MATRA PEMBARUAN
Jurnal Inovasi Kebijakan

ARTIKEL

Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah

The Implementation of Policy for the Establishment of a Cyber Incident Response Team to Support Information Security in the Government Sector

Prabaswari [1*], **Muhamad Alfikri** [2], **Irdam Ahmad** [3]

[1,2,3] Universitas Pertahanan

[1,2,3] IPSC Sentul Bogor

prabaswari@doktoral.idu.ac.id

OPEN ACCESS

Citation: Prabaswari., Alfikri, M., & Ahmad, I., (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. Matra Pembaruan. 6(1), 1-13

Received: January 16, 2022

Accepted: May 09, 2022

Published: May 31, 2022

Abstrak: Semenjak dunia mengalami pandemi Covid-19, seluruh kegiatan kehidupan masyarakat ikut beradaptasi. Terjadi peningkatan yang signifikan pada aktivitas online masyarakat baik untuk bekerja, belajar, transaksi, bersosialisasi, dan sebagainya. Peningkatan aktivitas online ini juga seiring dengan peningkatan kejahatan siber, tak terkecuali pada sistem yang dimiliki Pemerintah. Untuk menanggulangi hal ini, Badan Siber dan Sandi Negara (BSSN) menerbitkan Peraturan Badan Siber dan Sandi Negara Nomor 10 tahun 2020 tentang Tim Tanggap Insiden Siber atau disebut juga dengan Cyber Security Incident Response Team (CSIRT). Tujuannya adalah untuk mewujudkan pertahanan keamanan siber nasional yang tangguh khususnya pada sektor pemerintah, perlu dibentuk CSIRT yang solid dan kompeten di setiap instansi pemerintah. Penelitian ini bertujuan untuk mempelajari, mendalami fakta dan menilai implementasi kebijakan BSSN terkait pembentukan CSIRT berdasarkan Peraturan BSSN No. 10/2020 dilihat dari konten kebijakan dan konteks implementasinya. Penelitian ini merupakan penelitian kualitatif dengan pendekatan deskriptif-eksploratif. Analisis implementasi menggunakan teori implementasi kebijakan Marilee S. Grindle. Hasil dari penelitian ini menunjukkan bahwa walaupun target pembentukan CSIRT pada sektor pemerintah hingga tahun 2024 telah mencapai 52%, implementasi Peraturan BSSN No.10/2020 masih belum optimal dilihat dari sisi konten kebijakan maupun konteks implementasinya. Kendala utama yang ditemukan adalah akibat kurangnya kesadaran keamanan informasi pada instansi Pemerintah Pusat dan Pemerintah Daerah sebagai pelaksana. Selain itu, sumber daya, terutama dari sisi kemampuan SDM, ketersediaan anggaran, dan posisi instansi BSSN juga menimbulkan masalah tersendiri yang pada akhirnya menghambat proses implementasi.

Kata Kunci: Tim Tanggap Insiden Siber, Implementasi Kebijakan, BSSN.

Abstract: *Since the COVID-19 pandemic hit the world, all daily activities have transformed. People's online activities for work, study, transactions, and socializing have increased significantly. This phenomenon increases cybercrime, targeting but not limited to government-owned systems. The National Cyber and Crypto Agency (BSSN) issued Regulation No. 10 of 2020, the Cyber Security Incident Response Team (CSIRT), to address this issue. Of course, establishing a solid and competent CSIRT in every government agency is required to realize cybersecurity resilience, particularly in the government sector. This research aims to explain the BSSN policy number 10/2020 regarding the CSIRT team and explore its implementation strategy. With descriptive-explanatory research methods, the theory used is public policy and implementation strategy Marilee S. Grindle. This study indicates that although the target of establishing CSIRT in the government sector until 2024 has reached 52%, the implementation of BSSN regulations No.10/2020 is still not optimal in terms of policy content and the context of its implementation. The main obstacle found is the lack of information security awareness in central government agencies and local governments as implementers. In addition, resources, especially in terms of Human Resouces capabilities, budget availability, and potition of BSSN Agency, olso cause their problems that ultimately humper the implementation process.*

Keywords: *CSIRT, Policy Implementation, BSSN.*

I. Pendahuluan

Fenomena meningkatnya penggunaan internet di masa pandemi Covid 19, nyatanya juga diimbangi dengan meningkatnya jumlah insiden siber seperti kejahatan siber dan kebocoran data di Indonesia. Beberapa insiden serangan siber yang masif dialami Indonesia di antaranya kebocoran data pada *platform online shopping Unicorn* di Indonesia seperti Bukalapak, Tokopedia, Bhinneka.com dan yang paling telak adalah bocornya data 279 juta data peserta BPJS Kesehatan (Fatimah, 2021). Menurut data Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) BSSN, terdapat serangan siber sebanyak sekitar 495 juta serangan sepanjang tahun 2020. Dan pada periode Januari – Juli 2021 jumlah serangan semakin meningkat yaitu sebesar 741 juta serangan (Pusopkamsinas BSSN, 2021). Hal ini menunjukkan terjadi peningkatan serangan yang cukup signifikan (hampir 2x lipat) bahkan pada periode yang lebih pendek.

Berdasarkan laporan tahunan periode 2021 diketahui bahwa jenis Anomali tertinggi adalah *Malware* sebanyak 129.414.907 insiden, disusul dengan Aktivitas *Trojan*, Kebocoran data, *Exploit*, Pengumpulan data, serangan aplikasi *web*, APT dan *Denial of Service* dan lainnya dengan jumlah total sekitar 56 juta serangan (Pusopkamsinas BSSN, 2021). Adapun lima *malware* yang terdeteksi dengan intensitas paling tinggi, di antaranya:

1. *Mylobot Botnet*, *botnet* yang dapat mengambil alih perangkat dengan sistem operasi Windows, menyebar melalui *spam* email dan *file* terinfeksi.
2. *Miningpool other malware*, pengumpulan sumber daya untuk penambangan *crypto currency*.
3. *External communication behavior of Mining Trojan*, perusakan *file* yang menyebabkan komputer terinfeksi menjadi lambat.
4. *Scanning Behavior of the Backdoor Program* Win32.Zeroaccess, *backdoor* pengunduhan *malware* yang menyerang Windows.
5. *Phising-site other Malware*, teknik pengelabuan *malware* melalui tautan jebakan berisi *malware*.

Dengan adanya fenomena ini, maka keamanan siber telah menjadi isu prioritas tidak hanya bagi Indonesia namun juga bagi seluruh negara di dunia, semenjak Teknologi Informasi dan Komunikasi (TIK) menjadi bagian yang terintegrasi dalam berbagai aspek kehidupan masyarakat tidak terkecuali sektor pemerintah.

Sebagaimana pernyataan Presiden Jokowi pada Pidato Kenegaraan Sidang DPR-DPD RI 2019 bahwa bangsa Indonesia saat ini sudah harus bersiap menghadapi ancaman kejahatan siber termasuk penyalahgunaan data. Hal ini karena data lebih berharga daripada minyak, sehingga keamanan siber menjadi hal penting yang perlu diatur dan dilaksanakan lebih lanjut (Rohendi, 2020).

