Bab I

Pendahuluan

A. Latar Belakang

Dewasa ini, pesatnya kemajuan dalam bidang teknologi informasi telah merubah pemikiran dunia serta menggeser pemahaman internasional terhadap suatu kekuatan (*power*) maupun kedaulatan suatu bangsa. Kedaulatan atau kekuatan suatu bangsa di era sekarang ini tidak hanya dinilai dari besarnya kekuatan militier ataupun ekonomi yang dimiliki bangsa tersebut, namun juga dilihat dari penguasaan dan kecanggihan suatau negara dalam memanfaatkan teknologi informasi. Hal ini dikarenakan abad ke-21 ataupun sering disebut abad informasi, hampir setiap aktivitas kehidupan mulai dari personal hingga pemerintahan tidak dapat lepas dari pemanfaatan, pengimplementasian, serta pemberdayaan di bidang teknologi informasi (Saputera, 2015).

Timbulnya arus transformasi dalam bidang teknologi informasi dan komunikasi telah menyebabkan kondisi masyarakat global menjadi saling terhubung dalam satu domain yang dikatakan sebagai ‘desa global’. Hasil dari sinergitas antara teknologi telekomunikasi, internet, dan penyiaran telah memicu terciptanya infrastruktur jaringan pita lebar yang berdampak pada lahirnya ekonomi baru. Munculnya jaringan pita lebar ini telah memberikan nilai yang positif dalam meningkatkan kualitas kehidupan sosial dan ekonomi melalui globalisasi ekonomi digital. Dilain sisi, terhubungnya global melalui jaringan pita lebar telah menciptakan ancaman baru terhadap kedaulatan negara. Dengan terhubungnya seluruh dunia telah menciptakan sebuah ruang lingkup baru yang dinamai dunia siber (*cyberspace*). Dunia maya telah memberikan banyak kemudahaan terhadap masyarakat global namun juga menimbulkan kerentangan serta ancaman baru yang mencakup kedaulatan negara.

Dampak dari kuatnya arus globalisasi pada dewasa ini telah memberikan indikasi terhadap setiap negara bahwa harus dapat membentuk serta mengembangkan keamanan negaranya dalam bidang siber agar dapat terhindar ataupun menahan serangan siber dari berbagai pihak yang diantaranya seperti melakukan peretasan, penyadpaan, perusakan sistem perangkat lunak penting. Negara-negara di dunia baiknya harus menyadari dewasa ini ancamn terhadap keamanan global lagi hanya mengandalkan kontak fisik semata, namun juga telah bergeser menjadi sifatnya digital serta virtual. Berangkat dari munculnya domain baru dalam dunia internasional kemudian melahirkan ancaman yang disebut dengan *cyberwarfare*. Sifat dari ancaman *cyberwarfare* itu sendiri ialah halus, tidak terlihat, dan sulit dirasakan dalam kehidupan nyata, akan tetapi akibat yang diraskan dari serangan siber sangatlah meatikan karena dapat secara langsung menyerang ke "jantung" pertahanan setiap negara, sehingga bahaya yang diciptakan sangatlah besar.

Definisi dari *cyberwarfare* itu sendiri ialah sebagai perang dalam dunia maya, namun Serangan yang ditujukan dalam *cyberwarfare* berbeda dengan serangan perang fisik ataupun perang konvensional. alat ataupun media yang menjadi komponen utama dalam perang *cyber* adalah internet dan komputer. Objek dari serangan siber itu sendiri Bukankah merupakan wilayah teritorial, wilayah fisik ataupun wilayah geografis tetapi objek yang menjadi tujuan serangan ialah dunia maya yang yang dikuasai oleh suatu negara. Dalam jangka waktu panjang, *cyberwarfare* akan memberikan dampak yang lebih luas dan dapat mengganggu kestabilan kedaulatan negara. Hukum kebiasaan internasional mengenal istilah *act of state doctrine* yang berarti setiap negara berdaulat wajib menghormati kemerdekaan negara berdaulat lainnya. Namun, yang terjadi di dalam *cyberwarfare* adalah negara tidak menghormati kedaulatan negara lain di dalam *cyberspace* dan melakukan penyerangan terhadap *cyber-infrastructure* milik negara lain.

