**JURNAL ILMIAH**

**TINJAUAN YURIDIS KEWENANGAN BADAN SIBER DAN SANDI NEGARA DALAM PENANGGULANGAN SERANGAN SIBER**

**Program Studi Ilmu Hukum**



**Oleh :**

**HIDAYAT**

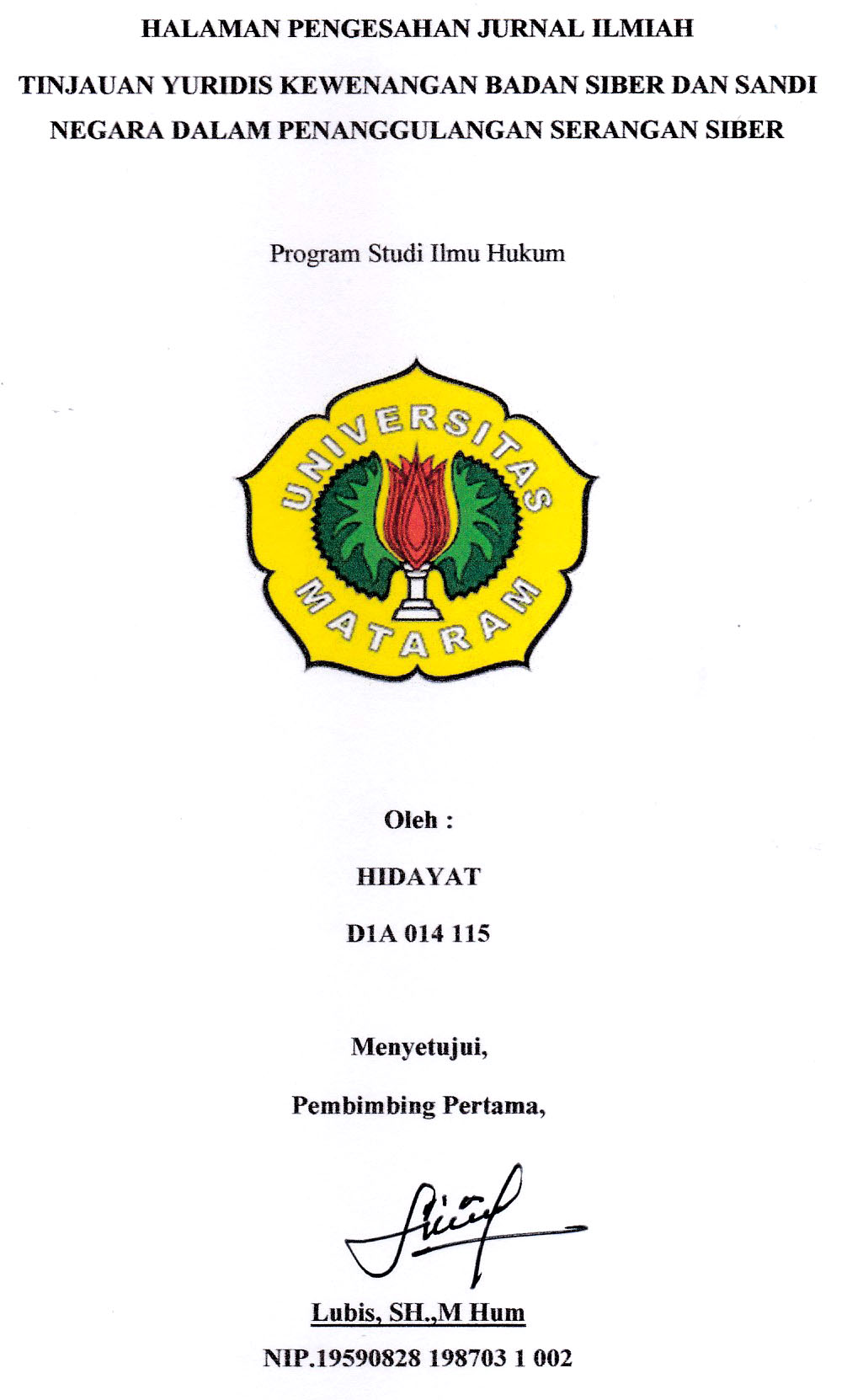
**D1A 014 115**

**FAKULTAS HUKUM**

**UNIVERSITAS MATARAM**

**MATARAM**

**2018**

****

ABSTRAK

TINJAUAN YURIDIS KEWENANGAN BADAN SIBER DAN SANDI NEGARA DALAM PENANGGULANGAN SERANGAN SIBER

HIDAYAT

D1A014115

FAKULTAS HUKUM

UNIVERSITAS MATARAM

Tujuan penelitian ini adalah untuk mengetahui dan memahami kewenangan dari Badan Siber dan Sandi Negara dalam menanggulangi serangan siber serta mengetahui hambatan yang dihadapi Badan Siber Dan Sandi Negara Dalam Penanggulangan Serangan Siber. Jenis penelitian yang digunakan penelitian Hukum Normatif, menggunakan pendekatan perundang-undangan dan pendekatan konseptual, Jenis bahan hukum yakni, bahan hukum primer, sekunder dan tersier. Bahan hukum dikumpulkan dengan studi dokumen, serta analisis menggunakan penafsiran sistematis. Hasil penelitian ini Badan Siber Dan Sandi Negara berwenang dalam melakukan penanggulangan insiden dan/atau serangan siber, pada bidang investigasi atau analisis dampak insiden, mitigasi pasca insiden, penanggulangan insiden dan pemulihan pasca insiden. Hambatan yang dialami Badan Siber Dan Sandi Negara dalam melakukan upaya penanggulangan serangan siber yakni infrastruktur teknologi komunikasi informasi yang belum merata, regulasi yang masih tumpang tindih, ketergantungan pada produk impor serta kurangnya kualitas dan kuantitas talenta sumber daya manusia di bidang siber.

Kata kunci : Badan Siber Dan Sandi Negara, Penanggulangan, Serangan Siber

***ABSTRACT***

***JURIDICAL REVIEW OF THE AUTHORITY OF NATIONAL CYBER AND CRYPTO AGENCY IN CONTROLLING THE CYBER ATTACK***

***HIDAYAT***

***D1A014115***

***FACULTY OF LAW***

***UNIVERSITY OF MATARAM***

*The purposes of this study are to discover and understand the authority of National Cyber and Crypto Agency in dealing with cyber attacks and find out the obstacle faced by National Cyber and Crypto Agency in overcoming cyber attack. This research is a normative law reseach type, by use of statute approach and conceptual approach, type object of law is primer, seconder and tertiary object. The object of law to collectable with document study, and the analysis use the systematic interpretation. The results of this study that National Cyber and Crypto Agency is an authorized agent to handle any cyber incident and/or attack, in the field of investigation or analyizing the impact, post-incident mitigation, incident management amd post-incident recovery. The obstacles experienced by National Cyber and Crypto Agency to overcome cyber attack are the infrastruscture of information communication technology that is not evenly distributed, overlapping regulations, dependence on impoted product and the lack of quality and quantity of human resources in cyberspace.*