Keamanan siber didefinisikan sebagai sekelompok perangkat, kebijakan, pengaturan, upaya perlindungan, pendekatan manajemen risiko, jaminan keamanan, pelatihan, praktik terbaik serta teknologi yang bisa dimanfaatkan untuk mengamankan aset organisasi terutama data dan informasi yang ada pada ruang siber (Khoironi, 2020). Oleh karena itu Badan Siber dan Sandi Negara (BSSN) selaku instansi yang melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi, mengeluarkan Peraturan BSSN Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber atau secara global dikenal juga dengan istilah *Cyber Security Incident Response Team* (CSIRT), sebagai salah satu implementasi pembukaan UUD 1945 alinea 4 yaitu melindungi segenap bangsa Indonesia, tidak terkecuali di ruang siber (Hertianto, 2021).

Pembentukan CSIRT menjadi prioritas bagi sektor pemerintah selaku institusi vital yang mengelola banyak sekali aset informasi strategis yang berkaitan tidak hanya dengan kelangsungan hidup masyarakat tetapi juga menyangkut stabilitas dan kedaulatan nasional (Ka Chung Ng, Xiaojun Zhang, 2021). Saat ini, tata kelola informasi juga beralih dalam bentuk digitalisasi pasca disahkannya Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) (Karnay, 2020).

Perpres SPBE dibuat untuk memodernisasi penyelenggaraan layanan pemerintah, serta menjadi salah satu *tools* reformasi birokrasi yang diharapkan dapat memberikan

output pelayanan publik yang berkualitas, profesional, transparan dan akuntabel (Yunas, 2020). Untuk mencapai output tersebut, keamanan menjadi salah satu aspek yang memegang peranan penting. Dengan demikian, segala data dan informasi yang diolah dalam aplikasi SPBE menjadi aset penting yang harus dilindungi keamanannya. *The Committee on National Security System* (CNSS) mendefinisikan keamanan informasi sebagai perlindungan terhadap informasi meliputi sistem dan perangkat keras yang digunakan dalam mengolah, menyimpan dan mentransmisikan informasi dari segala macam gangguan maupun insiden siber (Romuald H., Jarosław N., Tomasz P., 2020).

Sesuai dengan Pasal 1 Peraturan BSSN No.10/2020, Insiden Siber didefinisikan sebagai salah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik. Sedangkan Tim Tanggap Insiden Siber / *Computer Security Incident Response Team* (CSIRT) adalah sekelompok orang yang bertanggungjawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya (Kepala Badan Siber dan Sandi Negara, 2020). Saat terjadi insiden, anggota Tim CSIRT dapat mengasistensi konstituen dalam menentukan apa yang terjadi dan memberitahu langkah yang perlu diambil untuk mengatasi masalah tersebut (M. Haidar, Y. G. Sucahyo, 2021).

Pada skala nasional, BSSN telah membentuk Gov-CSIRT Indonesia yang merupakan CSIRT sektor Pemerintah berdasarkan Keputusan Kepala BSSN Nomor 570 Tahun 2018. Organisasi ini diketuai oleh BSSN dengan konstituen Gov-CSIRT Indonesia yang meliputi seluruh Pemerintah Daerah dan Pemerintah Pusat (BSSN, 2018). Dalam pelaksanaannya, Gov-CSIRT Indonesia memiliki misi, sebagai berikut:

1. Membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber sektor pemerintah;
2. Membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah;
3. Membangun kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber sektor pemerintah; dan
4. Mendorong pembentukan CSIRT pada sektor pemerintah baik pada tingkat pusat dan daerah.

Pembentukan CSIRT sektor pemerintah di tingkat pusat maupun daerah sejatinya merupakan tuntutan kebutuhan zaman dan amanat kebijakan, sebagaimana tercantum dalam Peraturan Presiden Nomor 18 tahun 2020 tentang RPJMN Tahun 2020-2024 bahwa salah satu proyek strategis Bidang Politik, Hukum, Pertahanan dan Keamanan adalah Pembentukan 121 CSIRT pada Kementerian/Lembaga dan Pemerintah Daerah (Pemerintah Republik Indonesia, 2020). Sampai dengan Januari 2022, target pembentukan telah terpenuhi 52,8% dengan jumlah CSIRT yang terbentuk yaitu 30 CSIRT di instansi Pemerintah Pusat dan 34 CSIRT di instansi Pemerintah Daerah (Prov/Kab/Kota). Dalam prosesnya, masih kurang sebanyak 57 titik CSIRT di instansi pemerintah yang harus terbentuk hingga tahun 2024 (BSSN, 2018).

Meskipun pembentukan organisasi CSIRT saat ini telah mencapai lebih dari 50% target, namun pada prinsipnya jumlah target 121 titik tersebut masih belum mengcover seluruh instansi pemerintah khususnya pemkot/kab/kota serta masih ditemui kendala dalam proses implementasinya. Dengan banyaknya insiden siber yang terjadi, pembentukan CSIRT menjadi urgen bagi seluruh instansi pemerintah. Merujuk gambaran kondisi tersebut, maka peneliti tertarik untuk mengetahui apakah kebijakan pembentukan CSIRT berdasarkan Peraturan BSSN No. 10/2020 telah terimplementasi dengan baik atau belum.

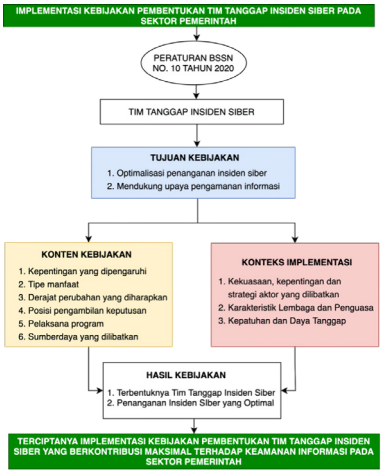
Menurut Van Horn dan Van Meter (Kurniawan et al., 2015), implementasi merupakan suatu atau serangkaian tindakan yang dilakukan baik secara perorangan, para petinggi atau kelompok pemerintah atau swasta yang dilakukan untuk mewujudkan tujuan yang telah ditetapkan dalam kebijakan. Dalam penelitian ini, implementasi kebijakan dipandang sebagai proses politik dan administrasi dengan merujuk pada teori implementasi kebijakan Grindle (Grindle, 1980; Mubarok *et al.*, 2020).

II. Metode

Penelitian ini berupaya menjawab pertanyaan apakah kebijakan pembentukan CSIRT berdasarkan Peraturan BSSN No. 10/2020 saat ini telah terimplementasi dengan baik atau belum? Pertanyaan tersebut akan dijawab melalui analisis yang menitikberatkan pada dua fokus yaitu, konten/isi kebijakan dan konteks implementasi kebijakan, sesuai dengan teori implementasi *Grindle*. Kebijakan ini diharapkan akan menghasilkan keluaran terbentuknya tim tanggap insiden siber dan penanganan insiden siber yang optimal sehingga akan menghasilkan *outcome* terciptanya implementasi kebijakan pembentukan tim tanggap insiden siber yang berkontribusi maksimal terhadap keamanan informasi sektor pemerintah.

