Tata Kelola Ekosistem Berbagi Informasi Keamanan Siber pada *Information Sharing and Analysis Center* (ISAC) Sektor Pemerintah Daerah di Indonesia

Fandi Aditya Putra[1)]

(1) Badan Siber dan Sandi Negara, fandi.aditya@bssn.go.id

Abstrak

Infrastruktur sejenis yang diterapkan oleh instansi Pemerintah Daerah menyebabkan serangan siber yang terjadi terus berulang di masa depan. Berbagi informasi keamanan siber antar instansi pemerintah di Pemerintah Daerah bermanfaat dalam proteksi keamanan siber pada masing-masing instansi Pemerintah Daerah. Tata kelola berbagi informasi keamanan siber melalui ISAC di sektor Pemerintah Daerah belum menjadi fokus penelitian sebelumnya. Pada penelitian ini, tata kelola berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah dianalisis berdasarkan NIST Cybersecurity Framework dan MITRE Building a National Cyber Information-Sharing Ecosystem. Hasilnya, terdapat 5 (lima) area tata kelola berbagi informasi keamanan siber, yaitu kebutuhan ISAC seperti model ekosistem dan klasifikasi informasi, entitas, jaringan informasi, teknologi, serta program kolaborasi dan koordinasi. Penelitian ini menunjukkan bahwa model yang dapat diterapkan merupakan model hybrid dengan kombinasi tiga model, empat klasifikasi informasi, empat peran entitas, lima spesifikasi keamanan privasi, serta delapan program kolaborasi dan koordinasi berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah. Manfaat dari penelitian ini yaitu memberikan ruang lingkup fundamental terhadap implementasi ekosistem berbagi informasi keamanan siber pada sektor Pemerintah Daerah dalam rangka strategi penanganan risiko keamanan siber.

Kata kunci: berbagi informasi keamanan siber, ekosistem, ISAC, Pemerintah Daerah, tata kelola.

1. PENDAHULUAN

Berbagi informasi keamanan siber dapat diimplementasikan ke dalam organisasi atau tim *ad-hoc* organisasi yaitu *Information Sharing and Analysis Center* (ISAC) dalam rangka implementasi strategi perlindungan serangan siber [1, 2]. Implementasi berbagi informasi keamanan siber ini diklasifikasikan ke dalam berbagai sektor kritis, seperti energi, kesehatan, transportasi, keuangan, transportasi, hingga administrasi pemerintah [3]. Namun, implementasi berbagi informasi keamanan siber memiliki tantangan yaitu ketidakpercayaan antar entitas di dalam sektor terkait hingga adanya isu privasi [4-6].

Salah satu sektor yang memuat informasi vital suatu negara yaitu sektor Pemerintah yang meliputi Pemerintah Daerah. Pelaksanaan Sistem Pemerintah Berbasis Elektronik (SPBE) atau dikenal sebagai *e-government* oleh Pemerintah Daerah merupakan implementasi nyata infrastruktur teknologi informasi yang strategis terhadap administrasi pemerintahan. Dengan implementasi tersebut, terdapat risiko keamanan seperti terjadinya pencurian data pribadi masyarakat hingga peretasan pada *website* dan kerentanan sistem [7]. Dalam kurun delapan bulan terakhir pada 2021, ditemukan sebanyak 33.748 kali peretasan terhadap situs pemerintah dengan mayoritas pada Pemerintah Daerah [7].

Infrastruktur yang sejenis pada instansi Pemerintah Daerah menyebabkan teknik serangan yang digunakan oleh kriminal siber terus berulang di masa depan. Dengan berbagi informasi keamanan siber antar instansi pemerintah di Pemerintah Daerah menyebabkan pertukaran informasi keamanan siber yang bermanfaat dalam proteksi yang dimiliki masing-masing instansi tersebut. Tata kelola keamanan siber yang baik dalam rangka mengatasi ancaman siber juga perlu diperhatikan oleh Pemerintah Daerah. Tata kelola keamanan siber menjadi sangat penting untuk memastikan keamanan siber yang terapkan oleh suatu organisasi berjalan dengan efektif dan efisien.

Pada penelitian sebelumnya dibahas mengenai model ekosistem berbagi informasi keamanan siber pada sektor kesehatan [8, 9]. Selain itu, pada penelitian lainnya dibahas model berbagi informasi antar entitas dengan menggunakan teknologi *blockchain* [10]. Salah satu aspek pada tata kelola keamanan siber yaitu proses atau aktivitas operasi keamanan siber juga ditunjukkan dalam penelitian terkait model berbagi informasi intelijen ancaman siber antar entitas dalam satu sektor [11-13]. Namun, secara keseluruhan belum ada penelitian yang memperhatikan permasalahan tata kelola keamanan siber pada berbagi informasi keamanan siber, terkhusus pada Pemerintah Daerah.

Dari sisi teknologi, berbagi informasi keamanan siber di dalam ISAC dapat dilakukan melalui layanan *cloud*, salah satunya penyimpanan *cloud*. Penelitian tentang implementasi keamanan pada berbagi informasi melalui *cloud* dibahas dengan teknik yang beragam pada beberapa penelitian sebelumnya. Salah satunya dengan skema perlindungan privasi dalam berbagi informasi [14, 15]. Perlindungan informasi pada pertukaran informasi antara dua entitas juga diusulkan dalam penelitian [14]. Usulan perlindungan privasi juga dapat menggunakan teknik

PRivacypreserving and Aggregatable Cybersecurity Information Sharing (PRACIS) dalam perlindungan informasi [16].

Penelitian terkait perlindungan teknologi belum memperhatikan aspek perlindungan privasi yang spesifik pada berbagi informasi keamanan siber dengan memanfaatkan penyimpanan *cloud.* Aspek perlindungan privasi dalam berbagi informasi keamanan siber pada sektor Pemerintah Daerah juga perlu diperhatikan dengan pemanfaatan teknologi tersebut. *Platform* dengan teknologi yang sesuai kriteria dan spesifikasi yang dibutuhkan pada ISAC di sektor Pemerintah Daerah juga perlu tetapkan sebelum mengimplementasikan berbagi informasi keamanan siber antar instansi di Pemerintah Daerah.

