BAB I

PENDAHULUAN

1.1 Latar Belakang

Meskipun sekarang telah merupakan fenomena umum, laju perubahan teknologi masih terus mengesankan. Teknologi Informasi dan Komunikasi (TIK) sekarang menjadi pusat cara manusia berinteraksi, baik secara sosial maupun komersial, dengan lebih dari satu triliun situs web menyediakan akses siap pakai ke berbagai informasi dan layanan yang sangat beragam. Tak terhindarkan bahwa beberapa orang akan menggunakan TIK dalam melakukan atau memfasilitasi kejahatan; yang kemudian disebut "kejahatan siber." Ini termasuk kejahatan di mana TIK menjadi target kegiatan kriminal, pelanggaran yang menjadikan TIK sebagai sarana kejahatan, serta pemakaian TIK yang bersifat insidental tetapi dapat memberikan bukti kejahatan. Sifat teknologi yang saling berhubungan membuat ini menjadi masalah global, dan selama beberapa dekade telah ada kesadaran internasional akan perlunya tindakan terkoordinasi.

Dalam menghadapi berbagai kasus kejahatan siber yang semakin marak terjadi, banyak pihak yang masih belum siap. Untuk dapat melawan kasus kejahatan siber, perlu pemahaman yang tepat mengenai apa itu kejahatan siber dan bagaimana hal itu menjadi salah satu ancaman terbesar bagi banyak negara di dunia. Ketika menyebutkan kejahatan siber, orang mungkin membayangkan seorang peretas dengan pakaian serba hitam mengetik dengan raut wajah serius di depan layar komputer mereka, yang menunjukkan latar belakang hitam dan font berwarna hijau.

Jika dilihat dari perspektif ini, dapat dikatakan bahwa kejahatan siber terdiri dari kejahatan dan komputer, namun kenyataannya tidak sesederhana itu. Karena kejahatan siber adalah kejadian yang relatif baru di panggung internasional, tidak ada definisi yang disepakati secara umum. Sarjana dan ahli pakar sama-sama telah mengemukakan teori dan konsep mereka dalam mendefinisikan kejahatan siber. Membayangkan gambaran langsung tentang kejahatan siber itu sulit, mengingat seberapa besar isi dan jangkauan dunia siber itu sendiri.

Dalam menganalisis kejahatan siber, para ahli harus mempertimbangkan bagaimana definisi secara langsung mempengaruhi jangkauannya (Payne 2020, 4). Satu pihak dapat membatasi kejahatan siber sampai di sektor bisnis, namun pihak lain dapat mendefinisikan kejahatan siber sebagai kejahatan yang dilakukan oleh individu dan berfokus pada aspek psikologisnya. Selain itu, definisi kejahatan siber mempengaruhi bagaimana intervensi dan kebijakan digunakan untuk menanggapi serta bagaimana mencegah kejahatan siber (Payne 2020, 6). Jika melihat kejahatan siber dari sudut pandang sosiologis atau psikologis, orang akan membangun kebijakan dan intervensi yang bertujuan untuk mengubah perilaku pelaku sambil mengedukasi calon pelaku dan korban. Sebaliknya, dari sudut pandang teknologi, orang akan menyusun kebijakan untuk menanggapi kejahatan yang terjadi di dunia siber saja, serat memanfaatkan teknologi yang lebih baru untuk mencegah serangan siber yang membawa bencana. Namun konsep kejahatan siber masih diperlukan untuk mendefinisikan maknanya dan menganalisis lebih lanjut besarnya dampak kejahatan ini pada tingkat nasional dan regional.

