KERJASAMA BADAN SIBER DAN SANDI NEGARA (BSSN) DAN *KOREA INTERNET AND SECURITY AGENCY* (KISA) DALAM MENINGKATKAN KEAMANAN CYBER DI INDONESIA (2022)

Diyah Pitaloka Rizki[1], Rijal Aditia[2]
Program Studi Hubungan Internasional,
Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Al-Ghifari Bandung
Email: *diyahpitaloka801@gmail.com*, *crewrizal009@gmail.com*

ABSTRAK

Peningkatan ancaman siber yang mengancam keamanan data dan stabilitas nasional Indonesia mendorong kerja sama antara Badan Siber dan Sandi Negara (BSSN) *dan Korea Internet and Security Agency (KISA*) pada 2022. Indonesia membutuhkan dukungan pengetahuan dan teknologi untuk memperkuat ketahanan sibernya karena pesatnya digitalisasi. Kolaborasi dengan Korea Selatan melalui KISA, yang memiliki pengalaman luas dalam keamanan siber, diharapkan dapat membantu Indonesia mengatasi ancaman siber yang semakin kompleks.

Penulisan ini bertujuan untuk menganalisis seberapa efektif kerja sama antara BSSN dan KISA dalam meningkatkan keamanan siber di Indonesia. Selain itu, tujuan penulisan ini adalah untuk mengidentifikasi efek kerja sama tersebut terhadap ketahanan siber nasional.

Penulisan ini menggunakan pendekatan neoliberalisme untuk mendapatkan pemahaman yang lebih baik tentang kerja sama antara BSSN dan KISA. Pendekatan ini menekankan pentingnya aliansi global untuk menghadapi ancaman bersama, seperti keamanan siber. Pendekatan kerja sama digunakan untuk menganalisis dinamika dan efektivitas kerja sama antara kedua lembaga ini dalam meningkatkan keamanan digital, sementara pendekatan keamanan nasional membantu menilai kontribusi kerja sama ini dalam melindungi aset dan kepentingan nasional.Studi ini mengkaji strategi, tantangan, dan hasil dari kemitraan internasional ini, dengan fokus pada bagaimana kedua lembaga bekerja sama untuk menangani ancaman siber dan meningkatkan postur keamanan secara keseluruhan di Indonesia. Area utama yang diteliti meliputi penyelarasan kerangka regulasi, integrasi sumber daya teknologi, dan efektivitas mekanisme komunikasi dan koordinasi antara BSSN dan KISA. Menggunakan metodologi kualitatif deskriptif, penelitian ini mengandalkan data dari sumber yang terpercaya. Penelitian ini menyoroti keberhasilan dan hambatan yang dihadapi dalam kerjasama ini, serta menawarkan wawasan tentang praktik terbaik dan rekomendasi untuk memperkuat upaya keamanan siber internasional di masa depan. Temuan menunjukkan bahwa meskipun kemajuan signifikan telah dicapai, adaptasi dan koordinasi yang berkelanjutan sangat penting untuk menghadapi lanskap ancaman siber yang terus berkembang.

Kata Kunci: Keamanan Siber, Badan Siber dan Sandi Negara (BSSN), Korea Internet and Security Agency (KISA), Kerja Sama Internasional, Neoliberalisme, dan Kerjasama Internasional

Pendahuluan

Kerja sama antara Badan Siber dan Sandi Negara (BSSN) dan Korea Internet and Security Agency (KISA) akan dimulai pada tahun 2022 sebagai tanggapan atas ancaman siber yang semakin meningkat di Indonesia yang dapat mengancam keamanan data dan stabilitas nasional. Ancaman seperti peretasan dan pencurian data semakin kompleks dan beragam seiring dengan pesatnya kemajuan teknologi informasi dan digitalisasi. Untuk memperkuat pertahanan sibernya, Indonesia membutuhkan dukungan dari negara lain yang memiliki pengalaman dalam bidang keamanan siber. KISA, yang memiliki pengalaman dan teknologi canggih, diharapkan dapat membantu Indonesia dalam membangun infrastruktur keamanan siber yang tangguh. Kerja sama ini menunjukkan komitmen kedua negara untuk memastikan lingkungan siber aman dan mendukung transformasi digital yang berkelanjutan.

Fokus dan konteks yang membedakan analisis kerja sama keamanan siber Indonesia-Australia oleh Muhamad Rizki Hapizon, Khairur Rizki, dan Mahmuluddin dari analisis kerja sama antara Badan Siber dan Sandi Negara (BSSN) dan Korea Internet dan Sandi Agensi (KISA). Analisis BSSN dan KISA lebih berfokus pada aspek teknis dan transfer teknologi global, sedangkan analisis Indonesia-Australia lebih menekankan pada hubungan bilateral dan strategi mitigasi dalam konteks geografis dan politik Kawasan. Selain itu, analisis yang digunakan dalam analisis sebelumnya mungkin lebih fokus pada pengaruh kebijakan luar negeri dan keamanan regional, sedangkan analisis yang menggunakan KISA berfokus pada pengembangan kapasitas dan infrastruktur keamanan siber nasional. Selain itu, konteks waktu kedua analisis ini berbeda; kerja sama Indonesia-Australia sering dikaitkan dengan respons terhadap kejadian siber tertentu. Sebaliknya, kolaborasi dengan KISA muncul sebagai tindakan proaktif untuk mencegah ancaman siber yang akan datang.