Dalam penelitian Zibak & Simpson, implementasi berbagi informasi keamanan siber memiliki pendekatan empat konsep komponen yang terlibat. Namun, berbagi informasi keamanan siber ini dapat diterapkan dengan memperhatikan wawasan yang dimiliki entitas terkait berbagi informasi keamanan siber tersebut [17]. Penelitian lainnya juga membahas mengenai teknologi dalam mendukung berbagi informasi, seperti *cyber threat intelligence sharing*, dengan mengidentifikasi kebutuhan entitas terkait jenis informasi yang ingin dibagikan pada platform yang dibentuk [11]. Berbagi informasi keamanan siber juga membutuhkan kerja sama antar entitas yang terlibat dengan model tata kelola, manajemen kepercayaan, hingga pemberian insentif [18]. Namun, dari keseluruhan penelitian tersebut, terdapat kekurangan mengenai permasalahan tata kelola keamanan siber terkait ekosistem dan aktivitas berbagi informasi keamanan siber yang nantinya akan diterapkan. Salah satu penerapan tersebut bisa dilakukan di berbagai sektor infrastruktur informasi vital, seperti Pemerintah Daerah.

Permasalahan utama yang muncul sebelum dibentuknya ekosistem berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah, tata kelola keamanan siber menjadi aspek fundamental dalam menata proses bisnis berbagi informasi keamanan siber yang diterapkan. Tata kelola keamanan siber terhadap implementasi berbagi informasi keamanan siber melalui ISAC di sektor Pemerintah Daerah juga belum menjadi fokus penelitian sebelumnya. Tata kelola berbagi informasi keamanan siber yang berhasil pada ISAC di sektor Pemerintah Daerah merupakan salah satu bentuk wujud dari pertahanan dan keamanan siber nasional. Serangan siber yang terus meningkat dengan semakin kompleksnya tren ancaman siber mengharuskan setiap sektor memperhatikan kapabilitas keamanan siber yang dimiliki.

Penelitian ini berfokus pada tata kelola berbagi informasi keamanan siber pada implementasi berbagi informasi keamanan siber di dalam ISAC sektor Pemerintah Daerah. Tata kelola berbagi informasi keamanan siber tersebut berfokus pada sumber daya manusia atau entitas *(people)*, proses *(process)*, dan teknologi *(technology)*. Penelitian ini memanfaatkan acuan kerangka kerja pada *NIST Cybersecurity Framework* dan *MITRE Building a National Cyber Information-Sharing Ecosystem* yang disesuaikan dalam pemanfaatannya pada sektor Pemerintah Daerah. Penelitian ini juga mendalami mengenai penerapan perlindungan privasi pada ISAC sektor Pemerintah Daerah dengan memanfaatkan *ISAC Privacy Policy*. Penyesuaian tata kelola berbagi informasi keamanan siber yang diusulkan ini juga mengacu pada peraturan terkait Pemerintah Daerah spesifik yang diimplementasikan di Indonesia.

Manfaat dari penelitian ini yaitu memberikan ruang lingkup fundamental terhadap implementasi ekosistem berbagi informasi keamanan siber pada sektor Pemerintah Daerah dalam rangka strategi penanganan risiko keamanan siber. Selain itu, penelitian ini bermanfaat dalam peningkatan tata kelola berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah guna meningkatkan kapabilitas dan eksistensi SPBE, terkhusus dari sisi keamanan siber di Indonesia dengan fokus sektor Pemerintah Daerah.

Penelitian ini disusun dengan struktur sebagai berikut: Bagian I terdiri atas pendahuluan, Bagian II berisi landasan teori, Bagian III berisi metode penelitian, Bagian IV berisi hasil penelitian dan analisis yang terdiri atas kebutuhan ISAC sektor Pemerintah Daerah, entitas pada ISAC sektor Pemerintah Daerah, Proses Jaringan Informasi Ekosistem ISAC sektor Pemerintah Daerah, program kolaborasi dan koordinasi pada ISAC sektor Pemerintah Daerah, dan teknologi berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah, serta Bagian V yang berisi kesimpulan.

2. LANDASAN TEORI

Dalam Bagian 2, landasan teori yang digunakan terkait penelitian ini yaitu *Information Sharing and Analysis Center, ISAC* di Berbagai Negara, dan Tata Kelola Keamanan Siber.

2.1. Information Sharing and Analysis Center

Information Sharing and Analysis Center (ISAC) merupakan sebuah wadah, dapat berwujud komunitas atau komunikasi, yang menyediakan layanan berbagi informasi keamanan siber berupa kerentanan siber, insiden siber, risiko siber, hingga ancaman siber [9]. Manfaat dari penerapan ISAC yaitu dalam rangka peningkatan kesadaran situasional terhadap ancaman siber, perlindungan hukum, kerja sama dan peningkatan kepercayaan antar entitas di dalamnya, pengurangan biaya atas ancaman siber, hingga fleksibilitas tata kelola organisasi berbagi informasi [9]. Kegiatan ISAC dapat berupa pusat analisis insiden siber, forum dan konferensi, implementasi platform situs kesadaran keamanan, hingga telekonferensi [19].

ISAC yang memuat *platform* teknologi harus

mendukung proses berbagi informasi keamanan siber disertai dengan analisis lanjutan terkait informasi oleh entitas yang berwenang di dalamnya [19]. Beberapa pendekatan yang dapat dipilih untuk tata kelola ISAC, yaitu sebagai berikut [19]:

1. Pendekatan tata kelola terstruktur;
2. Tata kelola dengan badan pendukung; dan
3. Tata kelola yang fleksibel.

2.2. ISAC di Berbagai Negara

Indonesia masih dalam tahap pengembangan penerapan ISAC di berbagai sektor infrastruktur informasi vital. Namun, ISAC sendiri sudah diimplementasikan di berbagai negara yang memiliki kapabilitas keamanan siber paling mumpuni di dunia, seperti Amerika Serikat dan Jepang. Amerika Serikat telah menerapkan ISAC pada berbagai sektor infrastruktur informasi vitalnya, salah satunya melalui *Multi-State ISAC* (MS-ISAC) yang melibatkan seluruh Pemerintah Daerah di Amerika Serikat [20]. Di Jepang, pelaksanaan layanan administrasi pemerintahan termasuk ke dalam sektor infrastruktur informasi vital dan menerapkan ISAC seperti *Financial ISAC*, *Japan ICT-ISAC*, dan *Japan Electricity ISAC* (JE-ISAC) [21].

