

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Cyber crime atau disebut dengan kejahatan dunia maya merupakan kejahatan yang menggunakan teknologi informasi dan komunikasi dengan menggunakan komputer, zaman global yang sedang berlangsung seperti saat ini mengubah kehidupan manusia baik secara komunikasi dan menunjang pekerjaan tidak bisa lepas dari peranan teknologi informasi dan komunikasi. Dalam hal ini, sebagai contoh maraknya penggunaan komputer yang menawarkan berbagai macam program aplikasi untuk menunjang efisiensi pekerjaan kita hingga merambat ke alat komunikasi yang juga menawarkan berbagai fasilitas program.

Pemanfaatan teknologi informasi dan komunikasi menyentuh hampir semua bidang mulai dari ekonomi, pendidikan, kesehatan hingga pertahanan dan keamanan. Teknologi informasi dan komunikasi sebagai salah satu unsur strategis dalam mendukung penyelenggaraan pertahanan dan keamanan sudah selayaknya mendapatkan perhatian lebih. Terlebih lagi dalam beberapa tahun terakhir, kejahatan yang melibatkan pembobolan atau pencurian informasi semakin gencar dan menyasar tidak hanya perorangan dan industri tetapi juga hingga ke level pemerintahan dalam bentuk penyadapan oleh intelijen luar negeri terhadap sejumlah pejabat pemerintahan Indonesia sehingga keamanan informasi sudah

selayaknya mendapatkan prioritas khususnya dalam menunjang kebutuhan Pertahanan Keamanan Nasional ¹.

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan internet dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalu dimukhtahirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat untuk lebih mendalam ada beberapa pendapat dibawah ini tentang apa yang dimaksud dengan *cyber crime*, diantaranya adalah menurut kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan mneyalahgunakan kemudahan teknologi digital ².

Walaupun kejahatan dunia maya atau *cyber crime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk

¹ Wirianto Pradono Yourdan, "Analisis kebijakan standardisasi keamanan perangkat telekomunikasi untuk menunjang kebijakan pertahanan dan keamanan nasional", *Buletin Pos dan Telekomunikasi* Vol. 13 No.2 (2015) hlm. 151-164.

² Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, (Jakarta: PT. Rafika Aditama, 2005), hlm. 40.

kegiatan kejahatan tradisional dimana peralatan komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi ³.

Cyber crime adalah contoh kecil dari kejahatan didunia maya yang saat ini masih terus datang dan itu tidak akan berhenti meskipun Indonesia memiliki organisasi intelejen yang kuat sekalipun, karena ancaman *cyber crime* bersifat continue, yang artinya meskipun dihentikan dari sektor A, maka dia akan bisa membuat cabang sektor didaerah lainnya karena kejahatan seperti ini tidak meninggalkan bukti fisik yang dapat diidentifikasi dengan alat pelacak. Namun dengan adanya Sumber Daya Manusia yang cukup ahli dibidang teknologi informasi dan mengerti akan keamanan protokol internet, hal ini tidak mustahil bahwa orang-orang yang bekerja dibidang intelejen bisa mengetahui sumber pelaku kejahatan dunia maya meskipun tidak datang langsung kepada si pelaku dengan bantuan teknologi informasi berbasis jaringan komputer dan internet.

Kekuatan pertahanan yang dimiliki oleh suatu negara dapat dilihat dari bentuk dan pengorganisasian intelijennya, dengan keberadaan institusi intelijen, maka perkembangan setiap wilayah bisa diolah dan dijadikan data ketahanan wilayah. Intelejen sebagai mata dan telinga negara memiliki peranan yang sangat penting dalam menjaga stabilitas dan mendeteksi suatu ancaman sedini mungkin. Untuk itulah Indonesia

³ Widodo, *Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime*, (Yogyakarta: Laksbang Mediatama, 2009), hlm. 24.

membentuk sebuah organisasi baru yang memiliki tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber yaitu dengan dibentuknya Badan Siber dan Sandi Negara.

Badan Siber dan Sandi Negara yang (selanjutnya disebut BSSN) resmi dibentuk sejak ditetapkannya Peraturan Presiden (yang selanjutnya disebut Perpres) Nomor 53 Tahun 2017 tentang Badan Siber Sandi Negara pada tanggal 19 Mei 2017 yang kemudian Perpres tersebut diperbarui lagi menjadi Perpres Nomor 133 Tahun 2017 Tentang Perubahan atas Perpres Nomor 53 tahun 2017 Tentang Badan Siber dan Sandi Negara pada tanggal 16 Desember 2017.

