BAB II

KERJA SAMA ASEAN MELALUI ASEAN CYBER CAPACITY PROGRAM (ACCP) DALAM MENGHADAPI ANCAMAN SIBER OLEH KELOMPOK LOCKBIT

Meningkatnya serangan siber oleh kelompok LockBit mendorong ASEAN memperkuat kolaborasi dalam bentuk kerjasama keamanan digital. Melalui ASEAN Cyber Capacity Program (ACCP), negara-negara anggota berupaya meningkatkan kapasitas teknis, koordinasi, dan kesiapsiagaan bersama untuk menghadapi ancaman siber yang semakin kompleks, sekaligus memperkuat ketahanan digital kawasan.

2.1 Cyber Crime Di Asean

2.1.1 Konsep Umum Cyber Crime

Perkembangan teknologi informasi dan komunikasi tidak hanya memberikan manfaat besar bagi kemajuan ekonomi dan sosial, tetapi juga menghadirkan tantangan baru berupa munculnya berbagai bentuk kejahatan siber (*cyber crime*). Menurut *United Nations Office on Drugs and Crime* (UNODC), *cyber crime* merupakan segala bentuk aktivitas kriminal yang melibatkan komputer, jaringan internet, atau perangkat digital sebagai alat, sasaran, maupun tempat terjadinya kejahatan (Citaristi, 2022). Secara umum, *cyber crime* dapat dibedakan menjadi dua kategori, yaitu kejahatan yang menargetkan sistem komputer (misalnya peretasan dan *malware*) serta kejahatan yang menggunakan sistem komputer sebagai sarana melakukan tindak pidana seperti penipuan daring, penyebaran konten ilegal, dan pencurian data pribadi (Grabosky, 2017).

Menurut Wall (2007), *cyber crime* mencakup berbagai aktivitas ilegal yang dilakukan di dunia maya, termasuk *hacking*, *phishing*, *identity theft*, *data breach*, dan *ransomware*. *Hacking* adalah tindakan memperoleh akses tidak sah ke dalam sistem komputer orang lain untuk mencuri, merusak, atau memanipulasi data. *Phishing* dilakukan dengan cara menipu korban agar memberikan informasi sensitif seperti kata sandi atau nomor kartu kredit melalui situs atau email palsu (Kshetri, 2019). *Identity theft* atau pencurian identitas terjadi ketika pelaku menggunakan data pribadi korban untuk tujuan ilegal, sedangkan *data breach* mengacu pada kebocoran data yang menyebabkan informasi rahasia terekspos ke pihak yang tidak berwenang (Vishnevskaya & Zudina, 2020). Salah satu bentuk *cyber crime* yang paling berbahaya saat ini adalah *ransomware*, yaitu serangan yang mengenkripsi data korban dan meminta tebusan untuk memulihkannya. Serangan *ransomware* meningkat pesat di seluruh dunia karena motif ekonomi yang kuat dan kemudahan distribusi melalui jaringan global. (Europol, 2023). Di kawasan Asia Tenggara, serangan *ransomware* menjadi ancaman utama bagi sektor publik dan swasta karena rendahnya tingkat kesadaran keamanan siber dan keterbatasan sumber daya teknis di beberapa negara (Secretariat, 2023d). Grabosky (2017) menegaskan bahwa karakteristik utama *cyber crime* adalah sifatnya yang lintas batas (*borderless*), anonim, dan sulit dilacak.

Hal ini menjadikan kerja sama internasional menjadi elemen penting dalam upaya pencegahan dan penegakan hukum terhadap pelaku kejahatan siber. Oleh karena itu, pembentukan kapasitas dan koordinasi antarnegara, seperti yang dilakukan melalui ASEAN Cyber Capacity Program (ACCP), menjadi strategi

yang relevan dalam memperkuat pertahanan digital kawasan. Dengan demikian, *cyber crime* merupakan fenomena kompleks yang terus berkembang seiring kemajuan teknologi. Kejahatan ini tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam keamanan nasional, privasi individu, dan kepercayaan publik terhadap transformasi digital global.

2.1.2 Kondisi Keamanan Siber di ASEAN

Perkembangan digital di kawasan Asia Tenggara telah menciptakan peluang besar dalam pertumbuhan ekonomi, namun juga membawa tantangan serius berupa meningkatnya ancaman kejahatan siber. Transformasi digital di sektor pemerintahan, keuangan, dan layanan publik di negara-negara ASEAN menjadikan kawasan ini sebagai target utama berbagai bentuk serangan siber, seperti *ransomware*, *phishing*, dan *data breach*. Menurut ASEAN Secretariat (2023d), digitalisasi ekonomi ASEAN berkembang sangat pesat dengan nilai ekonomi digital yang diperkirakan mencapai 1 triliun dolar AS pada tahun 2030. Namun, percepatan digital ini tidak diimbangi dengan kesiapan keamanan siber yang merata antarnegara anggota. Interpol (2023) melaporkan bahwa kejahatan siber di Asia Tenggara meningkat sekitar 40% dibandingkan tahun sebelumnya, dengan bentuk serangan yang paling dominan adalah *ransomware* dan penipuan daring (*online fraud*). Peningkatan ini menunjukkan adanya kesenjangan signifikan dalam infrastruktur pertahanan siber di antara negara anggota ASEAN. Negara dengan sistem keamanan digital yang kuat seperti Singapura dan Malaysia telah membangun pusat tanggap insiden siber nasional (*Computer Emergency Response Team/CERT*), sementara negara berkembang seperti Laos dan Myanmar

masih menghadapi keterbatasan sumber daya manusia, infrastruktur, serta kebijakan keamanan digital ((ITU), 2022).

Selain perbedaan kesiapan, tantangan utama dalam penguatan keamanan siber ASEAN adalah kurangnya koordinasi regional dan standar keamanan yang seragam. Menurut International Telecommunication Union (2022) melalui *Global Cybersecurity Index (GCI)*, terdapat kesenjangan yang signifikan dalam skor kesiapan siber antarnegara ASEAN, di mana Singapura menempati peringkat tertinggi dengan indeks kesiapan 98,52, sedangkan Laos dan Myanmar masih di bawah 40 poin. Kesenjangan ini menjadikan kawasan ASEAN rentan terhadap serangan lintas batas yang memanfaatkan kelemahan di negara dengan sistem keamanan rendah. Sebagai respons terhadap kondisi tersebut, ASEAN meluncurkan ASEAN Digital Masterplan 2025 yang menekankan pentingnya memperkuat kapasitas keamanan digital regional, meningkatkan kesadaran publik terhadap ancaman siber, dan membangun kerja sama teknis antarnegara (Secretariat, 2023d). Salah satu inisiatif penting dalam upaya tersebut adalah pelaksanaan ASEAN Cyber Capacity Program (ACCP) yang bertujuan meningkatkan kemampuan teknis dan koordinasi penanganan insiden siber lintas batas (Dowling, 2022).