Negara lainnya yang menerapkan ISAC yaitu Britania Raya dan Australia. Britania Raya menerapkan berbagi informasi keamanan siber pada *Cyber-Security Information Sharing Partnership* (CiSP) yang melibatkan Pemerintah di dalamnya [22]. Negara maju lainnya yang menerapkan ISAC yaitu Australia dengan melibatkan ekosistem Pemerintah Daerah, baik pemerintah bagian dan pemerintah teritorial, ke dalam jaringan berbagi informasi siber Australia [3].

2.3. Tata Kelola Keamanan Siber

Tata kelola keamanan siber mengacu pada seperangkat tanggung jawab yang dilakukan oleh organisasi yang menangani risiko terkait keamanan siber dari sisi strategis [23]. Berbagi informasi merupakan strategi keamanan siber yang penting dan harus dilakukan secara aman dalam melindungi informasi yang dimiliki, baik melalui pertukaran informasi secara privat dan aman [23]. Tata kelola keamanan siber dapat memfasilitasi persyaratan berbagi informasi tersebut [23]. Tata kelola keamanan siber yang efektif harus mencakup komponen seperti strategi dan tujuan keamanan siber, kepatuhan, akuntabilitas, standardisasi, hingga sumber daya [23].

Dalam mewujudkan tata kelola keamanan siber, terdapat kerangka kerja terkait yang memiliki komponen yang dibutuhkan. Kerangka kerja tersebut seperti *NIST Cybersecurity Framework* yang berisi mengenai pengelolaan dan peningkatan program keamanan siber [24]. Tata kelola merupakan salah satu komponen yang diperhatikan di dalam kerangka kerja tersebut. Tata kelola penting dalam menilai risiko dan respons risiko potensial yang berimplikasi terhadap privasi keamanan siber organisasi [24]. Tata kelola juga memperhatikan proses penilaian implementasi tindakan dan pengendalian organisasi terhadap program keamanan siber yang dilakukannya.

Selain *NIST Cybersecurity Framework*, terdapat kerangka kerja lainnya yaitu *MITRE Building a National Cyber Information-Sharing Ecosystem* memiliki kerangka dasar penentuan model dari penerapan berbagi informasi keamanan siber. Aspek yang dibasa di dalam kerangka kerja MITRE tersebut meliputi aspek sumber daya manusia, proses, model ekosistem, dan teknologi yang digunakan terkait berbagi informasi siber antar entitas [25]. MITRE memiliki beberapa model ekosistem yang dapat diimplementasikan ke dalam proses jaringan informasi berbagi informasi keamanan siber antar entitas [26]. Kerangka kerja tersebut tentunya dapat diterapkan di berbagai sektor, salah satunya sektor Pemerintah Daerah yang tergolong ke dalam infrastruktur informasi vital suatu negara.

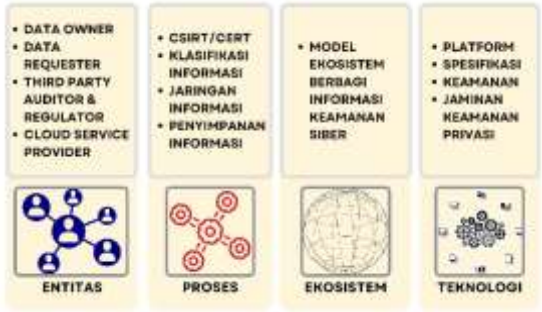
3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif. Pendekatan tersebut menggunakan proses pengumpulan, penyajian, dan analisis data yang berkaitan dengan tata kelola berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah. Objek utama dalam penelitian ini yaitu ekosistem berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah yang dikaitkan dengan implementasinya di Indonesia. Tata kelola berbagi informasi keamanan siber ini akan mengacu pada jaringan informasi keamanan siber yang berhubungan dengan ekosistem tersebut.

Penelitian ini memanfaatkan dua kerangka kerja utama dalam menyusun tata kelola berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah. Kerangka kerja tersebut yaitu *NIST Cybersecurity Framework*, *MITRE Cyber Information-Sharing Models*, dan *MITRE Building a National Cyber Information-Sharing Ecosystem. NIST Cybersecurity Framework* berfokus pada komponen tata kelola keamanan siber yang dikaitkan dengan proses berbagi informasi keamanan siber. *MITRE Building a National Cyber Information-Sharing Ecosystem* berfokus pada aspek sumber daya manusia, proses, model ekosistem, dan teknologi yang digunakan terkait berbagi informasi siber antar entitas [25]. Kedua kerangka kerja tersebut disesuaikan dengan kondisi implementasi organisasi pada sektor Pemerintah Daerah di Indonesia.

Selain kerangka kerja di atas, berbagi informasi keamanan siber turut memperhatikan jaminan keamanan privasi terhadap organisasi atau entitas yang terlibat di dalamnya. Penelitian ini juga memanfaatkan kerangka kebijakan pada *ISAC Privacy Policy*. Kerangka kebijakan tersebut digunakan untuk memperkaya perlindungan informasi keamanan siber yang dipertukarkan di dalam jaringan berbagi informasi keamanan siber.

Komponen tata kelola ekosistem berbagi informasi keamanan siber ditunjukkan pada Gambar 1.



Gambar 1. *Komponen Tata Kelola Ekosistem Berbagi Informasi Keamanan Siber*

Berdasarkan komponen yang ditunjukkan pada Gambar 1, teknik analisis data dalam penelitian ini yaitu sebagai berikut:

1. Identifikasi kebutuhan ISAC sektor Pemerintah Daerah dengan memperhatikan model ekosistem yang berkaitan dengan proses berbagi informasi keamanan siber yang diterapkan pada ISAC sektor Pemerintah Daerah;
2. Analisis entitas yang terkait pada ISAC sektor Pemerintah Daerah dan peranan entitas tersebut di dalam ekosistem berbagi informasi keamanan siber yang dibangun. Entitas tersebut berkaitan dengan sumber daya dan penggerak proses bisnis berbagi informasi keamanan siber di sektor Pemerintah Daerah;
3. Identifikasi proses jaringan informasi keamanan siber yang diterapkan dengan mengklasifikasikan informasi yang dibagikan sesuai dengan kebutuhan sektor;
4. Identifikasi program kolaborasi dan koordinasi terkait berbagi informasi keamanan siber yang diterapkan pada ISAC sektor Pemerintah Daerah; dan
5. Identifikasi teknologi berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah. Teknologi yang dimaksud seperti pemanfaatan *platform* dan aspek keamanannya.

