BAB VI

PENUTUP

VI.1 Kesimpulan

Penelitian ini menyoroti bagaimana Taiwan mengimplementasikan *National Cyber Security Program* (NCSP) selama periode 2019-2023. Rentang waktu ini menjadi titik penting karena bersamaan dengan meningkatnya ancaman siber dari Tiongkok, percepatan transformasi digital akibat pandemi COVID-19, serta memanasnya dinamika geopolitik di kawasan terutama dengan Tiongkok. Ketiga faktor ini secara bersamaan memberikan tekanan besar terhadap upaya Taiwan dalam menjaga stabilitas ekonomi digitalnya. Kesimpulan yang disampaikan merupakan hasil sintesis dari analisis ancaman siber yang dihadapi Taiwan dan respons kebijakan yang diambil melalui berbagai pilar implementasi NCSP, sebagaimana telah diuraikan pada bagian sebelumnya.

Temuan dari penelitian ini menunjukkan bahwa ancaman siber dari Tiongkok terhadap Taiwan selama 2019-2023 bersifat sistematis, berkelanjutan, dan menjadi bagian dari strategi jangka panjang. Serangan ini mencakup aktivitas spionase digital terhadap sektor-sektor strategis seperti semikonduktor, serangan destruktif menggunakan ransomware seperti ColdLock, serta operasi oleh kelompok peretas canggih seperti AMOEBA dan MustangPanda yang memanfaatkan celah rantai pasokan. Selain itu, kampanye disinformasi juga meningkat, dengan tujuan memengaruhi opini publik dan merusak stabilitas politik, seperti yang terlihat saat pemilu 2020, protes di Hong Kong 2019, dan pandemi COVID-19.

Sebagai respons, Taiwan memperkuat kebijakan keamanan sibernya melalui implementasi NCSP, khususnya dalam transisi dari fase kelima ke fase keenam. Strategi ini berfokus pada empat pilar utama: perlindungan infrastruktur kritis, pengembangan industri keamanan siber, peningkatan kapasitas talenta melalui pendidikan dan pelatihan, serta kerja sama internasional. Taiwan juga membentuk lembaga-lembaga baru seperti MODA, ACS, dan NICS, serta menjalin

kolaborasi dengan mitra seperti AS dan Jepang untuk memperkuat pertahanan siber nasional secara menyeluruh. Strategi yang dibentuk melalui NCSP telah mencerminkan upaya adaptif untuk melindungi sektor-sektor strategis, termasuk industri semikonduktor yang menjadi tulang punggung ekonomi digital Taiwan. Perlindungan terhadap infrastruktur kritis dan pembangunan ekosistem keamanan digital juga menjadi elemen penting dalam menjaga keberlanjutan pertumbuhan ekonomi berbasis teknologi tinggi.

Berbagai respons kebijakan tersebut menunjukkan keseriusan Taiwan dalam menghadapi ancaman yang semakin kompleks. Namun, sejumlah tantangan masih menghambat efektivitasnya, terutama kekurangan talenta keamanan siber yang belum terselesaikan, belum adanya respons terpadu terhadap ancaman berbasis AI, keterbatasan anggaran dan penegakan kebijakan, serta ketidakseimbangan fokus antara keamanan sistem TI dan OT. Ketergantungan tinggi terhadap mitra internasional juga menjadi risiko jika tidak diimbangi dengan penguatan kapasitas dalam negeri, yang menjadikan adaptasi dan pengembangan mandiri sebagai kebutuhan mendesak dalam menjaga keberlanjutan stabilitas ekonomi digital Taiwan.

Secara keseluruhan, menjawab rumusan masalah penelitian ini, bisa disimpulkan bahwa NCSP merupakan upaya penting Taiwan untuk menghadapi serangan siber dari Tiongkok dan menjaga stabilitas ekonomi digitalnya. Program ini sudah memberikan kemajuan nyata, terutama dalam membangun sistem pertahanan dan kerja sama internasional. Namun, masih ada tantangan internal yang harus diatasi, terutama soal kekurangan talenta dan perlunya penyesuaian kebijakan terhadap ancaman-ancaman baru seperti AI. Stabilitas ekonomi digital Taiwan adalah hasil dari proses yang terus bergerak, bukan sesuatu yang bisa dicapai sekali saja. Serangan disinformasi dari Tiongkok, meskipun tidak langsung menyerang infrastruktur ekonomi, bisa merusak kepercayaan publik dan menurunkan minat investasi yang pada akhirnya juga membahayakan fondasi ekonomi digital itu sendiri.