Penelitian ini bertujuan untuk mengevaluasi seberapa efektif kerja sama antara Badan Siber dan Sandi Negara (BSSN) dan Korea Internet and Security Agency (KISA) dalam meningkatkan keamanan siber di Indonesia. Selain itu, penelitian ini bertujuan untuk mengidentifikasi dampak kerja sama tersebut terhadap ketahanan siber nasional, serta keuntungan dan kerugian dari penerapan kerja sama tersebut.

Penelitian ini menggunakan pendekatan kualitatif, yang mengumpulkan dan menganalisis data dari wawancara, dokumen, dan laporan untuk memahami dinamika kerja sama. Hasil diskusi menunjukkan bahwa kerja sama berhasil meningkatkan infrastruktur teknis dan kapasitas keamanan siber Indonesia serta memperkuat tanggapan terhadap ancaman siber. Namun, masalah seperti perbedaan budaya dan kebijakan organisasi masih perlu diatasi untuk meningkatkan hasil kerja sama. Penelitian ini menemukan bahwa kerja sama BSSN dan KISA merupakan langkah penting dalam membangun ketahanan siber Indonesia. Kerja sama ini harus dilanjutkan dan diperkuat untuk menghadapi ancaman yang muncul di era digital.

Konten materi dalam penelitian ini mencakup analisis berbagai aspek kerja sama antara Badan Siber dan Sandi Negara (BSSN) dan Korea Internet and Security Agency (KISA), termasuk transfer teknologi, pelatihan, dan

pengembangan kebijakan keamanan siber. Penelitian ini juga menyoroti pentingnya strategi kolaboratif dalam meningkatkan kapasitas teknis dan infrastruktur keamanan siber Indonesia. Impak dari kerja sama ini diharapkan dapat memperkuat ketahanan siber nasional, meminimalkan risiko ancaman siber, dan mendorong pengembangan kebijakan yang lebih efektif dalam menghadapi tantangan di dunia digital. Selain itu, hasil penelitian ini dapat memberikan wawasan bagi pengambil kebijakan dalam merumuskan strategi keamanan siber yang lebih komprehensif dan responsif terhadap dinamika global. Dengan demikian, kerja sama ini tidak hanya berdampak pada keamanan nasional, tetapi juga pada peningkatan kepercayaan masyarakat terhadap keamanan informasi di Indonesia.

Tinjauan Teoritis

Neoliberalisme

Teori neoliberal dalam hubungan internasional menekankan betapa pentingnya kerja sama antarnegara untuk menangani masalah global. Teori ini didasarkan pada keyakinan bahwa negara dapat memperoleh keuntungan melalui kerja sama yang menguntungkan dan keterikatan (interdependensi) yang kuat di berbagai bidang, seperti ekonomi dan keamanan. Karena setiap negara bergantung pada keberhasilan dan stabilitas negara lain dalam sistem internasional yang kompleks, menurut Keohane dan Nye(Keohane, dan Nye 1977), hubungan interdependen antara negara meningkatkan keinginan untuk bekerja sama.

Neoliberalisme menekankan pentingnya kerjasama antarnegara, meskipun berada dalam sistem internasional yang anarkis. Fokus utama dari pandangan ini adalah keyakinan bahwa meskipun sistem internasional cenderung tidak teratur dan tidak memiliki otoritas sentral, kerjasama antarnegara masih dapat terjadi dan bahkan dapat dipertahankan. Neoliberalis percaya bahwa optimisme terhadap kemungkinan kerjasama ini didasarkan pada pemahaman bahwa negara-negara, meskipun bersifat egois, tetap memiliki kepentingan bersama yang dapat diupayakan melalui kerjasama.

Menurut perspektif neoliberalis, sensitivitas yang berlebihan negara terhadap pencapaian relatifnya, atau bagaimana negara tersebut memandang kesuksesan atau kegagalannya dibandingkan dengan negara lain, sangat dipengaruhi oleh persepsi mereka terhadap tindakan dan kapabilitas negara lain. Dalam konteks ini, kapabilitas dianggap penting hanya ketika mempengaruhi intensi dan tujuan negara. Neoliberalis juga menekankan peran penting institusi dan rezim internasional dalam memfasilitasi kerjasama ini. Mereka percaya bahwa institusi dan rezim tersebut berfungsi sebagai sarana di mana prinsip-prinsip, norma, aturan, dan prosedur pengambilan keputusan diterapkan, sehingga kerjasama antarnegara menjadi lebih mungkin terjadi (Dugis 2018).

Lebih jauh lagi, perilaku negara dapat dibatasi dan diatur oleh norma dan aturan yang telah disepakati dalam rezim internasional. Institusi dan rezim ini juga menciptakan peluang transparansi bagi setiap negara anggotanya, yang pada gilirannya mengurangi beban transaksi dan mengurangi risiko kecurangan oleh negara lain. Pengalaman kerjasama melalui institusi sering kali menghasilkan

berbagai bentuk kesamaan baru, yang seiring waktu menjadi sumber kekuatan yang memperkuat dan menjaga keberlangsungan kerjasama antarnegara tersebut. Dengan demikian, neoliberalisme menawarkan pandangan yang relatif optimis tentang kemampuan negara-negara untuk bekerja sama dalam sistem internasional yang pada dasarnya tidak teratur.

