BAB V

PENUTUP

5.1 Kesimpulan

Adapun kesimpulan dari hasil seluruh proses penelitian yang dilakukan peneliti dengan berbagai cara baik secara holistic maupun teoritis, peneliti melihat bahwa keamanan siber di Indonesia sudah tergolong cukup mandiri dalam hal Pembangunan kapasitas siber nya namun pada masa itu kurangnya kepercayaan diri pada pemangku kepentingan dan pejabat terkait. Indoensia telah mencapai tingkat kemandirian yang cukup signifikan dalam menghadapi tantangan di dunia siber. Kebijakan-kebijakan keamanan siber yang diadopsi oleh Indonesia sebagian besar mengacu pada standar yang telah ditetapkan oleh National Institute of Standards and Technology (NIST) dari Amerika Serikat, serta beberapa prinsip yang berasal dari kerangka kerja keamanan siber yang dikembangkan oleh Inggris.

Pada tahun 2017, di mana serangan siber yang terjadi hanya mengganggu reputasi dengan aksi-aksi seperti defacement pada situs web. Namun, saat ini, terjadi pergeseran paradigma di mana kasus-kasus keamanan siber yang melibatkan kebocoran data dan social engineering semakin mengemuka. Hal ini menunjukkan bahwa pelaku kejahatan siber semakin canggih dalam pendekatan mereka dan mampu menyusup ke dalam sistem dengan lebih rapi.

Walaupun demikian, adanya kemandirian dalam menghadapi tantangan keamanan siber tidak berarti Indonesia dapat mengabaikan kerjasama internasional.

Upaya untuk tetap berkolaborasi dengan negara-negara lain dalam memerangi ancaman siber masih sangat penting, terutama dalam berbagi informasi mengenai tren serangan terbaru, teknik-teknik perlindungan yang efektif, dan perkembangan teknologi keamanan terkini.

Oleh karena itu, kesimpulan utama adalah bahwa Indonesia telah mengalami kemajuan yang signifikan dalam mengamankan dunia siber di dalam negeri. Meskipun mengacu pada kerangka kerja yang telah ada, negara ini mampu menyesuaikan dan mengembangkan kebijakan-kebijakan keamanan siber yang sesuai dengan kebutuhan dan ancaman yang berkembang. Namun, tantangan di masa depan akan semakin kompleks, dan Indonesia perlu tetap waspada, terus meningkatkan kapabilitas keamanan sibernya, dan menjaga kolaborasi internasional untuk menghadapi ancaman yang terus berkembang di dunia siber. Dengan pengaruh organisasi kawasan dalam keamanan siber mempengaruhi pandangan dan akses pengembangan kapasitas keamanan siber Indonesia menjadi lebih luas dan bisa bersaing dengan negara anggota lainnya.

Secara keseluruhan, Indonesia telah melakukan upaya-upaya untuk beradaptasi dengan tiga tujuan dan pilar ASEAN Cybersecurity Cooperation Strategy I untuk meningkatkan keamanan siber Indonesia dengan pembangunan kapasitas keamanan siber dengan kerjasama regional maupun pembentukan badan khusus seperti *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) dan Badan Siber dan Sandi Negara (BSSN) kedua Lembaga ini bersinergi langsung dalam proses peningkatan,pendeteksian dan penanggulangan masalah keamanan siber serta berpartisipasi Berpartisipasi aktif

dalam forum-forum ASEAN dan kerjasama internasional dalam bidang keamanan siber, seperti ASEAN CERT *Incident Drill*, ASEAN *Ministerial Conference on Cybersecurity*, dan kerjasama bilateral dengan negara-negara mitra ASEAN dan berbagai mekanisme strategi Kerjasama ASEAN lainnya

5.2 Saran

5.2.1 Saran Teoritis

Untuk meningkatkan penelitian di masa depan mengenai pengaruh Kerjasama ASEAN Cybersecurity Cooperation Strategy terhadap Keamanan Siber Indonesia pada periode 2017-2020, beberapa saran implementasi dapat diikuti. Pertama, mempertimbangkan analisis yang melibatkan jangka waktu yang lebih panjang, termasuk masa setelah periode penelitian, guna mendapatkan gambaran yang lebih komprehensif tentang perkembangan keamanan siber nasional. Kedua, pendekatan metodologi kuantitatif yang lebih rinci, seperti analisis statistik mendalam tentang insiden dan respons keamanan siber, dapat memberikan pandangan obyektif terhadap dampak kolaborasi ASEAN. Selanjutnya, fokus pada studi kasus insiden konkret yang terjadi di Indonesia dapat memberikan wawasan mendalam tentang kontribusi kerjasama ASEAN dalam menanggapi ancaman tersebut.