Pembentukan BSSN ditujukan untuk menggantikan Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara guna menjamin terselenggaranya kebijakan dan program pemerintah di bidang keamanan siber. BSSN merupakan lembaga pemerintah non kementerian yang (selanjutnya disebut LPNK) yang berada di bawah perintah Presiden dan bertanggung jawab kepada Presiden melalui menteri yang menyelenggarakan koordinasi, sinkronisasi, dan pengendalian penyelenggaraan pemerintahan di bidang hukum dan keamanan.

BSSN sebagaimana termuat dalam Perpresnya, merupakan lembaga pemerintah non kementerian yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan,

mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber. Posisi kelembagaan sebagai lembaga pemerintah non kementerian, pada saat tertentu akan mengalami kesulitan terutama saat melakukan tugas koordinasi dengan lembaga negara atau lembaga peradilan yang dalam tugasnya juga melakukan kegiatan pengamanan siber dan persandian.

Pada posisi yang demikian, BSSN sesungguhnya memerlukan posisi kelembagaan yang independen baik dalam menjalankan tugasnya maupun karena konten yang harus diamankan. Membandingkan dengan identifikasi tugas kelembagaan yang dimiliki oleh Badan Intelijen Negara yang (selanjutnya disebut BIN) yang juga memiliki tugas operasional dan tugas koordinasi, maka berdasarkan Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara yang (selanjutnya disebut UU Intelijen Negara), menyebutkan bahwa BIN merupakan alat negara yang menyelenggarakan fungsi Intelijen dalam negeri dan luar negeri.

Mengingat BSSN ini dibentuk dari lembaga sebelumnya yaitu Lembaga Sandi Negara (yang selanjutnya disebut LEMSANEG), jadi BSSN disini memiliki tugas baru yaitu dibidang siber dan fungsi sandi negara dimana fungsi ini adalah fungsi intelejen yang sudah banyak dimiliki oleh lembaga-lembaga intelejen yang sudah ada di Indonesia seperti Badan Intelijen Strategis Tentara Nasional Indonesia (selanjutnya disebut BAIS TNI), Intelijen Kejaksaan Agung Republik Indonesia (selanjutnya disebut Intelijen Kejaksaan RI), BIN, *Cyber Crime* POLRI.

Tentunya dengan banyaknya fungsi intelejen yang sudah dimiliki oleh banyak lembaga intelejen, BSSN ini seperti anak lembaga yang baru lahir dan belum mengerti akan tugas dan fungsinya yang masih samar-samar. Padahal tanpa membentuk lembaga baru pun sebenarnya Indonesia saat ini sudah memiliki unit untuk menangani ancaman siber yaitu BIN dan *Cyber Crime* POLRI yang memiliki kewenangan penyelidikan dan penyidikan untuk menangani kasus semacam *cyber crime*. Disinilah problematika yang sedang dihadapi pemerintah sekarang, karena untuk membentuk sebuah organisasi atau lembaga negara dibutuhkan anggaran yang tidak sedikit dan lagi belum untuk masalah sarana dan prasarana yang harus disediakan untuk kepentingan lembaga tersebut demi terciptanya keamanan nasional dibidang siber.

1.2. Rumusan Masalah

Dari uraian latar belakang masalah diatas, penulis mendapati permasalahan dengan menyimpulkan rumusan masalah sebagai berikut :

1. Mengapa dibentuk BSSN dengan tidak mengoptimalkan peran dari BIN, BAIS TNI, Intelijen Kejaksaan RI, *Cyber Crime* POLRI, dan LEMSANEG ?
2. Bagaimana jika ada *overlapping* antara BSSN, BIN, BAIS TNI, Intelijen Kejaksaan RI, *Cyber Crime* POLRI, dan LEMSANEG ?

1.3. Tujuan Penulisan

1. Untuk mengetahui dibentuknya Badan Siber dan Sandi Negara di Indonesia.
2. Untuk mengetahui jika terjadi tumpang tindih kewenangan antara Badan Siber dan Negara dengan lembaga-lembaga intelejen yang sudah ada.

