BAB V
PENUTUP

V.1 KESIMPULAN

Melalui penelitian ini dapat disimpulkan bahwa kerjasama keamanan antara ASEAN dengan Indonesia melalui BSSN memberikan dampak yang signifikan dalam menanggulangi kejahatan siber di Asia Tenggara 2019-2021. Penelitian ini menunjukkan bahwa BSSN telah memainkan peran sentral dalam memfasilitasi koordinasi dan pertukaran informasi antar-negara ASEAN dalam menanggulangi ancaman kejahatan siber. Bentuk realisasi dari kerjasama ini adalah ASEAN Cybersecurity Coorporation Strategy 2017-2020, BSSN dengan United States-Asean Business Council dalam Siber Sektor Ekonomi Digital 2020, hingga Forum of The 8th ASEAN Ministerial Conference on Cybersecurity (AMCC) 2023. Ketiga upaya kerjasama itu kemudian menghasilkan beberapa capaian kunci yang terbagi menjadi tiga aspek.

Melalui aspek ***Policy Coordination*** kerjasama yang dilakukan berupaya mencapai koordinasi yang lebih baik di seluruh badan sektoral ASEAN yang mengawasi keamanan siber, para Pemimpin negara anggota ASEAN menyetujui Pernyataan Pemimpin ASEAN tentang Kerjasama Keamanan Siber tahun 2018 untuk menetapkan arah diskusi siber. Selain itu, ASEAN Digital Masterplan (ADM) 2025 dikembangkan pada tahun 2021 untuk menyarankan tindakan yang dapat diambil oleh pemerintah dan regulator di negara-negara anggota ASEAN untuk mencapai visi ASEAN sebagai komunitas digital dan blok ekonomi terkemuka, yang didukung oleh layanan, teknologi, dan ekosistem digital yang aman dan transformatif. Dalam aspek ***Incident Response*** hasil yang ingin dicapai adalah memperkuat respons terhadap insiden keamanan siber ASEAN guna mengamankan pertumbuhan ekonomi digital ASEAN dalam menghadapi serangan siber lintas batas yang semakin canggih, ASEAN menyepakati pembentukan CERT ASEAN untuk memfasilitasi pertukaran informasi terkait ancaman dan serangan secara tepat waktu di antara CERT Nasional negara anggota. ASEAN CERT juga akan mendorong pengembangan kapasitas dan koordinasi terkait CERT, namun dengan cara yang tidak mengambil alih atau mengganggu peran operasional,

mandat dan fungsi CERT Nasional masing-masing. Aspek ***Capacity Building*** mencanangkan inisiatif peningkatan kapasitas yang lebih bertarget, ASEAN menyelesaikan studi Kerangka Kematangan CERT ASEAN pada tahun 2020 yang menilai postur keamanan siber negara anggota, serta tindakan pelatihan dan pengembangan yang diperlukan untuk memenuhi kebutuhan kapasitas siber negara anggota.

Salah satu ancaman keamanan siber yang signifikan di ASEAN adalah meningkatnya serangan siber yang menargetkan infrastruktur penting dan sistem pemerintahan. Serangan terhadap infrastruktur penting dapat mengganggu layanan penting, membahayakan data sensitif, dan bahkan menimbulkan ancaman terhadap keamanan nasional. Salah satu inisiatif utama yang diambil oleh ASEAN adalah pembentukan ASEAN Cybersecurity Cooperation Strategy (ACCS) atau Strategi Kerja Sama Keamanan Siber ASEAN. Strategi ini bertujuan untuk memperkuat kerja sama dan kolaborasi regional dalam mengatasi ancaman siber dan membangun ketahanan siber. Perjanjian ini menekankan pentingnya berbagi informasi, peningkatan kapasitas, dan pengembangan kerangka umum untuk keamanan siber *ASEAN Cybersecurity Cooperation Strategy Draft*.

