BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Penelitian ini menunjukkan bahwa kerja sama keamanan siber antara Indonesia dan Inggris merupakan bentuk implementasi kerja sama bilateral yang tidak hanya berorientasi pada pertukaran kepentingan strategis, tetapi juga secara nyata diarahkan pada penguatan kapasitas nasional Indonesia di bidang keamanan siber. Melalui kerangka MoU yang mencakup sembilan area kerja sama, kedua negara berupaya menjawab tantangan meningkatnya ancaman siber seiring dengan percepatan transformasi digital di Indonesia.

Dalam teori *capacity building*, kerja sama Indonesia-Inggris dapat dipahami sebagai proses penguatan kapasitas yang berlangsung pada berbagai level, mulai dari individual, organizational, hingga environment dan strategic level, sebagaimana dikemukakan oleh Matachi (2006). Program-program yang diimplementasikan menunjukkan bahwa peningkatan kapasitas tidak dilakukan secara parsial, melainkan melalui pendekatan komprehensif yang mengombinasikan pelatihan teknis, pertukaran informasi, peningkatan kesadaran publik, serta latihan bersama berskala internasional.

Pada level *individual*, kegiatan *Threat Hunting* dan DCM IV menjadi contoh konkret peningkatan kapasitas sumber daya manusia keamanan siber Indonesia. Melalui pelatihan berbasis simulasi nyata yang didukung oleh BAE Systems dan difasilitasi oleh Inggris, para peserta dari BSSN memperoleh peningkatan keterampilan teknis, pengetahuan operasional, serta kemampuan analitis dalam mendeteksi dan memitigasi ancaman siber secara proaktif. Program ini sejalan dengan pandangan Milèn (2001) bahwa meningkatkan kapasitas yang telah ada lebih efisien dibandingkan membangun kapasitas dari awal. Threat hunting juga secara langsung memperkuat kemampuan cybersecurity dalam aspek CIA Triad (*confidentiality, integrity, dan availability*), karena meningkatkan deteksi dini serta respons terhadap ancaman siber yang kompleks dan dinamis.

Pada level *organizational*, pertukaran informasi ancaman siber melalui Shadowserver Foundation memperkuat kapasitas kelembagaan BSSN sebagai institusi yang bertanggung jawab atas keamanan siber nasional. Informasi berupa laporan strategis seperti *Indonesia Country Threat Report* maupun data operasional terkait *potential compromise* menunjukkan adanya alur intelijen siber yang mencakup deteksi, analisis, penyampaian informasi, hingga mitigasi. Dalam konteks ini, *Shadowserver* berperan sebagai penyedia intelijen siber yang dapat ditindaklanjuti, sementara BSSN berfungsi sebagai institusi nasional yang mengolah dan memanfaatkan intelijen tersebut. Kerja sama ini mencerminkan fungsi kontra intelijen siber, sekaligus menunjukkan bahwa capacity building pada level organisasi tidak hanya berkaitan dengan peningkatan SDM, tetapi juga dengan penguatan sistem, prosedur, dan mekanisme respons nasional. Namun demikian, kendala teknis seperti perbedaan format data juga memperlihatkan bahwa peningkatan kapasitas memerlukan penyelarasan standar dan interoperabilitas sistem agar hasil kerja sama dapat dioptimalkan.

Pada level *environment*, peningkatan kesadaran keamanan siber masyarakat melalui media seperti Podcast #JelajahRuangSiber mencerminkan upaya membangun ekosistem sosial dan budaya yang mendukung keamanan siber. Program ini menunjukkan bahwa keamanan siber tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh perilaku dan kesadaran pengguna. Meskipun dampaknya masih terbatas dari sisi jangkauan audiens, inisiatif ini tetap relevan sebagai bagian dari upaya membentuk budaya sadar keamanan siber. Temuan ini menegaskan bahwa capacity building pada level environment memerlukan pendekatan yang lebih luas, berkelanjutan, dan terintegrasi dengan sistem pendidikan serta kampanye publik agar mampu memberikan dampak yang lebih signifikan terhadap ketahanan siber nasional.