Jumlah CSIRT yang terbentuk di instansi pemerintah menjadi indikator kontribusi dari implementasi kebijakan pembentukan tim tanggap insiden siber. Bruce Schneier dalam (Catota & Frankie E., 2018) menyatakan bahwa upaya perlindungan keamanan siber bergantung pada kekuatan rantai terlemah. Mengutip pendapat tersebut, maka keamanan siber di sektor pemerintah secara keseluruhan ditentukan oleh kemampuan seluruh komponen penyusun sektor tersebut, yaitu instansi pemerintah yang ada di pusat dan daerah tanpa terkecuali. Kebijakan pembentukan tim tanggap insiden siber akan berkontribusi maksimal terhadap keamanan informasi pada sektor pemerintah ketika seluruh instansi pemerintah baik pusat dan daerah telah memiliki CSIRT yang operasional. Adapun, kerangka konseptual penelitian ini diilustrasikan pada gambar 1.

Gambar 1. Kerangka Konseptual Penelitian.



Sumber: Diolah oleh Penulis

Data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh dengan metode wawancara terstruktur terhadap tiga orang informan dari BSSN. Seluruh informan dipilih berdasarkan pengetahuan di bidang keamanan siber dan pengalaman kerja yang sudah lebih dari lima tahun berkarir di bidang keamanan siber, serta lebih dari 3 tahun menangani CSIRT. Detail kualifikasi informan ditunjukkan pada Tabel 1.

Tabel 1. Informan Penelitian.

Informan	Masa Kerja	Pendidikan	Tanggal Wawancara
A.N.	> 15 tahun	S1	03/01/2022 dan 16/03/2022
R.P.	> 15 tahun	S1	10/01/2022
A.H.	> 15 tahun	S2	10/01/2022 dan 18/03/2022

Sumber: Diolah oleh Penulis

III. Hasil dan Pembahasan

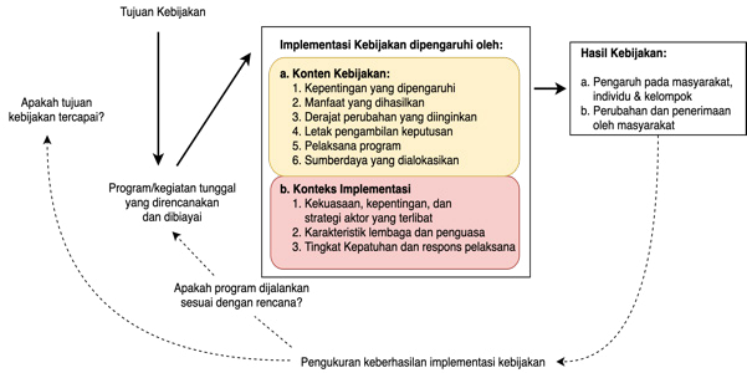
III.1. Implementasi Kebijakan Sebagai Proses Politik dan Administrasi

Implementasi kebijakan adalah salah satu tahapan penting dalam siklus kebijakan, karena keberhasilan dari implementasi kebijakan akan menentukan ketercapaian hasil kebijakan yang diharapkan (Mubarok *et al.*, 2020). Grindle menyatakan bahwa keberhasilan implementasi kebijakan dipengaruhi oleh dua variabel besar, yaitu

konten/Isi kebijakan (*content of policy*) dan lingkungan implementasi (*context of implementation*). Konten kebijakan meliputi: (1) *Interest Affected* (Kepentingan yang dipengaruhi); (2) *Type of Benefits* (manfaat yang dihasilkan); (3) *Extent of Change Envision* (Derajat perubahan yang diinginkan; (4) *Site of Decision Making* (Letak pengambilan keputusan; (5) *Program Implementor* (Pelaksana program); dan (6) *Resource Committed* (Sumber daya yang dialokasikan). Sementara lingkungan kebijakan mencakup: (1) *Power, Interest, and Strategy of Actor Involved* (Kekuasaan, kepentingan, dan strategi dari aktor yang terlibat); (2) *Institution and Regime Characteristic* (Karakteristik lembaga dan pimpinan); dan (3) *Compliance and Responsiveness* (Tingkat kepatuhan dan respons pelaksana) (Grindle, 1980; Mubarok *et al.*, 2020). Implementasi kebijakan menurut Grindle diilustrasikan pada Gambar 2.

Dalam konteks kerangka tersebut, tujuan Peraturan BSSN No. 10 Tahun 2022 tentang Tim Tanggap Insiden Siber adalah optimalisasi penanganan insiden siber dan mendukung upaya pengamanan informasi nasional. Ruang lingkup nasional direpresentasikan dalam beberapa sektor. Pemerintah adalah salah satu sektor tersebut. Untuk mengimplementasikan Peraturan BSSN No. 10 Tahun 2022, pelaksana (instansi pemerintah) akan menurunkan program/kegiatan yang direncanakan untuk mencapai tujuan. Hasil dari implementasi yang diharapkan adalah terbentuknya tim tanggap insiden siber dan adanya penanggulangan insiden siber yang optimal (Ka Chung Ng, Xiaojun Zhang, 2021). Sedangkan outcome yang diharapkan adalah terciptanya keamanan informasi pada sektor pemerintah dalam mewujudkan keamanan informasi nasional.

Gambar 2. Implementasi Kebijakan Sebagai Proses Politik dan Administrasi.



Sumber: diolah dari Mubarok (Mubarok *et al.*, 2020)

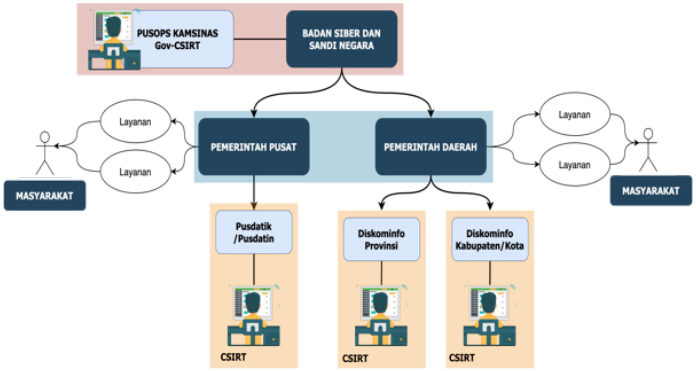
III.2. Analisa Konten Kebijakan

III.2.1.Kepentingan yang Dipengaruhi

Pada kategori ini akan dilihat pihak mana saja yang terlibat serta sejauh mana pengaruh dari kepentingan terhadap implementasi suatu kebijakan (Rahmadanita *et al.*, 2019). Dalam implementasi kebijakan ini, sasarannya adalah seluruh instansi pemerintah pusat maupun daerah. Implementasi kebijakan dilaksanakan secara nasional dengan BSSN sebagai Pembina atau koordinator. Sehingga terdapat tiga aktor yang kepentingannya dipengaruhi yaitu BSSN sebagai Pembina, Instansi Pemerintah Pusat dan Daerah sebagai pemberi layanan, serta Masyarakat itu sendiri sebagai penerima layanan. Struktur hierarki aktor dalam pembentukan CSIRT sektor pemerintah diilustrasikan pada Gambar 3.

Kepentingan yang terpengaruh dalam implementasi kebijakan ini dapat terlihat dari tujuan dibentuknya CSIRT yaitu untuk melakukan penanganan insiden siber yang efektif dan efisien guna melindungi keberlangsungan proses bisnis organisasi, kelancaran pelayanan publik dan kepentingan umum. Sedangkan dalam RPJMN khusus terkait Program Prioritas dinyatakan bahwa manfaat Pembentukan 121 CSIRT sektor Pemerintah adalah menurunnya insiden serangan siber; dan meningkatnya integrasi dan sharing data informasi antar-stakeholder terkait (baik pemerintah, swasta, dan komunitas siber lainnya).