1.4. Manfaat Penulisan

1.4.1. Manfaat Teoritis

- a. Hasil Penelitian ini diharapkan dapat memberikan informasi tentang pembentukan Badan Siber dan Sandi Negara di Indonesia.
- b. Memberi pemikiran baru dan pemahaman tentang keberadaan Badan Siber dan Sandi Negara.

1.4.2. Manfaat Praktis

Secara praktis diharapkan masyarakat mengetahui peran dari Badan Siber dan Sandi Negara di Indonesia.

1.5. Keaslian Penelitian

Dikarenakan belum banyak atau sedikitnya referensi yang meneliti tentang Lembaga Badan Siber dan Sandi Negara, maka dari itu hanya ada penelitian sebelumnya sebagai berikut :

Tabel 1 : Keaslian Penelitian dan Korelasinya

Penelitian Sebelumnya	Judul Penelitian	Fokus Pembahasan	Korelasi dengan Penelitian
Rocky Tumbur Pandapotan Siahaan, SH. Universitas Airlangga, 2015	Penyadapan Oleh Badan Intelijen Negara Dalam Memperoleh Bukti Permulaan Tindak Pidana	Memberikan deskripsi bahwa penyadapan pada dasarnya merupakan tindak pidana dalam tahap penyelidikan yang dilakukan oleh aparat penegak hukum dalam menangani perkara tindak pidana luar biasa	Membantu memberikan sumbangan pemikiran dalam fungsi dan tugas Badan Intelijen Negara dalam identifikasi masalah penyadapan yang dalam skripsi saya fokus pada fungsi intlejennya
Ginanjari Sapto Hadi Universitas Pembangunan Veteran Jawa Timur, 2012	Tindak Pidana <i>Cyber Crime</i> Dalam Persepektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik	Memberikan deskripsi bahwa apabila dalam proses pembuktian yang dilakukan oleh tim dari Kepolisian tidak menemukan bukti maka berkas kasus tidak dapat lengkap atau P21, maka berkas tersebut tidak dapat dilimpahkan ke pengadilan tetapi dalam proses pembuktian pada perkara <i>Cyber Crime</i> ini tentu saja dapat dilakukan dengan mengajukan bukti persidangan dengan hasil berupa print out atau dokumen elektronik.	Dalam skripsi penulis Ginanjari ini, membantu saya gambaran tentang penanganan kasus <i>Cyber Crime</i> yang ditangani oleh Polisi Republik Indonesia

Dimas Dyonata Aswitok, S.H. Universitas Trunojoyo Madura, 2018	Kewenangan Satuan Tugas Pungutan Liar Dalam Persepektif Hukum Tata Negara	Penelitian ini fokus pada pembahasan tentang wewenang SATGAS SABER PUNGLI yang juga dimiliki POLRI, Kejaksaan Agung, dan KPK	Korelasi penelitian ini dengan skripsi saya adalah sama- sama membahas tentang <i>overlapping</i> pembentukan lembaga negara.
--	--	---	---

Sumber : Kreasi Penulis

1.6. Metode Penelitian Hukum

1.6.1. Jenis Penelitian

Dalam penelitian ini, jenis penelitian yang digunakan oleh penulis adalah penelitian hukum normatif. Penelitian hukum normatif (*normatif law research*) menggunakan studi kasus hukum normatif berupa produk perilaku hukum, misalnya mengkaji rancangan undang-undang, pokok kajiannya adalah hukum yang dikonsepskan sebagai norma atau kaidah yang berlaku dalam masyarakat dan menjadi acuan perilaku setiap orang, sehingga penelitian hukum berfokus pada inventarisasi hukum positif dan doktrin, penemuan dalam perkara *in concreto*, sistematik hukum, taraf sinkronisasi hukum, perbandingan hukum, dan sejarah hukum ⁴.

1.6.2. Pendekatan Penelitian

Berdasarkan obyek penelitian, penelitian ini mempergunakan beberapa pendekatan. Pendekatan pertama adalah pendekatan perundang-

⁴ Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*, (Bandung : PT.Citra Aditya Bakti, 2004), cet 1, hlm 52.

undangan (*statute approach*) yaitu pendekatan yang menggunakan undang-undang sebagai kajiannya. Pendekatan kedua yaitu pendekatan kasus (*case approach*) adalah Pendekatan ini dilakukan dengan melakukan telaah pada kasus-kasus yang berkaitan dengan isu hukum yang dihadapi.