Indonesia sebagai negara berkembang sedikit tertinggal dalam perkembangan teknologi informasi, hal ini akibat dari

strategi pengembangan teknologi yang tidak optimal dan cenderung mengabaikan penelitian ilmiah dan teknologi. Dampaknya, terjadi ketimpangan dimana penguasaan teknologi tidak sebanding dengan alih teknologi dari negara industri maju yang dapat mengubah Indonesia menjadi negara berbasis teknologi. Negara-negara di dunia telah menggeser pandangan terhadap pertahanan nasionalnya yang dahulu lebih menitik beratkan pada pertahanan militer menjadi pertahanan non-militer yang dipandang jauh lebih berbahaya pada era teknologi informasi saat ini. Ini menjadi indikasi yang kuat bahwa Indonesia harus sadar dan selalu mengikuti perkembangan teknologi dengan cepat untuk mengantisipasi dampak-dampak yang ditimbulkan terhadap pertahanan nasional (Saudi, 2017).

Mengacu pada analisis data sistem monitoring traffic ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*) kasus ancaman siber yang dialami Indonesia tercatat bahwa serangan cyber yang diterima oleh Indonesia mencapai 1 juta insiden dan angka ini akan terus mengalami peningkatan setiap harinya yang disebabkan oleh lemahnya sistem pertahanan siber yang tidak dapat diketahui. Serangan siber yang dialami oleh Indonesia juga berdampak pada institusi pemerintahan di mana tercatat dalam kurun waktu 1998 - 2009 Indonesia menerima sebanyak 2.138 serangan yang diterima oleh institusi pemerintahan milik Indonesia. Serangan *cyber* yang diterima Indonesia Biasanya berupa *distributed denial of service* yang menyerang *Domain Name service* (DNS) CCTLD- ID yaitu domain .id terutama .co.id. Kasus serangan cyber lainnya Yang diterima oleh Indonesia malware serta *malicious code*, serangan siber ini biasanya Disisipkan ke dalam suatu file dan website maupun *phising site*, spionase industri dan penyanderaan sumber daya informasi kritis, maupun *black campaign* partai politik atau penistaan keyakinan dan penyebaran kabar bohong (*hoax*) untuk tujuan provokasi politis serta rekayasa ekonomi. Minimnya sumber daya dan akses terhadap aparat penegak hukum kepada penyedia layanan internet di luar negeri. Hal ini menyebabkan

Indonesia belum dapat mengantisipasi walaupun telah diterbitkan undang-undang ITE sebagai payung hukumnya.(Setiawan, 2011).

Indonesia telah menerapkan pertahanan cyber yang dipegang ataupun dijalankan oleh masing-masing institusi dan lembaga nasional ataupun swasta yang bertujuan dalam melindungi dunia maya untuk menopang infrastruktur kritis mereka. Namun, perlindungan nasional terhadap dunia maya ya dalam rangka kebijakan siber nasional belum tercantum pada suatu regulasi yang berbentuk perundang-undangan. Jika berkaca kepada negara lain telah banyak negara-negara di dunia menerapkan undang-undang mengenai keamanan siber hal ini disebabkan karena ketergantungan yang kuat terhadap teknologi informatika. seperti yang telah dijelaskan bahwa keamanan siber Indonesia berada di bawah payung hukum undang-undang ITE, dalam menciptakan pertahanan negara mealui keamanan siber tidaklah cukup jika hanya mengacu pada undang-undang tersebut. Masalah lainnya yang yang dialami oleh Indonesia terkait keamanan siber ialah pembagian fungsional mengenai kewenangan dan otoritas yang yang memiliki kewajiban dalam menghadapi ancaman *cyber* seperti *cyber terrorism*, *cybercrime*, *cyber hactivism* ataupun *cyberwarfare* yang belum jelas.

Sebagai respon atas banyaknya kasus serangan siber di Indonesia dan untuk menciptakan optimalisasi keamanan siber di Indonesia kemudian dibentuklah Badan Siber dan Sandi Negara dalam rangka mengoptimalisasi ketahan siber nasional serta sebagai model institusi keamanan siber nasional. Joko Widodo resmi membentuk Badan Siber dan Sandi Negara setelah diterbitkannya Perpres No. 53 Tahun 2017 tentang Badan Siber dan Sandi Nasional, pada tanggal 19 Mei 2017. Mengingat arti penting dari badan ini dalam mengatasai permasalahan keamanan siber, Penulis di sini ingin mengetahui mengapa Indonesia mendirikan Badan Siber dan Sandi Negara (BSSN).