Gambar 3. Hierarki Pembentukan CSIRT Sektor Pemerintah.



Sumber: diolah dari Enisa (Enisa, 2020)

Dari tujuan ini dapat dijelaskan bahwa kepentingan yang terpengaruh adalah seluruh sektor Pemerintah dan masyarakat umum sebagai penerima layanan. Implikasi dari adanya kebijakan ini adalah seluruh sektor khususnya sektor pemerintah harus segera membentuk CSIRT-nya dalam kurun waktu sampai dengan tahun 2024. Namun dalam perjalanannya tidak sedikit kendala dan resistensi yang terjadi. Dari hasil wawancara, ditemukan fakta bahwa sebelumnya, penanganan insiden masih belum terorganisir dan masih dijalankan secara manual per kasus, juga dilakukan mandiri tanpa adanya koordinasi dengan instansi lainnya. Banyaknya proses manual dan kurangnya koordinasi dalam penanganan insiden akan menurunkan efektivitas upaya penanganan insiden itu sendiri (Catota & Frankie E., 2018). Akibatnya, insiden tidak bisa ditangani dengan sistematis dan terorganisir (Catota & Frankie E., 2018).

Fakta menarik lainnya yang diperoleh dari hasil wawancara adalah bahwa kebanyakan penanganan insiden hanya bergantung pada satu orang admin yang dianggap menguasai sistem. Terkadang dikarenakan keterbatasan pengetahuan dan kapabilitas maka sering kali suatu aplikasi yang terkena serangan siber bukannya dilakukan prosedur penanggulangan dan pemulihan alih-alih dilakukan penonaktifan atau *take down*, sambil menunggu "bala bantuan" datang, baik menggunakan konsultan keamanan IT atau dari pihak yang dianggap lebih berkompeten. Kasus seperti ini banyak ditemukan di instansi Pemerintah Daerah. Penanganan insiden dengan pendekatan tersebut memakan waktu yang tidak sebentar, sehingga pemulihan sistem atau aplikasi menjadi terkendala, yang pada akhirnya mengakibatkan gangguan pada pelayanan publik (Ka Chung Ng, Xiaojun Zhang, 2021).

Dengan pembentukan CSIRT diharapkan penanganan insiden bisa lebih sistematis dan terorganisir (Catota & Frankie E., 2018). Setelah terbentuk, maka CSIRT pada instansi pemerintah pusat atau daerah tersebut harus diregistrasi pada CSIRT Nasional, yang dalam hal ini diampu oleh BSSN. Berdasarkan alur tersebut, kebanyakan resistensi terjadi karena organisasi merasa tidak memiliki SDM dan perangkat yang mumpuni hingga alasan pendanaan yang terbatas. Selain itu, berdasarkan hasil wawancara, diperoleh informasi bahwa ego sektoral masih sering ditemukan pada Kementerian, sehingga mereka enggan meregistrasi CSIRT mereka kepada BSSN (BSSN merupakan instansi berupa Badan yang posisinya dianggap tidak setara dengan Kementerian). Amanat pembentukan CSIRT yang dimuat dalam sebuah Peraturan Badan dan bukan Undang-Undang dinilai tidak cukup memiliki kekuatan "mengatur" khususnya bagi Kementerian. Hal ini berdampak pada lambatnya pembentukan CSIRT di lingkungan Kementerian. Di titik ini, kewenangan BSSN sebagai koordinator keamanan siber nasional mengalami hambatan. Meskipun pada Perpres 53 tahun 2017 sudah dinyatakan bahwa tugas BSSN adalah sebagai koordinator dalam bidang keamanan siber, namun sepanjang belum ada Undang-Undang maka dasar aturan ini dianggap belum cukup kuat untuk bisa mengatur K/L lainnya.

Hambatan serupa tidak ditemukan pada instansi Pemerintah Daerah. Pemerintah Daerah relatif lebih kooperatif akibat adanya amanat UU 23 tahun 2014 tentang Pemerintahan Daerah di mana urusan Persandian dan Keamanan Informasi menjadi urusan wajib yang harus dilaksanakan oleh Pemerintah Daerah dan dibina oleh Lembaga Sandi Negara yang saat ini telah bertransformasi menjadi BSSN.

Dari ulasan di atas, dapat ditarik kesimpulan bahwa berdasarkan aspek kepentingan yang dipengaruhi, kebijakan pembentukan CSIRT pada sektor pemerintah masih sulit untuk diimplementasikan. Kesulitan terjadi utamanya akibat kebijakan ini dipengaruhi oleh kepentingan instansi yang masih resisten untuk bekerja sama dengan BSSN sebagai Pembina.

III.2.2. Tipe Manfaat yang Dihasilkan

Berdasarkan hasil wawancara, didapatkan bahwa manfaat yang dihasilkan dari kebijakan pembentukan CSIRT pada sektor pemerintah adalah instansi pemerintah mampu menangani insiden siber yang terjadi di ruang lingkup tanggung jawab mereka secara sistematis dan terorganisir melalui mitigasi awal, dan pengoordinasian dalam jangka waktu tertentu. Sementara manfaat yang dirasakan bagi masyarakat adalah pelayanan publik yang dapat diakses setiap saat, andal dan bebas gangguan atau hambatan. Pada dasarnya biaya investasi yang dianggarkan untuk pembentukan CSIRT akan jauh lebih murah jika dibandingkan dengan *potential loss* dan penurunan tingkat kepercayaan masyarakat yang mungkin terjadi jika suatu insiden siber melumpuhkan layanan pemerintah. Jika *website* atau aplikasi milik pemerintah dapat diretas maka masyarakat akan merasa khawatir data mereka bisa disebarluaskan dan disalah gunakan, sebagaimana yang pernah terjadi pada sistem milik BPJS Kesehatan tahun 2021 silam menyebabkan turunnya tingkat kepercayaan publik kepada pemerintah selaku pengelola data publik.

Dilihat dari tujuan pembentukan CSIRT, secara eksplisit, menurunnya insiden serangan siber merupakan manfaat langsung bagi seluruh instansi pemerintah dan secara tidak langsung kepada masyarakat luas yang mendapat layanan *e-government*. Berdasarkan hasil wawancara, diketahui bahwa instansi yang sudah memiliki CSIRT lebih mampu menghalau dan cenderung cepat pulih dari suatu serangan siber. Ini adalah hal positif mengingat masyarakat mengharapkan proses bisnis layanan dapat terus berjalan dengan baik tanpa adanya hambatan dan down time yang disebabkan oleh insiden keamanan siber.

Dilihat dari sisi manfaat, kebijakan pembentukan CSIRT pada sektor pemerintah telah menghasilkan manfaat yang diharapkan walaupun belum optimal. Seluruh titik CSIRT harus terbangun dan saling terhubung, sehingga kendala pada satu bagian akan berdampak pada bagian lainnya baik secara tangible maupun intangible.