Dalam konteks keamanan, khususnya keamanan siber, neoliberalisme menekankan bahwa ancaman-ancaman lintas batas dapat lebih efektif dihadapi melalui kolaborasi antarnegara. Dengan adanya institusi atau mekanisme kerja sama, seperti perjanjian siber atau aliansi keamanan, negara-negara dapat saling mendukung dalam mencegah dan enangani serangan siber. Dengan demikian, neoliberalisme mendorong kerja sama multilateral untuk mencapai stabilitas dan ketertiban di ranah internasional, yang berfungsi melindungi kepentingan dan keamanan nasional masing-masing negara (Keohane 1984).

Teori neoliberalisme relevan untuk diterapkan dalam penelitian tentang kerjasama antara BSSN dan KISA dalam meningkatkan keamanan siber di Indonesia karena pendekatan ini menekankan pentingnya kolaborasi internasional dan peran sektor swasta dalam mengatasi tantangan global, termasuk ancaman siber. Dengan menggunakan kerangka neoliberalisme, penelitian ini dapat menggali bagaimana BSSN dan KISA bekerja sama untuk memperkuat kapasitas pertahanan siber melalui kebijakan yang sejalan dengan prinsip-prinsip pasar terbuka, inovasi teknologi, dan kolaborasi internasional, yang bertujuan untuk menciptakan ekosistem siber yang lebih aman dan tangguh di Indonesia.

Kerjasama Internasional

Kerja sama internasional adalah suatu bentuk hubungan antar bangsa yang bertujuan untuk memajukan kepentingan nasional masing-masing negara. Kerjasama ini melibatkan seperangkat aturan, prinsip, norma, dan prosedur pengambilan keputusan yang mengatur fungsi rezim internasional. Negara-negara yang terlibat dalam kerjasama internasional memiliki tujuan bersama atau *common interest*, karena tanpa adanya kesamaan kepentingan, kerjasama tersebut menjadi tidak mungkin terwujud. Menurut K.J Holsti, kerjasama awalnya timbul sebagai respons terhadap sejumlah masalah yang muncul di tingkat nasional, regional, maupun global(Holsti 1988). Keberagaman permasalahan tersebut menuntut perhatian tidak hanya dari satu negara saja. Oleh karena itu, setiap negara terlibat dalam kerjasama dengan mengusulkan solusi atau saran untuk penanggulangan masalah yang dihadapi. Proses ini melibatkan negosiasi, tawar-menawar, perundingan, serta penilaian bukti-bukti yang dikumpulkan guna memperkuat salah satu usul yang diajukan. Keseluruhan proses tersebut diakhiri dengan pembentukan suatu perjanjian yang pada akhirnya memberikan kepuasan bagi semua pihak yang terlibat

Kerjasama internasional dibentuk dengan maksud mencapai kesejahteraan bersama. Dalam konteks ini, kerjasama internasional menjadi suatu keharusan karena adanya ketergantungan timbal balik dan meningkatnya kompleksitas kehidupan manusia dalam lingkup masyarakat internasional. Terdapat dua bentuk kerjasama internasional, yaitu bilateral dan multilateral. Bentuk kerjasama bilateral umumnya digunakan untuk mengejar kepentingan suatu negara terhadap

negara lain yang dianggap memiliki potensi untuk memenuhi kebutuhan tersebut, melibatkan hanya dua negara. Sementara itu, bentuk kerjasama multilateral biasanya terjadi dalam kerangka institusi regional dan organisasi internasional, melibatkan lebih dari dua negara sekaligus(Haryanto 2015).

Kemanan *Cyber*

Konsep keamanan siber membahas perlindungan sistem digital dan data dari berbagai ancaman siber yang dapat merusak atau mengganggu infrastruktur teknologi suatu negara. Ini karena aspek kehidupan sehari-hari semakin terhubung melalui teknologi digital. Oleh karena itu, keamanan siber menjadi sangat penting bagi negara-negara untuk menjaga kedaulatan dan stabilitas mereka sendiri. Keamanan siber mencakup upaya untuk melindungi data, menjaga integritas jaringan, dan menjamin ketersediaan sistem informasi dari serangan yang mengganggu(Stallings, 2018). Keamanan siber di Indonesia semakin menjadi perhatian, terutama karena ancaman siber yang meningkat yang melibatkan pencurian data dan sabotase sistem(Badan Siber dan Sandi Negara 2022).

Untuk mengatasi ancaman siber, Badan Siber dan Sandi Negara (BSSN) bekerja sama dengan berbagai organisasi internasional, termasuk *Korea Internet and Security Agency (*KISA), untuk meningkatkan kemampuan keamanan siber nasional. Kerja sama ini termasuk pertukaran teknologi, pelatihan, dan pembuatan protokol keamanan yang dapat meningkatkan pertahanan siber Indonesia(KISA 2022).

Dalam arti yang lebih luas, keamanan siber adalah bagian dari pertahanan nasional selain melindungi sistem informasi dari serangan. Menurut Keohane dan Nye (Keohane, dan Nye 1977), karena negara-negara saling bergantung dan saling bergantung, ancaman siber lintas negara menjadi ancaman kolektif yang membutuhkan tindakan bersama. Indonesia mendapatkan akses ke teknologi dan pengetahuan baru melalui kerja sama antara BSSN dan KISA. Ini meningkatkan keamanan digital negara dan posisi Indonesia dalam ekosistem keamanan siber global. Metode ini mendukung pengembangan keamanan yang menyeluruh dan menunjukkan komitmen Indonesia untuk membuat dunia digital yang lebih aman bagi semua pemangku kepentingan.