2.1.3 Jenis-Jenis Cyber Crime yang Umum di ASEAN

Kejahatan siber di kawasan ASEAN terus meningkat seiring dengan berkembangnya transformasi digital di sektor publik dan swasta. Beberapa jenis *cyber crime* yang paling umum terjadi di wilayah ini antara lain ransomware,

phishing dan penipuan daring, pelanggaran data (data breach), serta spionase siber (cyber espionage).

Ransomware menjadi salah satu ancaman terbesar di kawasan, di mana pelaku kejahatan mengenkripsi sistem komputer korban dan menuntut pembayaran tebusan untuk memulihkan akses. Serangan jenis ini meningkat pesat di Asia Tenggara pada periode 2022–2024, dengan kelompok seperti Lockbit yang menargetkan institusi keuangan, rumah sakit, serta lembaga pemerintahan di Indonesia, Malaysia, dan Filipina (Europol, 2023). Salah satu kasus besar terjadi pada Agustus 2023, ketika LockBit menyerang Bank Syariah Indonesia (BSI) dan menyebabkan gangguan layanan nasional selama beberapa hari, disertai kebocoran 1,5 terabyte data nasabah yang kemudian dijual di dark web (Aditya Priyatna Darmawan, 2025). Pada 2022, LockBit juga menyerang Kementerian Pertahanan Filipina, mengeklaim mencuri dokumen internal yang bersifat rahasia, sedangkan di Malaysia, serangan ransomware terhadap KPJ Healthcare pada 2023 mengakibatkan kebocoran data medis ribuan pasien. Menurut *ASEAN Cybercrime Operations Desk*, serangan ransomware menimbulkan kerugian ekonomi signifikan serta gangguan pada layanan public (Interpol, 2023).

Phishing dan penipuan daring, menjadi modus paling sering ditemukan di kawasan ASEAN. Kejahatan ini dilakukan dengan memanipulasi korban agar memberikan informasi pribadi, seperti kata sandi dan nomor rekening bank. Tahun 2022–2023, Indonesia mencatat lebih dari 12.000 kasus phishing terkait penipuan undangan pernikahan, kurir palsu, dan aplikasi investasi. Malaysia melalui MyCERT mencatat 25% peningkatan kasus phishing sepanjang 2023,

terutama yang menargetkan pengguna bank digital. Meningkatnya penggunaan media sosial dan aplikasi pembayaran digital di Asia Tenggara menjadi faktor utama yang mempermudah pelaku melakukan penipuan berbasis daring (Citaristi, 2022).

Pelanggaran data (data breach), terhadap lembaga keuangan dan pemerintahan juga menjadi perhatian utama. Menurut laporan *ASEAN Digital Masterplan 2025*, masih banyak negara anggota yang belum memiliki mekanisme keamanan siber memadai untuk melindungi data sensitif, terutama di sektor publik. Contoh nyata adalah kebocoran data 279 juta penduduk Indonesia pada 2021 dari BPJS Kesehatan, yang kemudian dijual di forum peretas. Di Thailand, pada 2022 terjadi kebocoran 55 juta catatan medis dari fasilitas kesehatan pemerintah. Akibatnya, kebocoran data sering kali dimanfaatkan oleh pelaku untuk pencurian identitas dan penjualan informasi pribadi di pasar gelap digital ((OECD), 2021).

Cyber espionage atau spionase siber, menjadi bentuk ancaman yang lebih kompleks, melibatkan upaya pengintaian dan pencurian data strategis oleh aktor negara maupun non-negara. *Global Cybersecurity Index* mencatat bahwa beberapa negara di Asia Tenggara masih rentan terhadap serangan semacam ini karena lemahnya deteksi dini terhadap aktivitas peretasan tingkat lanjut ((ITU), 2022). Misalnya, pada 2023, kelompok APT yang diduga berasal dari Tiongkok melakukan infiltrasi terhadap jaringan Kementerian Pertahanan Vietnam dan perusahaan energi nasional. Pada 2022, kelompok APT “OceanLotus” kembali menyerang institusi telekomunikasi di Thailand dan Malaysia. Spionase siber

sering kali menargetkan sektor energi, pertahanan, dan telekomunikasi, yang berperan penting dalam stabilitas ekonomi dan keamanan nasional kawasan (Grabosky, 2017).

Variasi jenis kejahatan siber di ASEAN menunjukkan bahwa kawasan ini membutuhkan pendekatan keamanan digital yang lebih terpadu dan kolaboratif. Melalui kerja sama regional, seperti *ASEAN Cyber Capacity Program (ACCP)*, negara-negara anggota diharapkan mampu meningkatkan ketahanan siber menghadapi ancaman yang semakin canggih dan lintas batas.

2.1.4 Dampak Kejahatan Siber di ASEAN

Menurut ASEAN Secretariat (2023d) Kejahatan siber telah memberikan dampak signifikan terhadap stabilitas ekonomi, sosial, dan keamanan di kawasan Asia Tenggara. ASEAN sebagai kawasan dengan pertumbuhan ekonomi digital tercepat di dunia menghadapi tantangan serius akibat meningkatnya frekuensi dan kompleksitas serangan siber.

Kerugian ekonomi yang ditimbulkan sangat besar, baik bagi sektor pemerintahan maupun swasta. Menurut laporan *Internet Organised Crime Threat Assessment (IOCTA)*, kerugian ekonomi global akibat serangan siber diperkirakan mencapai miliaran dolar per tahun, dan Asia Tenggara menjadi salah satu kawasan dengan tingkat kerentanan tinggi karena kesenjangan kapasitas keamanan digital antarnegara (Europol, 2023). Kerentanan tersebut terlihat jelas pada sektor UMKM, yang umumnya belum memiliki sistem keamanan siber memadai. Tahun 2022, lebih dari 3.600 UMKM di Indonesia dilaporkan menjadi korban penipuan digital melalui modus phishing dan pencurian data transaksi.

Banyak pelaku usaha mikro, kecil, dan menengah (UMKM) di wilayah ini belum memiliki sistem keamanan siber yang memadai, sehingga mudah menjadi sasaran pencurian data dan penipuan daring (OECD, 2021).