III.2.3. Derajat Perubahan yang Diinginkan

Arah perubahan pembentukan CSIRT di sektor pemerintah dimaksudkan untuk menjamin keberlangsungan layanan *e-government* bisa tetap diakses dan berjalan dengan lancar tanpa hambatan yang disebabkan oleh insiden siber. Dalam implementasi kebijakan ini, terdapat perubahan yang diinginkan untuk mendukung implementasi kebijakan yang lebih baik. Perubahan tersebut, dibagi dalam perubahan fisik dan perilaku, sebagai berikut:

a. Perubahan Fisik

1. Tersedianya *Point of Contact* (PoC) atau narahubung sebagai pintu utama pelaporan saat terjadi insiden siber di sektor pemerintah;
2. Adanya bantuan dan kolaborasi dalam penanganan insiden keamanan siber sektor pemerintah, dengan waktu operasional 24/7;
3. Adanya mekanisme atau forum berbagi informasi, pengetahuan dan *lesson learned* antar CSIRT pemerintah teregistrasi.

b. Perubahan Perilaku

1. Meningkatnya kesadaran dan budaya keamanan informasi pada sektor pemerintah; dan
2. Menurunnya resistensi sektoral antar instansi pemerintah.

Dari hasil wawancara dan pengamatan, ditemukan fakta bahwa dilihat dari sisi derajat perubahan yang diinginkan, perubahan fisik nomor 1 telah tercapai dengan adanya BSSN sebagai PoC untuk memfasilitasi pelaporan saat insiden siber terjadi. Perubahan fisik nomor 2 tercapai sebagian karena masih dalam proses berjalan. Poin ini akan tercapai seutuhnya ketika seluruh instansi pemerintah baik pusat maupun

daerah telah memiliki CSIRT yang dapat beroperasi selama 24/7. Perubahan fisik nomor 3 belum tercapai karena hingga saat ini belum terdapat mekanisme efektif yang mewadahi kebutuhan berbagi informasi, pengetahuan, dan *lesson learned* antar CSIRT pemerintah teregistrasi. Sedangkan perubahan perilaku baik pada poin 1 maupun 2 belum tercapai karena berdasarkan fakta di lapangan, masih ditemukan resistensi instansi khususnya Kementerian untuk patuh pada Peraturan BSSN ini. Resistensi tersebut menjadi salah satu penanda bahwa kesadaran keamanan informasi disektor pemerintah masih kurang dan belum membudaya. Dengan kesadaran terinternalisasinya budaya keamanan informasi, maka kemungkinan terjadinya resistensi tersebut akan sangat kecil.

III.2.4. Posisi Pengambilan Keputusan

Posisi pengambil keputusan adalah hal penting dalam menjamin keberhasilan implementasi suatu kebijakan. Jika suatu kebijakan kurang memperhatikan posisi pengambil keputusan maka tidak mustahil kebijakan tersebut dapat menemui kegagalan. Sebagaimana tercantum dalam dokumen Perpres 18/2020 tentang RPJMN 2020-2024, Pembentukan 121 *Computer Security Incident Response Team* (CSIRT) menjadi Proyek Prioritas Strategis/*Major Project* (MP) untuk memperkuat Stabilitas Polhukhankam dan Transformasi Pelayanan Publik. MP tersebut didasari oleh direktif Presiden dalam upaya penguatan dan ketahanan siber serta mendukung upaya transformasi digital. Sasaran utama MP ini adalah stabilitas keamanan siber sektor pemerintah dengan mempertimbangkan tingginya serangan siber yang ditujukan ke domain pemerintah, baik pusat maupun daerah (Proses, 2022). Kemudian didukung dengan diterbitkannya Perban BSSN 10 Tahun 2020 tentang Tim Tanggap Insiden Siber. Selanjutnya upaya Pembentukan CSIRT ini ditegaskan kembali dalam Perpres 85 Tahun 2021 yang disahkan pada tanggal 9 September 2021 tentang Rencana kerja Pemerintah Tahun 2022.

Dalam implementasinya, merujuk ilustrasi pada Gambar 3, CSIRT pada Pemerintah Pusat terletak pada unit eselon II yang membidangi masalah TIK di instansi tersebut, seperti Pusdatin/Pusdatik. Sedangkan pada Pemerintah Daerah, terletak pada Dinas Komunikasi dan Informatika (Diskominfo) yang juga merupakan unit eselon II.

Selain itu jaringan yang sudah terbentuk antara jajaran Pemprov/kab/kota dengan BSSN selaku Gov-CSIRT pusat juga memberi kontribusi positif dalam pembentukan CSIRT pada lingkup Pemerintah Daerah. Pengambilan keputusan dengan alur *Top Down*, arahan direktif langsung dari Presiden yang kemudian didukung oleh peraturan dan program kerja BSSN dirasa cukup efektif dalam mendorong implementasi kebijakan pembentukan CSIRT di sektor pemerintah. Target tahunan yang ditetapkan pada RPJMN sejak tahun 2020 (15 CSIRT) – 2021 (25 CSIRT) dapat dikatakan tercapai dengan efektif melalui hasil evaluasi MP 2020-2021. Hasil ini menunjukkan adanya penyesuaian target prioritas karena kebijakan pembatasan berskala besar sebagai dampak dari pandemi Covid-19. Walaupun demikian, *output*/kegiatan prioritas Pembentukan CSIRT pada sektor pemerintah dapat dilaksanakan dengan baik sesuai dengan amanat RPJMN 2020-2024.

Berdasarkan posisi pengambilan keputusan, kebijakan pembentukan CSIRT pada sektor pemerintah telah tepat sasaran dengan menempatkan CSIRT pada unit kerja eselon II yang bertanggungjawab terkait masalah TIK di instansi yang bersangkutan. Sedangkan dilihat dari sisi makro, posisi pengambilan keputusan nasional yang terletak pada BSSN juga dinilai tepat. Hanya saja, posisi BSSN yang merupakan Badan yang “tidak setingkat” dengan beberapa instansi pusat dalam hal ini Kementerian acapkali menyulitkan implementasi. Sementara pembentukan CSIRT adalah upaya yang sangat dibutuhkan dalam rangka menangani insiden siber, pembentukan CSIRT di kementerian berjalan lebih lambat dibandingkan dengan pembentukan CSIRT di instansi Pemerintah Daerah. Setidaknya ada tiga faktor pemicunya yaitu: 1) belum adanya keinginan untuk membentuk CSIRT; 2) kurangnya kekuatan “mengatur” dari BSSN; 3) kurangnya kesadaran keamanan siber.

III.2.5. Pelaksana Kebijakan

Implementasi suatu kebijakan membutuhkan peran dan tanggung jawab dari para pelaksana kebijakan. Keberhasilan pelaksanaan program dan pencapaian target juga bergantung pada siapa yang ditunjuk sebagai pelaksana kebijakan. RPJMN 2020-2024 mengamanatkan BSSN sebagai instansi pelaksana untuk pembentukan 121 CSIRT sektor pemerintah. Namun dalam pelaksanaannya, BSSN tidak dapat menjadi satu-satunya pelaksana proyek tersebut. Dengan diturunkannya Perpres menjadi Perban 10 Tahun 2020, maka pelaksana dari kebijakan ini adalah seluruh instansi pemerintah.