Pengaruh ancaman ini tentunya menyebar merata ke seluruh negara anggota ASEAN, tidak terkecuali Indonesia. Melansir data yang telah dihimpun BSSN, setidaknya sepanjang tahun 2020 terdapat 316,1 juta kasus serangan siber yang terjadi di Indonesia. Jumlah tersebut meningkat secara signifikan dibanding dengan tahun 2019 yang memiliki 290,3 kasus tercatat yang artinya telah mengalami peningkatan signifikan hanya dalam kurun waktu satu tahun tercatat pada 2020 hingga 2021 serangan siber di Indonesia telah menyentuh angka 582,9 juta kasus, dimana kategori serangan terbanyak diantaranya; malware, denial of service (DoS), dan trojan activity. Tren kejahatan siber yang terjadi sepanjang tahun tersebut didominasi oleh ransomware dan indeks data leaks.

Menyadari ancaman terhadap keamanan nasional melalui ruang maya ini, pemerintah tentunya tidak tinggal diam. Banyaknya kasus kejahatan siber yang melanda berbagai sektor di Indonesia, pemerintah mulai memberikan perhatian lebih terhadap ruang siber untuk membangun infrastruktur keamanan sistem yang kuat untuk menghadapi potensi ancaman siber. Ketetapan ini kemudian menjadikan

keamanan siber sebagai isu prioritas nasional yang tertuang dalam Rencana Pembangunan Jangka Menengah Nasional (RPJMN) IV tahun 2020-2024 dalam prioritas nasional 7, yaitu memperkuat stabilitas politik, hukum, pertahanan, keamanan (Polhukanham), kemudian termasuk ke dalam Program Prioritas (PP) 5 dalam Rencana Kerja Pemerintah (RKP) hingga tahun 2022. Sejalan dengan konsolidasi dan penataan struktur kelembagaan Pemerintah pada waktu itu, landasan hukum Lembaga Sandi Negara terus diperbarui, berturut-turut pada 18 Juli 1994 dengan Keppres Nomor 54/1994, lalu pada 7 Juli 1999 dengan Keppres Nomor 77/1999, dan terakhir dengan Keppres Nomor 103/2001. Hingga pada tahun 2017 ketika diterbitkan nya Perpres Nomor 53 Tahun 2017 yang mengatur Peleburan Lembaga Keamanan Informasi Pemerintah yang mencakup Lemsaneg, Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (Kemenkominfo) menjadi sebuah lembaga Badan Siber dan Sandi Negara (BSSN) kemudian disempurnakan dengan Perpres Nomor 133 tahun 2017 yang ditandatangani langsung oleh Presiden Joko Widodo dan kemudian diperbarui kembali pada Perpres Nomor 28 Tahun 2021 tentang BSSN.

Pembentukan BSSN menunjukkan adanya bentuk konkret dalam komitmen pemerintah untuk menjamin keamanan ruang siber. BSSN sendiri memiliki fungsi yang mencangkup penyusunan dan pelaksanaan kebijakan teknis dalam bidang keamanan siber dan sandi, koordinasi, dan pengawasan pelaksanaan tugas dalam ruang lingkup BSSN yang bertanggung jawab langsung terhadap presiden serta mendukung upaya penguatan terhadap sektor keamanan siber demi menjamin keamanan nasional. Berbagai fenomena yang terjadi juga meningkatkan kebutuhan akan adanya BSSN dalam upaya membantu pemerintah memastikan adanya kebijakan dalam upaya penguatan teknis serta infrastruktur keamanan siber (Badan Siber dan Sandi Negara, 2020). Seperti yang telah dibahas sebelumnya, ancaman tidak hanya bersumber dari aktor nasional, namun juga datang dari pihak eksternal baik dalam kawasan atau pun secara global. Oleh karena itu, upaya mitigasi ancaman yang dilakukan oleh BSSN tidak hanya berbentuk *technical* namun juga *international cooperation* yang dilakukan dengan berbagai pihak baik global maupun kawasan ASEAN. Kerja sama yang dilakukan pemerintah melalui BSSN

ataupun badan lainnya dalam bentuk *transfer of knowledge* dan *transfer of technology* yang diharapkan dapat mempercepat kesiapan dan meningkatkan kualitas keamanan siber Indonesia dalam menghadapi permasalahan yang terjadi di ruang siber yang dalam siklus nya terus berkembang setiap harinya.