Gangguan terhadap layanan publik dan menurunnya kepercayaan masyarakat menjadi dampak lain yang serius. Serangan terhadap sistem layanan kesehatan, pendidikan, dan pemerintahan menghambat pelayanan publik dan menimbulkan keresahan sosial ((UNODC), 2020). Contohnya, pada Juli 2021, terjadi kebocoran data 279 juta penduduk Indonesia dari BPJS Kesehatan, menyebabkan kekhawatiran publik luas dan menurunkan kepercayaan terhadap tata kelola keamanan data pemerintah. Pada 2022, Malaysia mengalami gangguan layanan digital pada sistem pajak nasional (LHDN) akibat upaya peretasan, yang menyebabkan penghentian layanan selama beberapa hari. Kejadian seperti kebocoran data warga atau pemadaman sistem digital di lembaga publik dapat menurunkan tingkat kepercayaan masyarakat terhadap institusi negara dan memperburuk persepsi terhadap kemampuan pemerintah dalam menjaga keamanan digital (Interpol, 2023).

Mengancam stabilitas keamanan nasional dan regional. Aksi cyber espionage dan cyber warfare dapat menimbulkan ketegangan antarnegara, terutama ketika infrastruktur strategis seperti sistem energi, perbankan, dan pertahanan menjadi sasaran serangan ((ITU), 2022). Tahun 2023, ketika jaringan Kementerian Pertahanan Vietnam diretas oleh kelompok APT yang diduga berasal dari luar negeri, menargetkan dokumen pertahanan dan komunikasi internal. Tahun 2022, perusahaan energi milik pemerintah Thailand juga menjadi korban

infiltrasi siber yang berpotensi mengganggu distribusi energi nasional. ITU (2022) mencatat bahwa sejumlah negara ASEAN masih memiliki kemampuan deteksi dini yang lemah, sehingga rentan terhadap serangan tingkat lanjut. Laporan ASEAN Digital Masterplan 2025 menekankan pentingnya kolaborasi antarnegara anggota untuk membangun ekosistem digital yang tangguh dan responsif terhadap ancaman lintas batas (Secretariat, 2023d).

2.1.5 Tantangan Penanganan Cyber Crime di ASEAN

Penanganan kejahatan siber di kawasan ASEAN menghadapi sejumlah tantangan yang kompleks, terutama terkait dengan kesenjangan kapasitas keamanan digital antarnegara, keterbatasan sumber daya manusia, serta lemahnya koordinasi lintas batas.

Kesenjangan kapasitas keamanan siber antarnegara menjadi hambatan utama dalam membangun sistem pertahanan digital regional. Negara-negara seperti Singapura dan Malaysia memiliki infrastruktur siber yang lebih maju, sementara negara-negara berkembang seperti Laos, Myanmar, dan Kamboja masih tertinggal dalam hal regulasi, pendanaan, serta kemampuan teknis (ASEAN Secretariat, 2023). Laporan *Global Cybersecurity Index (GCI) 2022* oleh ITU juga menunjukkan perbedaan signifikan dalam kesiapan keamanan digital antarnegara anggota ASEAN, baik dalam kebijakan maupun penerapan teknologi pertahanan siber.

Keterbatasan sumber daya manusia (SDM) di bidang keamanan siber menjadi tantangan serius. Menurut OECD (2021), banyak negara berkembang di Asia Tenggara belum memiliki tenaga ahli yang cukup dalam bidang digital

forensik, analisis ancaman, dan penegakan hukum berbasis teknologi. Akibatnya, upaya investigasi kejahatan siber sering kali lambat dan kurang efektif (UNODC, 2020).

Koordinasi lintas batas dan mekanisme berbagi informasi antarnegara ASEAN masih lemah. Kejahatan siber bersifat lintas batas dan sering melibatkan jaringan global, namun mekanisme kerja sama hukum antarnegara di kawasan ini masih terbatas (Interpol, 2023). Laporan *ASEAN Cybercrime Operations Desk* menyoroti bahwa ketidaksamaan sistem hukum dan kebijakan privasi data antarnegara menjadi kendala utama dalam pertukaran informasi dan kolaborasi penyelidikan (Europol, 2023).

Sebagai upaya penanganan berbagai tantangan *cyber crime*, ASEAN berupaya memperkuat kerja sama melalui inisiatif seperti *ASEAN Cyber Capacity Program (ACCP)*, yang bertujuan meningkatkan kemampuan teknis dan koordinasi antarnegara dalam mencegah, mendeteksi, serta menanggapi insiden siber. Namun, efektivitasnya masih sangat bergantung pada komitmen politik dan investasi jangka panjang dari masing-masing negara anggota (ASEAN Secretariat, 2023).

2.1.6 Pentingnya Kerja Sama Regional

Kejahatan siber merupakan ancaman lintas batas yang tidak dapat diatasi oleh satu negara secara mandiri. Sifat global dari serangan siber memungkinkan pelaku beroperasi dari berbagai yurisdiksi, sehingga penanganannya membutuhkan koordinasi dan kerja sama antarnegara (UNODC, 2020). Dalam

konteks Asia Tenggara, kerja sama regional menjadi sangat penting mengingat adanya kesenjangan kemampuan keamanan digital dan perbedaan regulasi di antara negara anggota ASEAN (Interpol, 2023). ASEAN memandang bahwa penguatan kolaborasi dalam bidang keamanan siber dapat meningkatkan kemampuan kolektif kawasan untuk mencegah, mendeteksi, dan merespons insiden siber.

ASEAN Digital Masterplan 2025 menegaskan pentingnya kerja sama dalam memperkuat ketahanan digital regional serta memperluas infrastruktur keamanan siber yang inklusif (ASEAN Secretariat, 2023). Salah satu inisiatif konkret dalam memperkuat kolaborasi lintas batas adalah ASEAN Cyber Capacity Program (ACCP), yang didukung oleh berbagai mitra internasional seperti Australia dan Singapura. Program ini bertujuan untuk membangun kapasitas teknis, memperkuat kebijakan keamanan digital, dan meningkatkan kemampuan investigasi kejahatan siber di antara negara anggota ASEAN (OECD, 2021). Melalui ACCP, ASEAN berupaya mendorong pertukaran pengetahuan, pelatihan teknis, serta harmonisasi kebijakan keamanan digital di kawasan (Europol, 2023).

2.2 Kelompok Cyber Lockbit

2.2.1 Kelompok Cyber Lockbit

Kelompok LockBit merupakan salah satu sindikat kejahatan siber paling aktif dan berbahaya di dunia yang beroperasi dengan model Ransomware-as-a-Service (RaaS). Model ini memungkinkan pengembang ransomware untuk

menyewakan perangkat lunak mereka kepada afiliasi yang melakukan serangan dan membagi hasil tebusan (Europol, 2023). LockBit pertama kali terdeteksi sekitar tahun 2019 dan dengan cepat berkembang karena kemampuannya melakukan serangan yang cepat, sistematis, dan sulit dideteksi (Research, 2023). Karakteristik utama LockBit adalah efisiensi operasionalnya yang tinggi dan struktur organisasinya yang menyerupai perusahaan profesional, dengan adanya sistem rekrutmen, kompensasi, dan dukungan teknis bagi afiliasi (CISA, FBI, & NCSC-UK, 2023a). Hal ini menjadikan LockBit sebagai model bisnis kriminal berbasis teknologi yang sangat adaptif dan berorientasi pada hasil.