Metode Penelitian

Metode penelitian merupakan suatu pendekatan ilmiah yang digunakan untuk mengumpulkan data dengan tujuan khusus serta manfaat yang diinginkan. Dalam menjalankan proses penelitian, peneliti perlu mengadopsi langkah-langkah atau strategi tertentu sebagai langkah untuk mengatasi hambatan yang muncul dan mencapai sasaran penelitian yang telah ditetapkan. Kehadiran permasalahan dalam penelitian membutuhkan pendekatan yang sistematis dan terstruktur untuk memastikan pencapaian hasil yang valid dan bermakna. Dalam konteks ini, pentingnya pemilihan metode yang sesuai dan relevan menjadi jelas. Hal ini memastikan bahwa setiap langkah penelitian diarahkan secara efektif menuju pencapaian tujuan yang telah ditetapkan. Oleh karena itu, digunakanlah pendekatan ilmiah yang dikenal luas sebagai metode penelitian untuk memastikan bahwa proses penelitian berlangsung dengan baik dan menghasilkan temuan yang dapat diandalkan. Sugiyono mendifinisikan metode penelitian sebagai pendekatan ilmiah untuk memperoleh data dengan tujuan dan kegunaan tertentu(Sugiyono

2018). Pendekatan ilmiah ini mencakup ciri-ciri keilmuan, yaitu rasional, empiris, dan sistematis

Dalam penelitian ini, penulis menggunakan metode penelitian kualitatif. Metode penelitian kualitatif digunakan untuk mengeksplorasi dan memahami makna yang diatributkan oleh individu atau kelompok terhadap masalah sosial atau kemanusiaan (Creswell 2010). Proses penelitian kualitatif melibatkan langkah-langkah penting seperti merumuskan pertanyaan-pertanyaan dan prosedur-prosedur, mengumpulkan data yang spesifik dari partisipan, menganalisis data secara induktif dari teman-tema khusus ke tema-tema umum, serta menafsirkan makna data(Creswell 2009).

Pembahasan

Kerjasama Antara BSSN dan KISA terhadap Peningkatan Keamanan Siber

Kerjasama antara BSSN dengan KISA secara resmi dimulai pada tahun 2019 dan merupakan langkah strategis yang diambil oleh Indonesia untuk memperkuat pertahanan sibernya. Inisiatif ini muncul di tengah meningkatnya ancaman siber yang semakin kompleks dan global. Dengan serangan siber yang menjadi lebih canggih dan melibatkan berbagai aktor, baik negara maupun non-negara, dengan menyadari hal tersebut perlunya memperkuat infrastruktur keamanan siber. Untuk mencapai tujuan tersebut, kerjasama internasional dengan negara-negara yang memiliki keunggulan di bidang keamanan siber menjadi sangat penting.

Korea Selatan merupakan salah satu negara yang telah terbukti memiliki infrastruktur dan kebijakan keamanan siber yang baik dan maju. KISA memiliki pengalaman panjang dalam mengelola keamanan siber di tingkat nasional dan internasional, serta dalam menangani ancaman siber yang beragam. Oleh karena itu, kerjasama dengan KISA menjadi pilihan yang sangat tepat bagi Indonesia untuk mengembangkan kapasitas sibernya. Salah satu fokus utama dari kerjasama ini adalah pengembangan kapasitas teknis. BSSN, sebagai lembaga yang bertanggung jawab atas keamanan siber di Indonesia, membutuhkan peningkatan kemampuan teknis untuk menghadapi tantangan yang semakin rumit di dunia siber. Melalui kerjasama ini, KISA menyediakan berbagai program pelatihan yang ditujukan untuk meningkatkan keterampilan teknis staf BSSN. Pelatihan tersebut mencakup berbagai aspek penting seperti deteksi ancaman, analisis forensik digital, dan pengelolaan insiden siber. Dengan adanya pelatihan ini, diharapkan staf BSSN dapat lebih siap dalam menghadapi berbagai bentuk ancaman siber dan mampu merespons insiden dengan lebih cepat dan tepat.

Selain pelatihan, kerjasama ini juga melibatkan transfer teknologi dari Korea Selatan ke Indonesia. KISA membantu BSSN dalam memperoleh akses ke teknologi terbaru yang dibutuhkan untuk memperkuat infrastruktur keamanan siber Indonesia. Teknologi ini meliputi sistem pemantauan siber yang canggih, perangkat lunak deteksi ancaman, serta platform analisis data yang mampu memproses informasi secara *real-time*. Dengan adanya teknologi ini, BSSN dapat meningkatkan efektivitas pengawasan dan penanganan ancaman siber, sehingga dapat meminimalkan risiko serangan yang dapat mengganggu stabilitas nasional. Pertukaran pengetahuan dan informasi juga menjadi komponen penting dalam kerjasama ini. KISA dan BSSN secara rutin berbagi informasi tentang tren

ancaman siber terbaru, strategi mitigasi, dan pengalaman dalam menangani insiden siber. Pertukaran ini tidak hanya memperkaya pengetahuan BSSN, tetapi juga membantu kedua lembaga dalam mengembangkan pendekatan yang lebih komprehensif dan efektif dalam melindungi infrastruktur digital masing-masing negara. Selain itu, pertukaran pengetahuan ini juga menciptakan sinergi yang memungkinkan kedua negara untuk mengantisipasi dan merespons ancaman siber dengan lebih baik.