Mengingat sifat penelitian ini, perspektif hukum akan digunakan untuk menggambarkan kejahatan siber dan apa yang dikandungnya. Istilah "*cybercrime*" berasal dari kata *cyber* dalam *cybernetics*. Kata *cyber* pada awalnya digunakan sebagai cara untuk menggambarkan segala sesuatu yang berhubungan dengan teknologi dan komputer (Adrienne dan Steinmetz 2020, 613). *Cybernetics* sendiri adalah studi tentang teknik dan matematika komputasi, yang didefinisikan oleh Norbert Wiener (Wiener 1948) sebagai "studi ilmiah tentang kontrol dan komunikasi pada hewan dan mesin." Namun, para sarjana hukum cenderung menentukan definisi kejahatan, bahkan secara umum, berdasarkan pandangan hukum daripada psikologis. Dari sini, orang dapat berasumsi bahwa definisi umum dari kejahatan dapat digunakan untuk membingkai kejahatan siber. Menurut Departemen Pendidikan Nasional (Departemen Pendidikan Nasional 2008), kejahatan adalah perbuatan jahat yang melanggar hukum, perilaku yang bertentangan dengan nilai dan norma yang telah disahkan oleh hukum tertulis. Sistem hukum pidana Indonesia memasukkan kejahatan siber ke kategori tindak pidana khusus meskipun unsur utamanya dapat disetarakan dengan beberapa pasal-pasal lain di dalam Kitab Undang-Undang Hukum Pidana (KUHP),

Salah satu serangan siber terbesar yang pernah dihadapi dunia adalah serangan *ransomware WannaCry* pada Mei 2017. Serangan ransomware ini menyebar melalui komputer yang mengoperasikan *Microsoft Windows*. File pengguna ditahan, dan tebusan Bitcoin diminta untuk pengembalian file (kaspersky 2022). Europol mengklaim bahwa *ransomware* dalam skala sebesar ini belum pernah terjadi sebelumnya, dengan perkiraan sekitar 200.000 komputer terinfeksi

di 150 negara (BBC News 2017). Menurut Kaspersky Lab, empat negara yang paling terkena dampaknya adalah Rusia, Ukraina, India, dan Taiwan (Financial Times 2017). Menurut perusahaan pemodelan risiko dunia siber, Cyence, kerugian ekonomi dari serangan siber dapat mencapai hingga US$4 miliar, dengan kelompok lain memperkirakan kerugian mencapai ratusan juta (Berr 2017). Pada Desember 2017, Inggris dan Amerika Serikat secara resmi menyatakan bahwa Korea Utara merupakan dalang dari serangan itu (BBC News 2017). Namun, Korea Utara membantah bertanggung jawab atas serangan siber tersebut (Nichols 2017).

Indonesia memiliki sejarah keamanan siber yang buruk, hal ini nampak jelas dari angka kerentanan akan serangan siber yang semakin melonjak hingga insiden siber yang berkali-kali terjadi pada bisnis dan lembaga pemerintahan. Kasus kejahatan siber yang paling terkenal mungkin ialah saat situs Telkomsel berisi keluhan akan internet yang mahal pada April 2017. Serangan yang diklasifikasikan sebagai *hacktivist* ini diduga datang dari grup *hacker* ternama, *Anonymous*. Laman Telkomsel berubah menjadi keluhan sang pelaku dengan latar belakang hitam. Nama Telkomsel juga berubah menjadi Telkomnyet. Sesuai dengan tangkapan layar yang beredar, situs Telkomsel berisi tulisan:

"Dear kampret, Lu jadi operator kagak usah mahal-mahal. Pegimane bangsa Endonesia mau maju kalo internet aja mahal. Makan aja susah apalagi beli kuota internet. Murahin harga kuota internet, nyet! Kagak usah pake dibagi-bagi 2G/3G/4G. gue kaga butuh HOOQ, VIU, iming-iming kuota music ame video lu. Gue cuma butuh KUOTA INTERNET. TITIK."