*Keyword: National Cyber and Crypto Agency, Countermeasures, Cyber Attack.*

1. **PENDAHULUAN**

Kebutuhan manusia dalam kehidupannya sangat komplit dan luas. Tidak terbatas pada kebutuhan materil saja melainkan juga kebutuhan non materil. Salah satu bentuk kebutuhan non materil yang selalu ingin diwujudkan tersebut adalah rasa aman.. Kehidupan yang tidak terlepas dari pengaruh teknologi ini juga memerlukan perlindungan dan adanya rasa aman dari penyalahgunaan teknologi oleh pihak-pihak yang tidak bertanggung jawab yang dapat mengakibatkan rusak, hilang bahkan musnahnya data informasi atau informasi elektronik yang dimiliki oleh seseorang atau instansi.

Pengakuan adanya hak seseorang atas perlindungan dan rasa aman tercantum dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyebutkan;

“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.”

Sebagai perwujudan komitmen pemerintah dalam memberikan perlindungan tersebut maka diberlakukan suatu peraturan perundang-undangan yang melindungi hak-hak tersebut melalui salah satunya produk legislasi yang berupa Kitab Undang-Undang Hukum Pidana yang pada perkembangannya sulit menjangkau jenis-jenis kejahatan yang dinilai baru dan berbeda dengan kejahatan konvensional, salah satunya kejahatan di bidang teknologi informasi yang disebut dengan kejahatan siber, juga dikenal sebagai serangan siber.

Usaha untuk menjangkau kejahatan dalam bidang siber yang tidak dapat diakomodir oleh Kitab Undang-Undang Hukum Pidana, dibentuklah suatu undang-undang khusus yang mengatur bidang siber dan mengenai tindak pidana di bidang siber yakni Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik jo Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, walaupun telah diberlakukan dan diadakannya perubahan namun serangan siber yang terjadi sulit untuk di tanggulangi, dikarenakan tindakan penanggulangan serangan siber pada mulanya dilakukan secara terpisah-pisah

Sebagai langkah antisipasi maka pemerintah membentuk Badan Siber dan Sandi Negara atau yang disingkat BSSN melaui Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara ,yang mempunyai tugas khusus untuk melakukan penyusunan kebijakan, pelaksana kebijakan dan evaluasi kebijakan dalam bidang siber khususnya penanggulangan serangan siber.

