

## BAB 6 KESIMPULAN DAN SARAN

### 6.1 Kesimpulan

Implementasi kebijakan China dalam pengembangan kabel bawah laut ini dibagi menjadi lima bagian kebijakan. Kebijakan pencegahan masalah siber dan pemantauan kabel bawah laut menunjukkan langkah preventif yang komprehensif: mulai dari pelindung fisik dan edukasi aktor lokal hingga sistem sensor dan patroli terpadu. Pendekatan ini mengurangi celah keamanan sejak awal baik yang bersifat fisik maupun digital sehingga negara dapat bereaksi lebih cepat terhadap potensi gangguan. Dalam kerangka Cyber-Realism, kedua kebijakan ini memperkuat *self-help*: membangun kapabilitas protektif dan intelijen siber untuk meminimalkan *asymmetry of information* dan menjaga kedaulatan komunikasi.

Kebijakan Protokol respons darurat dan kebijakan standarisasi pemasangan kabel menegaskan pentingnya kesiapsiagaan dan aturan teknis yang seragam. Tim darurat 24/7 dan prosedur notifikasi cepat membuat resolusi insiden lebih terkoordinasi, sementara standar material, enkripsi, dan audit tahunan memastikan interoperabilitas dan keamanan berkelanjutan. Dari sudut Cyber-Realism, keduanya adalah wujud *deterrence* dan kontrol struktural negara mempertahankan *advantage* dengan respons agresif-defensif serta memaksakan norma teknis yang memperkuat posisinya di arena internasional.

Kebijakan Pengembangan infrastruktur termasuk inisiatif “Peace Cable” dan CIABS, menekankan investasi jangka panjang di sektor kabel bawah laut. Dengan menggabungkan riset lokal, kerjasama multilateral, dan jalur alternatif, negara tidak hanya memperkuat konektivitas, tetapi juga memperluas pengaruh teknisnya sekaligus membatasi kompetitor. Secara keseluruhan, Bab lima menegaskan bahwa melalui rangkaian kebijakan preventif, responsif, regulatif, dan strategis, negara memproyeksikan “*hard cyber power*” secara terstruktur sebuah manifestasi nyata prinsip Cyber-Realism dalam menjaga keamanan dan kedaulatan siber global.

Secara teoritis, tulisan ini memperkuat gagasan Cyber-Realism bahwa negara merespons dinamika dunia maya dengan cara yang mirip seperti di dunia

fisik melalui kombinasi kontrol, pertahanan, dan proyeksi kekuatan. China memanfaatkan kabel bawah laut sebagai arena politik kekuatan siber (*cyber power politics*), dan memperkuat posisi tawarnya dalam forum-forum standar internasional. Namun, efektivitas kontrol semacam ini di lapangan tetap bergantung pada kesiapan teknis para mitra, kapasitas institusional mereka, serta kepercayaan bahwa kebijakan siber China akan menghormati prinsip kedaulatan data.

## 6.2 Saran

Setelah menarik pelajaran dari keseluruhan penelitian, bagian ini mengemukakan saran teoritis dan praktis untuk memperkaya literatur dan memperbaiki implementasi kebijakan siber China di proyek submarine cable, khususnya di kawasan Indo-Pasifik.

### 6.2.1 Saran Teoritis

Pertama, penelitian selanjutnya dapat memperluas kerangka analisis dengan mengkombinasikan teori cyber realism dan teori kompleksitas keamanan (*security complex*) untuk menangkap dinamika interaksi multilapisan antara aktor negara, perusahaan korporasi, dan masyarakat sipil digital. Kombinasi teori ini akan membantu merinci bagaimana kebijakan keamanan siber coralized (terfragmentasi) dapat memengaruhi atau memperburuk dilematis keamanan kolektif di kawasan.

Kedua, perlu ada eksplorasi lebih lanjut mengenai dampak normative: bagaimana Indonesia, Australia, atau India membangun norma bersama melalui platform regional untuk mengatur submarine cable. Kajian kebijakan perbandingan lintas negara dapat menyingkap variabel politik domestik yang mempengaruhi kecepatan dan kedalaman penerapan standar keamanan siber.

Ketiga, disarankan penelitian kualitatif lapangan yang melibatkan wawancara dengan pembuat kebijakan, operator kabel, dan pengguna akhir /di negara-negara penerima untuk memahami persepsi risiko siber dan faktor-faktor yang mendorong atau menghambat adopsi teknologi

pemantauan. Pendekatan bottom-up ini akan melengkapi data sekunder dengan perspektif praktis yang kaya.

Keempat, studi kuantitatif jangka panjang mengenai insiden siber di jalur submarine cable, correlated dengan intensitas patroli atau cakupan monitoring, dapat menguji hipotesis bahwa tingkat keamanan siber berbanding lurus dengan frekuensi kegagalan atau kejahatan digital. Data semacam ini akan memperkuat bukti empiris efektivitas kebijakan dan teknologi yang diimplemen oleh China.

### **6.2.2 Saran Praktis**

Pertama, pemerintah China serta operator kabel perlu meningkatkan transparansi melalui pembentukan trusted third party audit internasional yang melibatkan lembaga independen dari negara mitra untuk memverifikasi kepatuhan terhadap standar enkripsi dan non-intervensi. Mekanisme audit semacam ini akan menumbuhkan rasa saling percaya dan mengurangi resistensi geopolitik.

Kedua, perluasan cakupan sistem pemantauan real-time harus dikawal dengan investasi pada infrastruktur sensing yang lebih terdistribusi, termasuk di jalur-jalur minor dan perintis, agar deteksi dini tidak hanya terjadi di rute utama. Selain itu, pengembangan algoritma machine learning untuk analisis anomali akustik perlu dimasukkan ke dalam roadmap teknologi nasional.

Ketiga, China dapat menjalin kemitraan teknis dengan negara-negara Indo-Pasifik untuk transfer pengetahuan dan pelatihan operasional patroli maritim, sehingga pihak lokal memiliki kapasitas untuk menjaga keamanan submarine cable setelah fase pembangunan selesai. Skema train-the-trainer dan joint exercises patroli di zona perlindungan kabel dapat membangun jaringan kerjasama operasional yang berkelanjutan.

Keempat, operator harus menyusun panduan respons insiden terintegrasi yang mencakup prosedur koordinasi lintas lembaga mulai dari penjaga pantai hingga cybersecurity emergency response teams (CERT)

agar penanganan gangguan fisik dan digital berjalan terpadu. Latihan simulasi insiden multi-dimensional secara periodik dapat meningkatkan kesiapsiagaan dan meminimalkan downtime layanan.

Kelima, bagi negara penerima di kawasan Indo-Pasifik, disarankan untuk membuat peta risiko kabel nasional yang memadukan analisis geopolitik, kepadatan data, dan sensitivitas data industri kritis. Peta ini dapat menjadi alat dasar dalam merancang kebijakan kontinjensi dan alur cadangan (redundancy) yang mengurangi ketergantungan pada satu rute atau penyedia. Dengan demikian, landasan kerja sama regional di bawah forum seperti ASEAN atau Quad dapat diperkuat melalui kebijakan harmonisasi keamanan submarine cable.

Dengan rangkaian saran ini, diharapkan kesenjangan antara teori dan praktik dapat dipersempit, sementara respons kolektif terhadap tantangan keamanan siber submarine cable di Indo-Pasifik menjadi lebih terstruktur, transparan, dan berkelanjutan.