BAB VI

PENUTUP

6.1 Kesimpulan

Penelitian "Strategi Keamanan Siber Indonesia untuk Mengatasi Ancaman Siber dengan Kehadiran Teknologi 5G" ini membahas mengenai strategi keamanan siber Indonesia untuk mengatasi ancaman siber dengan kehadiran teknologi 5G. Berdasarkan hasil penelitian, usaha Indonesia dalam mengimplementasikan teknologi jaringan terbaru, teknologi 5G, dipandang telah memunculkan kebutuhan akan strategi keamanan siber yang baru pula. Hal ini didukung oleh Konsep Dilema Keamanan Penggunaan Ganda yang digunakan; sekaligus oleh pendapat kedua narasumber penelitian, Pegawai Badan Siber dan Sandi Negara (BSSN) dari Direktorat Strategi Keamanan Siber dan Sandi dan Pengamat Keamanan Siber; di mana teknologi 5G tidak hanya dapat memberikan peluang bagi pembangunan nasional, tetapi juga memunculkan ancaman siber baru bagi keamanan siber Indonesia. Dengan demikian, terdapat **korelasi positif** antara hasil penelitian dan pemikiran awal penulis bahwa diperlukan pengembangan strategi keamanan siber untuk menghadapi ancaman siber yang hadir dari kemunculan teknologi 5G di Indonesia.

Selama ini, Indonesia telah menerapkan strategi keamanan siber dengan mengacu kepada 5 (lima) Pilar The Global Cybersecurity Index (GCI) 2017 oleh International Telecommunication Union (ITU) yang meliputi aspek hukum, aspek teknis, aspek organisasi, aspek pengembangan kapasitas, dan aspek kerja sama. Dalam penelitian, kelima aspek Strategi Keamanan Siber Nasional di atas dikomparasikan dengan pemikiran William Yeoh (2022) mengenai *critical success factors* (CSF) untuk mengukur tingkat keberhasilan peningkatan keamanan siber dengan standar internasional. Kelima kriteria penentu Yeoh meliputi aspek organisasi, aspek infrastruktur, aspek strategis, aspek proses, dan aspek eksternal.

Dari hasil penelitian, penulis melihat bahwa pemerintah Indonesia, dengan BSSN sebagai titik fokus dalam bidang keamanan siber, telah mengusahakan berbagai cara untuk menjalankan strategi keamanan siber nasional. Berkaca pada pemikiran Yeoh, tingkatan pelaksanaan Strategi Keamanan Siber Nasional Indonesia sesuai dengan kelima kriteria dapat diurutkan dari yang terbaik sampai yang terburuk. Urutan menurut pandangan penulis antara lain: **Pemenuhan kriteria pertama adalah dalam Aspek Kerja Sama.** Dalam hal ini, pemerintah Indonesia telah mengadakan kerja sama dengan pemangku kepentingan keamanan siber, baik dari dalam maupun dari luar negeri. Namun demikian, pemerintah masih harus mendorong kerja sama yang juga secara khusus membahas mengenai keamanan siber untuk mengatasi ancaman siber dengan kehadiran teknologi 5G.

Pemenuhan kriteria kedua adalah dalam Aspek Organisasi. Pemerintah Indonesia telah mengembangkan strategi dan kebijakan keamanan siber nasional. Pemerintah juga telah membentuk BSSN sebagai badan yang bertanggung jawab dalam bidang keamanan siber. Namun demikian, pemerintah masih harus mengembangkan strategi dan tindakan lanjutan yang secara spesifik membahas mengenai aspek keamanan siber untuk menghadapi ancaman siber dengan kehadiran teknologi 5G.

Pemenuhan kriteria ketiga adalah dalam Aspek Pengembangan Kapasitas. Pemerintah Indonesia tidak hanya telah membentuk standar, pedoman, dan dokumen panduan bagi aktor-aktor keamanan siber; tetapi juga telah mendorong pengembangan, pelatihan, serta pelaksanaan kampanye untuk meningkatkan kesadaran akan keamanan siber di masyarakat Indonesia. Namun demikian, pemerintah masih harus mengusahakan agar beragam tindakan yang telah dan yang akan dilakukan terkait teknologi 5G memiliki kualitas dan bersifat merata di seluruh Indonesia.