B. Rumusan Masalah

Berdasarkan latar belakang di atas serta melihat potensi ancaman yang ada penulis merumuskan permasalahan sebagai berikut: **Mengapa Indonesia mendirikan Badan Siber dan Sandi Negara ?**

C. Kerangka teoritik

Kerangka dasar teori adalah bagian dalam sebuah penelitian yang akan menjelaskan variable-variabel dan hubungan antara variable yang berdasarkan pada konsep atau pada definisi tertentu. Pada bagian kerangka dasar teori ini akan di kemukakan teori-teori yang merupakan acuan pada bagian penelitian yang dilakukan.

1. Teori Sekuritisasi

Teori sekuritisasi masuk ke dalam salah satu teori keamanan yang kerangka berpikirnya lebih berkembang dari teori keamanan tradisional. Fokus dari teori keamanan itu sendiri lebih kepada ada aktor negara dan ancaman militer sedangkan terdapat pemahaman dan definisi dari teori sekuritisasi yang lebih luas daripada ancaman tradisional di mana faktor utamanya ialah negara. Teori Sekuritisasi memunculkan perdebatan baru mengenai definisi keamanan serta siapa maupun bagaimana melakukan tindakan keamanan itu sendiri.

Terdapat uraian yang dapat menjeleaskan pengidentifikasian terhadap pendekatan kebijakan keamanan sekuritisasi. Pertama, ialah mengidentifikasi proses konstruksi terhadap pendekatan sekuritisasi ini diterapkan dalam mengeluarkan kebijakan. Sudut pandang mengenai keamanan dan ancaman yaitu lebih bergantung terhadap peran sebuah aktor dalam memahami dan membentuk ancaman dari kondisi sebenarnya menjadi ancaman keamanan itu sendiri. Definisi dari sekuritisasi yang sebenarnya dapat diimplementasikan untuk menggambarkan bagaimana konstruksi diskursif terhadap suatu ancaman, lebih dalam lagi mengenai hasil dari suatu konstruksi dapat memberikan

dampak terhadap kondisi politik sehingga memungkinkan aktor mengabaikan dan melanggar aturan-aturan maupun hukum yang seharusnya berlaku. (Soesilowati, 2011).

Pengkondisian sekuritisasi mengacu pada teorinya dapat dilakukan melalui rekayasa politik, yaitu menghubungkannya dengan kondisi darurat atua krisis melalui tindakan yang sulit untuk diterima dalam kondisi normal. Kondisi ini dikuatkan dengan statement yang dikemukakan oleh Buzan yaitu :

"... an actor has claimed a right to handle the issue through extraordinary means, to break the normal political rules of the games." (Buzan et al.1998, 24)

Melalui statement tersebut pengkodisan suatu keadaan menjadi darurat memungkinkan aktor untuk menyalahi ataupun melanggar aturan yang berlaku. Aktor politik dalam suatu negara yang memiliki otoritas ataupun wewenang yang kuat dalam menciptakan pertahanan negara, sudah selayaknya menciptakan keamanan yang tidak melanggar hak individu ketika menyelesaikan persoalan negara yang sedang dihadapi, namun dengan menerapkan rekayasa politik dengan alasan keamanan untuk menciptakan keamanan dari ancaman ataupun kondisi krisis yang besar, hal ini membuat setiap kewenangan dapta menjadi legal. Indonesia merupakan negara terbesar di Asia Tenggara dengan potensi ekonomi serta politik Kawasan regional. Tentu saja, masalah dunia siber sudah selayaknya menjadi sebuah masalah serius seiring jumlah akses dalam bidang politik, pertahanan negara, ekonomi melalui jaringan sistem internet dalam jumlah besar. Sehingga hal ini menimbulkan masalah yang tidak dapat dikatakan sepele terutama dalam keamanan data akses tersebut. Tidak hanya Indonesia, namun negara-negara lain juga memiliki masalah yang sama yaitu *cyberwarfare*. Kebutuhan akan keamanan dunia siber menjadi nyata dan mendesak karena pengaruhnya memiliki potensi merusak atau mengganggu negara bahkan seluruh dunia (Saudi, 2017).