Kerjasama antara BSSN dan KISA juga mencakup pengembangan kebijakan dan kerangka kerja yang lebih baik untuk keamanan siber. KISA berbagi pengalaman dan praktik terbaik dalam merumuskan kebijakan keamanan siber, yang kemudian dapat diadaptasi oleh BSSN untuk konteks Indonesia. Kerjasama ini memungkinkan Indonesia untuk mengadopsi standar keamanan siber internasional yang diakui secara luas, serta mengintegrasikannya ke dalam kebijakan nasional. Dengan demikian, Indonesia dapat memperkuat kebijakan keamanan sibernya, yang tidak hanya relevan secara lokal, tetapi juga sesuai dengan perkembangan global. Pada tahun-tahun awal kerjasama, BSSN dan KISA telah mencatat beberapa pencapaian penting. Salah satu keberhasilan utama adalah peningkatan kemampuan deteksi ancaman siber di Indonesia. Dengan dukungan teknologi dan pelatihan dari KISA, BSSN berhasil mengembangkan sistem pemantauan yang lebih canggih dan responsif. Sistem ini mampu mendeteksi ancaman secara lebih cepat dan akurat, sehingga meminimalkan risiko kerugian yang disebabkan oleh serangan siber.

Kerjasama antara BSSN dan KISA merupakan langkah penting dalam membangun ketahanan siber di Indonesia. Dengan dukungan dari KISA, Indonesia tidak hanya mampu meningkatkan kapasitas teknis dan infrastruktur keamanannya, tetapi juga dapat memperkuat posisinya di panggung global dalam hal keamanan siber. Keberlanjutan dan pengembangan lebih lanjut dari kerjasama ini akan menjadi kunci dalam menghadapi tantangan keamanan siber yang semakin kompleks di masa depan. BSSN dengan KISA dalam upaya meningkatkan keamanan siber di Indonesia sepanjang tahun 2022.

Tidak hanya itu, BSSN dan KISA juga akan berkolaborasi dalam penelitian dan pengembangan teknologi keamanan siber baru. Kolaborasi ini diharapkan menghasilkan solusi yang lebih efektif dalam menghadapi berbagai ancaman siber yang terus berkembang. Melalui kerja sama ini, diharapkan pula akan ada simulasi dan latihan bersama yang dapat menguji kesiapan kedua belah pihak dalam menghadapi insiden siber besar. Selain aspek teknis, kolaborasi ini juga mencakup penyusunan regulasi dan kebijakan keamanan siber yang lebih efektif. Dengan pengalaman Korea Selatan yang lebih maju dalam bidang keamanan siber, KISA dapat memberikan panduan bagi BSSN dalam mengembangkan kerangka kerja regulasi yang mampu menghadapi tantangan masa depan. Dengan adanya kolaborasi ini, diharapkan Indonesia dapat memperkuat pertahanan siber nasional dan meningkatkan kesadaran serta respons terhadap ancaman siber, baik di sektor pemerintah maupun swasta.

Teori kerja sama internasional menyatakan bahwa negara-negara cenderung bekerja sama untuk mengatasi tantangan global yang tidak bisa dihadapi secara

sepihak. Keamanan siber adalah salah satu isu yang bersifat global, di mana ancaman yang muncul dapat dengan mudah melintasi batas negara dan mempengaruhi berbagai pihak secara simultan. Dalam konteks ini, kolaborasi antara BSSN Indonesia dan KISA Korea Selatan adalah aplikasi nyata dari teori tersebut. BSSN, sebagai otoritas yang bertanggung jawab atas keamanan siber di Indonesia, dan KISA, sebagai badan keamanan siber di Korea Selatan, sama-sama menyadari bahwa ancaman siber di era modern memerlukan pendekatan kolaboratif. Dengan berbagi informasi mengenai ancaman siber, teknologi, serta praktik terbaik, kedua lembaga ini saling memperkuat kemampuan mereka dalam mendeteksi dan merespons serangan siber. Contohnya, melalui pelatihan bersama dan pertukaran teknologi, Indonesia dapat mengakses metode deteksi dan respons yang telah terbukti efektif di Korea Selatan. Metode ini dapat diadaptasi dan diterapkan di Indonesia untuk menghadapi tantangan spesifik yang ada.

Kerjasama ini menggambarkan bagaimana negara-negara bisa saling mendukung untuk menangani ancaman global yang berpotensi merongrong keamanan nasional mereka. Keamanan nasional merujuk pada perlindungan integritas, kedaulatan, dan kesejahteraan negara dari berbagai ancaman, termasuk ancaman siber. Kolaborasi antara BSSN dan KISA dalam konteks ini menunjukkan bahwa kerjasama internasional dapat memperkuat keamanan nasional. Ancaman siber seperti serangan *ransomware* atau pencurian data sensitif memiliki potensi merusak infrastruktur kritis dan mengancam stabilitas negara. Dengan memanfaatkan keahlian dan pengalaman KISA, BSSN dapat meningkatkan kemampuannya dalam mengelola ancaman siber. Kolaborasi ini berperan penting dalam pengembangan dan penerapan kebijakan keamanan siber yang lebih efektif, memperkuat perlindungan terhadap infrastruktur kritis, serta memastikan respons yang cepat dan efisien terhadap insiden siber. Selain itu, kerjasama ini juga berkontribusi pada pengembangan standar keamanan siber yang lebih baik, yang pada akhirnya membantu melindungi aset nasional dan mengurangi kerentanan terhadap serangan siber.