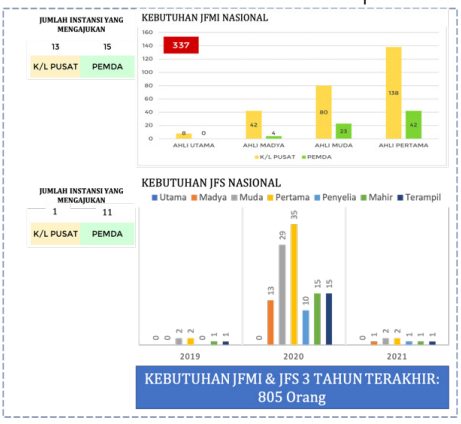
Selain itu, pada Perpres 95 Tahun 2018 tentang SPBE juga mengamanatkan setiap instansi Pusat dan Daerah untuk mengelola keamanan Jaringan Intra instansi pusat dan pemerintah daerah masing-masing. Dalam lingkup pemerintah daerah, pembentukan CSIRT digawangi oleh Dinas Kominfo masing-masing Pemda, yang melakukan usulan program kegiatan dan anggaran dan kemudian diusulkan ke dalam RKPD, RPJMD dan LKPJ, hingga realisasi kemudian registrasi kepada CSIRT yang telah dibentuk kepada CSIRT pusat yaitu BSSN.

Dilihat dari sisi pelaksana kebijakan, BSSN bersama pemerintah pusat dan daerah sebagai pelaksana kebijakan dinilai tepat. Namun yang banyak menjadi kendala adalah kurangnya sumber daya manusia yang kompeten dalam bidang keamanan siber khususnya penanggulangan insiden sehingga masih banyak instansi pusat dan daerah yang merekrut pihak ketiga . Pihak ketiga yang dimaksud di sini merujuk pada perusahaan swasta yang bergerak di bidang keamanan siber untuk mengembangkan sistem *monitoring* jaringan dan menyediakan SDM untuk mengelola sistem tersebut sekaligus berperan sebagai CSIRT.

III.2.6. Sumber Daya yang Dialokasikan

Masalah sumber daya menitikberatkan pada alokasi SDM, anggaran, prasarana dan sarana, serta kewenangan yang dibutuhkan untuk mengimplementasikan kebijakan pembentukan CSIRT pada sektor pemerintah secara optimal. Sumber daya merupakan faktor paling jelas yang dapat mempengaruhi keberhasilan implementasi kebijakan (Mubarok et al., 2020).

Pertama, terkait SDM, terdapat kesenjangan yang cukup lebar antara jumlah dan kompetensi SDM yang dibutuhkan untuk mengelola CSIRT dengan apa yang tersedia di lapangan saat ini. Sekurang-kurangnya terdapat 650 Instansi Penyelenggara Negara dan 1000 Instansi Penyelenggara Layanan Publik. Apabila diasumsikan masing-masing instansi membutuhkan paling sedikit lima orang yang memiliki kompetensi di bidang Keamanan Siber, maka total SDM yang dibutuhkan adalah 18.054 orang. Di Indonesia, terdapat dua jabatan fungsional yang relevan dengan tusi keamanan siber, yaitu Jabatan Fungsional Sandiman (JFS) dan Jabatan Fungsional Manggala Informatika (JFMI). Gambar 4 menunjukkan total kebutuhan JFS dan JFMI tahun 2019, 2020, dan 2021 berdasarkan hasil validasi kebutuhan yang diajukan oleh K/L/D/I kepada BSSN. Dari hasil perhitungan tersebut, kurang dari 1000 personel yang diajukan untuk mengurusi keamanan siber di instansi pemerintah.



Sumber: Diolah oleh Penulis

Gambar 4. Total Kebutuhan JFS dan JFMI tahun 2019, 2020, dan 2021 berdasarkan hasil validasi kebutuhan yang diajukan K/L/D/I kepada BSSN.

Hal ini menjadi kendala utama yang dihadapi oleh BSSN sebagai Pembina maupun instansi pusat dan daerah sebagai pengelola CSIRT. Untuk mengatasi kesenjangan ini, BSSN mengadakan program *training* dan *workshop* pengelolaan CSIRT. Namun demikian, karena keterbatasan yang dimiliki oleh BSSN dalam hal personel *trainer* dan keterbatasan SDM di instansi pemerintah yang memiliki kesesuaian kompetensi untuk dikembangkan, maka program *transfer knowledge* masih berjalan lambat.

Kedua, terkait dengan anggaran dan sarana. Pada prinsipnya untuk MP Penguatan NSOC – SOC dan Pembentukan 121 CSIRT, Pemerintah telah mengalokasikan dana sebesar 8 triliun selama 5 tahun yang bersumber dari APBN (Perpres 18/2020). Namun, untuk T.A. 2022 ini sesuai dengan Perpres 85/2021 telah dialokasikan pendanaan proyek prioritas Strategis pada RKP 2022 khusus untuk Pembentukan CSIRT sejumlah Rp. 14.290.600.000, - untuk Pembangunan dan Penguatan Tim Cepat Tanggap keamanan Siber (CSIRT) sektor Pemerintah, dengan target 27 KLD di mana disebutkan instansi pelaksana/penanggung jawab adalah BSSN. Karena sepenuhnya bergantung dengan APBN dan APBD, maka tidak banyak hal yang dapat dilakukan untuk menambah alokasi anggaran untuk mengakselerasi proses pembentukan CSIRT. Masalah anggaran ini kemudian berdampak secara langsung terhadap prasarana dan sarana yang dibutuhkan untuk membangun CSIRT. Alokasi anggaran memiliki korelasi linear terhadap penyediaan prasarana dan sarana.

Berikutnya, masalah kewenangan. Dari sisi kewenangan, amanat yang diberikan kepada BSSN sebagai instansi yang bertanggungjawab mengkoordinasikan masalah keamanan siber sudah tepat. Dalam konteks pembentukan CSIRT di sektor pemerintah pun, BSSN menerbitkan kebijakan yang mengarahkan pada tanggung jawab masing-masing sektor untuk membentuk CSIRT masing-masing. Hal ini juga sudah tepat. Hanya saja, masalah terdapat pada kewenangan tidak tertulis atas kedudukan BSSN sebagai sebuah Badan, yang posisinya dianggap masih lemah untuk mengatur Kementerian karena belum didukung Undang-Undang (hanya Perpres) sehingga menyulitkan implementasi kebijakan secara optimal.

III.3. Analisa Konteks Implementasi Kebijakan

Setelah analisis konten, peneliti kemudian menganalisis masalah terkait implementasi kebijakan pembentukan CSIRT pada sektor Pemerintah yang berfokus pada konteks implementasi. Temuan penelitian dijabarkan sebagai berikut:

III.3.1.Kekuasaan, Kepentingan, dan Strategi Aktor yang Terlibat

Berdasarkan pengamatan dan pembahasan, kondisi penerapan konteks kategori 1 ini masih terdapat beberapa kekurangan. Pada awalnya target 121 CSIRT pemerintah diperuntukkan bagi 34 titik Pemprov dan 87 titik KL Pemerintah Pusat. Namun pada perjalanannya kendala PSBB terjadi karena pergeseran target dari 10 Pemprov menjadi 10 Pemkab/kota. Namun hal ini tidak menurunkan esensi dari pentingnya pembangunan CSIRT, sehingga kedepannya usaha untuk membangun CSIRT di seluruh Pemprov dan KL Pusat tetap akan dilanjutkan, bahkan jika 121 titik CSIRT sesuai target RPJMN telah dipenuhi, usaha pembentukan CSIRT pada seluruh instansi lain yang belum terbangun akan tetap di asistensi oleh BSSN.