VI.2 Saran

Berdasarkan kesimpulan yang telah diuraikan, berikut ini beberapa saran praktis dan teoritis yang diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan keamanan siber di masa depan, baik untuk Taiwan maupun sebagai pembelajaran bagi negara lain, serta untuk pengembangan studi ilmiah terkait.

VI.2.1 Saran Praktis

Untuk menjaga keberlanjutan stabilitas ekonomi digitalnya, Taiwan perlu terus memperkuat pengembangan kapasitas siber domestik yang mandiri dan resilien terhadap dinamika ancaman global. Penguatan ini tidak cukup hanya melalui kerja sama internasional, tetapi juga menuntut konsolidasi ekosistem siber nasional yang lebih terintegrasi. Kolaborasi antara pemerintah, sektor swasta, dan akademisi menjadi kunci dalam mendorong inovasi teknologi lokal dan menciptakan talenta siber yang mampu menjawab kebutuhan industri strategis seperti semikonduktor. Reformasi kerangka kebijakan NCSP juga perlu diarahkan agar lebih responsif terhadap ancaman darurat seperti serangan siber berbasis kecerdasan buatan (AI), serta didukung oleh alokasi anggaran yang berpihak pada sektor-sektor krusial. Pendekatan ini dapat membantu Taiwan membangun sistem pertahanan siber yang tidak hanya reaktif, tetapi juga strategis dan berkelanjutan.

Meskipun fokus utama penelitian ini adalah pada studi kasus Taiwan, pendekatan strategis yang diambil dapat menjadi pembelajaran penting bagi Indonesia dalam membangun kebijakan keamanan siber yang visioner dan terintegrasi dengan agenda pembangunan ekonomi digital nasional. Pengalaman Taiwan menunjukkan bahwa kunci ketahanan digital terletak pada sinergi antara perlindungan infrastruktur kritis, kemandirian teknologi, dan pengembangan SDM secara kolaboratif. Bagi Indonesia, adopsi strategi serupa dapat menjadi fondasi untuk memperkuat posisi dalam arsitektur keamanan regional, sekaligus meningkatkan daya saing ekonomi digital di tengah persaingan global yang semakin kompleks.

Dalam konteks ini, keamanan siber bukan hanya isu teknis, melainkan komponen strategis dalam menjaga kedaulatan digital dan arah masa depan pembangunan nasional.

VI.2.2 Saran Teoritis

Penelitian ini menunjukkan bahwa pendekatan keamanan non-tradisional perlu mempertimbangkan ancaman siber sebagai bentuk agresi pada era saat ini yang tidak hanya bersifat teknis, tetapi juga berdampak sistemik terhadap stabilitas nasional dan ekonomi digital. Kasus Taiwan memperlihatkan bahwa keamanan digital dan resiliensi ekonomi saling berkaitan erat, sehingga konsep keamanan non-tradisional sebaiknya diperluas untuk mencakup dinamika ancaman digital lintas sektor. Temuan ini juga menegaskan pentingnya melihat keamanan siber bukan hanya sebagai isu teknis, tetapi sebagai bagian dari strategi politik dan diplomasi dalam menghadapi tekanan eksternal.

Dari perspektif teori kebijakan siber, efektivitas kebijakan seperti NCSP dipengaruhi oleh kemampuan negara dalam beradaptasi secara responsif terhadap perkembangan ancaman, terutama yang berbasis teknologi seperti AI. Sementara itu, dalam kerangka ekonomi digital, penelitian ini menekankan bahwa keberlanjutan pertumbuhan digital tidak bisa dilepaskan dari pembangunan ketahanan siber yang kuat dan terintegrasi. Implikasi ini membuka ruang bagi pengembangan teori yang lebih menyeluruh, dengan menggabungkan faktor domestik seperti tata kelola, kapasitas SDM, dan desain kelembagaan, serta faktor eksternal seperti interdependensi digital dan rivalitas geopolitik dalam studi keamanan dan kebijakan siber.