BAB VI
PENUTUP

6.1 Kesimpulan

Penelitian ini menyoroti implementasi National Cybersecurity Strategy (NCSS) Korea Selatan selama periode 2019–2022, yang diluncurkan pada masa pemerintahan Presiden Moon Jae In. Perumusan strategi ini tidak terlepas dari perkembangan pola serangan siber Korea Utara yang mengalami peningkatan intensitas sekaligus transformasi sasaran dan motif operasional. Jika pada fase sebelumnya serangan lebih terkonsentrasi pada institusi pemerintahan dan simbol-simbol negara, sejak 2017 aktivitas siber Korea Utara semakin diarahkan pada sektor finansial, lembaga perbankan, aset kripto, serta infrastruktur ekonomi digital yang berdampak langsung terhadap stabilitas ekonomi dan kepercayaan publik.

Perluasan target yang disertai dengan motif perolehan keuntungan ekonomi dan pembiayaan rezim tersebut menunjukkan bahwa serangan siber telah berkembang dari sekadar instrumen tekanan politik menjadi instrumen strategis yang menyentuh fondasi ketahanan nasional. Rangkaian insiden tersebut tidak hanya menimbulkan kerugian material, tetapi juga memunculkan efek terhadap ekosistem ekonomi digital Korea Selatan dimana menggerus kepercayaan publik terhadap keamanan sistem keuangan, serta memperlihatkan keterbatasan kerangka regulasi keamanan siber sektoral yang sebelumnya berlaku. Dalam konteks ini, keamanan ruang siber negara tidak hanya semata berkaitan dengan perlindungan institusi pemerintahan, melainkan juga perlindungan masyarakat sebagai pengguna utama infrastruktur digital. Dinamika serangan siber inilah yang melatarbelakangi kebutuhan untuk memperbarui kerangka kebijakan sebelumnya dan membangun strategi keamanan siber yang lebih terintegrasi, sistematis, dan berjangka panjang.

Berdasarkan keseluruhan analisis, dapat disimpulkan bahwa implementasi NCSS 2019 pada masa pemerintahan Presiden Moon Jae-in merupakan manifestasi konkret dari proses sekuritisasi ruang siber dalam kerangka keamanan nasional Korea Selatan. Negara secara aktif membingkai serangan siber yang berasal dari Korea Utara sebagai ancaman eksistensial terhadap stabilitas nasional, infrastruktur

kritis, serta keberlangsungan fungsi pemerintahan. Dalam kerangka teori sekuritisasi, negara berperan sebagai *securitizing actor* yang mengangkat isu siber dari ranah teknis menjadi isu keamanan nasional yang memerlukan respons strategis jangka panjang dan terinstitusionalisasi.

Melalui NCSS 2019, keamanan siber diposisikan sebagai domain strategis yang setara dengan domain keamanan konvensional. Kebijakan ini menjadi tonggak penting karena untuk pertama kalinya Korea Selatan memiliki strategi keamanan siber nasional yang bersifat komprehensif dan berjangka panjang. Secara struktural, implementasi NCSS 2019 dijalankan melalui tata kelola tiga tingkat yang terpusat pada level nasional namun bersifat koordinatif lintas sektor dan agensi. Pada tingkat nasional, National Security Office (NSO) berperan sebagai otoritas tertinggi dalam koordinasi strategis kebijakan keamanan siber dengan dukungan intelijen dari National Intelligence Service (NIS). Pada tingkat sektoral, kementerian terkait mengintegrasikan kebijakan keamanan siber ke dalam regulasi dan pengawasan di bidang masing-masing. Sementara itu, pada tingkat agensi, fungsi pemantauan dan respons insiden dilaksanakan oleh badan teknis seperti Korea Internet & Security Agency (KISA) dan National Cyber Security Center (NCSC). Struktur ini memastikan bahwa arah kebijakan nasional diterjemahkan ke dalam pelaksanaan operasional yang terdistribusi namun terintegrasi.

Pada tataran implementatif per-pilar, pengamanan infrastruktur informasi kritis dilakukan oleh NCSC pada sektor energi, transportasi, keuangan, dan layanan publik seperti KEPCO, KHNP, KORAIL, dan NHIS. Semua institusi vital diwajibkan menerapkan pelaporan insiden 24 jam serta *security by design* pada ICS. Di sektor keuangan, KISA melaksanakan audit ISMS terhadap bursa kripto dan FIU sebagai unit intelijen keuangan negara memperketat pengawasan AML serta transaksi mencurigakan pada aset digital. Dalam peningkatan kapasitas respons, NCSC mengoperasikan *System for Sharing National Cyber Threat Information*, membangun 91 pusat pemantauan keamanan, serta mengembangkan analisis pola *malware* untuk memperkuat sistem deteksi dan peringatan dini nasional. Tata kelola kolaboratif dijalankan melalui koordinasi NSO dengan dukungan di bidang militer, MCC, serta kemitraan formal antara NCSC, KISA, dan perusahaan keamanan siber swasta seperti AhnLab dan SK Shieldus. Pilar inovasi industri diwujudkan oleh

MSIT dengan pendanaan R&D, program Scale-up TIPS, serta penguatan riset melalui NSRI dan latihan CCE untuk pengembangan talenta siber. Budaya keamanan siber diperkuat melalui Eulji Exercise sebagai latihan darurat nasional, sedangkan kepemimpinan global diwujudkan melalui K-Cybersecurity Promotion Strategy serta partisipasi aktif dalam UN GGE dan OEWG sebagai forum multilateral dalam pembahasan tata kelola keamanan siber. Secara keseluruhan, implementasi per-pilar menunjukkan bahwa NCSS 2019 diterjemahkan ke dalam program, unit, dan mekanisme institusional yang terintegrasi dalam arsitektur keamanan siber nasional.