Mengacu pada konteks legal, Indonesia memiliki kebijakan dalam menangnin masalah keamanan siber dengan mengeluarkan perundang-undangan, yaitu Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, UU mengenai keamanan siber yang telah diterbitkan oleh Pemerintah Indonesia hanya berfokus terhadap perlindungan transaksi elektronik dan belum menyentuh ruang lingkup siber yang lebih luas. Lemahnya undang-undang tersebut dapat dilihat dari beberapa contoh kasus yang dialami oleh pemerintah Indonesia. Pada tahun 2013, Pemerintah Indonesia menjadi sasaran penyadapan yang dilakukan oleh Badan Intelijen Australia dimana kasus penyadapan tersebut didapatkan dari seorang mantan anggota *National Security Agency* (NSA) Amerika, Edward Snowden. Dokumen yang bocor ke publik tersebut berisikan daftar-daftar target serangan penyadapan melalui telepon dimana Mantan Presiden Indonesia Susilo Bambang Yudhoyono serta Sembilan aktor politik terdekat di lingkaran presiden (Putra, Datumaya, & Sumari, 2016).

Kasus lainnya yang menjadi perhatian pemerintah Indonesia, melalui Lembaga Indonesia Security Incidents Response Team on Internet Infrastructure (ID-SIRTII) telah mencatat 48.4 juta kasus serangan siber yang ditujukan kepada Indonesia pada tahun 2014. Serangan-serangan siber tersebut juga menyerang situs-situs resmi pemerintah Indonesia seperti paspampres.mi.id, revolusimental.go.id, kesad.mil.id. Selain itu ID-SIRTII juga mencatat bahwa Indonesia sebagai negara terbesar di dunia yang terserang malware pada awal tahun 2015. Selain serangan-serangan yang berupa melumpuhkan ataupun mencuri data, dunia maya di Indonesia dimanfaatkan sebagai media propaganda, perekrutan anggota, atupun sarana penympangan ideologi yang aktor utamanya lebih mengarah kepada kelompok teroris serta Gerakan radikal lainnya. Berkaca pada kondisi keamanan siber Indonesia tersebut, aktor-aktor politik dengan wewenang kuat di Indonesia menciptakan isu-isu ancaman

keamanan siber Indonesia yang sudah darurat dan harus segera dilakukan tindakan dengan melibatkan berbagai cara (Putra et al., 2016).

Menyikapi hal itu pada tahun 2017 Menteri Koordinator Politik, Hukum, dan Keamanan yang pada saat itu dijabat oleh Wiranto mendesak pembentukan Badan Siber dan Sandi Negara (BSSN) kepada Presiden Joko Widodo. Kebijakan ini diusulkan oleh Wiranto setelah melakukan kunjungan kerja ke Singapura dengan pembahasan *cyber security*. Wiranto menyatakan *"Saya baru saja dari Singapura untuk melakukan suatu rapat koordinasi antarnegara mengenai cyber security. Di sana, Indonesia dianggap suatu negara yang paling penting dan punya potensi, bagaimana mengembangkan cyber security,"* kata Wiranto Seperti dikutip dari detik.com. Beliau juga berpendapat bahwa saat ini serangan siber di Indonesia sudah parah. Bila tidak segera diatasi, hal itu bisa sangat mengganggu. Wiranto juga menyampaikan untuk membentuk badan siber sesegera mungkin seperti dikutip dari detik.com "*Segera, segera. Karena ini sudah sangat mendesak*," kata Wiranto. Selain itu beliau juga menyampaikan bahwa badan siber baru tersebut akan menjadi payung dari semua Lembaga siber yang telah ada yakni BIN, Pertahanan, Mabes TNI, dan Polri (Damarjati, 2017).

Keterlibatan aktor-aktor penting politik Indonesia membuat Presiden Joko Widodo mengambil tindakan atas hal tersebut. Doronga kuat dari aktor politik tersebut membuat Presiden Joko Widodo mengambil langkah serius dengan mengeluarkan kebijakan untuk membentuk Badan Siber dan Sandi Negara melalui Peraturan Presiden nomor 53 tahun 2017 yang kemudian direvisi Perpres nomor 133 tahun 2017. Dalam suatu kesempatan Presiden Joko Widodo memaparkan bahwa Badan Siber dan Sandi Negara dibentuk sebagia Lembaga yang sangat penting dan dibutuhkan oleh negara

dalam mengantisipasi laju perkembangan dunia maya yang sangat cepat pertumbuhannya (Egeham, 2018).

2. Teori Kelembagaan

Teori Institusi memiliki definisi bahwa suatu Lembaga terbentuk akibat dari tekanan lingkungan institusional sehingga terjadi institusionalisasi. Dasar dari pemikiran teori tersebut ialah sebagai pertahanan hidup, sehingga suatu organisasi harus berperan untuk meyakinkan publik bahwa organisasi termasuk dalam entitas yang sah dan layak untuk mendapatkan dukungan. Scott (2008) memaparkan bahwa teori tersebut memiliki fungsi sebagai penjelasan terhadap tindakan serta pengambilan keputusan dalam suatu organisasi publik (Scott, 2008).