Walapun begitu, kasus *web defacement* Telkomsel tidak meninggalkan kerusakan yang parah. Setelah diretas, pihak Telkomsel langsung memitigasi masalah dan meminta maaf kepada nasabah mereka atas kelalaian pihak operator. Salah satu kasus kejahatan siber yang ekstrim pernah menimpa mantan presiden Indonesia, Susilo Bambang Yudhoyono. Isu ini pertama kali dimuat dalam laporan dari *The Guardian* dan ABC pada 18 November 2013. Laporan tersebut berisi bocoran dokumen dari *whistleblower* Edward Snowden, yang menulis bahwa agen mata-mata Australia telah menyadap telepon mantan Presiden Indonesia Susilo Bambang Yudhoyono (SBY), mantan wakil presiden Bodieono dan Jusuf Kalla, serta mantan menteri senior lainnya. Pada bulan Agustus 2009, *Defence Signals Directorate* (DSD) Australia memantau SBY melalui teleponnya selama lima hari. Dokumen Snowden juga mencatat adanya dugaan Australia mengintai daftar rekaman panggilan SBY.

Berita tersebut menjadi kejutan yang mencemaskan pemerintah Indonesia. Sebagai pemimpin negara, mantan Presiden SBY sepatutnya memiliki sikap yang sangat tertutup terhadap isi percakapan di teleponnya. Kementerian juga harus menjaga privasi terkait negara dan pemerintah juga. Intersepsi ilegal adalah kasus darurat yang sulit dilacak dan dipecahkan. Pada saat itu, kurangnya sumber daya manusia yang ahli akan *cybercrime* menjadi kendala bagi pemerintah Indonesia. Isu tersebut mengganggu keamanan nasional, dimana warga negara Indonesia sempat mempertanyakan keamanan data privasi Indonesia. Walaupun ini merupakan kasus lama, pemerintah Indonesia masih bisa belajar dari isu ini. Tindakan untuk

mencegah kasus kebocoran data seperti ini agar tidak terulang kembali di kemudian hari sangat diperlukan.

Dalam menghadapi kejahatan siber, pemerintah Indonesia telah menetapkan strategi keamanan siber yang dapat dilihat melalui *Global Cybersecurity* Index (GCI). GCI merupakan metriks pengukuran komitmen Indonesia sebagai negara anggota *International Telecommunication Union* (ITU) akan keamanan sibernya. Indeks ini mencakup menjadi lima aspek: hukum, struktur organisasi, kerjasama internasional, peningkatan kapasitas, serta teknikal dan prosedural (ITU 2020). Aspek hukum mencakup berbagai undang-undang yang dikeluarkan demi menangani kejahatan siber, seperti UU Tentang Informasi dan Transaksi Elektronik (ITE) No. 11 Tahun 2008; UU Telekomunikasi No. 36 Tahun 1999; Peraturan Pemerintah (PP) tentang Penyelenggaraan Sistem & Transaksi Elektronik No. 82 Tahun 2012; Peraturan Menteri Kominfo No. 26 Tahun 2007 serta Peraturan Menteri Pertahanan RI Nomor 82 Tahun 2014, dan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).. Dalam struktur organisasi, ada pembentukan Badan Siber dan Sandi Negara (BSSN) dari Peraturan Presiden No. 53 Tahun 2017,

Kerjasama internasional memungkinkan pembentukan berbagai badan penanganan siber nasional untuk bekerjasama dengan negara luar (Islami 2017), seperti *Indonesia Computer Emergency Response Team* (ID-CERT); dan *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII). Selain itu, terdapat juga organisasi formal dan non-formal yang mengurus isu-isu siber (Arianto dan Anggraini 2019), yaitu Dewan Teknologi Informasi dan Komunikasi

(TIK); *Computer Security Incident Response Team* (CSIRT); dan *Indonesia Telecommunication User Group* (IDTUG). Pada pembangunan kapasitas, ada berbagai program dan bimbingan yang bertujuan untuk mengedukasi instansi pemerintahan akan dunia siber dan bagaimana cara untuk mengamankannya. Ada pula Standar Nasional Indonesia (SNI) yang mengawasi Sistem Manajemen Keamanan Informasi (SMKI) dan Indeks Keamanan Informasi yang mengevaluasi menganalisis kesiapan pengamanan informasi di instansi pemerintah berbasis ISO/IEC (BSN 2016).