Pendekatan kualitatif yang lebih mendalam, melalui wawancara dengan ahli keamanan siber dan perwakilan pemerintah, dapat mengungkapkan dinamika dan tantangan dalam implementasi kerjasama ASEAN di dalam konteks keamanan

siber. Membandingkan pengaruh kerjasama ASEAN dengan negara-negara anggota lainnya dapat memberikan pemahaman yang lebih baik tentang dampak dan kesamaan upaya kolaborasi dalam kawasan. Selain itu, pengukuran kapasitas keamanan siber Indonesia dengan mengidentifikasi indikator kunci, serta kajian dampak ekonomi dan sosial dari kerjasama tersebut, akan memberikan perspektif yang lebih lengkap mengenai peningkatan kemampuan dan manfaat yang diperoleh dari kerjasama ASEAN.

Dengan mengimplementasikan saran-saran tersebut, penelitian di masa depan akan dapat memberikan analisis yang lebih komprehensif dan mendalam mengenai pengaruh Kerjasama ASEAN Cybersecurity Cooperation Strategy terhadap Keamanan Siber Indonesia selama periode 2017-2020.

5.2.2 Saran Praktis

Untuk mengatasi beberapa tantangan yang ada salah satunya peningkatan alokasi anggaran menjadi kunci. Investasi yang lebih besar dalam pengembangan Kamsiber akan memungkinkan adopsi teknologi canggih, pelatihan yang lebih baik, pengembangan tim keamanan yang kuat, serta penelitian dan pengembangan kontinu. Dengan anggaran yang memadai, organisasi akan lebih mampu merespons dan mencegah serangan siber yang semakin berkembang, melindungi infrastruktur kritis, dan menjaga data dan informasi dari ancaman yang dapat merusak.

Oleh karena itu, untuk mengatasi dampak negatif dari kekurangan SDM dalam keamanan siber, organisasi perlu memprioritaskan investasi dalam tim keamanan siber yang kuat. Ini mencakup merekrut, melatih, dan mempertahankan

personel yang berkualitas dalam bidang keamanan siber, serta memastikan akses ke alat-alat dan teknologi yang diperlukan. Dengan mengalokasikan sumber daya yang memadai, organisasi dapat lebih efektif dalam merespons ancaman siber, melindungi infrastruktur penting, dan memitigasi risiko serangan yang semakin kompleks.

Selanjutnya, untuk mengatasi dampak negatif dari kurang optimalnya infrastruktur, penting bagi organisasi untuk mengalokasikan sumber daya yang cukup untuk membangun infrastruktur keamanan siber yang kuat. Ini meliputi implementasi perangkat keras dan perangkat lunak keamanan yang diperlukan, pembangunan sistem pemantauan dan deteksi yang canggih, serta pengembangan rencana respons dan pemulihan yang efektif. Dengan memiliki infrastruktur yang memadai, organisasi dapat lebih baik melindungi sistem, data, dan infrastruktur mereka dari ancaman siber dan merespons serangan dengan lebih cepat dan efektif.

Secara keseluruhan, pengalokasian anggaran yang memadai untuk pengembangan keamanan siber, tim keamanan siber yang berkualitas, dan infrastruktur keamanan yang kuat akan menjadi faktor penentu dalam mengatasi tantangan keamanan siber yang semakin kompleks dan berkembang. Dengan adanya investasi yang tepat, organisasi akan dapat mengurangi risiko serangan, menjaga keberlanjutan operasional, dan memberikan perlindungan optimal terhadap ancaman-ancaman siber yang dapat mengganggu stabilitas dan integritas sistem serta informasi yang dijalankan.