Berdasarkan latar belakang yang telah penyusun paparkan di atas, penyusun tertarik untuk meneliti lebih mendalam mengenai kewenangan Badan Siber Dan Sandi Negara dalam penanggulangan serangan siber, oleh karena itu penyusun mengangkat hal tersebut dalam penelitian dengan judul Tinjauan Yuridis Kewenangan Badan Siber Dan Sandi Negara Dalam Penanggulangan Serangan Siber.

Penelitian ini membahas permasalahan mengenai bagaimana kewenangan Badan Siber Dan Sandi Negara Dalam Penanggulangan Serangan Siber ? dan apa saja kendala atau hambatan yang dihadapi Badan Siber Dan Sandi Negara Dalam Penanggulangan Serangan Siber ?. Tujuan penelitian ini adalah untuk mengetahui dan memahami kewenangan dan kendala dari Badan Siber dan Sandi Negara dalam menanggulangi serangan siber. Jenis penelitian ini adalah penelitian Hukum Normatif dengan menggunakan pendekatan Perundang-undangan dan Pendekatan konseptual. Jenis bahan hukum yakni, bahan hukum primer, sekunder dan tersier. Bahan hukum dikumpulkan dengan studi dokumen, serta analisis menggunakan penafsiran sistematis.

1. **HASIL PENELITIAN DAN PEMBAHASAN**
   1. **Kewenangan Badan Siber Dan Sandi Negara Dalam Penanggulangan Serangan Siber**

Dalam Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara jo Peraturan Presiden Nomor 133 Tahun 2017 Tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara, beberapa tugas dan fungsi dari BSSN yang merupakan kewenangannya selaku lembaga khusus yang dibentuk untuk mengamankan bidang siber di indonesia. Tugas BSSN tersebut terdapat pada Pasal 2 dan fungsi dari BSSN terdapat dalam Pasal 3.

Pasal 2 Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara menyatakan,

BSSN mempunyai tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber.

Dari bunyi Pasal 2 di atas dapat dilihat bahwa tugas BSSN adalah melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur terkait keamanan siber.

Berdasarkan Pasal 2 Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara yang menyatakan BSSN memiliki tugas mengkonsolidasikan atau badan yang memperkuat dan meneguhkan hubungan semua unsur terkait keamanan siber, keberadaan dari BSSN di dalam sektor pengamanan siber berposisi sebagai pusat koordinator atau *coordinating center* dalam melakukan pengamanan dalam bidang siber di Indonesia yang memanfaatkan serta mengembangkan semua unsur yang telah di bentuk dalam masing-masing instansi atau bidang.

Sedangkan Pasal 3 menyatakan,

Dalam melaksanakan tugas sebagaimana dimaksud dalam Pasal 2, BSSN menyelenggarakan fungsi:

1. penyusunan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi e-commerce, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber;
2. pelaksanaan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi e-commerce, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan, penanggulangan kerentanan, insiden dan/atau serangan siber;
3. pemantauan dan evaluasi kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi e-commerce, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber;
4. pengoordinasian kegiatan fungsional dalam pelaksanaan tugas BSSN dan sebagai wadah koordinasi bagi semua pemangku kepentingan;
5. pelaksanaan pembinaan dan pemberian dukungan administrasi kepada seluruh unit organisasi di lingkungan BSSN;
6. pengawasan atas pelaksanaan tugas BSSN;
7. pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN; dan
8. pelaksanaan kerjasama nasional, regional, dan internasional dalam urusan keamanan siber.

Dari bunyi Pasal 3 di atas bahwa ada empat (4) fungsi pokok BSSN yakni melakukan penyusunan, pelaksanaan, pemantauan dan evaluasi serta pengoordinasi teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi e-commerce, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber.

Dalam Pasal 3 Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara yang membahas mengenai fungsi dari BSSN secara jelas menyatakan fungsi dari BSSN salah satunya adalah pemulihan penanggulangan insiden dan atau serangan siber. Maka dari pernyataan Pasal 3 ini memberikan kewenangan secara langsung atributif oleh hukum melalui peraturan perundang-undangan khususnya Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara kepada BSSN sendiri dalam melakukan pemulihan dan penanggulangan insiden dan/atau serangan siber.