Sesuai dengan Undang-Undang No. 2 tahun 2002 tentang Kepolisian Republik Indonesia, POLRI wajib menjaga keamanan nasional dari berbagai ancaman. Pasal 2 mencakup fungsi POLRI yaitu: salah satu fungsi pemerintahan Negara di bidang pemelihara keamanan dan ketertiban masyarakat, penegak hukum, perlindungan, pengayoman dan pelayanan masyarakat. Selain itu, tugas pokok POLRI yang tertuang dalam pasal 13 juga menggarisbawahi kewajiban POLRI untuk melindungi keamanan Indonesia, diantaranya:

a memelihara keamanan dan ketertiban masyarakat;

b menegakkan hukum; dan

c memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

Dari sisi POLRI, upaya menangani kejahatan siber nasional terletak pada pembentukan Direktorat Tindak Pidana Siber (DITTIPIDSIBER) pada 3 Februari 2017, yang sebelumnya ditangani oleh Unit *Cybercrime* Subdirektorat V dari

Direktorat Tindak Pidana Ekonomi Khusus (DITTIPIDEKSUS). Menurut websitenya di patrolisiber.id, Direktorat Tindak Pidana Siber (Dittipidsiber) adalah "satuan kerja yang berada di bawah Bareskrim POLRI dan bertugas untuk melakukan penegakan hukum terhadap kejahatan siber." Secara umum, Dittipidsiber menangani *computer crime* dan *computer-related crime*. *Computer crime* merupakan jenis kejahatan siber yang memakai komputer sebagai alat utama. Beberapa bentuk kejahatannya mencakup pengubahan tampilan situs web (*web defacement*), peretasan sistem elektronik (*hacking*), gangguan sistem (*system interference*), intersepsi ilegal (*illegal interception*), dan manipulasi data (*data manipulation*). *Computer-related* crime, di sisi lain, ialah kejahatan siber yang memakai komputer sebagai alat bantu, misalnya ujaran kebencian (*hate speech*), pencemaran nama baik (*online defamation*), pengancaman *online* (*online threat*), perjudian *online* (*online gamble*), penipuan *online* (*online fraud*), pemerasan *online* (*online extortion*), pornografi *online* (*online pornography*), pencurian data (*data theft*), dan akses ilegal (*illegal access*).

Selain berbagai strategi nasional yang telah diambil dan ditetapkan, Indonesia juga mengambil bagian dalam kerangka kerja AMMTC, bagi anggota ASEAN untuk berkonsultasi dan mendiskusikan langkah-langkah yang perlu diambil demi menuntaskan kejahatan transnasional. Indonesia melihat AMMTC sebagai cara untuk memperkuat kerja sama keamanan serta mendorong negara-negara ASEAN lainnya untuk memperkuat aturan melawan kejahatan siber. Penanganan kejahatan siber harus berjalan di dua sisi, yaitu dari dalam serta luar negeri. Dari dalam, pemerintah Indonesia dapat memakai dan meningkatkan

perangkat hukum yang ada. Dari luar negeri, Indonesia dapat menggunakan forum AMMTC untuk memaksimalkan implementasi program kerja yang ada dan memutakhiran dokumen sesuai dengan strategi kawasan Asia Tenggara yang terus berkembang. Oleh karena itu, peran Indonesia dalam forum AMMTC dalam menangani kejahatan siber akan dianalisis dalam penelitian ini. Kemudian akan dibandingkan dengan indeks pengukuran *Global Cybersecurity Index* (GCI).