1.6.3. Sumber Bahan Hukum

Konsekuensi melaksanakan penelitian normatif, maka bahan yang dipergunakan dalam penelitian ini adalah bahan hukum, sebagai berikut:

a. Bahan Hukum Primer

Bahan hukum primer pada penelitian ini adalah bahan hukum yang menjadi fokus dalam melakukan penelitian skripsi ini, seperti :

1. UUD NRI Tahun 1945.
2. Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 2 dan Tambahan Lembaran Negara Republik Indonesia Nomor 4168).
3. Undang-undang Nomor 3 Tahun 2002 Tentang Pertahanan Negara (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 3).
4. Undang-undang Nomor 16 Tahun 2004 Tentang Kejaksaan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 67).

5. Undang-Undang Nomor 34 Tahun 2004 Tentang Tentara Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 127).
6. Undang-Undang nomor 17 tahun 2011 tentang Intelejen Negara (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 105 dan Tambahan Lembaran Negara Republik Indonesia Nomor 5249).
7. Peraturan Presiden Nomor 10 Tahun 2010 Tentang Susunan Organisasi Tentara Nasional Indonesia.
8. Peraturan Presiden Nomor 38 Tahun 2010 Tentang Organisasi dan Tata Kerja Kejaksaan Republik Indonesia.
9. Peraturan Presiden nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara.

b. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum pendukung untuk pengkayaan dan penguatan bahan hukum primer. Bahan hukum sekunder sebagaimana dimaksud, meliputi :

1. Risalah sidang pembentukan peraturan perundang-undangan.
2. Pendapat para ahli.
3. Buku-buku literatur hukum.
4. Skripsi dan tesis.
5. Disertasi atau laporan penelitian.

6. Artikel

c. Bahan Hukum Tersier.

Adapun bahan hukum tersier, diantaranya adalah sebagai berikut:

1. Kamus hukum.
2. Kamus bahasa.

1.6.4. Teknik Pengumpulan Bahan Hukum

Pengumpulan bahan hukum, baik itu bahan hukum primer, bahan hukum sekunder maupun bahan hukum tersier dilakukan dengan teknik sebagai berikut :

a. Bahan Hukum Primer

Pengumpulan bahan hukum primer dilakukan dengan cara studi kepustakaan hukum, inventarisasi peraturan perundang-undangan, dokumen-dokumen terkait dan dikelompokkan berdasarkan level atau hirarki peraturan perundang-undangan.

b. Bahan Hukum Sekunder

Bahan hukum sekunder dikumpulkan dengan melakukan kajian kepustakaan dan penelusuran terkait dengan hasil-hasil penelitian, seperti jurnal.

c. Bahan Hukum Tersier

Pengumpulan bahan hukum tersier dilakukan dengan melalui penelaahan pustaka, baik secara manual maupun melalui internet.

1.6.5. Analisis Bahan Hukum

Analisis bahan hukum merupakan langkah akhir dalam penelitian, sebelum memperoleh kesimpulan. Bahan hukum yang telah terkumpul dikaji, sehingga dapat dipergunakan untuk memperoleh gambaran dan jawaban yang jelas dan tepat terhadap permasalahan yang diteliti. Analisis yang dipergunakan dalam penelitian skripsi ini adalah yuridis kualitatif, yakni dengan cara mengumpulkan bahan hukum dan menghubungkan dengan gejala yang ada.

1.7. Sistematika Penulisan

Hasil Penelitian ini akan disusun dalam sistematika penulisan sebagai berikut :

Bab I : Pendahuluan

Dalam bab ini penulis akan membagi dalam 7 (tujuh) sub bab, yaitu Latar Belakang Masalah, Rumusan Masalah, Tujuan Penulisan, Manfaat Penulisan, Keaslian Penelitian, Metode Penelitian, dan Sistematika Penulisan.

Bab II : Tinjauan Pustaka

Dalam bab ini berisi landasan teori yang akan digunakan untuk menganalisis permasalahan yang ada dalam penulisan ini.

Bab III : Hasil Penelitian dan Pembahasan

Dalam bab ini berisi hasil penelitian dan pembahasan untuk menjawab permasalahan yang diangkat mengenai analisa terhadap Kewenangan Badan Siber dan Sandi Negara.

Bab IV : Penutup

Dalam bab ini berisikan penutup yang menguraikan secara singkat kesimpulan akhir dari pembahasan dan jawaban atas rumusan permasalahan dan disertai dengan saran saran yang didasarkan atas permasalahan yang diteliti.