Selain itu, LockBit dikenal karena melakukan serangan terhadap berbagai sektor penting seperti kesehatan, pemerintahan, manufaktur, dan pendidikan di seluruh dunia, termasuk Asia Tenggara (Interpol, 2023). Kelompok ini juga menggunakan strategi double extortion, yakni mengenkripsi data korban sekaligus mengancam untuk mempublikasikan data yang dicuri apabila tebusan tidak dibayar (Ltd, 2023). Dampak aktivitas LockBit sangat signifikan terhadap keamanan siber global. Oleh karena itu, lembaga internasional seperti Europol dan Cybersecurity and Infrastructure Security Agency (CISA) terus meningkatkan kerja sama internasional untuk melacak dan menindak jaringan ransomware ini (Europol, 2023). Dengan demikian, pemahaman terhadap struktur, metode, dan strategi LockBit menjadi penting untuk memperkuat pertahanan siber nasional dan regional.

2.2.2 Evolusi dan Varian Lockbit

Kelompok LockBit telah mengalami perkembangan signifikan sejak kemunculannya pada tahun 2019, dengan berbagai versi yang menunjukkan peningkatan kemampuan teknis dan kompleksitas operasional. Versi awal, LockBit 1.0, pertama kali diidentifikasi pada tahun 2019 dan dikenal karena fokus pada otomatisasi serangan terhadap sistem jaringan dan kecepatan dalam proses enkripsi (Trend Micro, 2023). Ransomware ini memanfaatkan alat pemindaian otomatis untuk mencari target yang rentan di jaringan perusahaan, sehingga mempercepat penyebaran (Europol, 2023).

Tahun 2021, muncul LockBit 2.0, yang membawa peningkatan besar dalam mekanisme enkripsi, efisiensi distribusi malware, dan strategi afiliasi Ransomware-as-a-Service (RaaS) (CISA, FBI, & NCSC-UK, 2023). Versi ini juga menambahkan kemampuan untuk menonaktifkan sistem keamanan internal korban, serta menggunakan portal kebocoran data publik untuk menekan korban agar membayar tebusan (Ltd, 2023). Tahun 2022, LockBit 3.0 (dikenal sebagai *LockBit Black*), muncul pada tahun 2022 dan menjadi salah satu ransomware paling canggih secara global. Varian ini memadukan fitur dari ransomware terkenal seperti *BlackMatter* dan *DarkSide*, serta memperkenalkan sistem double extortion dan bug bounty program, di mana LockBit menawarkan hadiah kepada siapa pun yang menemukan kelemahan dalam sistem mereka (Unit, 2023).

Tahun 2024, varian terbaru LockBit Green dilaporkan menggunakan sebagian kode sumber dari *Conti ransomware*, yang memperkuat kemampuannya dalam penghindaran deteksi antivirus dan enkripsi multi-threaded (Kaspersky,

2024). Perkembangan setiap versi LockBit menunjukkan peningkatan profesionalisme dan inovasi teknis yang signifikan, menjadikannya salah satu ancaman paling serius dalam lanskap keamanan siber global, termasuk kawasan ASEAN yang menjadi target potensial karena infrastruktur digital yang berkembang pesat namun belum sepenuhnya aman (Interpol, 2023).

2.2.3 Metode Serangan Lockbit

Kelompok LockBit menggunakan rangkaian teknik yang terorganisir untuk menyerang korban dan memaksimalkan tekanan guna memperoleh pembayaran tebusan. Mereka menginfeksi sistem dengan malware yang dirancang untuk menyusup ke jaringan korban, mengeksploitasi kerentanan, dan menyebar secara lateral sebelum melakukan enkripsi massal pada file penting organisasi (CISA et al., 2023a). Proses ini sering melibatkan penggunaan *initial access brokers*, eksploitasi RDP yang kurang aman, serta alat otomasi untuk pemindaian dan penyebaran payload ransomware (Europol, 2023).

Kelompok LockBit menerapkan strategi double extortion, yaitu mengekstrak salinan data sensitif sebelum enkripsi dan kemudian mengancam mempublikasikan data yang dicuri ketika target menolak membayar tebusan. Taktik ini meningkatkan tekanan psikologis dan risiko reputasi bagi korban, sehingga meningkatkan kemungkinan pembayaran (Unit, 2023). Portal kebocoran data yang dikelola pelaku juga digunakan untuk mempublikasikan cuplikan data sebagai bukti dan ancaman lanjutan (Europol, 2023). Menyamarkan aliran pembayaran, LockBit dan afiliasinya memanfaatkan mata uang kripto sebagai sarana pembayaran tebusan.

Kripto memudahkan transfer lintas batas dan memberikan tingkat anonimitas relatif bagi pelaku, meskipun analisis rantai blok (blockchain) dan kerja sama internasional telah mulai melacak aliran dana tersebut (Kaspersky, 2024). Kombinasi teknik teknis (enkripsi, pemindahan lateral), taktik tekanan (publikasi data/double extortion), dan mekanisme pembayaran kripto membuat LockBit menjadi ancaman yang sangat efektif dan sulit ditangani tanpa koordinasi respons yang terintegrasi.

2.2.4 Target dan Wilayah Operasi

Kelompok ransomware seperti LockBit menunjukkan pola penargetan yang relatif konsisten: lembaga pemerintahan, perusahaan multinasional, dan sektor keuangan menjadi sasaran utama karena tingginya nilai data dan dampak operasional yang dapat meningkatkan kemungkinan pembayaran tebusan. Serangan terhadap fasilitas publik dan institusi keuangan tidak hanya menimbulkan kerugian finansial langsung, tetapi juga mengganggu kontinuitas layanan kritikal sehingga meningkatkan tekanan untuk membayar (CISA et al., 2023a). Di kawasan ASEAN, LockBit dan varian-varian cikal bakalnya dilaporkan menjadi ancaman signifikan. Insiden-insiden besar yang dilaporkan di wilayah ini termasuk serangan yang mengganggu layanan pusat data nasional menegaskan bahwa negara-negara seperti Indonesia, Thailand, dan Filipina kerap muncul sebagai target karena kombinasi aset digital yang bernilai tinggi dan adanya celah kesiapan siber di beberapa instansi. Kasus nyata serangan pada Pusat Data Nasional Indonesia (Juni 2024) yang dikaitkan dengan varian LockBit 3.0 memperlihatkan bagaimana infrastruktur bersama dan layanan publik dapat

menjadi target prioritas pelaku (Tommy & Nasution, 2025). Serangan LockBit bersifat lintas negara: pelaku memanfaatkan akses awal pada satu titik jaringan lalu bergerak lateral ke sistem lain, atau menyerang lampiran/penyedia layanan bersama yang melayani banyak entitas lintas yurisdiksi.