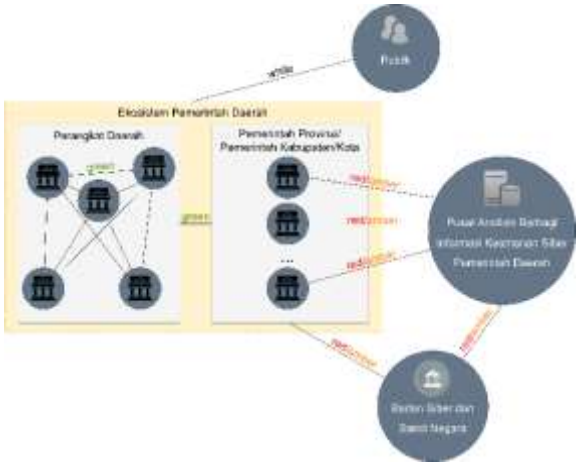
4. HASIL PENELITIAN DAN ANALISIS

4.1. Kebutuhan ISAC Sektor Pemerintah Daerah

Berbagi informasi keamanan siber sangat bermanfaat dan dibutuhkan bagi sektor Pemerintah Daerah untuk memutus rantai serangan siber yang berulang pada sistem teknologi informasinya. Peran Pemerintah Daerah dalam menjalani administrasi pemerintahan memuat informasi sensitif yang kompleks dan memiliki dampak masif secara nasional. Penerapan SPBE guna mendukung administrasi pemerintahan ini perlu diiringi dengan kualitas keamanan terhadap informasi tersebut. Instansi Pemerintah yang berjalan secara masing-masing tentunya akan mengulang kesalahan serangan siber yang sama tanpa adanya komunikasi antar instansi pemerintah. Insiden siber yang terjadi juga tentunya akan memiliki dampak negatif terhadap keuangan negara.

Implementasi ISAC pada sektor Pemerintah Daerah salah satunya dengan menerapkan berbagi informasi seputar perkembangan keamanan siber secara berkelanjutan dari tingkat informasi publik hingga informasi sensitif berklasifikasi rahasia/terbatas. Implementasi ISAC memiliki berbagai tantangan, namun pemanfaatannya sangat berguna dalam efisiensi sumber daya yang dimiliki oleh personel keamanan pada Pemerintah Daerah. Ekosistem yang terbentuk di dalam jaringan informasi keamanan siber pada ISAC sektor pemda tentunya memiliki hubungan antar entitas di dalamnya. Informasi keamanan siber yang dibagikan di dalam jaringan informasi tersebut tidak berasal dari klasifikasi informasi yang sama. Terdapat 4 klasifikasi informasi berdasarkan *Traffic Light Protocol* (TLP), yaitu *red* (rahasia), *amber* (terbatas), *green* (terbatas untuk komunitas), dan *white* (terbuka atau informasi publik).

Ekosistem berbagi informasi keamanan siber yang diusulkan pada sektor Pemerintah Daerah ditunjukkan pada Gambar 2. Ekosistem ini disesuaikan berdasarkan model pada referensi yang digunakan dalam penelitian ini dengan implementasi sektor Pemerintah Daerah, yang melibatkan Perangkat Daerah, instansi pembina keamanan siber, maupun publik. Ekosistem tersebut merujuk pada pemanfaatan informasi keamanan siber di lingkungan Pemerintah Daerah berbasis risiko keamanan siber yang optimal atas implementasi ekosistem berbagi informasi keamanan siber.



Gambar 2. *Model Ekosistem Berbagi Informasi Keamanan Siber pada Sektor Pemerintah Daerah*

Ekosistem pada Gambar 2 melibatkan Pemerintah Daerah yang terdiri dari Pemerintah Provinsi dan Pemerintah Kabupaten/Kota hingga Perangkat Daerah. Pemerintah Provinsi dan Pemerintah Kabupaten/Kota memiliki otonomi daerah, sehingga informasi keamanan siber yang mereka kelola dapat secara penuh di bawah kebijakan instansi masing-masing tersebut. Ekosistem

Pemerintah Daerah tentunya berhubungan erat dengan instansi pembina sekaligus regulator terkait keamanan siber, yaitu Badan Siber dan Sandi Negara (BSSN). Selain itu, informasi keamanan siber yang biasanya berupa informasi digital (dalam ranah siber) merupakan salah satu aset yang perlu disimpan secara aman. Dengan model ekosistem tersebut, peran dari Pusat Analisis Informasi Keamanan Siber Pemerintah Daerah diperlukan. Pusat tersebut dapat berupa *cloud provider* pihak ketiga tepercaya atau dapat berupa *cloud provider* salah satu entitas terpercaya di dalam jaringan tersebut.

Model ekosistem yang diusulkan pada Gambar 2 menjelaskan beberapa model yang diterapkan. Model yang diterapkan yaitu model *hybrid.* Model tersebut berisi model *hub-and-spoke* dan *post-to-all* serta model *source-subscriber*. Penyesuaian model ekosistem tersebut berdasarkan klasifikasi informasi yang sesuai pada ekosistem jaringan berbagi informasi keamanan siber sektor Pemerintah Daerah.

1. Model *Hub-and-Spokes.* Model ini merupakan model yang paling tepat digunakan untuk informasi berklasifikasi rahasia/terbatas, seperti TLP: *red* dan TLP: *amber*. Sumber informasi rahasia/terbatas ini perlu diolah dengan teliti karena berhubungan dengan berjalannya proses bisnis instansi. Model ini menyajikan salah satu entitas yang menjadi *hub.* Entitas tersebut merupakan entitas yang memiliki keamanan tinggi dalam penyimpanan informasi dan mudah diakses oleh entitas yang berkepentingan. Model ini diterapkan untuk berbagi informasi keamanan siber antar Pemerintah Provinsi dan Pemerintah Kabupaten/Kota yang di dalamnya memuat informasi siber yang sensitif.
2. Model *Post-to-All.* Model ini sangat sesuai diterapkan pada ekosistem Pemerintah Daerah. Di dalam ekosistem tersebut, setiap Pemerintah Daerah baik entitas Pemerintah Provinsi, Pemerintah Kabupaten/Kota, serta Perangkat Daerah, bisa memberikan informasi berklasifikasi TLP: *green* satu sama lain. Informasi seperti ini dapat bermanfaat untuk meningkatkan proteksi dan *situational awareness* di lingkungan Pemerintah Daerah. Validasi informasi secara mandiri dapat diterapkan pada model ini, karena model ini berfokus pada berbagi informasi secara berkala oleh tiap entitas di Pemerintah Daerah. Informasi yang dibagikan dengan TLP: *green* berhubungan dengan *lesson learned* keamanan siber.
3. Model *Source-subscribers.* Model ini ditunjukkan dari sisi interaksi antara entitas publik dengan ekosistem Pemerintah Daerah dengan TLP: *white* secara *broadcast.* Model ini sangat sesuai karena publik (masyarakat) dapat menerima segala jenis informasi terkait keamanan siber dengan klasifikasi informasi *white* (seperti *advisory*, imbauan, laporan monitoring berkala, tips dan peringatan dini keamanan) dari entitas Pemerintah Daerah melalui internet.