ASEAN terkenal sebagai pakar regional di bidang ekonomi karena melimpahnya sumber daya, bahan baku dan industri antar negara anggota untuk berkontribusi pada produksi perekonomian ASEAN. Lokasi yang strategis Asia merupakan faktor dalam pertumbuhan ekonomi khususnya di negara-negara seperti Singapura, Malaysia, Brunei, Indonesia dan Filipina, yang dikenal sebagai ASEAN 6. memperoleh berbagai sumber daya alam dan keanekaragaman hayati menghasilkan berbagai kemampuan berproduksi untuk berbagai bidang termasuk pertanian, manufaktur, jasa dan ekspor. *Foreign Direct Investment* (FDI) yang kuat dengan jaringan produksi yang sangat baik, rezim investasi progresif kawasan perdagangan bebas mencatat pencapaian kolaboratif regional yang kuat. Hingga saat ini, upaya regional untuk mengadopsi strategi keamanan siber yang komprehensif masih berjalan lambat dan terfragmentasi. Untuk mengeksplorasi pesatnya teknologi dan dinamisme revolusi industri 4.0, penelitian melalui investigasi eksperimental harus dilakukan, yang menyulitkan pemerintah untuk menerima percepatan revolusi industri. Modifikasi dalam bisnis, pendidikan, e-commerce, manufaktur, dan perawatan kesehatan harus disatukan ke dalam sistem yang lebih modern dalam struktur organisasi atau korporasi. Hal ini mungkin memerlukan upaya yang besar.

V.2 SARAN

V.2.1 Saran Praktis

. Penelitian ini berupaya menjabarkan bagaimana implementasi dari kerjasama yang dilakukan pemerintah Indonesia melalui BSSN dengan ASEAN dalam bidang keamanan siber dapat disimpulkan adalah, bahwa melalui kerja sama yang dilakukan oleh BSSN dengan ASEAN dapat berbentuk *transfer of knowledge* dan *transfer of technology*, yang dapat diimplementasikan melalui berbagai forum yang mengkaji struktur keamanan dan kerja sama untuk mengembangkan struktur keamanan yang dapat diaplikasikan secara regional. Kerjasama keamanan siber antara BSSN dan ASEAN akan mampu meningkatkan ketahanan Indonesia dalam menanggulangi kejahatan siber di Asia Tenggara.

Penelitian ini memberikan beberapa saran untuk meningkatkan kerjasama keamanan siber di ASEAN. Secara praktis, perlu dilakukan penguatan kapasitas teknis melalui pelatihan dan kolaborasi internasional guna menghadapi serangan kejahatan siber yang semakin kompleks. Peningkatan koordinasi antar-lembaga di tingkat nasional dan regional juga krusial untuk mempercepat pertukaran informasi dan respons terhadap ancaman. Selain itu, meningkatkan kesadaran publik tentang keamanan siber melalui kampanye edukasi dan seminar dapat mengurangi risiko penggunaan teknologi secara tidak aman.

V.2.2 Saran Teoritis

Secara teoritis, studi ini dapat menjadi dasar untuk pengembangan teori baru tentang kerjasama keamanan siber di tingkat regional. Penggalian lebih dalam tentang faktor-faktor yang mempengaruhi efektivitas kerjasama ini, seperti regulasi nasional, kebijakan internasional, dan dinamika politik regional, dapat memberikan wawasan baru bagi literatur keamanan internasional. Pengadopsian pendekatan perbandingan dengan negara-negara di luar ASEAN juga penting untuk mengidentifikasi praktik terbaik dalam menghadapi tantangan keamanan siber. Studi kasus dan analisis lintas-batas dapat membantu mengilustrasikan strategi yang berhasil diimplementasikan dalam kerangka kerjasama keamanan siber yang lebih luas.

Terakhir, mengintegrasikan pendekatan keamanan nasional dan regional dalam konteks globalisasi digital adalah krusial. Hal ini tidak hanya melibatkan

adaptasi kebijakan dan strategi keamanan yang responsif terhadap perubahan teknologi, tetapi juga memastikan bahwa keamanan siber menjadi bagian integral dari agenda keamanan nasional dan regional di ASEAN. Dengan menerapkan saran-saran ini secara komprehensif, diharapkan kerjasama keamanan siber di ASEAN dapat ditingkatkan, menjadikan kawasan ini lebih tangguh dalam menghadapi tantangan keamanan digital yang semakin kompleks dan beragam.