1.2 Rumusan Masalah

Berdasarkan uraian yang telah dijelaskan dalam latar belakang, maka penelitian ini dilakukan untuk menjawab pertanyaan: **Bagaimana efektivitas strategi POLRI melalui AMMTC dalam memberantas kejahatan siber di Indonesia?**

1.3 Tujuan Penelitian

Sesuai dengan latar belakang dan rumusan masalah yang ada, tujuan penelitian yang ingin dicapai peneliti adalah:

1. Melalui AMMTC, Indonesia yang diwakili oleh POLRI ingin menyelesaikan kasus kejahatan siber yang meningkat, jadi penelitian ini bertujuan untuk melihat dan menganalisa efektivitas langkah langkah yang diambil oleh POLRI lewat AMMTC untuk menangani kasus kejahatan siber di Indonesia.

2. Lewat pengukuran *Global Cybersecurity Index (GCI)*, peneliti ingin meninjau efektivitas strategi nasional dan hasil kinerja POLRI melawan kejahatan siber.

1.4 Manfaat Penelitian

Adapun manfaat yang diharapkan dapat diperoleh melalui penelitian yang dilakukan yaitu:

1.4.1 Manfaat Akademis

a. Penelitian ini diharapkan dapat memberi pemahaman akan kejahatan siber dalam pengembangan studi Ilmu Hubungan Internasional.
b. Penelitian ini diharapkan dapat menambah data ASEAN dan para anggotanya mengenai bahaya kejahatan siber dan penyelesaiannya.

1.4.2 Manfaat Praktis

a. Bagi ASEAN, penelitian ini diharapkan dapat memberikan pandangan tentang seberapa baik kinerja AMMTC sebagai forum regional.
b. Bagi POLRI, penelitian ini diharapkan dapat memperkaya informasi melalui analisis data akan bagaimana ASEAN, khususnya AMMTC, dalam memerangi kejahatan siber.
c. Bagi peneliti selanjutnya, penelitian ini diharapkan dapat menjadi sumber data dari perspektif POLRI dalam menghapus kejahatan siber melalui AMMTC, agar perspektif lain yang belum dipetakan dapat dieksplorasi.

1.5 Metode Penelitian

Sebagaimana dicatat oleh Denzin dan Lincoln (Erickson 2011), penelitian kualitatif adalah seperangkat praktik penafsiran yang kompleks. Sebagai formasi sejarah yang terus berubah, penelitian kualitatif menyambung ketegangan dan kontradiksi, termasuk perselisihan tentang metode serta bentuk temuan dan interpretasi data. Metode penelitian kualitatif adalah bidang yang kompleks, dinamis dan digemari oleh berbagai metodologi dan praktik penelitian. Oleh karena itu, 'penelitian kualitatif' bukanlah satu kesatuan, tetapi merupakan payung yang mencakup keragaman yang sangat besar (Punch 1998, 139). Tiga aspek keragaman ini menyangkut teknik pengumpulan data, teknik validasi data, dan teknik analisis data.

Kompleksitas kejahatan siber membutuhkan pertimbangan metodologis dan strategi penelitian yang membuat perspektif kualitatif sangat efektif. Demi mengurai dan memahami seluk-beluk kejahatan siber, dampak, serta pemecahan masalah ini secara regional dan nasional, peneliti menggunakan metode kualitatif. Penelitian kualitatif juga digunakan untuk mendeskripsikan dan menganalisis pola hubungan timbal balik antara POLRI dan AMMTC. Penelitian kualitatif membantu peneliti lebih memahami apa yang harus dilakukan saat menganalisis data, dan memungkinkan peneliti menghasilkan analisis yang lebih baik dan berbobot.

1.5.1 Jenis dan Tipe Penelitian

Penelitian menggunakan metode kualitatif dengan jenis penelitian studi kasus yang merupakan turunan dari pendekatan kualitatif dengan tipe penelitian deskriptif analisis dimana penulis mencoba secara terstruktur menjelaskan ancaman kejahatan siber di Indonesia dan menganalisis bagaimana POLRI sebagai badan penegak hukum menangani masalah ini lewat AMMTC sebagai forum regional ASEAN, serta meninjau efektivitas langkah-langkah Indonesia dan POLRI lewat *Global Cybersecurity Index* (GCI).