4.2. Entitas pada ISAC Sektor Pemerintah Daerah

Entitas yang terlibat dalam ekosistem ISAC sektor Pemerintah Daerah pada umumnya dibagi ke dalam empat peran. Peran tersebut diringkas dan dikaitkan dengan sektor Pemerintah Daerah di Indonesia pada Tabel 1.

Berdasarkan Tabel 1, terdapat empat peran entitas di dalam ekosistem ISAC sektor Pemerintah Daerah:

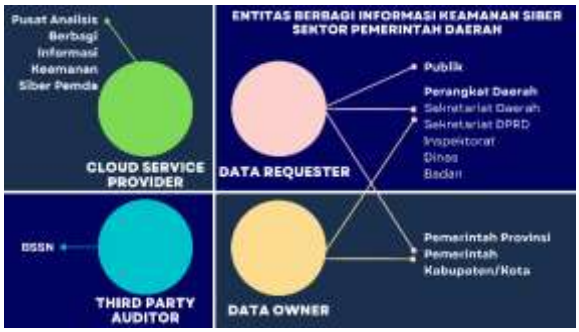
1. *Cloud Service Provider*: Entitas yang memiliki tugas dalam penyimpanan, pengolahan, dan analisis informasi keamanan siber yang dipertukarkan oleh entitas dengan fokus informasi berklasifikasi rahasia/terbatas (TLP: *red/amber*).
2. *Third Party Auditor*: Entitas yang memiliki tugas dalam memantau informasi keamanan siber yang dipertukarkan di dalam ekosistem berbagi informasi keamanan siber untuk dijadikan bahan kebijakan teknis di bidang keamanan siber.
3. *Data Requester*: Entitas yang memiliki hak dalam meminta informasi keamanan siber yang dipertukarkan di dalam ekosistem berbagi informasi keamanan siber.
4. *Data Owner*: Entitas yang memiliki tugas dan hak dalam memberikan informasi keamanan siber yang dipertukarkan di dalam ekosistem berbagi informasi keamanan siber.

Tabel 1. Daftar Entitas

Peran	Definisi	Entitas
CSP	*Cloud Service Provider*	Pusat Analisis Berbagi Informasi Keamanan Siber Pemerintah Daerah
TPA	*Third Party Auditor*	BSSN
DR	*Data Requester*	1. Pemerintah Provinsi 2. Pemerintah Kabupaten/Kota 3. Perangkat Daerah 4. Publik
DO	*Data Owner*	1. Pemerintah Provinsi 2. Pemerintah Kabupaten/Kota 3. Perangkat Daerah

Entitas baik *data requester* dan *data owner* yang memiliki akses ke dalam informasi keamanan siber berklasifikasi rahasia/terbatas (TLP: *red/amber*) sewajarnya sudah memiliki tim khusus di bidang keamanan siber. Contoh dari tim tersebut seperti *Computer Security Incident Response Team* (CSIRT) atau *Computer Emergency Response Team* (CERT). CSIRT atau CERT merupakan salah satu tim yang khusus menangani keamanan dan insiden keamanan siber pada masing-masing organisasi. CSIRT tersebut

terdiri dari sumber daya manusia yang mumpuni di bidang keamanan siber. Secara pembagian entitas, dianalogikan di dalam Gambar 3.



Gambar 3. *Entitas Berbagi Informasi Keamanan Siber Sektor Pemerintah Daerah*

CSIRT/CERT memiliki peran penting dalam isu kepercayaan berbagi informasi keamanan siber antar entitas di dalam ekosistem ISAC. Pemerintah Daerah, baik Pemerintah Provinsi dan Pemerintah Kabupaten/Kota yang memiliki otonomi daerah perlu memiliki CSIRT/CERT tersebut. Informasi dapat dibagikan kepada pihak internal masing-masing dengan adanya persetujuan pertukaran informasi pada forum ISAC sektor Pemerintah Daerah tersebut, seperti informasi bagi/untuk personel penanggung jawab CSIRT (*person in charge*) dan direktur atau pimpinan instansi terkait.

4.3. Proses Jaringan Informasi Ekosistem ISAC Sektor Pemerintah Daerah

Sesuai dengan struktur tata kelola berbagi informasi keamanan siber pada taksonomi model [27], Inisiasi program berbagi informasi keamanan siber dapat dilakukan oleh Pemerintah Pusat maupun berasal dari salah satu entitas Pemerintah Daerah itu sendiri. Dalam urusan keamanan siber di Indonesia, Pemerintah Pusat, yaitu BSSN, secara tugas dan fungsi dapat menginisiasi pembentukan ekosistem ISAC dalam rangka berbagi informasi keamanan siber. Apabila BSSN menginisiasi program tersebut, BSSN dapat membantu proses berbagi informasi keamanan siber dengan turut serta menyediakan Pusat Analisis Informasi Keamanan Siber Pemerintah Daerah.

Inisiasi pemerintah pusat seperti BSSN dapat membantu proses bisnis keamanan siber dalam skala nasional seperti isu kriminal siber dan keamanan nasional. Kekurangan implementasi keamanan siber pada sektor Pemerintah Daerah dapat didorong oleh BSSN melalui program berbagi informasi keamanan siber di sektor Pemerintah Daerah. Implementasi ISAC di sektor Pemerintah Daerah juga dapat menjadi sebuah manifestasi dalam mewujudkan kedaulatan keamanan siber di Indonesia. ISAC dapat membantu proses efisiensi program keamanan siber pada sektor Pemerintah Daerah, terutama dalam melindungi infrastruktur informasi vital nasional dalam urusan administrasi pemerintahan.