Keamanan siber, sebagai salah satu aspek dari keamanan nasional, berfokus pada perlindungan sistem informasi dan data dari ancaman yang berpotensi merusak. Kolaborasi antara BSSN dan KISA menekankan pentingnya kerjasama dalam bidang ini untuk membangun pertahanan siber yang lebih kuat. Di era digital saat ini, di mana serangan siber semakin kompleks dan canggih, pendekatan yang terintegrasi dan berkelanjutan sangat diperlukan untuk mengurangi risiko.

Neoliberalisme menekankan pentingnya kerjasama internasional dan keterlibatan sektor swasta dalam menangani tantangan global, termasuk keamanan siber. Dalam konteks ini, kerjasama BSSN dan KISA mencerminkan prinsip neoliberalisme dengan mendorong keterbukaan, kolaborasi lintas negara, dan penerapan teknologi modern untuk meningkatkan kapasitas pertahanan siber Indonesia. Neoliberalisme juga mendukung gagasan bahwa pasar terbuka dan inovasi teknologi dapat menjadi kunci dalam memperkuat keamanan siber, yang sejalan dengan tujuan BSSN dan KISA untuk menciptakan ekosistem siber yang lebih aman dan tangguh melalui kolaborasi internasional. Sedangkan konsep *e-*

Government, yang melibatkan penggunaan teknologi informasi oleh pemerintah untuk meningkatkan efisiensi dan layanan publik, menjadi relevan dalam konteks kerjasama ini. Dengan semakin berkembangnya *e-Government* di Indonesia, kebutuhan akan keamanan siber yang kuat menjadi semakin mendesak. Kerjasama antara BSSN dan KISA tidak hanya membantu meningkatkan keamanan siber secara umum, tetapi juga mendukung pengembangan *e-Government* yang aman dan andal. Melalui kolaborasi ini, BSSN dapat memanfaatkan keahlian dan pengalaman KISA dalam membangun sistem keamanan siber yang efektif, yang pada gilirannya memperkuat infrastruktur *e-Government* Indonesia.

Kerjasama ini mencakup berbagai inisiatif, seperti program pelatihan untuk personel keamanan siber, simulasi serangan untuk menguji ketahanan sistem, serta pertukaran intelijen ancaman. Misalnya, pelatihan bersama dapat memperkuat keterampilan teknis tim keamanan siber di Indonesia, memungkinkan mereka untuk lebih baik dalam mendeteksi dan merespons ancaman. Di sisi lain, pertukaran intelijen ancaman memberikan BSSN wawasan yang lebih mendalam tentang taktik dan teknik yang digunakan oleh aktor-aktor ancaman, sehingga memungkinkan mereka untuk lebih proaktif dalam melindungi sistem dan data yang dimiliki.

Dampak Kerjasama BSSN dan KISA terhadap Keamanan Siber di, Indonesia

Bagi Indonesia, kerjasama ini memperkuat infrastruktur dan kemampuan pertahanan siber nasional. Dengan bantuan KISA, BSSN memperoleh akses ke teknologi mutakhir dan metode canggih dalam mendeteksi dan menangani ancaman siber. Ini sangat penting mengingat Indonesia menghadapi tantangan besar dalam mengamankan jaringan dan sistem informasi dari serangan siber yang semakin kompleks. Melalui kolaborasi ini, BSSN dapat mempercepat pengembangan kemampuan teknis dan operasionalnya, termasuk peningkatan keterampilan sumber daya manusia dalam bidang keamanan siber. Selain itu, kerjasama ini juga mendorong adopsi standar keamanan siber internasional yang lebih ketat di Indonesia. Dengan mengimplementasikan praktik terbaik dari Korea Selatan, yang dikenal memiliki sistem keamanan siber yang maju, Indonesia dapat meningkatkan ketahanan terhadap berbagai jenis ancaman siber. Hal ini termasuk perlindungan terhadap infrastruktur kritis seperti energi, transportasi, dan komunikasi, yang sangat rentan terhadap serangan siber.

Di sisi lain, Korea Selatan juga mendapatkan manfaat dari kerjasama ini. Melalui pertukaran informasi dan intelijen ancaman, KISA dapat memahami lebih baik lanskap ancaman siber di Asia Tenggara, khususnya di Indonesia. Ini penting bagi Korea Selatan untuk memperluas cakupan pengawasan ancaman global dan mengidentifikasi potensi serangan yang dapat mempengaruhi kepentingan nasionalnya di kawasan tersebut.

Kerjasama ini juga memperkuat hubungan diplomatik antara Indonesia dan Korea Selatan, membangun kepercayaan dan komitmen bersama untuk menjaga keamanan siber secara kolektif. Dengan demikian, kedua negara tidak hanya memperkuat keamanan siber nasional mereka, tetapi juga berkontribusi pada

stabilitas keamanan siber di tingkat regional dan internasional. Secara keseluruhan, kerjasama antara BSSN dan KISA memberikan dampak positif yang nyata, khususnya bagi Indonesia yang dapat memanfaatkan pengalaman dan teknologi dari Korea Selatan untuk memperkuat pertahanan sibernya. Ini membantu Indonesia menjadi lebih siap dan tangguh dalam menghadapi ancaman siber yang terus berkembang, sekaligus mempererat hubungan strategis dengan Korea Selatan di bidang keamanan siber.