Scot dalam Hessels dan Terjesen (2008) menjelaskan bahwa struktur sosial yang telah mencapai ketahanan tertinggi merupakan suatu definsi dari kelembagaan dan budaya normative, regulative, kognitif yang sarat dengan perubahan merupakan aspek-aspek dari kelembagaan. Aspek-aspek tersebut mempengaruhi sumber daya dan kegiatan dalam memberikan stabilitas serta makna dalam kehidupan sosial secara bersamaan. Sebagi upaya dalam menciptakan stabilitas tersebut maka ada beberapa unsur yang perlu diperhatikan dalam sebuah Lembaga, seperti *norms, rules, cultural benefit*, peran dan sumber daya material. Unsur-unsur tersebut lah yang berperan dalam membentuk komitmen sebuah organisasi sebagai upaya memberikan stabilitas melalui berbagai program dan kebijakan yang ada (Scott, 2008).

Scott (2008) dalam Villadsen (2011) juga mendefinisikan melalui aspek-aspek diatas dapat menjelaskan peran suatu organisasi dan pengambilan keputusannya yang dipengaruhi oleh aturan dan keyakinan yang berjalan dalam lingkungan organisasi. Sebagai contoh seperti organisasi yang berfokus pada layanan publik, untuk mengambil keputusan organsasi tentunya dipengaruhi terhadap aturan dan

keyakinan yang berlaku pada pemerintah pusat, pemerintah daerah, dan lingkungan masyarakat. Melalui permisalan tersebut dapat disimpulkan bahwa suatu organisasi merupakan pihak yang dalam menerapkan kebijakannya harus mempunyai komitmen kuat dalam menjalankan tugasnya sehingga tujuan akhir dari kebijakan yang dikeluarkan dapat tercapai (Scott, 2008).

Mengacu pada teori kelembagaan oleh Scott, melihat lingkungan sosial yang telah berubah menjadi masyarakat digital dimana aktor-aktor didalam lingkungan tersebut termasuk aktor individu, dunia usaha, pemerintah, kelompok-kelompok tertentu, telah menciptakan budaya digital dimana aktor-aktor tersebut dapat bebas berinterkasi dan berkomunikasi. Pergeseran budaya tersebut tentunya dapat memicu gesekan kepentingan yang dapat menimbulkan konflik baru dalam masyarakat digital. Melihat kondisi tersebut, Indonesia berusaha menciptakan keamanan dunia digital dengan menerbitkan UU ITE. Namun pada kondisi lapangan Indonesia juga menghadapi permasalahan lebih besar dalam pembagian kewenangan serta otoritas untuk menanggulangi dampak lainnya seperti *cyber crime, cyber terrorism, cyber hacktivism, ataupun cyberwarfare*.

Dengan adanya tekanan-tekanan yang timbul dari lingkungan institusi di Indonesia mengharuskan pemerintah Indonesia membentuk sebuah Lembaga yang dapat menanggulangi ancaman diatas. Oleh sebab itu, Pemerintah Indonesia mengeluarkan kebijakan untuk mendirikan institusi yang dapat mengatasi ancaman tersebut dengan mendirikan Badan Siber dan Sandi Negara. Lembaga baru ini memiliki tugas selain meyakinkan publik Indonesia sebagai Lembaga yang dapat mengatasi ancaman dunia maya, disamping itu Badan Siber dan Sandi Negara bertugas sebagai koordinator Lembaga-lembaga lainnya yang memiliki peran penting dalam mengatasi ancaman siber tersebut. Mengingat bahwa dampak dari ancaman siber itu sendiri dapat mempengaruhi

ketahanan hidup sosial masyarakat Indonesia yang berdampak tidak hanya berdampak pada kerugian ekonomi saja, namun juga hak individu serta dapat mengganggu keutuhan dan kedaulatan negara. Maka, dengan dibentuknya Badan Siber dan Sandi Negara ialah sebuah keharusan dan kebutuhan guna menjawab perubahan lingkungan sosial yang terjadi dalam institusi maupun masyarakat Indonesia.