Tabel 2. Hubungan Klasifikasi Informasi dengan Ekosistem ISAC pada Sektor Pemerintah Daerah

Klasifikasi Informasi	Entitas	Model Ekosistem
Red/Amber	1. Pemerintah Provinsi 2. Pemerintah Kabupaten/Kota 3. BSSN 4. Pusat Analisis Berbagi Informasi Keamanan Siber Pemerintah Daerah	*Hub-and-Spoke*
Green	1. Pemerintah Provinsi 2. Pemerintah Kabupaten/Kota 3. Perangkat Daerah	*Post-to-All*
White	1. Pemerintah Provinsi 2. Pemerintah Kabupaten/Kota 3. Perangkat Daerah 4. Publik	*Source-Subscriber*

Penerapan jaringan informasi keamanan siber pada ISAC sektor Pemerintah Daerah ini diklasifikasikan berdasarkan klasifikasi informasi, seperti penerapan TLP. Penerapan TLP ini difokuskan dalam informasi berklasifikasi rahasia atau terbatas yang harus terjamin kerahasiaan dan keamanannya. Tabel 2 merupakan keterkaitan klasifikasi informasi keamanan siber dengan entitas yang terlibat serta model ekosistem jaringan informasi keamanan siber terkait.

Pemerintah Provinsi (Pemprov) dan Pemerintah Kabupaten/Kota (Pemkab/Pemkot) direpresentasikan oleh CSIRT/CERT yang dikelola dan diberikan tanggung jawab kepada Kepala Dinas di bidang komunikasi, informasi, persandian, dan teknologi informasi. Perangkat Daerah direpresentasikan oleh seluruh unsur pembantu Kepala Daerah dalam urusan administrasi pemerintahan tertentu. Berdasarkan Tabel 2, dijabarkan penjelasan sebagai berikut:

1. TLP: *Red/Amber*. Model yang melibatkan *hub* sebagai pusat penyimpanan dan pertukaran informasi dan *spokes* yang terhubung sebagai pemberi dan penerima informasi (model *hub-and-spokes*). TLP: *Red* memiliki informasi sensitif yang terbatas bagi personel yang berhubungan dengan penanggung jawab di bidang keamanan siber (seperti Gubernur, Bupati/Walikota, Kepala Dinas terkait). Informasi berklasifikasi TLP: *Red* dibagikan hanya kepada pihak di dalam pertukaran, pertemuan (rapat terbatas), atau percakapan tertentu pada saat informasi tersebut diungkapkan. Informasi berklasifikasi TLP: *Red* ini sangat sensitif, sehingga pada beberapa situasi hanya dibagikan secara lisan/langsung. TLP: *Amber* memiliki informasi sensitif yang terbatas

bagi personel yang memang membutuhkan informasi tersebut, seperti perwakilan penanggung jawab keamanan siber masing-masing instansi (Kepala Dinas terkait hingga personel yang bertanggung jawab/ berhubungan dengan pengungkapan informasi).

2. TLP: *Green*. Model yang melibatkan antar entitas pengirim dan penerima (Pemprov, Pemkab/Pemkot, dan Perangkat Daerah) untuk saling berbagi informasi keamanan siber (model *post-to-all*). Penerima hanya terbatas bagi ekosistem Pemerintah Daerah melalui jaringan khusus terbatas pada komunitas anggota di dalamnya.
3. TLP: *White.* Model yang melibatkan entitas di dalam ekosistem Pemerintah Daerah (Pemprov, Pemkab/Pemkot, dan Perangkat Daerah) untuk berbagi informasi publik bagi masyarakat luas (model *source-subscribers*). Informasi ini merupakan informasi publik yang dapat diakses oleh masyarakat untuk meningkatkan kesadaran terhadap keamanan siber.

4.4. Teknologi Berbagi Informasi Keamanan Siber pada ISAC Pemerintah Daerah

Berbagi informasi keamanan siber membutuhkan teknologi berupa platform untuk membantu proses pertukaran dan penyimpanan informasi di dalam ISAC. Informasi yang dipertukarkan pada umumnya memiliki klasifikasi yang berbeda-beda. Klasifikasi informasi berdasarkan TLP FIRST dibagi menjadi empat, yaitu *red, amber, green,* dan *white.*

Teknologi informasi yang melindungi pertukaran informasi berklasifikasi, seperti TLP: *Red* dan *Amber* perlu memiliki keamanan tingkat tinggi. Informasi perlu dilindungi berdasarkan keamanan platform teknologi hingga teknik keamanan yang mendukung, seperti penerapan enkripsi dan protokol keamanan. Teknologi informasi yang diterapkan oleh lingkungan instansi Pemerintah Daerah dikenal dengan penerapan SPBE. Keamanan SPBE yang menjadi dasar teknologi tersebut harus diamankan untuk mencegah terjadinya insiden siber seperti kebocoran informasi.

Spesifikasi teknologi yang dibutuhkan dalam berbagi informasi keamanan siber harus menjamin aspek keamanan, yaitu kerahasiaan, keutuhan, dan ketersediaan informasi. Kerahasiaan berlaku terhadap informasi berklasifikasi TLP: *Red* dan *Amber*. Keutuhan berlaku terhadap informasi berklasifikasi TLP: *Red, Amber, Green,* dan *White.* Ketersediaan informasi juga berlaku bagi seluruh klasifikasi informasi, namun ketersediaan memiliki tingkat kritis yang tinggi terhadap informasi yang bersifat cepat ditindak, seperti informasi penanganan insiden, *patch* keamanan, hingga kerentanan sistem informasi.