Pemenuhan kriteria keempat adalah dalam Aspek Teknis. Pemerintah Indonesia telah menyediakan berbagai penunjang implementasi teknologi 5G. Hal ini termasuk pembangunan infrastruktur berupa perangkat keras maupun lunak,

penyediaan sumber daya teknologi dan manusia yang berkemampuan untuk dapat menggunakan infrastruktur secara maksimal, hingga pembuatan standar dan pedoman bagi infrastruktur teknologi 5G itu sendiri. Namun demikian, pemerintah masih harus meningkatkan kepastian akan keamanan siber dari infrastruktur teknologi 5G.

Terakhir, **pemenuhan kriteria kelima adalah dalam Aspek Hukum.** Dalam hal ini, pemerintah Indonesia telah mengeluarkan berbagai peraturan yang mendukung pelaksanaan keamanan siber nasional. Pemerintah juga telah membentuk BSSN yang bertugas membentuk arah strategi keamanan siber nasional demi mencapai ranah siber nasional yang aman. Namun demikian, pemerintah masih harus mengembangkan peraturan keamanan siber nasional yang kuat, terpusat, terstruktur, serta mencakup aspek keamanan siber yang secara khusus membahas mengenai ancaman siber dari kehadiran teknologi 5G.

6.2 Saran

Dengan hasil penelitian "Strategi Keamanan Siber Indonesia untuk Mengatasi Ancaman Siber dengan Kehadiran Teknologi 5G" ini, penulis melihat bahwa di samping usaha yang telah dilakukan, pemerintah Indonesia, dengan BSSN sebagai titik fokus, masih perlu melakukan pengembangan terhadap strategi keamanan siber nasional. Beberapa rekomendasi Strategi Keamanan Siber Indonesia untuk mengatasi ancaman siber dengan kehadiran teknologi 5G, dengan membandingkan antara Strategi Keamanan Siber Nasional oleh BSSN dan 5 (lima) Poin Tingkat Keberhasilan Kritis *(Critical Success Factor)* oleh William Yeoh (2022) dalam mengukur strategi keamanan siber, adalah sebagai berikut:

6.2.1 Aspek Hukum

Dengan perbandingan antara Aspek Hukum dari Strategi Keamanan Siber Nasional oleh BSSN dan pemikiran Yeoh (2022) Tingkat Keberhasilan Kritis dalam Aspek Organisasi, Infrastruktur, dan Proses, berikut merupakan rekomendasi strategi

keamanan siber nasional untuk mengatasi ancaman siber dengan kehadiran teknologi 5G dari Aspek Hukum:

- Perlu disusun Undang-undang tentang Keamanan dan Ketahanan Siber Nasional. Hal ini diperlukan karena UU yang ada belum terpusat dan masih tersebar. Sebagai contoh UU ITE (untuk mengatur pengelolaan informasi dan transaksi elektronik), UU PDP (untuk mengatur perlindungan terhadap data pribadi), dan lain-lain. Dengan UU tersebut, pemerintah dapat mengusahakan keamanan siber nasional secara lebih terpusat dan terstruktur, termasuk untuk mengakomodasi keamanan siber teknologi 5G;
- Perlu disusun Undang-undang tentang Persandian untuk mendukung dan memperkuat peran BSSN. Hal ini diperlukan karena BSSN baru mampu menetapkan himbauan dan tidak dapat menetapkan peraturan dengan efek kepatuhan, yang mana keadaan ini tentu mempengaruhi keefektifan peran BSSN. Dengan UU tersebut, pemerintah dapat menguatkan peran BSSN, apalagi dengan mengingat kebutuhan akan keamanan siber akan terus meningkat seiring dengan perkembangan teknologi digital, seperti dengan perkembangan teknologi 5G;
- Perlu disusun Undang-undang untuk meningkatkan peran pemerintah dalam mengatasi keterbatasan infrastruktur telekomunikasi. Hal ini diperlukan karena pemerintah baru memiliki Undang-undang No.11/2020 tentang Cipta Kerja yang mengizinkan kerja sama pengembangan infrastruktur dengan mekanisme *business-to-business* (B2B), tanpa keikutsertaan pemerintah. Dengan UU tersebut, pemerintah tidak hanya dapat lebih terlibat, tetapi juga dapat secara aktif mendorong pemerataan dalam pengembangan infrastruktur telekomunikasi terbaru, termasuk teknologi 5G;
- Perlu disusun peraturan terkait standar teknis dan sertifikasi keamanan alat telekomunikasi. Hal ini diperlukan karena pemerintah baru memiliki Peraturan Menteri tentang Standar Teknis Alat Dan/Atau Ketentuan Operasional