Kewenangan yang diberikan dalam hubungannya dengan serangan siber (*cyber attack*) terbatas hanya pada pemulihan dan penanggulangan. Proses pemulihan insiden dan/atau serangan siber dilakukan setelah terjadinya serangan siber yang merusak komputer atau sistem komunikasi, sedangkan proses penanggulangan insiden dan/atau serangan siber dilakukan sebelum terjadinya serangan siber yang hal ini merupakan upaya preventif dari penanggulangan serangan siber.

Dalam menghadapi insiden atau serangan siber yang merupakan tugas dan fungsinya sebagaimana dalam Pasal 2 dan Pasal 3 Peraturan Presiden Nomor 35 Tahun 2017 Tentang Badan Siber dan Sandi Negara, BSSN memiliki deputi yang fokus pada penanggulangan dan pemulihan insiden atau serangan siber yaitu Deputi Bidang Penanggulangan dan Pemulihan. Menurut Pasal 19 Peraturan Presiden Nomor 35 Tahun 2017 Tentang Badan Siber dan Sandi Negara, Deputi Penanggulangan dan Pemulihan bertugas

Deputi Bidang Penanggulangan dan Pemulihan mempunyai tugas melaksanakan penyusunan dan pelaksanaan kebijakan teknis di bidang penanggulangan dan pemulihan keamanan siber pada jaringan komunikasi pemerintah, infrastruktur vital nasional, dan ekonomi digital.

Tugas pada deputi ini dalam penyusunan kebijakan serta pelaksanaan kebijakan penanggulangan dan pemulihan keamanan siber pada jaringan komunikasi pemerintah, infrastruktur vital nasional dan ekonomi digital. Dalam melaksanakan tugasnya Deputi Penanggulangan dan pemulihan memiliki beberapa fungsi sebagaimana terdapat dalam Pasal 20 menyebutkan

Dalam melaksanakan tugas sebagaimana dimaksud dalam Pasal 19, Deputi Bidang Penanggulangan dan Pemulihan menyelenggarakan fungsi:

1. Penyusunan kebijakan teknis di bidang investigasi dan analisis dampak insiden, mitigasi pasca insiden, penanggulangan insiden, dan pemulihan pasca insiden di bidang keamanan siber;
2. Koordinasi dan pelaksanaan investigasi dan analisis dampak insiden, mitigasi pasca insiden, penanggulangan insiden, dan pemulihan pasca insiden di bidang keamanan siber;
3. Pengendalian pelaksanaan kebijakan teknis di bidang investigasi dan analisis dampak insiden, mitigasi pasca insiden, penanggulangan insiden, dan pemulihan pasca insiden di bidang keamanan siber;
4. Pelaksanaan evaluasi dan pelaporan di bidang investigasi dan analisis dampak insiden, mitigasi pasca insiden, penanggulangan insiden, dan pemulihan pasca insiden di bidang keamanan siber; dan
5. Pelaksanaan fungsi lain yang diberikan oleh Kepala.

Fungsi Deputi Penanggulangan dan Pemulihan BSSN, memiliki empat bidang fokus dalam melakukan penyusunan kebijakan, koordinasi dan pelaksanaan, pengendalian dan evaluasi insiden atau serangan siber yakni : a. Bidang investigasi dan analisis dampak insiden atau serangan siber, b. Mitigasi pasca insiden atau serangan siber, c. Penanggulangan insiden atau serangan siber serta, d. Pemulihan pasca insiden atau serangan siber.

1. Investigasi Dan Analisis Dampak Insiden Atau Serangan Siber

Dalam Kamus Besar Bahasa Indonesia, Investigasi diartikan sebagai penyelidikan dengan mencatat atau merekam fakta melakukan peninjauan, percobaan, dan sebagainya, dengan tujuan memperoleh jawaban atas pertanyaan (tentang peristiwa, sifat atau khasiat suatu zat, dan sebagainya);penyidikan. Maka deputi ini memiliki fungsi untuk melakukan penyelidikan terhadap serangan siber yang telah terjadi, penyelidikan tersebut dapat meliputi bentuk dan jenis serangan, asal serangan atau profil penyerang, investigasi ini merupakan bagian dari pemulihan.

1. Mitigasi Pasca Insiden Atau Serangan Siber

Setelah atau pasca insiden serangan siber terjadi, deputi ini juga memiliki fungsi mitigasi. Mitigasi atau proses pengurangan resiko dengan pembangunan fisik atau penyadaran dan peningkatan kemampuan untuk mengatasi insiden atau serangan siber. sebelum dapat mempengaruhi atau mengancam target.