1.5.2 Sumber dan Teknik Pengumpulan Data

Data telah didefinisikan sebagai semua sumber informasi yang dihasilkan oleh orang-orang dalam konteksnya (Largan dan Morris 2019). Terdapat dua jenis data, yaitu data primer dan sekunder. Boslaugh (Boslaugh 2007) menjelaskan bahwa perbedaan antara data primer dan sekunder adalah peran orang yang mengumpulkan data dan orang yang menganalisisnya. Data yang dikumpulkan oleh peneliti atau tim peneliti untuk dianalisis di bawah topik pertimbangan dan menggunakan prosedur yang sesuai dengan masalah penelitian didefinisikan sebagai data primer, sedangkan data yang dikumpulkan oleh orang lain untuk tujuan lain adalah data sekunder.

Dalam penelitian ini yang menjadi sumber data primer adalah transkrip wawancara dengan pihak terkait. Sumber data sekunder yang dipakai adalah buku, literatur, artikel, jurnal, laporan maupun dokumen resmi dari Bagian Konvensi Internasional Divisi Hubungan Internasional Markas Besar POLRI yang sesuai dengan penelitian yang dilakukan. Teknik pengumpulan data yang akan dilakukan

adalah data primer dengan teknik pengumpulan data melalui wawancara, serta data sekunder yaitu dokumentasi melalui pendekatan *library research* dan *online research.* Adapun gambaran langkah-langkah yang akan diambil adalah sebagai berikut:

1. Wawancara dengan AKBP Wino Sumarno, S.S., M.Pd, selaku Kasubag Aspasaf dari Bagian Konvinter Divhubinter Mabes POLRI, serta AKBP Endo Priambodo dari Direktorat Tindak Pidana Kejahatan Siber (Dittipidsiber) Mabes POLRI.
2. *Library research* akan dilakukan dengan mencari sumber-sumber yang terkait dengan judul penelitian. Sejauh ini tempat yang akan dituju untuk mengumpulkan sumber adalah Perpustakaan Nasional Indonesia (Perpusnas), Perpustakaan Universitas Kristen Indonesia (UKI).
3. *Online research* juga dilaksanakan lewat pengumpulan data dan informasi dari internet untuk mencari berbagai sumber yang berkaitan bagi penelitian.

Tabel 1.1. Sumber dan Teknik Pengumpulan Data

Sumber Data	**Teknik Pengumpulan Data**		**Aspek Data**
Primer	Wawancara	(a) Wawancara dengan Kepala Sub Bagian Organisasi Internasional dari Bagian Konvinter Divhubinter Mabes POLRI, serta perwakilan dari Dittipidsiber Mabes POLRI	(a) Data terkait dengan penelitian agar dapat dijelaskan sesuai dengan data yang sudah dicari.
Sekunder	Dokumentasi	(a) *Library research* di Perpustakaan Nasional Indonesia (b) *Library research* di Perpustakaan Universitas Kristen Indonesia (UKI) (c) *Online research* di berbagai *website* terkait	(a) Data terkait dengan penelitian agar dapat dijelaskan sesuai dengan data yang sudah ada.

Sumber: Hasil olahan peneliti, 2022

1.5.3 Teknik Validasi Data

Validitas, dalam penelitian kualitatif, mengacu pada cara-cara peneliti dapat menegaskan bahwa temuan mereka sesuai dengan pengalaman partisipan. Dengan kata lain, validitas mengacu pada kualitas dan ketelitian sebuah penelitian. Validitas adalah pendekatan untuk mencapai kompleksitas melalui cara-cara sistematis dalam menerapkan dan menilai kekakuan suatu studi (Ravitch dan Carl, Qualitative Research: Bridging the Conceptual, Theoretical, and Methodological 2019). Terlepas dari semuanya, ada metode yang peneliti gunakan untuk membantu meningkatkan ketelitian serta validitas dari studi penelitian kualitatif. Dalam penelitian ini, teknik validasi yang digunakan adalah triangulasi.