Sertifikasi Alat Telekomunikasi, Permen Kominfo Nomor 16 Tahun 2018. Namun demikian, peraturan ini belum menetapkan standar teknis dan sertifikasi terkait keamanan dari penggunaan alat telekomunikasi itu sendiri. Dengan peraturan tersebut, pemerintah dapat memastikan keamanan dari penggunaan teknologi, termasuk teknologi 5G;

- Perlu disusun pedoman teknis pengujian dan standar keamanan perangkat telekomunikasi 5G. Hal ini diperlukan untuk melengkapi pedoman teknis dan standar keamanan perangkat yang sudah ada, Peraturan Direktur Jenderal Sumber Daya dan Perangkat Pos dan Informatika 5/2021 tentang Standar Teknis Alat Telekomunikasi dan/atau Perangkat Telekomunikasi Berbasis Standar Teknologi, sekaligus untuk menjamin keamanan dari perangkat telekomunikasi yang menunjang teknologi 5G; dan
- Perlu dilakukan peninjauan kembali pada Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Hal ini diperlukan untuk memastikan relevansi UU tersebut dalam mengakomodasi peningkatan kebutuhan seiring dengan perkembangan teknologi telekomunikasi yang cepat dan dinamis, seperti dengan peningkatan kebutuhan melalui kehadiran teknologi 5G.

6.2.2 Aspek Teknis

Dengan perbandingan antara Aspek Teknis dari Strategi Keamanan Siber Nasional oleh BSSN dan pemikiran Yeoh (2022) Tingkat Keberhasilan Kritis dalam Aspek Organisasi dan Infrastruktur, berikut merupakan rekomendasi strategi keamanan siber nasional untuk mengatasi ancaman siber dengan kehadiran teknologi 5G dari Aspek Teknis:

- Perlu disusun skema pengawasan bagi penyelenggaraan sertifikasi penyedia produk teknologi informasi dan telekomunikasi, termasuk bagi para penyedia teknologi 5G. Hal ini diperlukan untuk dapat memastikan penyelenggaraan sertifikasi diikuti dengan sebagaimana mestinya;

- Perlu dipertimbangkan pemberian sanksi bagi penyedia produk teknologi informasi dan telekomunikasi yang tidak memiliki sertifikasi. Hal ini diperlukan untuk dapat memastikan setiap penyedia produk memenuhi standar kelayakan dalam mengoperasikan produk, termasuk dalam mengoperasikan teknologi 5G;
- Perlu dikembangkan langkah-langkah atau skema besar keamanan siber teknologi 5G yang lebih kuat, termasuk menerapkan deteksi dan respons ancaman yang berpusat pada telekomunikasi, serta praktik dan kesadaran keamanan yang kuat untuk dapat memitigasi risiko ancaman siber dari teknologi ini (Blackman, 2023).
- Perlu dibuat standar keamanan siber yang lebih mendetail untuk Infrastruktur Informasi Vital. Hal ini diperlukan untuk dapat memastikan keamanan siber di infrastruktur informasi vital negara yang akan menggunakan teknologi 5G. Belum lagi mengingat teknologi 5G juga akan digunakan secara menyeluruh di Ibukota Nusantara Baru yang tentu akan memiliki infrastruktur informasi vital baru pula; dan
- Perlu dibuat laboratorium pengujian dalam negeri terkait keamanan perangkat telekomunikasi. Hal ini diperlukan untuk melengkapi laboratorium pengujian dalam negeri terkait perangkat teknologi informasi yang sudah dibangun. Dengan kelengkapan laboratorium pengujian, pemerintah tidak hanya dapat memastikan kelayakan implementasi dari perangkat, tetapi juga keamanan dari perangkat telekomunikasi, seperti perangkat baru teknologi 5G.

6.2.3 Aspek Organisasi

Dengan perbandingan antara Aspek Organisasi dari Strategi Keamanan Siber Nasional oleh BSSN dan pemikiran Yeoh (2022) Tingkat Keberhasilan Kritis dalam Aspek Organisasi dan Strategis, berikut merupakan rekomendasi strategi keamanan

siber nasional untuk mengatasi ancaman siber dengan kehadiran teknologi 5G dari Aspek Organisasi:

- Perlu disusun *roadmap* terkait target penerapan keamanan siber terukur dari implementasi teknologi 5G. Hal ini diperlukan karena pemerintah baru memiliki *roadmap* mengenai implementasi dari teknologi (*Roadmap* Nasional 5G), tetapi belum memiliki *roadmap* mengenai aspek keamanan siber dari implementasi itu sendiri. Keadaan ini tentu membutuhkan perhatian, mengingat potensi ancaman siber dengan implementasi teknologi 5G;
- Perlu dibentuk alat pengukuran kematangan dan keamanan, dan/atau katalog penilaian risiko keamanan secara mandiri oleh pemerintah terkait penggunaan teknologi. Hal ini meliputi identifikasi aset, ancaman, kerentanan, dan usaha mitigasi untuk dapat memastikan keamanan siber dalam penggunaan teknologi 5G; dan
- Perlu dilakukan evaluasi dalam sistem keamanan, sistem penyimpanan, enkripsi data dan perlindungan *server* secara menyeluruh untuk mengurangi kerentanan keamanan siber nasional terhadap serangan siber (Darisman, 2024). Dengan sistem yang aman, keamanan siber nasional juga akan menjadi lebih siap, termasuk untuk menghadapi ancaman siber dengan implementasi teknologi 5G.

6.2.4 Aspek Pengembangan Kapasitas

Dengan perbandingan antara Aspek Pengembangan Kapasitas dari Strategi Keamanan Siber Nasional oleh BSSN dan pemikiran Yeoh (2022) Tingkat Keberhasilan Kritis dalam Aspek Organisasi, Infrastruktur, dan Proses, berikut merupakan rekomendasi strategi keamanan siber nasional untuk mengatasi ancaman siber dengan kehadiran teknologi 5G dari Aspek Pengembangan Kapasitas:

- Perlu dilakukan peningkatan kualitas sumber daya manusia pengguna teknologi digital. Hal ini diperlukan karena peningkatan kuantitas pengguna internet dan sosial media di Indonesia tergolong sangat pesat, tanpa diikuti oleh peningkatan kualitas dari pengguna yang sebanding.

  Dengan peningkatan kualitas pengguna, seluruh pengguna dapat mengantisipasi ancaman siber dengan kehadiran teknologi digital, termasuk teknologi 5G, dan juga dapat menjaga keamanan siber masing-masing.

- Perlu dilakukan peningkatan pemerataan infrastruktur digital. Hal ini diperlukan karena pemerataan infrastruktur di Indonesia masih tergolong kurang, apalagi di daerah pedesaan dan pelosok.

  Dengan peningkatan pemerataan infrastruktur, seluruh pemangku kepentingan dapat memperoleh kesempatan yang sama dalam menggunakan teknologi digital, termasuk teknologi 5G.

- Perlu dibangun kesadaran terkait keamanan siber bagi seluruh pemangku kepentingan, yakni pemerintah, operator, penyedia perangkat teknologi informasi dan telekomunikasi, akademisi, hingga masyarakat umum. Hal ini karena kehadiran teknologi 5G tidak hanya menjanjikan peluang pembangunan yang baru, tetapi ancaman siber yang baru pula. Usaha yang dapat dilakukan seperti pembuatan karya (buku, selebaran informasi, *social media content*, dan lain-lain) dan kegiatan *transfer knowledge* (acara webinar atau seminar, *social media campaign, training, boot camp*, dan lain-lain) literasi digital.

  Dengan peningkatan kesadaran, seluruh pemangku kepentingan dapat mengantisipasi ancaman siber dalam penggunaan teknologi digital, termasuk teknologi 5G, dan juga dapat menjaga keamanan siber masing-masing.

6.2.5 Aspek Kerja Sama

Dengan perbandingan antara Aspek Kerja Sama dari Strategi Keamanan Siber Nasional oleh BSSN dan pemikiran Yeoh (2022) Tingkat Keberhasilan Kritis dalam Aspek Eksternal, berikut merupakan rekomendasi strategi keamanan siber nasional untuk mengatasi ancaman siber dengan kehadiran teknologi 5G dari Aspek Kerja Sama:

- Perlu dilakukan peningkatan kolaborasi dan kerja sama antara para pemangku kepentingan, yakni pemerintah, operator, penyedia perangkat teknologi informasi dan telekomunikasi, akademisi, hingga masyarakat umum dalam menumbuhkembangkan ekosistem keamanan siber yang baik, terutama untuk mengatasi ancaman siber dengan implementasi teknologi 5G; dan
- Perlu dilakukan peningkatan kolaborasi dan kerja sama antara para pemangku kepentingan, yakni pemerintah, operator, penyedia perangkat teknologi informasi dan telekomunikasi, akademisi, hingga masyarakat umum dalam meningkatkan kesadaran dan mendorong literasi keamanan siber yang baik, terutama untuk mengatasi ancaman siber dengan implementasi teknologi 5G.