Namun demikian, secara keseluruhan temuan penelitian ini menunjukkan bahwa NCSS 2019 lebih efektif sebagai kerangka pengelolaan respons negara dibandingkan sebagai instrumen pencegahan absolut terhadap serangan. NCSS 2019 terbukti mampu membentuk fondasi institusional dan operasional yang relatif solid dalam menghadapi serangan siber Korea Utara yang berkelanjutan. Akan tetapi, kebijakan ini belum sepenuhnya mampu menghentikan ataupun menurunkan intensitas serangan siber tersebut. Hal ini terlihat dari tinjauan keberlanjutan ruang lingkup keamanan siber Korea Selatan pada periode setelahnya, yakni 2023–2024, di mana serangan siber Korea Utara masih berlangsung secara berulang, adaptif, dan berkembang mengikuti dinamika teknologi. Jika efektivitas kebijakan diukur berdasarkan indikator penurunan intensitas atau perubahan karakter serangan, maka NCSS 2019 tidak dapat dikatakan berhasil secara preventif. Serangan tetap terjadi dan menunjukkan kemampuan adaptasi dari aktor ancaman.

Meskipun demikian, temuan tersebut tidak serta-merta menunjukkan kegagalan total kebijakan. NCSS 2019 berfungsi sebagai kerangka institusional dan operasional yang membentuk pola respons Korea Selatan terhadap serangan siber yang terus terjadi. Dampaknya terlihat pada meningkatnya koordinasi lintas sektor, penguatan mekanisme berbagi intelijen, konsolidasi peran lembaga keamanan siber nasional, serta kemampuan respons cepat yang tetap dipertahankan dan dikembangkan. Dengan kata lain, *impact* utama NCSS 2019 terletak pada aspek pengelolaan dan mitigasi serangan siber, bukan pada pencegahan terjadinya serangan itu sendiri.

Dengan demikian, dapat disimpulkan bahwa NCSS 2019 bersifat berkelanjutan secara institusional, tetapi terbatas secara preventif. Kebijakan ini berhasil membangun fondasi jangka panjang dan operasional yang relatif solid bagi keamanan siber Korea Selatan melalui kombinasi penguatan teknis domestik, kolaborasi lintas aktor, serta peran aktif dalam kepemimpinan internasional, dalam menghadapi dinamika serangan siber berkelanjutan Korea Utara.

6.2 Saran

6.2.1 Saran Praktis

Penulis menilai bahwa fenomena keamanan siber yang dihadapi Korea Selatan menunjukkan perlunya peningkatan kapasitas perlindungan keamanan siber secara lebih serius. Korea Selatan pada dasarnya tidak memiliki keterbatasan baik dari sisi teknologi maupun sumber daya manusia, namun masih menghadapi kelemahan pada aspek implementasi strategi keamanan siber yang telah dirancang. Kondisi tersebut berdampak pada ketiadaan konsekuensi yang substansial terhadap Korea Utara sebagai aktor penyerang, sehingga berpotensi melemahkan posisi Korea Selatan dalam menghadapi eskalasi ancaman siber. Namun, mengingat kompleksitas hubungan antar Korea yang pada periode tertentu relatif stabil dan tidak berada dalam eskalasi tinggi, penulis menilai bahwa lemahnya penekanan pada aspek penegakan hukum dan konsekuensi langsung dalam kebijakan keamanan siber masih dapat dipahami. Pendekatan yang tidak terlalu konfrontatif tersebut sejalan dengan upaya menjaga stabilitas dan hubungan damai antar kedua negara, khususnya pada masa pemerintahan Moon Jae-in. Akan tetapi, apabila keamanan siber ditempatkan dalam kerangka perlindungan kedaulatan nasional secara lebih tegas, maka tuntutan kebijakannya menjadi berbeda. Dalam konteks ini, Korea Selatan perlu memiliki perlindungan teknis yang jauh lebih kuat dan konsekuensi nyata bagi penyerang.

6.2.2 Saran Akademis

Penulis merekomendasikan adanya kajian lanjutan yang secara khusus menelaah implementasi kebijakan keamanan siber Korea Selatan pada periode terkini. Dinamika politik domestik Korea Selatan yang mengalami pergantian

pemerintahan dalam beberapa tahun terakhir menunjukkan adanya potensi pergeseran orientasi dan prioritas kebijakan keamanan siber nasional. Kondisi tersebut berimplikasi pada semakin kompleksnya tata kelola keamanan di ruang siber, baik dari sisi kelembagaan, strategi, maupun arah implementasi kebijakan. Oleh karena itu, penelitian yang berfokus pada evolusi dan keberlanjutan kebijakan keamanan siber Korea Selatan pasca NCSS 2019 menjadi relevan dan memiliki nilai akademik yang tinggi. Kajian semacam ini tidak hanya dapat memperkaya pemahaman mengenai konsistensi atau perubahan arah kebijakan di bawah kepemimpinan yang berbeda, tetapi juga membuka ruang eksplorasi terhadap bagaimana dinamika politik domestik memengaruhi respons negara terhadap ancaman siber yang terus berkembang. Dengan munculnya kepemimpinan baru dalam struktur pemerintahan Korea Selatan, penelitian lanjutan di bidang ini berpotensi memberikan kontribusi signifikan bagi pengembangan studi keamanan siber dan kebijakan keamanan nasional secara lebih luas.