1. Penanggulangan Insiden Atau Serangan Siber

. Penanggulangan insiden atau serangan siber terbagi manjadi 3 (tiga) bagian yakni preemtif, preventif dan represif. a.) Tindakan Pre-emtif : Dalam penanggulangan serangan siber secara pre-emtif ini Deputi Penanggulangan dan Pemulihan dapat melakukan koordinasi sebagaimana disebutkan yang merupakan fungsinya, koordinasi yang dilakukan dapat dilakukan diantaranya dengan Deputi Bidang Identifikasi dan Deteksi.

Istilah identifikasi dalam bahasa indonesia memiliki arti sebagai bentuk proses pengenalan, sedangkan deteksi diartikan usaha menemukan dan menentukan keberadaan, anggapan atau kenyataan, sedangkan menurut NIST (*National Institute of Standars and Technology*) memberikan pengertian identifikasi dan deteksi sebagai bagian dari Framework fungsi dalam keamanan siber.

*Identify (function) Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities, Detect (function) Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event*.[[1]](#footnote-1)

Terjemahan bebasnya Mengidentifikasi (fungsi)Mengembangkan pemahaman organisasi untuk mengelola *cybersecurity* risiko sistem, aset, data, dan kemampuan.Mendeteksi (fungsi)Mengembangkan dan melaksanakan kegiatan sesuai untuk mengidentifikasi terjadinya peristiwa *cybersecurity*. b.) Tindakan Preventif :Usaha preventif pada intinya menekankan kepada pencegahan atau penghindaran dari beberapa pihak terhadap tindak pidana dengan menghilangkan setiap kesempatan insiden atau serangan siber. maka untuk melakukan kegiatan preventif ini Deputi Penanggulangan dan Pemulihan dapat melakukan koordinasi dengan Deputi Bidang Proteksi.Dalam rangka melaksanakan tugas dan fungsi keamanan siber BSSN juga memiliki Deputi Bidang Proteksi. Dalam Kamus Besar Bahasa Indonesia proteksi diartikan sebagai perlindungan. Disebutkan bahwa dalam Pasal 16 Peraturan Presiden Nomor 25 Tahun 2017 Tentang Badan Siber Dan Sandi Negara, Deputi Bidang Proteksi memiliki fungsi

1. penyusunan kebijakan teknis di bidang jaminan keamanan informasi, infrastruktur informasi kritikal nasional dan publik di bidang keamanan siber;
2. koordinasi dan pelaksanaan kebijakan teknis di bidang keamanan siber pemerintah, jaminan keamanan infrastruktur informasi kritikal nasional dan publik;
3. pengendalian pelaksanaan kebijakan teknis di bidang jaminan keamanan informasi dan infrastruktur informasi kritikal nasional dan publik di bidang keamanan siber;
4. pelaksanaan evaluasi dan pelaporan di bidang jaminan keamanan informasi, infrastruktur informasi kritikal nasional dan publik di bidang keamanan siber; dan
5. pelaksanaan fungsi lain yang diberikan oleh Kepala sesuai dengan bidangnya.

Dari pasal 16 di atas bahwa fungsi deputi bidang proteksi hanya pada jaminan keamanan infromasi, infrastruktur infromasi krtikal nasional dan publik. Menurut NIST kritikal infrastruktur adalah

*Critical Infrastructure is Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters*.[[2]](#footnote-2)

Terjemahannya Kritis Infrastruktur adalahSistem dan aset, baik fisik maupun virtual, sehingga penting untuk Amerika Serikat bahwa ketidakmampuan atau kerusakan sistem dan aset tersebut akan memiliki dampak melemahkan pada cybersecurity, keamanan ekonomi nasional, kesehatan publik nasional atau keselamatan, atau kombinasi dari hal-hal tersebut.

Dalam melakukan perlindungan atau proteksi khususnya pada kritikal nasional banyak cara dilakukan disesuaikan dengan kebutuhan salah satunya *Access Control System*Akses kontrol didefinisikan sebagai jantungnya keamanan.