Pola ini diperkuat oleh temuan observatorium intelijen siber yang menunjukkan bahwa ransomware modern menggunakan ekosistem jasa kriminal (mis. *initial access brokers*, RaaS affiliates, dan portal kebocoran data) yang memfasilitasi operasi multi-jurisdiksi sehingga investigasi dan penegakan hukum menjadi kompleks tanpa kolaborasi lintas batas (Aditya Priyatna Darmawan, 2025). Akhirnya, payung teknologi bersama (mis. shared cloud services, central data centers, third-party vendors) sering menjadi vektor penyebaran yang memungkinkan serangan berdampak luas di beberapa negara sekaligus (Europol, 2023). Secara implikatif, karakter target dan pola operasi tersebut menuntut peningkatan koordinasi regional (pertukaran intelijen insiden, standarisasi praktik mitigasi, dan latihan respons bersama) untuk memutus rantai serangan lintas batas. Laporan-laporan penegak dan badan intelijen siber merekomendasikan integrasi mekanisme berbagi ancaman dan penguatan kapasitas CSIRT/LEA di tingkat regional agar respons terhadap serangan terkoordinasi dan efektif (Interpol, 2024).

2.2.5 Dampak Serangan Lockbit

Serangan ransomware Lockbit telah menjadi salah satu ancaman paling merugikan bagi sektor publik dan swasta di seluruh dunia. Dampak utama dari

serangan ini adalah kehilangan data penting dan gangguan operasional yang signifikan pada lembaga korban. Menurut laporan Europol (2023), Lockbit bertanggung jawab atas lebih dari 25% insiden ransomware global, dengan kerugian finansial yang mencapai ratusan juta dolar AS per tahun. Selain itu, efek lanjutan dari serangan ini adalah penurunan produktivitas dan biaya pemulihan sistem yang sangat besar (Kaspersky, 2024). Serangan Lockbit menimbulkan kerugian besar bagi perusahaan dan pemerintah karena adanya pembayaran tebusan dalam bentuk mata uang kripto serta biaya pemulihan infrastruktur digital (CISA et al., 2023a). Hal ini menunjukkan bahwa dampak kejahatan siber tidak hanya bersifat teknis tetapi juga memiliki konsekuensi ekonomi dan reputasional yang luas. Serangan Lockbit telah meningkatkan kesadaran global terhadap pentingnya kebijakan keamanan siber nasional dan regional. Negara-negara di kawasan ASEAN, termasuk Indonesia, mulai memperkuat kebijakan siber dan meningkatkan kolaborasi internasional dalam menangani ancaman ransomware (Secretariat, 2023d).

Upaya internasional dalam menghadapi kelompok ransomware Lockbit menunjukkan pentingnya kolaborasi lintas negara dalam menjaga keamanan siber global. Menurut Europol (2024), operasi gabungan antara Europol, FBI, dan lembaga penegak hukum dari lebih dari 10 negara berhasil menurunkan infrastruktur digital utama Lockbit, termasuk penyitaan server dan penangkapan operator kunci. Keberhasilan ini membuktikan efektivitas pendekatan multi-nasional dalam penegakan hukum siber. Selain itu, Interpol (2024) melaporkan bahwa kerja sama antara Interpol’s Cybercrime Directorate dan lembaga

keamanan nasional berperan penting dalam mendeteksi, melacak, dan membongkar jaringan ransomware lintas batas. Kerja sama ini memperkuat kapasitas intelijen siber, termasuk dalam pelatihan forensik digital dan pelacakan transaksi kripto yang digunakan untuk pembayaran tebusan. Di kawasan Asia Tenggara, inisiatif seperti ASEAN Cyber Capacity Program (ACCP) berperan besar dalam meningkatkan ketahanan siber regional melalui pelatihan teknis, pembentukan pusat koordinasi insiden, serta pertukaran pengetahuan antarnegara anggota (ASEAN Secretariat, 2023). Dengan dukungan dari mitra global seperti Australia dan Uni Eropa, program ini membantu memperkuat kemampuan ASEAN dalam mendeteksi, menanggapi, dan memulihkan serangan ransomware seperti Lockbit. Secara keseluruhan, strategi global menghadapi Lockbit menegaskan bahwa kolaborasi internasional dan pembangunan kapasitas regional merupakan kunci dalam mengurangi risiko kejahatan siber lintas batas dan melindungi infrastruktur digital yang kritis.

2.3 ASEAN *Cyber Capacity Program* (ACCP)

2.3.1 Latar Belakang Terbentuknya ASEAN *Cyber Capacity Program*

Program ASEAN Cyber Capacity Program (ACCP) diluncurkan pada tahun 2016 sebagai hasil kolaborasi antara ASEAN Secretariat dan Pemerintah Australia, dengan tujuan memperkuat kapasitas keamanan siber di kawasan Asia Tenggara. Pembentukan ACCP berangkat dari kesadaran akan meningkatnya ancaman siber global yang bersifat lintas batas dan dapat mengganggu stabilitas politik, ekonomi, serta keamanan nasional di negara-negara anggota ASEAN (Secretariat, 2016b). Menurut laporan ASEAN Secretariat (2023a), meningkatnya

insiden seperti ransomware, pencurian data, dan serangan terhadap infrastruktur digital mendorong perlunya kerja sama regional yang sistematis dan berkelanjutan. ACCP hadir sebagai platform pelatihan dan pengembangan kapasitas teknis, kebijakan, serta diplomasi siber bagi negara anggota ASEAN. Sementara itu, OECD (2021) menekankan bahwa kolaborasi antarnegara di bidang keamanan siber menjadi faktor penting dalam menciptakan ketahanan digital yang adaptif, terutama di tengah pertumbuhan ekonomi digital dan transformasi teknologi yang cepat. Selain itu, Department of Foreign Affairs and Trade (DFAT) Australia (2020) mencatat bahwa ACCP merupakan bagian dari komitmen Australia dalam mendukung stabilitas siber kawasan Indo-Pasifik, dengan fokus pada peningkatan kemampuan deteksi ancaman, respons insiden, dan kebijakan siber yang inklusif. Secara keseluruhan, pembentukan ACCP menjadi tonggak penting dalam sejarah diplomasi siber ASEAN, yang tidak hanya berorientasi pada peningkatan kapasitas teknis, tetapi juga pada penguatan solidaritas regional dalam menghadapi ancaman siber global**.**

Program ASEAN Cyber Capacity Program (ACCP) dirancang dengan tujuan utama untuk memperkuat kapasitas teknis dan kebijakan keamanan siber di kawasan Asia Tenggara. Melalui ACCP, negara-negara anggota ASEAN didorong untuk mengembangkan kemampuan dalam deteksi, mitigasi, dan respons terhadap insiden siber, sekaligus membangun mekanisme kerja sama lintas batas yang efektif (Secretariat, 2023d). Selain aspek teknis, ACCP juga menitikberatkan pada pengembangan kebijakan siber yang selaras dan berbasis kolaborasi antarnegara, guna memastikan terciptanya lingkungan digital yang aman, stabil, dan terbuka.