Triangulasi adalah seperangkat proses yang peneliti gunakan untuk meningkatkan validitas suatu penelitian. Hal ini umumnya dianggap memiliki sumber atau metode yang berbeda menantang dan/atau mengkonfirmasi suatu titik atau serangkaian interpretasi. Secara umum, triangulasi melibatkan "perspektif yang berbeda" (U. Flick 2007, 41) atau "memeriksa kesimpulan (pernyataan, klaim, dst) melalui lebih dari satu sudut pandang" (Schwandt 2015, 307). Tujuan penggunaan strategi triangulasi adalah untuk mempertimbangkan apakah peneliti memiliki cukup data dan jenis data yang tepat untuk memberikan kualitas dan kedalaman informasi untuk menjawab pertanyaan penelitian dengan percaya diri; serta memastikan peneliti telah terlibat dalam pengumpulan data terpercaya yang sistematis dan ketat yang akan memungkinkan munculnya interpretasi yang paling autentik dan stabil (Ravitch dan Carl, Qualitative Research: Bridging the Conceptual, Theoretical, and Methodological 2019).

1.5.4 Teknik Analisa Data

Analisis data dalam penelitian kualitatif adalah klasifikasi dan interpretasi bahan linguistik (atau visual) demi membentuk pernyataan tentang dimensi implisit dan eksplisit serta struktur pembuatan makna dalam materi dan apa yang diwakili di dalamnya (U. Flick 2013, 5). Analisis data kualitatif juga diterapkan untuk menemukan serta menggambarkan isu-isu di lapangan atau struktur dan proses dalam rutinitas dan praktik. Seringkali, analisis data kualitatif menggabungkan pendekatan analisis kasar materi (ikhtisar, kondensasi, ringkasan) dengan pendekatan analisis rinci (interpretasi hermeneutik, penjabaran kategori, atau struktur yang diidentifikasi). Tujuan akhirnya cenderung sampai pada pernyataan yang dapat digeneralisasikan dengan membandingkan berbagai bahan, teks atau beberapa kasus.

Miles and Huberman (Miles, Huberman dan Saldaña 2014) melihat tiga teknik dalam menganalisa data: (1) kondensasi data, (2) penyajian data, serta (3) kesimpulan dan verifikasi. Dalam penulisan proposal skripsi, peneliti menjalani langkah pertama untuk memfokuskan dan menyederhanakan data. Setelah data sudah lebih padat, data di organisasikan lagi hingga memungkinkan penarikan kesimpulan. Pada langkah terakhir, data akan dipertanyakan kebenarannya melalui hasil akhir penelitian hingga kesimpulan final dapat ditarik.

1.6 Sistematika Penulisan

Penelitian ini terdiri atas empat bab, juga terdapat sub-bab yang telah disesuaikan dengan isi pembahasan penelitian ini, yang terdiri atas:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan yang menjelaskan tentang Upaya POLRI dalam Pemberantasan Kejahatan Siber melalui Mekanisme AMMTC.

BAB II KAJIAN PUSTAKA

Bab ini berisi tinjauan pustaka, kerangka konseptual, kerangka pemikiran, dan argumen utama yang menjelaskan tentang mengapa POLRI memutuskan bahwa kejahatan siber di Indonesia dapat ditangani lewat AMMTC.

BAB III PEMBAHASAN

Bab ini peneliti mendeskripsikan dan menjelaskan mengenai perkembangan serta kasus-kasus kejahatan siber di Indonesia, hingga asal mula AMTC serta bagaimana POLRI menangani kasus kejahatan siber yang belakangan ini makin marak lewat kerangka AMMTC dalam berbagai bentuk kerjasamanya. Serta pengukuran tindakan pemerintah Indonesia dan POLRI melawan kejahatan siber lewat *Global Cybersecurity Index* (GCI).

BAB IV PENUTUP

Bab ini berisi kesimpulan dan rekomendasi terkait hasil akhir dari penelitian.