Akses kontrol dapat berupaidentifikasi, autentifikasi, autorisasi, model akses kontrol, teknik akses kontrol, metodeakses kontrol, administrasi akses kontrol dan ancaman terhadap akses kontrol. Akseskontrol dapat didefinisikan pula sebagai kemampuan untuk mengijinkan hanya penggunayang diberi otorisasi, program atau proses sistem atau akses sumber daya. Ataupunpemberian hak atau penolakan, berdasarkan model keamanan khusus, kepastian perijinanuntuk mengakses sumber daya.[[3]](#footnote-3)

Selain itu juga proteksi juga dapat dilakukan dengan Kriptografi atau ilmu persandian, oleh karena alasan perlindungan di bidang keamanan siber dibutuhkan jaminan keamanan, seperti yang dikatakan Mulyadi

Sandi atau yang juga populer dengan istilah kriptografi menjadi bagian yang tidak terpisahkan dari teknologi informasi dan komunikasi. Urgensi keberadaan kriptografi adalah bagaimana data-data/informasi berupa gambar, suara, maupun tulisan atau dalam bentuk lainnya yang bersifat privat senantiasa terjamin keamanannya dari waktu ke waktu seiring berkembangnya teknik-teknik serangan, pencurian, modifikasi, pemalsuan di dunia siber ataupun perkembangan TIK itu sendiri. Maka, implementasi kriptografi mau tidak mau harus mampu menjawab perkembangan tersebut[[4]](#footnote-4)

c.) Tindakan Represif : Upaya ini sering disebut juga dengan penegakan hukum *(law enforcement)*. Penanggulangan dengan upaya represif untuk menindak para pelaku tindak pidana sesuai dengan perbuatannya serta memperbaikinya kembali agar mereka sadar bahwa perbuatan yang dilakukan adalah melanggar hukum dan merugikan. Maka untuk upaya represif terhadap insiden atau serangan siber deputi dapat melakukan koordinasi dengan beberapa pihak dalam organisasi BSSN seperti Deputi Bidang Pemantauan dan Pengendalian dan diluar organisasi BSSN yakni aparat penegak hukum seperti Kepolisian Negara Republik Indonesia.

1. Pemulihan Pasca Insiden Atau Serangan Siber

Dalam pemulihan, administrator mengembalikan sistem untuk beroperasi secara normal, mengkonfirmasi bahwa sistem berfungsi normal, dan (jika ada) pemulihan kerentanan untuk mencegah insiden serupa. Pemulihan melibatkan tindakan seperti memulihkan sistem, membangun kembali sistem dari awal, mengganti file dikompromikan dengan versi baru, menginstal patch, mengubah password, dan menguatkan jaringan perimeter keamanan (misalnya, aturan firewall, daftar batas router kontrol akses), meningkatkan sistem login serta monitoring jaringan secara berkala.

* 1. **Bentuk-Bentuk Koordinasi BSSN dengan Beberapa Unsur Terkait Keamanan Siber**

BSSN sebagaimana daam Pasal 2 Peraturan Presiden Nomor 53 Tahun 2017 merupakan lembaga utama yang mengkoordinasikan kegiatannya dalam keamanan di bidang siber maka BSSN untuk merealisasikan kegiatan penanggulangan siber dapat melakukan tindakan-tindakan yang untuk mencegah dan menanggulangi serangan siber dengan berkoordinasi dengan beberapa pihak terkait keamanan siber.

Berdasarkan hal tersebut untuk penanganan *cyber crime* atau kejahatan mayantara BSSN dapat melakukan koordinasi dengan penyidik aparat Kepolisian ataupun PPNS Kementerian Komunikasi dan Informatika dalam hal. BSSN dapat melakukan pelaporan ataupun pengaduan terhadap serangan siber yang telah dikategorikan sebagai tindak pidana sebagaimana yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Jo Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Selain pelaporan dan pengaduan terhadap tindak pidana dalam bidang elektronik BSSN dapat juga melakukan tindakan investigasi atau penyidikan. Tugas penyidikan yang diberikan kepada Badan Siber Dan Sandi Negara khususnya kepada organ dalam Badan Siber Dan Sandi Negara yakni kepada Deputi Bidang Pemantauan Dan Pengendalian sebagaimana dalam Pasal 24 huruf a dan b Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara menyebutkan bahwa;

Dalam melaksanakan tugas sebagaimana dimaksud dalam Pasal 23, Deputi Bidang Pemantauan dan Pengendalian menyelenggarakan fungsi:

1. Penyusunan kebijakan teknis di bidang standardisasi sumber daya, sertifikasi produk, akreditasi lembaga pendidikan dan pelatihan dan lembaga sertifikasi profesi sumber daya keamanan siber, serta penyidikan, digital forensik dan penapisan konten;
2. Koordinasi dan pelaksanaan kebijakan teknis di bidang standardisasi sumber daya, sertifikasi produk, akreditasi lembaga pendidikan dan pelatihan dan lembaga sertifikasi profesi sumber daya keamanan siber, serta penyidikan, digital forensik dan penapisan konten;