Aspek keamanan privasi merupakan salah satu aspek yang perlu dimiliki oleh kemampuan teknologi yang diterapkan. Keamanan privasi sebagai syarat dasar entitas di dalamnya (elemen Pemerintah Daerah) untuk ikut serta dalam ekosistem berbagi informasi keamanan siber. Kebijakan keamanan privasi harus diterapkan beriringan dengan penerapan teknologi yang diimplementasikan oleh entitas di dalamnya. Komponen kebijakan keamanan privasi di dalam penerapan ISAC sektor Pemerintah Daerah yaitu sebagai berikut:

1. Metode Pengungkapan Informasi: informasi yang diungkapkan di dalam teknologi/platform yang diterapkan harus menjamin hak dan kewajiban terhadap entitas di dalamnya, baik pemilik dan penerima informasi maupun pengolah informasi.
2. Akses dan Pengubahan Informasi: informasi dapat diakses oleh setiap entitas yang berhak dengan syarat dan ketentuan tertentu. Informasi yang beredar di dalamnya juga dilindungi, sehingga informasi yang beredar tidak dengan mudahnya diubah yang mengakibatkan informasi menjadi tidak valid.
3. Subjek Data: setiap subjek data seperti hak entitas hingga pengolah data merupakan ruang lingkup subjek data. Setiap subjek data yang berada di dalam ekosistem berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah ini tunduk pada hukum yang berlaku, terutama yang berkaitan dengan data pribadi.
4. Kebijakan *Cookies* pada *Browser* (teknologi/ platform yang digunakan): pemanfaatan platform yang berkaitan dengan *browser* perlu diperhatikan kebijakan terkait manajemen *cookies. Cookies* pada *browser* dapat dimanfaatkan untuk kebutuhan pengguna namun rentan terhadap isu privasi entitas.
5. *Automated Decision-making & Profiling* (korespondensi, URL & *IP Address*): penerapan teknologi berbagi informasi keamanan siber ini berkaitan dengan beberapa otomatisasi, sehingga keputusan dapat terlibat tanpa adanya bantuan manusia. Proses ini tentunya membuat sistem berbagi informasi keamanan siber menjadi lebih efisien. Namun, dalam pengaturannya, perlu adanya korespondensi antara entitas dengan sistem teknologi ISAC dalam berkomunikasi (seperti melalui *email,* atau komunikasi lainnya). Selain itu, perlu adanya pengaturan terkait URL dan *IP Address* dalam rangka potensi insiden keamanan.

4.5. Program Kolaborasi dan Koordinasi pada ISAC Sektor Pemerintah Daerah

Implementasi berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah juga harus memperhatikan pelaksanaan program kolaborasi dan koordinasi antar entitas di dalamnya. Program ini harus mendukung pengendalian risiko terhadap kerahasiaan, keutuhan, dan ketersediaan atas informasi dan proses kegiatan di dalamnya. Program kolaborasi dan koordinasi antar entitas di dalam ekosistem berbagi informasi keamanan siber telah

diterapkan oleh ISAC Pemerintah Daerah di negara maju yang memiliki kapabilitas keamanan siber yang cukup mumpuni.

Program implementasi berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah yang dapat diterapkan di Indonesia dijabarkan pada Tabel 3. Program tersebut mengacu pada *MITRE Building a National Cyber Information-Sharing Ecosystem.*

Pada Tabel 3, terdapat delapan program kolaborasi dan koordinasi terkait berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah. ISAC dapat berwujud sebagai sebuah organisasi atau sebuah kesepakatan *ad-hoc* antar instansi Pemerintah Daerah yang mewadahi dan menfasilitasi program kegiatan berbagi informasi keamanan siber. Program tersebut dilaksanakan untuk meningkatkan kapabilitas keamanan siber di sektor Pemerintah Daerah dalam jangka panjang.

Tabel 3.Program Kolaborasi dan Koordinasi pada ISAC Pemerintah Daerah

Program	Deskripsi	Unsur Informasi Berklasifikasi
Cyber Session	Sesi diskusi berbagi informasi antara defender dan analis oleh masing-masing instansi/sektor Provinsi tentatif, 1-2 minggu/pertemuan.	*Red, Amber*
Cyber Portal	Platform berupa portal *website* yang diakses oleh *expert* & analis untuk berbagi & diskusi terkait informasi sensitif.	*Red, Amber*
Kolaborasi Penelitian Ancaman Siber	Platform repositori & analisis, analisis ancaman, kerentanan, dan sumber ancaman	*Red, Amber*
Handshake Group	Aplikasi media sosial yang aman untuk fasilitasi interaksi antar anggota	*Red, Amber*
Cyber Exchange Forums	Forum antar anggota terkait diskusi panel, strategi ISAC, hingga sesi berbagi informasi.	*Amber, Green*
Group Email List	Daftar ini bermanfaat untuk memiliki akses dan hak terhadap informasi yang dibagikan.	*Green*
ISAC Website	Platform *website* yang menyediakan layanan pertukaran informasi antar anggota.	*Green, White*
ISAC Annual Conference	Rangkaian konferensi seputar berbagi informasi bagi anggota dan akademisi. Terdapat sesi pleno di pagi hari dan sesi *breakout* di siang-sore hari, presentasi poster, hingga *plenary session* di akhir sesi.	*Green, White*

Manfaat dari program ini yaitu peningkatan kemampuan dan kapabilitas keamanan siber pada masing-masing instansi. Selain itu, program ini disusun untuk jangka panjang oleh setiap instansi Pemerintah Daerah di dalamnya dengan tujuan untuk mengurangi risiko keamanan siber yang terjadi di masa depan. Tingginya risiko keamanan siber yang terjadi di masa depan, seperti insiden siber yang merugikan aset negara maupun publik, dapat dikurangi dengan adanya program kolaborasi dan koordinasi tersebut.

5. KESIMPULAN DAN SARAN

Tata kelola berbagi informasi keamanan siber yang berhasil pada ISAC di sektor Pemerintah Daerah dapat meningkatkan kapabilitas keamanan siber. Terdapat 5 (lima) area tata kelola berbagi informasi keamanan siber, yaitu kebutuhan ISAC seperti model ekosistem dan klasifikasi informasi, entitas, jaringan informasi, teknologi, serta program kolaborasi dan koordinasi. Model ekosistem berbagi informasi keamanan siber pada ISAC sektor Pemerintah Daerah melibatkan model *hybrid*, yang berisi model *hub-and-spokes, post-to-all,* dan *source-subsribers*. Klasifikasi informasi yang terlibat yaitu informasi berklasifikasi rahasia hingga terbuka/publik. Dalam proses berbagi informasi, entitas yang terlibat meliputi entitas di dalam ekosistem Pemerintah Daerah, BSSN, dan Pusat Analisis Informasi Keamanan Siber Pemerintah Daerah, hingga masyarakat/publik. Proses jaringan informasi perlu diklasifikasikan berdasarkan klasifikasi informasi yang dibagikan di dalam ekosistem. Teknologi yang mendukung proses juga harus memperhatikan unsur kerahasiaan, keutuhan, dan ketersediaan informasi di dalamnya, serta keamanan privasi entitas yang bergabung. Dalam implementasinya, program kolaborasi dan koordinasi dibagi ke dalam 8 (delapan) program unggulan.