Melalui kerjasama ini, BSSN dan KISA berbagi informasi, teknologi, dan praktik terbaik untuk meningkatkan kemampuan dalam mendeteksi dan merespons ancaman siber. Teori kerjasama internasional mendukung gagasan bahwa melalui interaksi dan kolaborasi, negara-negara dapat mencapai hasil yang lebih efektif daripada bekerja sendiri. Kerjasama ini memungkinkan kedua negara untuk memanfaatkan sumber daya dan keahlian yang ada, yang pada gilirannya memperkuat kapasitas pertahanan siber mereka. Dengan dukungan dari KISA, BSSN dapat meningkatkan kapabilitas teknis dan operasionalnya, termasuk dalam perlindungan infrastruktur kritis dan pengelolaan insiden siber. Hal ini secara langsung berkontribusi pada peningkatan keamanan nasional Indonesia, karena negara menjadi lebih siap dalam menghadapi dan menanggulangi serangan siber yang dapat mengancam stabilitas dan kesejahteraan masyarakat.

Implementasi teknologi canggih dan praktik terbaik dari Korea Selatan membantu BSSN memperkuat ketahanan siber Indonesia. Ini mencakup peningkatan kemampuan dalam deteksi dini, mitigasi, dan respons terhadap insiden siber. Selain itu, pertukaran intelijen ancaman antara kedua negara memungkinkan Indonesia untuk lebih proaktif dalam menangani berbagai ancaman siber, dengan pemahaman yang lebih baik tentang taktik dan teknik yang digunakan oleh pelaku ancaman.

Hambatan dan Tantangan dalam Implementasi Kerjasama BSSN dengan KISA

Implementasi kerjasama antara BSSN dengan KISA menghadapi berbagai hambatan dan tantangan yang kompleks. Salah satu hambatan utama adalah perbedaan regulasi dan kebijakan nasional terkait keamanan siber di Indonesia dan Korea Selatan. Kedua negara memiliki kerangka hukum dan standar operasional yang berbeda, yang dapat mempersulit upaya penyelarasan dalam kerjasama. Oleh karena itu, penting bagi kedua belah pihak untuk mengembangkan kerangka kerja yang kompatibel tanpa mengorbankan kedaulatan masing-masing. Selain itu, keterbatasan sumber daya dan kapasitas juga menjadi tantangan signifikan dalam implementasi kerjasama ini. Perbedaan tingkat kemajuan teknologi dan kapasitas operasional antara BSSN dan KISA dapat mempengaruhi efektivitas program-program kolaboratif yang dijalankan. Untuk mengatasi hambatan ini, diperlukan upaya untuk meningkatkan kapasitas sumber daya manusia, teknologi, dan anggaran di kedua lembaga agar kerjasama dapat berjalan secara efektif dan berkelanjutan.

Hambatan lain yang muncul adalah dalam hal komunikasi dan koordinasi antar lembaga. Mengingat kompleksitas dan jumlah stakeholder yang terlibat, terutama ketika melibatkan dua negara dengan budaya dan pendekatan yang

berbeda terhadap keamanan siber, komunikasi yang efektif menjadi sangat penting. Jalur komunikasi yang jelas dan koordinasi yang kuat harus dibangun untuk menghindari kesalahpahaman atau keterlambatan dalam pelaksanaan kerjasama. Selanjutnya, perbedaan budaya dan pendekatan terhadap masalah keamanan siber juga menambah tantangan dalam kerjasama ini. Misalnya, perbedaan antara pendekatan preventif dan reaktif dalam menangani ancaman siber dapat mempengaruhi ekspektasi dan strategi yang diterapkan. Oleh karena itu, perlu adanya upaya untuk menemukan keseimbangan dan membangun pemahaman bersama yang kuat di antara kedua belah pihak.

Tidak kalah penting, tantangan teknis dan infrastruktur juga harus diperhatikan. Perbedaan dalam infrastruktur teknis dan standar operasional antara BSSN dan KISA dapat menyulitkan integrasi sistem atau pelaksanaan program-program teknis. Agar kerjasama dapat beroperasi dengan efisien, perlu dilakukan penyelarasan teknologi dan infrastruktur yang digunakan. Dengan mengatasi berbagai hambatan dan tantangan ini, kerjasama antara BSSN dan KISA dapat berjalan lebih efektif dan memberikan dampak positif yang signifikan terhadap peningkatan keamanan siber di kedua negara.