D. Hipotesa

Mengacu pada rumusan masalah dan kerangka teori yang telah dipaparkan diatas, maka hipotesa yang diajukan penulis sebagai berikut :

1. Adanya badan atau instansi khusus dalam penanganan serangan siber adalah sebagai upaya mewujudkan keamanan nasional.
2. Kedudukan kelembagaan yang optimal akan mampu mengatasi berbagai masalah dan tantangan masalah siber sehingga dapat meningkatkan pertumbuhan ekonomi nasional.

E. Metode Penelitian

Penulis menggunakan dua metode penelitian dalam menuliskan penelitian, diantaranya ialah metode deskriptif analitis dan metode historis :

1. Metode deskriptif analitis ialah metode yang digunakan dengan menggambarkan suatu peristiwa atau masalah secara sistematif hingga menjadi kajian yang diangkat sebagai topik yang sistematik dan menganalisis peristiwa yang diangkat menjadi topik melalui sudut pandang sebab-akibat dan penyusunan data. Metodi ini menganalisis masalah yang terjadi dalam ruang lingkup hubungan internasional termasuk dalam kegiatan, hubungan, pandangan, sikap, serta proses yang tengah berlangsung. Disamping itu, metodi ini juga memberikan pemaparan dalam menjelaskan hubungan, menguji hipotesa, membuat prediksi, serta menarik kesimpulan dan dampak dari masalah yang ingin dipecahkan.

2. Metode Historis Analis, ialah suatu metode yang digunakan untuk menganalisis sebuah kajian terdahulu secara garis besar untuk memahami kondisi saat ini agar perkembangannya lebih memungkinkan dimasa mendatang melalui cara dengan mengumpulkan, mengevaluasi, memverivikasi, serta mnegistensikan bukti-bukti kuat dan berguna untuk mendapatkan pehamanan dalam perkembangannya dimasa mendatang dengan sumber-sumber yang tersedia sebagai dasarnya.

F. Batasan Penelitian

Dalam penelitian ini peneliti membatasi masalah seputar kebijakan dan strategi Indonesia dalam menghadapi perang *cyber*. Kurun waktu yang dipilih mulai pada sebelum pemerintahan Presiden Joko Widodo sampai awal terbentuknya Badan Siber dan Sandi Negara.

G. Tujuan Penelitian

Tujuan yang ingin dicapai oleh penulis dalam menuliskan penelitian ini ialah sebagai berikut :

1. Memperoleh gambaran tentang kebijakan *cybersecurity* di Indonesia saat ini.
2. Memetakan prospek pengembangan *cybersecurity* di Indonesia dan tantangannya.
3. Mendapatkan kesimpulan efektivitas Badan Siber dan Sandi Negara menjadi payung pertahanan siber Indonesia.

H. Sistematika Skripsi

Sistematika penulisan yang akan dipaparkan oleh penulis dari penelitian ini ialah sebagai berikut :

1. BAB I merupakan landasan dalam melakukan penelitian dengan membahas latar belakang maslah, rumusan masalah, kerangka teori, penarikan hipotesa, Batasan masalah, tujuan penelitian, metode serta mengumpulan data yang digunakan oleh penulis.
2. Bab II penulis akan memaparkan mengenai keterlibatan Indonesia dalam *cyberwar* untuk pertama kalinnya. Namun

sebelumnya akan diulas terlebih dahulu mengenai tren dan pola *cyber attack* yang ada termasuk target, pelaku, dan dampak dari *cyber attack* tersebut.

3. Bab III akan berisi analisis mengenai alasan Indonesia sebagai mendirikan Lembaga baru yang berfokus pada pertahanan *cyber*. Bab ini akan dibagi menjadi dua bagian. Yang pertama akan mengulas *cyberattack* yang pernah terjadi di Indonesia. Bagian kedua kemudian akan melihat bagaimana strategi keamanan *cyber* Indonesia sebelum dibentuknya Badan Sber dan Sandi Negara.
4. Bab IV akan berisi analisis mengenai teori seukritisasi yang diterapkan oleh Indonesia dalam membentuk Badan Siber dan Sandi Negara terkait kepentingan pertahanan *cyber*nya untuk mempertahankan diri dari kemungkinan timbulnya *cyberwar*. Sedangkan bagian kedua akan membaha mengenai startegi petahanan *cyber* Indonesia melalui Badan Siber dan Sandi Negara dilihat dari Global *Cybersecurity* Index.
5. Bab V ialah penarikan kesimpulan dari penelitian yang telah dilakukan.