Implementasi berbagi informasi keamanan siber di sektor Pemerintah Daerah perlu menentukan *leading sector* yang membantu tugas dan fungsi kemandirian sektor Pemerintah Daerah di luar instansi pembina yaitu BSSN. Pada penelitian selanjutnya, kebutuhan berbagi informasi keamanan siber perlu ditinjau berdasarkan penelitian survei untuk memperoleh data dan kondisi di lapangan secara komprehensif. Survei ini akan menunjukkan kondisi kebutuhan berbagi informasi keamanan siber antar instansi Pemerintah. Selain itu, survei yang dilakukan dapat menunjukkan isu berbagi informasi keamanan siber seperti isu privasi dan kepercayaan antar entitas.

REFERENSI

[1] Z. Aviram, "Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views," *Journal of Cybersecurity*, vol. 4, no. 1, pp. 1-8, 2018.

[2] I. Vakilinia and S. Sengupta, "Fair and private rewarding in a coalitional game of cybersecurity information sharing," *IET Information Security*, vol. 13, no. 6, pp. 530-540, 2019, doi: 10.1049/iet-ifs.2018.5079.

[3] L. Nevill, *Cyber Information Sharing: Lessons for Australia*. ASPI International Cyber Policy Centre (ICPC), 2017.

[4] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Computers & Security*, vol. 87, 2019, doi: 10.1016/j.cose.2019.101589.

[5] B. Guo, X. Deng, J. Tian, Q. Guan, and X. Zheng, "A Secure Incentive Mechanism for Competitive Organization Data Sharing: A Contract Theoretic Approach," *IEEE Access*, vol. 7, pp. 60067-60078, 2019, doi: 10.1109/ACCESS.2019.2915387.

[6] A. Mermoud, M. M. Keupp, K. Huguenin, M. Palmie, and D. P. David, "To share or not to share: A behavioral perspective on human participation in security information sharing," *Journal of Cybersecurity*, vol. 5, no. 1, pp. 1-13, 2019, doi: 10.1093/cybsec/tyz006.

[7] S. C. Dewanti, "Urgensi Sistem Keamanan Siber Pemerintah," *Kajian Singkat Terhadap Isu Aktual dan Strategis Bidang Politik Dalam Negeri*, vol. XIII, no. 16, pp. 25-30, 2021.

[8] J. Hautamäki and T. Kokkonen, "Model for Cyber Security Information Sharing in Healthcare Sector," in *Proc. of the 2nd International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, Istanbul, Turkey, 2020: IEEE.

[9] E. M. Sedenberg and D. K. Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," *JSTOR*, vol. 30, no. University of California, Berkeley, School of Law, 2015.

[10] Y. Zhang, S. Deng, Y. Zhang, and J. Kong, "Research on Government Information Sharing Model Using Blockchain Technology," in *10th International Conference on Information Technology in Medicine and Education (ITME)*, Qingdao, China, 2019: IEEE, pp. 726-729, doi: 10.1109/ITME.2019.00166.

[11] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, "Towards a Maturity Model for Inter-Organizational Cyber Threat Intelligence Sharing: A Case Study of Stakeholders' Expectations and Willingness to Share," in *MKWI 2018*, Lüneburg, 2018: Leuphana Universität Lüneburg, pp. 1409-1420.

[12] T. Takahashi, Y. Kadobayashi, and K. Nakao, "Toward global cybersecurity collaboration: Cybersecurity operation activity model," in *Proceedings of ITU Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services (K-2011)*, Cape Town, South Africa, 2011: IEEE, pp. 1-8.

[13] D.-J. van Veen, R. S. Kudesia, and H. R. Heinimann, "An Agent-Based Model of Collective Decision-Making: How Information Sharing Strategies Scale With Information Overload," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 3, pp. 751-767, 2020, doi: 10.1109/tcss.2020.2986161.

[14] K. Yan, W. Shen, Q. Jin, and H. Lu, "Emerging Privacy Issues and Solutions in Cyber-Enabled Sharing Services: From Multiple Perspectives," *IEEE Access*, vol. 7, pp. 26031-26059, 2019, doi: 10.1109/access.2019.2894344.

[15] L. Zhang, Y. Cui, and YiMu, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing," *IEEE System Journal*, vol. 14, no. 1, pp. 387-397, 2020.

[16] J. M. de Fuentes, L. González-Manzano, J. Tapiador, and P. Peris-Lopez, "PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing," *Computers & Security*, vol. 69, pp. 127-141, 2017, doi: 10.1016/j.cose.2016.12.011.

[17] A. Zibak and A. Simpson, "Towards Better Understanding of Cyber Security Information Sharing," presented at the 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, 2019.

[18] A. Deljoo, T. van Engers, R. Koning, L. Gommans, and C. de Laat, "Towards Trustworthy Information Sharing by Creating Cyber Security Alliances," presented at the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018.

[19] (2017). *ENISA Information Sharing and Analysis Center -ISACs- Cooperative models*.

[20] T. C. f. I. S. (CIS), *MS-ISAC Multi-State Information Sharing & Analysis Center Service Guide*. 2018.

[21] L. W. II, M. Tsuchiya, and R. Repko, "Improving Cybersecurity Cooperation between the Governments of the United States and Japan," *SASAKAWA USA*, 2020.

[22] ENISA, *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. European Union Agency For Network And Information Security (ENISA), 2015.

[23] S. Yusif and A. Hafeez-Baig, "A Conceptual Model for Cybersecurity Governance," *Journal of Applied Security Research*, vol. 16, no. 4, pp. 490-513, 2021, doi: https://doi.org/10.1080/19361610.2021.1918995.

[24] (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*.

[25] B. J. Bakis and E. D. Wang, *Building a National Cyber Information-Sharing Ecosystem*: MITRE, 2017.

[26] MITRE, *Cyber Information-Sharing Models: An Overview*: MITRE, 2012.

[27] E. M. Sedenberg and J. X. Dempsey, "Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs," *arXiv Journal*, no. Cornell University, pp. 1-27, 2018.