Dari perspektif *cybersecurity*, seluruh program kerja sama Indonesia–Inggris secara umum mendukung penguatan tiga pilar utama keamanan siber, yaitu pencegahan, deteksi, dan respons. Pertukaran intelijen siber memperkuat deteksi dini, pelatihan threat hunting meningkatkan kemampuan mitigasi, sementara latihan DCM IV menguji kesiapsiagaan dan respons institusional.

Dengan demikian, kerja sama ini tidak hanya meningkatkan kapasitas teknis, tetapi juga memperkuat ketahanan siber nasional secara lebih menyeluruh.

Dalam konteks kerja sama bilateral, temuan penelitian ini menunjukkan bahwa kerja sama keamanan siber Indonesia–Inggris dilandasi oleh prinsip saling membutuhkan. Indonesia memperoleh akses terhadap pengetahuan, pengalaman, dan praktik terbaik yang belum sepenuhnya dimiliki secara domestik, sementara Inggris memperkuat posisinya sebagai mitra strategis dalam pengembangan kapasitas keamanan siber di kawasan Indo-Pasifik. Namun demikian, penelitian ini juga menegaskan adanya tantangan penting, terutama terkait kehati-hatian dalam menyampaikan kebutuhan nasional, selektivitas dalam menerima bantuan eksternal, serta upaya memastikan agar seluruh bentuk kerja sama tetap sejalan dengan kebijakan dan kepentingan strategis Indonesia.

Secara keseluruhan, penelitian ini menyimpulkan bahwa implementasi kerja sama keamanan siber Indonesia–Inggris telah memberikan kontribusi nyata terhadap peningkatan kapasitas keamanan siber Indonesia pada berbagai level. Program-program seperti pertukaran informasi *Shadowserver*, *Threat Hunting*, *Defence Cyber Marvel* IV, serta inisiatif peningkatan kesadaran siber menunjukkan bahwa *capacity building* dalam bidang keamanan siber merupakan proses jangka panjang yang membutuhkan kombinasi antara dukungan eksternal dan penguatan kapasitas internal. Keberlanjutan dan efektivitas kerja sama ini sangat bergantung pada kemampuan Indonesia, khususnya BSSN, dalam mengelola kerja sama internasional secara strategis, memastikan alih pengetahuan yang berkelanjutan, serta menjaga kemandirian nasional dalam menghadapi ancaman siber yang semakin kompleks.

6.2 Saran Akademis dan Saran Praktis

Untuk saran akademis bagi peneliti selanjutnya yang tertarik pada topik serupa, disarankan untuk melakukan penelitian lanjutan yang bersifat evaluatif untuk mengukur efektivitas dan dampak jangka panjang dari program-program kerja sama ini. Penelitian tersebut dapat melibatkan survei kepada para alumni pelatihan dan analisis statistik mengenai insiden siber sebelum dan sesudah

program, untuk mengukur tingkat efektifitas pengembangan kapasitas yang diukur. Selain itu, dapat juga melakukan penelitian komparatif yang membandingkan model kerja sama keamanan siber Indonesia-Inggris dengan model kerja sama Indonesia bersama negara lain (misalnya Amerika Serikat atau Australia) dapat memberikan wawasan yang lebih mengenai strategi diplomasi siber Indonesia.

Yang kedua yaitu saran praktis kepada Pemerintah Indonesia, khususnya Badan Siber dan Sandi Negara (BSSN), disarankan beberapa hal. Pertama, inisiatif seperti mengubah Kelas Siber IKM menjadi format *e-module* yang dapat diakses secara massal adalah langkah yang tepat dan perlu dititu untuk program lainnya yang menyasar masyarakat luas. Perlu dikembangkan model *mentoring* agar para ahli yang telah dilatih dapat menyebarkan pengetahuannya secara lebih luas di dalam negeri. Kedua, untuk mengatasi masalah mendasar terkait rendahnya literasi digital, BSSN perlu memperkuat kolaborasi dengan Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi untuk membuat kurikulum dasar keamanan siber sejak dini di tingkat pendidikan formal, yang dapat mencontoh program *CyberFirst* di Inggris. Ketiga, sambil terus menyerap pengetahuan dari mitra internasional, pemerintah perlu merumuskan kebijakan yang lebih kuat untuk mendorong pertumbuhan keamanan siber dalam negeri agar dapat mengurangi ketergantungan pada teknologi dan tenaga ahli asing di masa depan.