Tugas penyidikan yang menjadi fungsi Deputi Pemantauan Dan Pengendalian ada pada bagian direktorat pengendalian informasi, investigasi dan forensik digital dengan sub direktorat dukungan penyidikan. Dalam pasal 180 Peraturan Kepala BSSN Nomor 2 Tahun 2018 Tentang Organisasi Dan Tata Kerja Badan Siber Dan Sandi Negara menyebutkan bahwa;

Subdirektorat Investigasi dan Dukungan Penyidikan mempunyai tugas melaksanakan penyiapan penyusunan, koordinasi, pelaksanaan, evaluasi, dan pelaporan kebijakan teknis di bidang investigasi penyelenggaraan persandian dan sumber daya persandian, serta kerja sama dan dukungan penyidikan tindak pidana kejahatan siber.

Penyidikan yang dimaksud dalam Pasal 24 Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara adalah dukungan penyidikan terhadap tindak pidana kejahatan siber. Dukungan penyidikan dari Badan Siber Dan Sandi Negara terhadap tindak pidana kejahatan siber yang dimaksudkan oleh Pasal 180 peraturan kepala BSSN Nomor 2 tahun 2018 yakni dapat berupa analisis penyandian dan forensik digital terhadap bukti digital untuk mendukung pembuktian tindak pidana kejahatan siber, sebagaimana dalam pasal 181 menyebutkan bahwa;

Subdirektorat Forensik Digital dan Analisis Kripto mempunyai tugas melaksanakan penyiapan penyusunan, koordinasi, pelaksanaan, evaluasi, dan pelaporan kebijakan teknis di bidang analisis penyandian dan forensik digital terhadap bukti digital untuk mendukung pembuktian tindak pidana kejahatan siber.

Selain hal itu, BSSN dapat melakukan koordinasi dengan Kementerian Komunikasi Dan Informatika dalam hal penindakan terhadap serangan siber yang terkategori sebagai hoaks atau berita dan atau informasi palsu yang menyesatkan dan merupakan propaganda masyarakat.

Dalam hal *cyber spionage* atau *cyber intelligence* **BIN sebagai lembaga terdepan dalam bidang Intelijen memang harus memperkuat lini cyber intelligence-nya, walaupun pemerintah sudah menandatangani terbentuknya Badan Siber dan Sandi Negara atau BSSN sebagai badan yang menjaga keamanan siber, namun tugas cyber intelligence tetaplah di tangan BIN. BSSN jelas tidak bermain di ranah tugas mata-mata yang mengawasi setiap potensi ancaman.**

Tugas dan fungsi BSSN dengan tugas dan fungsi deputi intelijen siber milik BIN berbeda, posisi BSSN dalam hal ini adalah sebagai central coordinator dalam bidang keamanan siber, yang tentu sebagaimana dalam Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara Pasal 2 , sedangkan posisi deputi intelijen siber milik BIN sebagai unit pelaksana intelijen yang menggunakan sarana siber untuk melakukan pendeteksian terhadap segala ancaman negara dengan demikian BIN memberikan penilaian tindakan-tindakan di wilayah siber yang bisa membahayakan keamanan nasional serta keberadaan BSSN tidak berarti meniadakan fungsi cyber intelligence BIN. Keduanya saling melengkapi dan bekerja sama untuk keamanan di bidang siber di Indonesia.

* 1. **Hambatan atau Kendala Badan Siber Dan Sandi Negara Dalam Penaggulangan Serangan Siber**

Dalam melaksanakan tugas dan fungsinya Badan Siber Dan Sandi Negara tentunya memiliki beberapa hal yang menjadi kendala serta hambatan. Hal ini dikarenakan lembaga ini merupakan lembaga baru yang merupakan pusat seluruh koordinasi dari pengamanan di bidang siber di Indonesia serta ini dikarenakan bidang siber terus mengalami kemajuan di dukung dengan teknologi yang semakin berkembang serta mudahnya mengakses informasi dan komunikasi.

Berdasarkan surat jawaban resmi Badan Siber dan Sandi Negara yang dikirimkan melalui Kepala Biro Hukum dan Humas Bapak Y.B. Susilo Wibowo, S.E, M,M., Selain memiliki potensi yang sangat besar di ranah ekonomi digital di indonesia, di sisi lain Indonesia juga mempunyai hambatan. Beberapa hambatan tersebut meliputi masalah belum meratanya infrastruktur teknologi informasi di berbagai daerah di indonesia, permasalahan-permasalahan regulasi-regulasi yang harus segera disesuaikan, serta adanya regulasi yang tumpang tindih antara di pusat dan daerah. Hambatan lain terkait ekonomi digital adalah struktur industri teknologi informasi yang masih ketergantungan terhadap jasa dan produk-produk impor. Ketiadaannya undang-undang dan/atau belum disahkannya undang-undang yang menguatkan kewenangan BSSN juga menjadi tantangan dalam upaya penguatan BSSN kedepan. Ditinjau dari sisi supply dan demand, suplai dari ranah ekonomi digital ini masih memiliki hambatan yaitu masih kurangnya kuantitas dan kualitas talenta sumber daya manusia. Indonesia masih memiliki kekurangan jumlah dan kompetensi sumber daya manusia di bidang *programming*, *coding* dan *cyber security*.