Dengan adanya pandemi, upaya yang dilakukan BSSN untuk melakukan diseminasi informasi terkait pentingnya CSIRT tentunya mengalami beberapa kendala. Selain itu pemotongan anggaran untuk penanganan pandemi Covid19 juga mempengaruhi realisasi dari pembentukan CSIRT yang sudah direncanakan sebelumnya. Pola koordinasi dan diseminasi bertransisi menjadi pola daring melalui *webinar* terkait sosialisasi pembentukan CSIRT. Pada kegiatan tersebut, BSSN memberi insentif khusus bagi instansi yang berminat membentuk CSIRT yaitu prioritas dalam kegiatan BSSN, serta pemberian pelatihan SDM CSIRT bersertifikasi.

Dalam hal kekuasaan, hubungan antara BSSN dengan Pemerintah Daerah lebih solid dibandingkan hubungan BSSN dengan Pemerintah Pusat. Hal ini karena UU 23 tahun 2014 tentang Pemerintahan Daerah menjadi basis hukum yang kuat bagi penyelenggaraan keamanan siber. Sementara di sisi pemerintah pusat, beberapa kementerian masih memiliki ego sektoral yang tinggi sehingga menimbulkan resistensi

terhadap BSSN yang merupakan instansi yang tidak setingkat. Untuk mewujudkan pembentukan CSIRT, masih dibutuhkan *lobby* politik karena keinginan dan kesadaran untuk membentuk CSIRT belum datang dari dalam instansi tersebut. Hal ini pada gilirannya mempersulit implementasi kebijakan.

III.3.2.Karakteristik Rezim yang Berkuasa

Karakteristik di sini merujuk pada respons, sikap politik, dan sudut pandang instansi yang direpresentasikan dari pimpinan instansi. Dalam fokus pembahasan ini, karakteristik instansi yang diperhatikan adalah karakteristik BSSN dan instansi pemerintah selain BSSN baik pusat maupun daerah sebagai pelaksana kebijakan.

Pendekatan koordinasi yang dilakukan BSSN dalam upaya pembentukan CSIRT berjalan sangat baik untuk Pemerintah daerah, namun kurang berjalan mulus bagi pemerintah pusat. Hal ini karena BSSN hanya merupakan LPNK sedangkan yang pembentukannya diamanatkan oleh Peraturan Presiden, sementara Kementerian dan Kemenko secara hierarkis berada satu tingkat di atas yang pembentukannya diamanatkan oleh Undang-Undang.

Dalam praktiknya, batasan hirarkis ini, diperparah dengan kurangnya kesadaran keamanan siber di lingkungan Kementerian, menimbulkan rasa enggan untuk segera membentuk CSIRT. Karakteristik BSSN dan Kementerian yang demikian pada akhirnya mempersulit implementasi kebijakan.

III.3.3.Kepatuhan dan Respons Pelaksana

Tingkat kepatuhan instansi pusat dan daerah, secara umum sangat bergantung pada pemahaman dan dukungan pimpinan tertinggi dari masing-masing instansi akan pentingnya pembentukan CSIRT. Pemahaman dalam konteks ini dipengaruhi kesadaran keamanan informasi, sementara komitmen pimpinan tertinggi merujuk pada penyediaan alokasi anggaran yang mumpuni.

Sejak disahkannya Perpres 18 Tahun 2020 tentang RPJMN 2020 s.d. 2024 dan kemudian didukung dengan diterbitkannya Perban 10 Tahun 2020, Pemerintah telah berupaya meningkatkan keamanan siber melalui pembangunan CSIRT khususnya pada sektor Pemerintah. Terhitung sejak tahun 2020 sampai dengan Januari 2022, telah dibangun 64 CSIRT sektor Pemerintah dari total 121 yang direncanakan dalam proyek strategis dengan rincian sebagaimana ditunjukkan pada Tabel 2.

Melihat hasil yang dicapai hingga tahun 2022 ini, lebih dari 50% target telah tercapai. Walaupun demikian, angka hanyalah angka. Penelitian ini menemukan bahwa masih terdapat respons yang kurang baik akibat kurangnya kesadaran keamanan informasi.

Sebagaimana telah diuraikan pula pada bagian kekuasaan, kepentingan, dan strategi aktor yang terlibat, pencapaian angka tersebut didukung dengan *lobby* politik yang menandakan bahwa keinginan dan kesadaran untuk membentuk CSIRT belum datang dari dalam instansi tersebut. Pembentukan CSIRT ini bukanya hanya sekedar menambah kompleks tugas dan fungsi yang harus diemban oleh pelaksana, melainkan sebuah kebutuhan yang harus dipenuhi dalam rangka mengantisipasi serangan siber. Masalah kepatuhan diperparah dengan ego sektoral dari instansi yang merasa berada lebih tinggi dari BSSN sedemikian sehingga timbul rasa enggan untuk mendukung implementasi kebijakan pembentukan CSIRT. Dengan demikian, kepatuhan pelaksana masih kurang dan menghambat proses implementasi.

Tabel 2. Pembentukan CSIRT pada Sektor Pemerintah per-Januari 2022.

Instansi Pusat				
1. Setneg	7. BSN	13. Ombusmen RI	20. LKPP	26. Kemenkes
2. Kemenlu	8. DPD RI	15. Kemenkominfo	21. Bappenas	27. Kejagung
3. Kemenkeu	9. BATAN	16. LAPAN	22. BPOM	28. Kemenhan
4. Kemendikbud	10. BPPT	17. PPATK	23. BPS	29. Kemenko ekonomi
5. KSP	11. Kemen Esdm	18. Kemendag	24. BKN	30. BIG
6. BSSN	12. Kemenhub	19. Kementan	25. LAN	

Instansi Pemerintah Daerah				
Tingkat Provinsi				
1. Jawa Timur	7. DI. Yogyakarta	13. Bali	19. Sumatera Selatan	
2. Jawa Barat	8. Kalimantan Selatan	14. Bengkulu	20. Papua	
3. Jawa Tengah	9. Nusa Tenggara Barat	15. Jambi	21. Kalimantan Timur	
4. DKI Jakarta	10. Gorontalo	16. Bangka Belitung	22. Riau	
5. Kepulauan Riau	11. Maluku	17. Papua Barat	23. Kalimantan Tengah	
6. Sumatera Barat	12. Banten	18. Sulawesi Barat	24. Sulawesi Selatan	
Tingkat Kabupaten / Kota				
1. Kab. Madiun	3. Kab. Pati	5. Kota. Tangerang Selatan	7. Kota. Cirebon	9. Kab. Banyumas
2. Kab. Kebumen	4. Kab. Gowa	6. Kab. Trenggalek	8. Kota Palembang	10. Kota Bandung

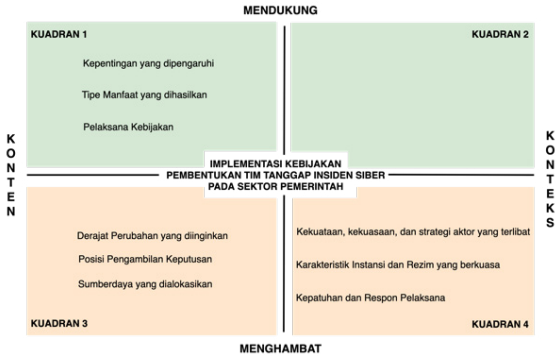
Sumber: BSSN, 2002

III.4. Kelemahan Model Implementasi Kebijakan Saat Ini

Berdasarkan ulasan pada bagian sebelumnya, ditemukan bahwa implementasi kebijakan pembentukan tim tanggap insiden siber yang ada saat ini masih memiliki kelemahan. Kelemahan ditemukan pada beberapa elemen dalam konten dan konteks kebijakan. Hal ini diilustrasikan pada Gambar 5.