Secara keseluruhan, dengan mengaitkan kerjasama antara BSSN dan KISA dengan teori kerjasama internasional, keamanan nasional, dan keamanan siber, terlihat jelas bahwa keberhasilan kerjasama ini tidak hanya bergantung pada komitmen kedua pihak untuk bekerja sama, tetapi juga pada kemampuan mereka dalam mengatasi berbagai perbedaan dan hambatan yang ada. Teori kerjasama internasional mengajarkan bahwa negara-negara seringkali harus menavigasi melalui perbedaan kepentingan, regulasi, dan pendekatan kebijakan yang beragam untuk mencapai tujuan bersama. Dalam konteks ini, BSSN dan KISA harus mampu menemukan titik temu di antara kepentingan nasional masing-masing yang berbeda, serta mengembangkan mekanisme kerjasama yang dapat mengakomodasi perbedaan tersebut tanpa mengorbankan kedaulatan atau keamanan nasional masing-masing negara. Dari perspektif keamanan nasional, penting untuk diingat bahwa kerjasama siber antara kedua negara ini juga harus dipandang sebagai bagian dari upaya yang lebih luas untuk melindungi kedaulatan dan integritas negara dari ancaman yang bersifat transnasional. Keamanan siber telah menjadi elemen integral dari strategi keamanan nasional di banyak negara, termasuk Indonesia dan Korea Selatan. Oleh karena itu, keberhasilan kerjasama ini sangat tergantung pada kemampuan kedua lembaga untuk menyelaraskan kebijakan keamanan siber mereka dengan prioritas keamanan nasional masing-masing. Ini mencakup peningkatan kapasitas teknis, peningkatan sumber daya manusia, serta pengembangan teknologi yang kompatibel yang dapat mendukung upaya pertahanan siber di kedua negara.

Lebih lanjut, teori keamanan siber menekankan bahwa ancaman siber bersifat dinamis dan terus berkembang, yang berarti bahwa kerjasama internasional dalam bidang ini harus fleksibel dan adaptif. Keberhasilan kerjasama BSSN dan KISA dalam jangka panjang akan sangat bergantung pada kemampuan mereka untuk terus memperbarui dan menyesuaikan strategi kerjasama mereka sesuai dengan perkembangan ancaman siber secara global. Hal ini membutuhkan mekanisme

komunikasi yang efektif, pertukaran informasi yang cepat dan akurat, serta koordinasi yang erat untuk memastikan bahwa respons terhadap ancaman dapat dilakukan secara efisien dan tepat waktu.

Dalam hal ini, membangun kerangka kerja yang kuat dan adaptif menjadi krusial. Kerangka kerja ini harus mampu mengakomodasi perbedaan budaya, regulasi, dan pendekatan teknis, sekaligus menyediakan landasan yang kokoh untuk pengembangan strategi bersama yang dapat terus berkembang seiring dengan perubahan landscape ancaman siber. Kerjasama antara BSSN dan KISA, jika dikelola dengan baik, dapat menjadi model bagi kerjasama siber internasional lainnya, menunjukkan bagaimana negara-negara dengan perbedaan signifikan dalam regulasi dan pendekatan dapat bekerja sama untuk mencapai keamanan siber yang lebih besar dan lebih terkoordinasi. Oleh karena itu, keberhasilan kerjasama ini akan sangat bergantung pada upaya terus-menerus kedua pihak untuk mengatasi hambatan yang ada, membangun kepercayaan, dan berinovasi dalam pendekatan mereka terhadap tantangan keamanan siber. Jika hal ini tercapai, kerjasama BSSN dan KISA tidak hanya akan meningkatkan keamanan siber di kedua negara, tetapi juga berkontribusi pada stabilitas dan keamanan siber di tingkat regional dan global.

Kesimpulan

Kerja sama antara BSSN dan KISA merupakan langkah strategis dalam memperkuat keamanan siber kedua negara untuk menghadapi ancaman siber yang semakin kompleks dan lintas batas, khususnya dalam melindungi infrastruktur kritis yang vital bagi stabilitas nasional dan ekonomi. Kesuksesan kolaborasi ini memerlukan kemampuan untuk mengatasi perbedaan regulasi, kebijakan, dan kapasitas teknis, serta pentingnya komunikasi yang efektif dan koordinasi yang kuat untuk merespons ancaman secara tepat waktu. Dengan ancaman siber yang terus berkembang, BSSN dan KISA harus bersifat adaptif dalam memperbarui strategi dan teknologi, sehingga dapat tetap relevan menghadapi tantangan baru. Fleksibilitas dan inovasi dalam kerangka kerja menjadi kunci untuk menjaga efektivitas kolaborasi ini dalam jangka panjang. Secara keseluruhan, sinergi antara BSSN dan KISA berpotensi besar meningkatkan keamanan siber di Indonesia dan Korea Selatan serta berkontribusi pada stabilitas keamanan siber global yang lebih berkelanjutan.

Referensi

Badan Siber dan Sandi Negara. 2022. *Laporan tahunan keamanan siber di Indonesia*. Jakarta: BSSN.

Creswell, John W. 2009. *Research design: Qualitative, Quantitative, and Mixed Methods Approaches*. Yogyakarta: Pustaka Pelajar.

Creswell, John W. 2010. *Research Design Pendekatan Kualitatif, Kuantitatif dan Campuran*. Yogyakarta: Pustaka Pelajar.

Dugis, Visensio. 2018. *Teori Hubungan Internasional*. Surabaya: Airlangga University Press.

Haryanto, I. 2015. *PROSES KERJASAMA INTERNASIONAL ANTARA PEMERINTAH , Global & Policy* .

Holsti, K. J. 1988. *Politik Internasional, Kerangka untuk Analisis*. Jakarta: Erlangga.

Keohane, R. O. 1984. *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.

Keohane, R. O., dan Joseph Nye. 1977. *Power and interdependence: World politics in transition.* Little, Brown.

KISA. 2022. *Annual report on cybersecurity cooperation*. Seoul: Korea Internet and Security Agency.

Stallings, W. 2018. *Network security essentials: Applications and standards*. Pearson.

Sugiyono, P. D. 2018. *Metode Penelitian Kombinasi (Mixed Methods)*. Bandung: Alfabeta.