1. **PENUTUP**

Kesimpulan pada penelitian ini : 1. Badan Siber Dan Sandi Negara memiliki kewenangan dalam melakukan penanggulangan insiden dan/atau serangan siber sebagaimana tertuang pada Pasal 3 Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara, bentuk penanggulangan serangan siber yang diberikan terdapat dalam fungsi Deputi Penanggulangan dan Pemulihan yang meliputi 4 (empat) bidang yakni Bidang Investigasi dan Analisis Dampak Insiden atau Serangan Siber, Bidang Mitigasi Pasca Insiden atau Serangan Siber, Penanggulangan Insiden atau Serangan Siber Dan Pemulihan Pasca Insiden atau Serangan Siber. 2. Hambatan atau kendala yang dialami Badan Siber Dan Sandi Negara dalam melakukan upaya penanggulangan serangan siber yakni infrastruktur teknologi komunikasi informasi yang belum merata, regulasi yang masih tumpang tindih, ketergantungan pada produk impor serta kurangnya kualitas dan kuantitas talenta sumber daya manusia di bidang siber .

Adapun saran yang penyusun berikan : 1. Perlu dilakukannya percepatan proses legislasi pada tubuh Badan Siber dan Sandi Negara untuk mengatur mengenai bentuk kegiatan, pembuatan pedoman atau rencana strategis Badan Siber Dan Sandi Negara dalam melakukan penanggulangan terhadap serang siber. 2. Diperlukannya penjelasan yang lebih detail mengenai fungsi dan tugas masing-masing Deputi dalam Badan Siber dan Sandi Negara, serta diperlukannya pendidikan atau pelatihan untuk meningkatkan sumber daya manusia yang ahli dalam di bidang teknologi.

1. **DAFTAR PUSTAKA**
2. Buku, Artikel dan Jurnal

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018 hlm. 7, dari laman <https://doi.org/10.6028/NIST.CSWP.04162018>, diakses pada tanggal 10 September 2018 pukul 12.05 WITA.

Siti Rohajawati, *Proteksi Dan Teknik Keamanan Sistem Informasi (Studi Kasus Pt. Percetakan Dan Penerbitan Jaya)*, (Makalah), Program Magister Teknologi Informasi Fakultas Ilmu Komputer Universitas Indonesia 2004, hlm. 14.

1. Peraturan Perundang-undangan

Indonesia, *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*;

Indonesia, *Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik*;

Indonesia*, Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara*;

Indonesia, *Peraturan Presiden Nomor 133 Tahun 2017 Tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara;*

Indonesia, *Peraturan Kepala Badan Siber Dan Sandi Negara Nomor 2 Tahun 2018 Tentang Organisasi Dan Tata Kerja Badan Siber Dan Sandi Negara.*

1. Website

Mulyadi, *Menilik Ruh Sandi dalam BSSN*, Artikel dan Opini, Sep 7, 2017, dari laman <http://BSSN.go.id> diakses pada tanggal 16 April 2018 pukul 14.30 WITA.

1. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018 hlm. 7, dari laman <https://doi.org/10.6028/NIST.CSWP.04162018>, diakses pada tanggal 10 September 2018 pukul 12.05 WITA [↑](#footnote-ref-1)
2. Ibid, hlm. 45 [↑](#footnote-ref-2)
3. Siti Rohajawati, *Proteksi Dan Teknik Keamanan Sistem Informasi (Studi Kasus Pt. Percetakan Dan Penerbitan Jaya)*, (Makalah), Program Magister Teknologi Informasi Fakultas Ilmu Komputer Universitas Indonesia 2004, hlm. 14 [↑](#footnote-ref-3)
4. Mulyadi, *Menilik Ruh Sandi dalam BSSN*, Artikel dan Opini, Sep 7, 2017, dari laman <http://BSSN.go.id> diakses pada tanggal 16 April 2018 pukul 14.30 WITA [↑](#footnote-ref-4)