Pada Gambar 5, kuadran kiri merupakan kuadran konten dan kuadran kanan merupakan kuadran konteks. Kuadran 1 menunjukkan posisi elemen konten yang mendukung implementasi kebijakan, sementara kuadran 3 menunjukkan posisi elemen yang menghambat implementasi kebijakan. Untuk konteks kebijakan, posisi elemen yang mendukung implementasi berada pada Kuadran 2 sementara posisi elemen yang menghambat berada pada kuadran 4. Menghambat dalam artian masih terdapat hal-hal yang perlu ditingkatkan dalam proses implementasi kebijakan.

Gambar 5. Kuadran Kelemahan Model Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah.



Sumber: Diolah oleh Penulis

Berdasarkan temuan penelitian, dari sisi konten kebijakan, kelemahan terdapat utamanya pada aspek derajat perubahan yang diinginkan, posisi pengambilan keputusan, dan sumber daya yang dialokasikan. Sedangkan dari sisi konteks implementasi, kelemahan terdapat pada seluruh aspek yang mempengaruhi implementasi kebijakan. Model implementasi kebijakan saat ini belum optimal sehingga membutuhkan intervensi untuk mencapai tujuan kebijakan dengan lebih baik.

IV. Kesimpulan

Berdasarkan temuan penelitian dapat diketahui bahwa kebijakan pembentukan Tim Tanggap Insiden Siber pada sektor pemerintah telah terimplementasi walaupun belum optimal. Dilihat dari konten dan konteks kebijakan, implementasi kebijakan pembentukan tim tanggap insiden siber masih memiliki kendala utamanya dalam

hal kurangnya kesadaran keamanan informasi pada instansi Pemerintah Pusat dan Pemerintah Daerah sebagai pelaksana. Rendahnya kesadaran keamanan informasi akan menimbulkan rasa enggan untuk patuh. Selain itu, sumber daya, terutama dari sisi kemampuan SDM, ketersediaan anggaran, dan posisi instansi BSSN juga menimbulkan masalah tersendiri yang pada akhirnya menghambat proses implementasi.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih sedalam-dalamnya kepada narasumber dari Pusopkamsinas BSSN, Dosen Pembimbing dari Universitas Pertahanan, dan seluruh rekan yang telah membantu kelancaran proses penulisan ini.

Daftar Referensi

BSSN. (2018). Gov CSIRT Indonesia. BSSN.

Catota & Frankie E. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity (Oxford), 4(1), 2057–2085. https://doi.org/https://doi.org/10.1093/cybsec/tyy002

Enisa. (2020). HOW TO SETUP UP CSIRT AND SOC GOOD PRACTICE GUIDE HOW TO SETUP UP CSIRT AND SOC ABOUT ENISA. https://doi.org/10.2824/056764

Fatimah, S. (2021). kompilasi-kasus-kebocoran-data-yang-heboh-terjadi-di-indonesia. Detikfinance.

Grindle, M. S. (1980). (1980). Public Choices and Policy Change: The Political Economy Of Reform In Developing Countries. s. The Johns Hopkins University Press. https://www.press.jhu.edu/books/title/2210/public-choices-and-policy-change

Hertianto, M. R. (2021). Tinjauan Yuridis Terhadap Perlindungan Anak Dalam Ruang Siber Di Indonesia. Jurnal Hukum & Pembangunan, 51(3), 555–573. https://doi.org/http://dx.doi.org/10.21143/jhp.vol51.no3.3123

Ka Chung Ng, Xiaojun Zhang, J. Y. L. T. & K. Y. T. (2021). Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective, Journal of Management Information Systems. Journal of Management Information Systems, 38:3, 732–764. https://doi.org/10.1080/07421222.2021.1962601

Kepala Badan Siber dan Sandi Negara. (2020). Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber. https://peraturan.bpk.go.id/Home/Download/167485/Peraturan%20BSSN%20Nomor%2010%20Tahun%202020.pdf

Karnay, S. (2020). Penerapan Electronic Government Pada Dinas Komunikasi Informatika Statistik Dan Persandian Provinsi Sulawesi Selatan (Doctoral Dissertation, Universitas Hasanuddin) http://repository.unhas.ac.id/id/eprint/1519

Khoironi, S. C. (2020). Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital. Jurnal Studi Komunikasi Dan Media, 24(1), 37. https://doi.org/10.31445/jskm.2020.2945

Kurniawan, E., Ratna Kusuma, A., & Idris, A. (2015). Implementasi Kebijakan Program Pemberdayaan Komunitas Adat Terpencil (KAT) Dalam Menanggulangi Kemiskinan Di Lokasi Sekulit Desa Munggu Kecamatan Longkali Kabupaten Paser. Jurnal Administrative Reform, 3(3), 374–385. https://doi.org/http://dx.doi.org/10.52239/jar.v3i3.577

M. Haidar, Y. G. Sucahyo, T. S. and A. G. (2021). "Analysis of Csirt Services in Facing Cyber Security Challenges in Indonesia." 2021 4th International Conference on Information and Communications Technology (ICOIACT), 154–159. https://doi.org/10.1109/ICOIACT53268.2021.9563925

Mubarok, S., Zauhar, S., Setyowati, E., & Suryadi, S. (2020). Policy Implementation Analysis: Exploration of George Edward III, Marilee S Grindle, and Mazmanian and Sabatier Theories in the Policy Analysis Triangle Framework. Journal of Public Administration Studies, 005(01), 33–38. https://doi.org/10.21776/ub.jpas.2020.005.01.7

Pemerintah Republik Indonesia. (2020). Peraturan Presiden Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024. Rencana Pembangunan Jangka Menengah Nasional 2020-2024, 313. https://peraturan.bpk.go.id/Home/Download/181262/Perpres%20Nomor%2018%20Tahun%202020%20-%20Lamp.%20I.pdf

Proses, S. (2022). 2L Lr 2Olr Dan. 096209.

Pusopkamsinas BSSN. (2021). Laporan Bulanan Monitoring Keamanan Siber Oktober 2021. https://cloud.bssn.go.id/s/XNagZMdsZFDCimR

Rahmadanita, A., Santoso, E. B., & Wasistiono, S. (2019). Implementasi Kebijakan Smart Government Dalam Rangka Mewujudkan Smart City Di Kota Bandung. Jurnal Ilmu Pemerintahan Widya Praja, 44(2), 81–106. https://doi.org/10.33701/jipwp.v44i2.279

Rohendi, A. (2020). Perlindungan Hukum Big Data. Jurnal Sain Manajemen, 2(2), 1–5. https://ejurnal.ars.ac.id/index.php/jsm/article/view/300/208

Romuald H., Jarosław N., Tomasz P., J. S. (2020). Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach. Procedia Manufacturing, 44, 647–654. https://doi.org/10.1016/j.promfg.2020.02.244

Yunas, N. S. (2020). Implementasi e-Government dalam Meminimalisasi Praktik Rent Seeking Behaviour pada Birokrasi Pemerintah Kota Surabaya. Matra Pembaruan, 4(1), 13–23. https://doi.org/10.21787/mp.4.1.2020.13-23