Program ini menjadi wadah bagi negara-negara anggota ASEAN untuk berbagi praktik terbaik serta meningkatkan kapasitas sumber daya manusia di bidang forensik digital, perlindungan data, dan penegakan hukum siber (Interpol, 2024).

2.3.2 Pembentukan Kerjasama Regional ACCP

Pembentukan ASEAN Cyber Capacity Program (ACCP) pada tahun 2016 menjadi langkah signifikan dalam memperkuat respons regional terhadap meningkatnya kejahatan siber. Sebelum ACCP hadir, diskusi dan kerja sama ASEAN terkait isu siber masih sangat terbatas. Inisiatif ini dipelopori oleh Singapura melalui pendanaan sebesar 10 juta dolar untuk mendukung pengembangan sumber daya, keahlian teknis, dan program pelatihan dalam rangka meningkatkan kapasitas keamanan siber negara-negara anggota. Selain itu, ACCP ikut memberikan rekomendasi mengenai pembentukan lembaga siber nasional serta penyusunan regulasi terkait keamanan digital (Secretariat, 2023a). Dorongan pembentukan program ini juga berkaitan dengan meningkatnya serangan siber yang menargetkan tidak hanya sektor pemerintahan, tetapi juga sektor keuangan dan masyarakat umum melalui situs web palsu yang menyerupai laman resmi pemerintah Singapura (Angel Aurelia & Andini Egista Maheswari S., 2024). Kondisi tersebut mendorong pemerintah Singapura untuk membentuk Cyber Security Agency (CSA) pada tahun 2015, yang kemudian dinilai mampu menangani isu keamanan siber dengan efektif, termasuk mengembangkan strategi keamanan siber nasional yang terdiri dari empat pilar utama (Rourke, 1995).

Empat pilar tersebut mencakup peningkatan perlindungan terhadap infrastruktur penting, penguatan kolaborasi pemerintah dengan sektor swasta dan

masyarakat, pengembangan sumber daya manusia di bidang keamanan siber, dan kerja sama internasional (Secretariat, 2023a). Kolaborasi lintas sektor menekankan bahwa keamanan siber bukan hanya tanggung jawab pemerintah, tetapi juga dunia usaha dan masyarakat, terutama dalam menghadapi risiko malware dan situs berbahaya. Penguatan kapasitas SDM dilakukan melalui pendidikan dan pelatihan untuk menciptakan profesional keamanan siber yang kompeten. Sementara itu, kerja sama internasional dipandang penting karena ancaman siber bersifat lintas batas, di mana serangan dapat berasal dari mana saja dan alamat IP sering kali tidak mencerminkan pelaku sebenarnya (Anastasya Zalsabilla Hermawan, M. Novianto Anggoro, Ditha Lozera, & Asif Faroqi, 2023). Oleh karena itu, pertukaran informasi intelijen, pemblokiran serangan, serta pembelajaran praktik terbaik menjadi elemen penting dalam menciptakan ketahanan siber kawasan ("ASEAN Cyber Capacity Program," 2024).

2.3.3 Kegiatan Utama ACCP

United Nations Office for Disarmament Affairs ((UNODA), 2021) menekankan pentingnya penyusunan norma perilaku bertanggung jawab di ruang siber (responsible state behavior) yang diadopsi dalam kerangka ACCP. Untuk memperkuat langkah ini diplomasi siber ASEAN sekaligus memastikan bahwa keamanan digital regional sejalan dengan prinsip hukum internasional dan tata kelola global yang etis. ASEAN Cyber Capacity Program (ACCP) merupakan salah satu inisiatif strategis ASEAN yang berfokus pada penguatan ketahanan siber regional melalui peningkatan kapasitas teknis, kebijakan, dan koordinasi antarnegara anggota. Program ini secara aktif melaksanakan berbagai kegiatan

utama yang mencakup pelatihan teknis, simulasi tanggap darurat siber, dan pembentukan jejaring kerja sama antar-CSIRT (Computer Security Incident Response Teams) di kawasan Asia Tenggara (Secretariat, 2023a).

Pelatihan teknis dan lokakarya yang diselenggarakan ACCP bertujuan untuk meningkatkan keterampilan profesional siber di negara anggota ASEAN, termasuk kemampuan dalam mendeteksi, menganalisis, dan menanggulangi serangan siber yang kompleks ((DFAT), 2020). Selain itu, kegiatan simulasi tanggap darurat insiden siber memberikan pengalaman langsung kepada peserta dalam menghadapi situasi krisis, memperkuat koordinasi lintas sektor, dan membangun kesiapan dalam menghadapi ancaman siber lintas batas ((DFAT), 2020). Salah satu hasil signifikan dari ACCP adalah pembentukan dan penguatan jaringan kerja sama antar-CSIRT di ASEAN, yang memungkinkan pertukaran informasi cepat mengenai ancaman dan insiden siber (ASEAN Secretariat, 2022).

Program ini juga berperan dalam mendukung penyusunan dan penerapan kebijakan keamanan siber nasional dan regional yang selaras dengan norma internasional mengenai perilaku bertanggung jawab di ruang siber (*responsible state behavior*). Dengan demikian, ACCP berfungsi tidak hanya sebagai wadah peningkatan kapasitas teknis, tetapi juga sebagai platform strategis dalam membangun ekosistem keamanan siber yang tangguh, kolaboratif, dan adaptif di kawasan ASEAN ((DFAT), 2020).

