lovell merupakan sebuah cara suatu negara untuk menggapai tujuan yang mempergunakan kekuatan/*power* yang ada baik berupa *soft power* (diplomasi dalam ruang lingkup penelitian ini seperti diplomasi siber)

maupun *hard power* (kekuatan militer dengan menggunakan strategi perang). Strategi keamanan untuk mengatasi adanya perang dunia siber menjadi sebuah implementasi untuk tetap mewaspadai adanya dampak negatif perkembangan teknologi yang tak mengenal batas teritorial disamping bahwa adanya dampak positif dalam kehidupan bernegara (Dlamini & Mbambo, 2019). Fenomena ancaman siber tentunya mengubah ranah strategi yang tidak hanya berkutat pada ancaman teritorial namun haruslah juga mengencangkan sabuk pertahanan keamanan siber.

Pertahanan keamanan siber yang menjadi fokus dalam penelitian ini adalah berupa pembajakan data-data internal yang sifatnya krusial, adanya pemalsuan identitas, serta berujung pada kejahatan siber yang tidak hanya berkedok sebagai teroris sebagai contohnya, namun dapat merangkap posisi sebagai masyarakat sipil, aparatur sipil negara, maupun akademisi (Cherry, 2017). Konstelasi/keadaan yang berujung terhadap keamanan negara memerlukan sebuah konsep strategi yang menjadi upaya dasar pemerintah untuk menganalisa sistem peregulasian keamanan nasional di Indonesia (Ramadhan, 2020).

1.7. Hipotesis

Penulis dalam tesis ini akan memaparkan hipotesis yang berindikasikan bahwa kebijakan pemerintah Indonesia dalam menghadapi ancaman kejahatan siber belum efektif karena;

1) Tingkat *IT literacy and information awareness* yang rendah sehingga tata kelola regulasi yang ada tidak menjadi solusi penanganan kasus kejahatan siber yang mencuat di Indonesia.

1.8. Tipe Penelitian

Tipe penelitian yang digunakan adalah penelitian kualitatif dan memuat serangkaian proses berpikir mulai dari data fakta yang dikumpulkan kemudian diambil kesimpulan secara umum. Metode ini diharapkan mampu terimplikasikan dan juga diadaptasikan dengan *current issue*. Penelitian yang berlandaskan cara-cara kualitatif mengindikasikan bahwa tidak adanya manipulasi atas hasil penelitian yang harus terjadi sesuai dengan praduga sementara penulis. Beberapa hal dalam sebuah penelitian yang turut dipertimbangkan yakni :

Peneliti menggunakan penelitian yang bersifat deskriptif dengan pendekatan kualitatif sehingga dapat menjawab pertanyaan peneliti (*research question*). Fokus penelitian ini adalah

untuk mengetahui faktor-faktor apa saja yang menghambat adanya keefektifan regulasi dalam mengungkap kasus kejahatan *cyber crime* di Indonesia.

1.9. Teknik Analisa Data

Teknik yang diperdalam untuk penulisan tesis ini terkait dengan;

1. Mengumpulkan data-data tentang fenomena yang diteliti.
2. Pengolahan. Pada tahapan ini peneliti mengolah data untuk pemilihan kategori yang dibutuhkan oleh masing-masing sub bab penelitian.
3. Analisa. Tahapan terakhir ini menjadikan data yang mentah dan sudah diolah tadi, untuk kemudian dianalisa dan diinterpretasikan oleh peneliti sehingga mempengaruhi proses pembentukan hasil akhir dari riset.

1.10. Metode Pengumpulan Data

Literatur yang berisikan data-data faktual menjadi cara yang didalami oleh penulis. Data literatur berupa buku-buku mengenai pemahaman *cyber crime* baik dari analisis kasus dan penerapan hukum *cyber* bagi pelaku kejahatan dunia maya. Penulis mendeskripsikan permasalahan yang berhubungan erat dengan kejahatan siber yang marak terjadi.

1.11. Sistematika Penulisan

Penulis menjabarkan sistematika penulisan dalam tesis ini yang dikelompokkan menjadi beberapa bab seperti ;

Bab 1 terdiri dari “Pendahuluan” yang membahas fundamen penelitian seperti latar belakang masalah, rumusan masalah, tujuan riset, kontribusi riset, tinjauan pustaka, hipotesis, tipe penelitian, teknik analisa data, metode pengumpulan data dan sistematika penulisan.

Bab 2 penulis mencoba memperdalam pendeskripsian terkait dengan “Ancaman Kejahatan Siber di Indonesia”. Pendeskripsian yang dituangkan oleh penulis dengan alur kerangka pemikiran untuk meninjau secara *general* terkait dengan kejahatan siber. Penulis juga mendalami berbagai ancaman yang dihadapi oleh para penegak hukum siber yang ada di Indonesia. Ancaman siber tersebut sangat berkaitan dengan penegakan dari amandemen regulasi yang berkaitan dengan tindakan nyata oleh pemerintah dalam menangani tindakan kejahatan siber di Indonesia.

Bab 3 yang terkait dengan “Kebijakan Peregulasian terhadap *Cyber Crime* di Indonesia”

menitikberatkan tentang keefektifan regulasi mengenai tata kelola regulasi. Tata Kelola regulasi terkait dengan penanganan kejahatan siber yang ada di Indonesia dan pembuktian hipotesis yang telah dikemukakan oleh penulis di dalam tesis ini.

Bab 4 Penulis menambahi dengan saran yang menjadi bahan perimbangan untuk penanggulangan regulasi kejahatan siber selama penelitian dilangsungkan.