2.3.4 Mitra dan Kolaborasi

Program ASEAN Cyber Capacity Program (ACCP) tidak hanya mengandalkan upaya negara anggota ASEAN, tetapi juga didukung oleh berbagai mitra internasional. Negara-negara seperti Australia, Jepang, Amerika Serikat, dan

Uni Eropa memberikan dukungan dalam bentuk pembiayaan, transfer teknologi, dan pelatihan kapasitas sumber daya manusia. Dukungan ini bertujuan untuk meningkatkan kesiapan teknis dan koordinasi lintas batas di ASEAN, sehingga kawasan lebih tangguh menghadapi ancaman siber lintas negara (ASEAN Secretariat, 2023). Selain pemerintah, ACCP juga melibatkan sektor swasta, akademisi, dan lembaga internasional sebagai bagian dari strategi kolaboratif untuk memperkuat ekosistem keamanan siber regional. Partisipasi sektor swasta mencakup penyediaan alat dan platform keamanan, sementara akademisi berperan dalam penelitian dan pengembangan kebijakan berbasis bukti (Interpol, 2024). Lembaga internasional seperti UNODC dan OECD memberikan panduan tentang standar internasional, praktik terbaik, dan norma perilaku bertanggung jawab di ruang siber ((OECD), 2021; (UNODC), 2020). Kolaborasi multi-pihak ini memungkinkan ACCP untuk membangun jaringan kerja sama yang berkelanjutan, meningkatkan pertukaran informasi, dan memperkuat kapasitas teknis di tingkat nasional maupun regional. Dengan demikian, model kemitraan ACCP menunjukkan bahwa penguatan ketahanan siber memerlukan sinergi antara pemerintah, sektor swasta, akademisi, dan lembaga internasional, bukan sekadar upaya unilateral masing-masing negara anggota ASEAN. Dalam periode 2023–2025, ASEAN Cyber Capacity Program (ACCP) memfokuskan kegiatannya pada peningkatan ketahanan terhadap ransomware dan ancaman kelompok siber seperti Lockbit.

Program ini berupaya memperkuat kesiapsiagaan negara anggota melalui pelatihan teknis lanjutan, simulasi tanggap darurat siber, serta penyusunan

protokol mitigasi insiden yang lebih efektif (ASEAN Secretariat, 2023). Salah satu pencapaian signifikan ACCP adalah pengembangan incident sharing platform, yang memungkinkan negara anggota ASEAN untuk saling bertukar informasi ancaman secara real-time. Platform ini meningkatkan efektivitas koordinasi lintas batas dan membantu CSIRT nasional dalam merespons serangan siber secara cepat (INTERPOL, 2024). Selain aspek teknis, ACCP mendorong harmonisasi kebijakan keamanan siber antarnegara ASEAN, termasuk penyusunan pedoman dan norma perilaku bertanggung jawab di ruang siber (*responsible state behavior*). Harmonisasi tersebut bertujuan menciptakan kerangka regulasi regional yang konsisten, memfasilitasi kerja sama internasional, dan memperkuat ketahanan digital kawasan ((OECD), 2021; (UNODC), 2020). Melalui kolaborasi multi-pihak antara pemerintah, sektor swasta, akademisi, dan lembaga internasional, ACCP telah berhasil memperluas cakupan kegiatan pelatihan, memperkuat jejaring CSIRT regional, dan meningkatkan kesadaran negara anggota akan risiko ransomware dan ancaman siber lintas negara. Secara keseluruhan, perkembangan ini menunjukkan bahwa ACCP berperan penting dalam membangun ekosistem keamanan siber ASEAN yang adaptif, kolaboratif, dan proaktif menghadapi ancaman global.

2.3.5 Urgensitas Indonesia Bergabung dengan ACCP

Masifnya kerugian akibat serangan siber serta rendahnya kapasitas pengetahuan banyak negara dan perusahaan di Asia Tenggara mendorong pentingnya kerja sama regional untuk menciptakan lingkungan ekonomi dan

perdagangan yang aman. Negara-negara ASEAN bersama organisasi internasional mulai mencari solusi kolektif untuk meningkatkan keamanan siber kawasan. Upaya ini kemudian diwujudkan melalui pembentukan ASEAN Cyber Capacity Program (ACCP) sebagai platform penguatan kapasitas, kolaborasi, dan peningkatan kesiapan menghadapi ancaman digital (P. Singapore, 2023). Bagi Indonesia, urgensi keikutsertaan dalam ACCP terletak pada perlunya meningkatkan ketahanan siber nasional, baik dalam aspek pencegahan, respons cepat, maupun pemulihan pasca-serangan. Partisipasi Indonesia dalam ACCP membuka peluang untuk memperoleh pengetahuan baru, pertukaran kebijakan, dan penguatan strategi keamanan siber yang lebih komprehensif (C. Singapore, 2024). Badan Siber dan Sandi Negara (BSSN) mencatat bahwa sepanjang beberapa tahun terakhir Indonesia secara konsisten berada di antara negara dengan jumlah insiden siber tertinggi di kawasan Asia Tenggara, dengan ratusan juta hingga miliaran anomali trafik siber terdeteksi setiap tahunnya. Serangan tersebut mencakup ransomware, phishing, kebocoran data, hingga serangan terhadap infrastruktur strategis dan layanan publik digital. Kondisi ini menunjukkan bahwa Indonesia merupakan target yang rentan sekaligus bernilai tinggi bagi kelompok kejahatan siber transnasional. Tahun 2023, BSSN mencatat sekitar 403.990.813 trafik anomali serangan siber di Indonesia, yang mencakup ancaman Trojan, ransomware, dan Advanced Persistent Threat (Negara, 2023). Kaspersky mendeteksi 97.226 serangan ransomware dan 97.465 phishing finansial, menunjukkan tingginya intensitas kejahatan siber yang menyasar pengguna dan sistem digital nasional (A. News, 2024).

Tahun 2024, Kaspersky mengidentifikasi lebih dari 36 juta ancaman siber lokal di Indonesia, meskipun terjadi penurunan sekitar 29,44% dibandingkan tahun sebelumnya (A. News, 2024). Namun, tingkat risiko tetap tinggi karena sekitar 35,6% pengguna masih menjadi target serangan berbasis web dan malware (Novianty, 2025). Data BSSN juga menunjukkan adanya 122,79 juta anomali trafik serangan siber sepanjang Januari Agustus 2024, dengan malware sebagai ancaman dominan (I. News, 2024). Selain itu, aktivitas ransomware tetap signifikan dengan lebih dari 500.000 insiden, di mana LockBit tercatat sebagai salah satu varian paling aktif dengan 102.798 aktivitas (ResearchGate, 2024). Selanjutnya di Tahun 2025, meskipun data masih bersifat parsial, tren ancaman siber di Indonesia tetap tinggi. Hingga kuartal I–III 2025 tercatat sekitar 900.000 insiden phishing, mengindikasikan bahwa kejahatan siber masih menjadi tantangan serius bagi keamanan digital nasional (Technology, 2025). Berbagai macam serangan di atas, menjadikan kerja sama siber di tingkat regional menjadi penting, pada forum ASEAN sebelumnya seperti AMMTC masih memusatkan perhatian pada isu kejahatan transnasional secara luas sehingga pembahasan mengenai kejahatan siber belum mendalam. Indonesia menilai bahwa ancaman siber bersifat lintas batas dan tidak dapat ditangani secara unilateral. Indonesia menekankan pentingnya pertukaran pengetahuan, peningkatan kapasitas sumber daya manusia, serta pelaksanaan latihan bersama (joint exercises) antarnegara ASEAN sebagai bagian dari ACCP.

Melalui ACCP, Indonesia memiliki ruang diskusi yang lebih terfokus dan intensif dalam memperkuat penanggulangan ancaman siber di tingkat kawasan (P.

Singapore, 2023). Selain itu, Indonesia memandang bahwa setiap negara perlu memiliki point of contact nasional dalam penanganan insiden siber lintas batas, karena koordinasi cepat sangat penting ketika serangan melibatkan dua negara atau lebih. Indonesia juga menekankan pentingnya mekanisme pertukaran pengetahuan dan latihan bersama antarnegara ASEAN untuk meningkatkan kesiapsiagaan kolektif dalam menghadapi perkembangan teknologi informasi dan kejahatan siber yang semakin kompleks (C. Singapore, 2024).

2.3.6 Tantangan Implementasi ACCP

Implementasi ACCP menghadapi sejumlah tantangan yang kompleks, meskipun program ini telah memberikan kontribusi signifikan dalam memperkuat ketahanan siber regional.

1. Perbedaan kapasitas teknis antarnegara anggota ASEAN. Negara-negara maju seperti Singapura dan Malaysia memiliki infrastruktur digital yang lebih canggih, sementara negara berkembang seperti Laos, Myanmar, dan Kamboja masih memiliki keterbatasan perangkat keras, perangkat lunak, serta kemampuan analisis siber (ASEAN Secretariat, 2023). Perbedaan ini menimbulkan kesenjangan dalam efektivitas pelatihan teknis dan respon insiden siber lintas negara.
2. Keterbatasan sumber daya manusia dan pendanaan menjadi kendala signifikan dalam implementasi ACCP. Menurut laporan INTERPOL (2024), beberapa negara anggota masih kekurangan tenaga profesional siber yang terlatih, sehingga kapasitas untuk merespons serangan ransomware atau ancaman siber lainnya menjadi terbatas. Pendanaan yang tidak merata juga

membatasi kemampuan negara anggota untuk menerapkan teknologi dan protokol keamanan terbaru secara konsisten.

3. Kurangnya kesadaran keamanan digital di sektor publik dan swasta. Banyak organisasi masih belum memiliki kebijakan internal yang memadai terkait proteksi data dan respon insiden siber. OECD (2021) menekankan bahwa kesadaran ini penting agar kebijakan ACCP dapat diadopsi secara efektif, serta memastikan praktik keamanan siber menjadi bagian dari budaya organisasi di tingkat nasional maupun regional.

Secara keseluruhan, meskipun ACCP telah berhasil meningkatkan kesiapsiagaan teknis dan koordinasi antarnegara, keberhasilan program ini sangat bergantung pada pengurangan kesenjangan kapasitas, peningkatan SDM, alokasi pendanaan yang memadai, serta peningkatan kesadaran keamanan digital di seluruh sektor publik dan swasta. Tantangan-tantangan ini menjadi fokus utama untuk memastikan ACCP dapat mencapai tujuan jangka panjang dalam memperkuat ketahanan siber ASEAN.

2.3.7 Relevansi ACCP terhadap Ancaman Lockbit

Ancaman ransomware yang dilakukan oleh kelompok siber seperti Lockbit menjadi salah satu isu kritis dalam keamanan digital di kawasan ASEAN. Lockbit dikenal dengan model Ransomware-as-a-Service (RaaS), kemampuan double extortion, serta distribusi serangan lintas negara yang cepat dan sulit dideteksi. Oleh karena itu, diperlukan upaya sistematis untuk meningkatkan kesiapsiagaan dan kapasitas penanganan insiden siber di negara-negara anggota ASEAN (Europol, 2023; Interpol, 2024). ASEAN Cyber Capacity Program (ACCP)

memainkan peran sentral. Program ini membantu negara anggota ASEAN membangun sistem deteksi dini terhadap ransomware, termasuk Lockbit, melalui pelatihan teknis, simulasi tanggap darurat siber, dan penguatan kemampuan CSIRT nasional. Pelatihan ini mencakup penguasaan teknik identifikasi malware, analisis forensik digital, serta mitigasi serangan secara cepat sehingga dampak ekonomi dan operasional dapat diminimalkan (Centre, 2022; Secretariat, 2023d). Selain penguatan kapasitas teknis, ACCP juga mendorong kerja sama lintas batas dalam pelacakan dan penegakan hukum terhadap kelompok siber global. Mekanisme berbagi informasi ancaman melalui incident sharing platform mempercepat koordinasi antar-CSIRT di ASEAN dan dengan lembaga internasional seperti Europol, Interpol, dan UNODC. Kolaborasi ini memungkinkan respons yang lebih cepat terhadap serangan ransomware, serta memfasilitasi identifikasi dan penangkapan afiliasi Lockbit yang beroperasi lintas negara (UNODC, 2020).

ACCP telah berkontribusi dalam pada pembangunan collective cyber resilience ASEAN, yakni kemampuan kolektif kawasan untuk menghadapi dan memitigasi ancaman siber yang kompleks dan bersifat lintas batas. OECD (2021) menekankan bahwa keberhasilan ketahanan siber regional bergantung pada kombinasi penguatan kapasitas teknis, harmonisasi kebijakan, dan kerja sama multi-stakeholder antara pemerintah, sektor swasta, akademisi, dan lembaga internasional. ACCP berperan sebagai fondasi yang menyatukan berbagai upaya ini sehingga ASEAN tidak hanya bereaksi terhadap ancaman siber, tetapi juga proaktif dalam membangun sistem pertahanan digital yang adaptif dan

berkelanjutan. Secara keseluruhan, ACCP meningkatkan kesiapsiagaan teknis, koordinasi lintas batas, dan kebijakan siber ASEAN. Program ini relevan dalam menghadapi ancaman Lockbit dan kelompok ransomware lainnya, sekaligus memperkuat posisi ASEAN sebagai kawasan yang tangguh dalam menghadapi risiko keamanan digital global. Keberhasilan ACCP menjadi indikator penting bagi negara anggota untuk meningkatkan keamanan siber nasional sekaligus kontribusi kolektif terhadap stabilitas digital kawasan.