

BAB IV

PENUTUP

4.1 Kesimpulan

Cyberspace merupakan hal yang perlu diperhatikan dalam dunia internasional, hal ini dikarenakan *cyberspace* menghadirkan membuat lahirnya kejahatan-kejahatan transnasional baru seperti *cybercrime*, *cyber attack*, *cyber espionage*, hingga *cyberterrorism*. Penyalahgunaan *cyberspace* perlu merupakan kejahatan yang sangat sulit untuk dihilangkan, semakin meningkatnya pengguna *cyberspace* maka semakin juga meningkatnya penyalahgunaan *cyberspace*. Ancaman siber saat ini sangat berpotensi untuk merusak pertahanan negara, Dalam ranah hubungan internasional saat ini negara negara didunia telah menganggap kejahatan yang lahir karena *cyberspace* sebagai ancaman nasional maupun internasional.

Australia saat ini merupakan salah satu negara yang sangat fokus dalam menanggapi ancaman siber, Australia telah mengalami berbagai macam serangan siber, sejak tahun 2011 serangan siber di Australia terus meningkat. Lebih dari 5000 insiden serangan siber yang direspon oleh *Australian Signals Directorate (ASD)* sejak tahun 2011 hingga 2017. Australia membentuk badan pertahanan siber negara dalam memperkuat *cybersecuritynya*, bagi Australia *cyberspace* merupakan prioritas

kebijakan luar negeri yang membuat Australia akan terlibat dalam keamanan *cyberspace* dalam nasional maupun internasional.

Australia membuat kebijakan strategi yaitu *Australia's International Cyber Engagement Strategy 2017*, strategi tersebut merupakan strategi dalam meningkatkan *cybersecurity* dan peluang dalam *cyberspace*. Didasari dengan buku putih kebijakan luar negeri Australia, Australia akan menegaskan kembali pemahaman akan pentingnya masalah *cyber* yang signifikan dan semakin penting bagi kebijakan luar negeri Australia. Dalam *Australia's International Cyber Engagement Strategy 2017* menjelaskan bahwa untuk meningkatkan *cybersecurity* nasional juga penting dalam meningkatkan *cybersecurity* mitra internasional, hal ini dikarenakan sifat global internet yang berarti bahwa ancaman *cyber* yang muncul dimana saja akan berdampak pada Australia. Pentingnya mitra internasional dalam menanggapi masalah siber membuat Australia melakukan diplomasi siber dengan mitra internasional, Australia melakukan diplomasi siber dengan Indonesia melalui *Cyber Cooperation Program*. Maka dari itu penelitian ini membahas analisis upaya Australia dalam penguatan *cybersecurity* melalui *Cyber Cooperation Program* dengan Indonesia.

Penelitian ini menggunakan konsep diplomasi siber dari Patryk Pawlak yaitu Peningkatan kapasitas menjadi pilar utama diplomasi siber dengan tujuan yang jelas yaitu memperkuat kerangka hukum nasional, menciptakan dan memperkuat tanggapan aksi, pelatihan, dan peningkatan kesadaran. Diplomasi siber Australia dengan Indonesia menggunakan strategi peningkatan kapasitas untuk saling memperkuat

cybersecurity kedua pihak, Australia melakukan peningkatan kapasitas untuk Indonesia dengan membuat program kerjasama peningkatan kesadaran dan pelatihan.

Pada peningkatan kesadaran, Australia melakukan *Cyber Policy Dialogue* dengan Indonesia yang dimana program *Cyber Policy Dialogue* ini dilakukan sebanyak 3 kali. *Cyber Policy Dialogue* merupakan upaya Australia dalam meningkatkan kesadaran dan kapasitas Indonesia dalam meningkatkan *cybersecurity* dan peluang siber. Dalam *Cyber Policy Dialogue I* dilakukan dialog percakapan mengenai isu-isu siber, ancaman siber, kebijakan dan strategi, serta pentingnya perkembangan siber regional dan internasional. Lalu dalam *Cyber Policy Dialogue II* Australia dan Indonesia membahas masing-masing kepentingan dan kepentingan bersama mereka dalam internet yang terbuka, bebas dan aman yang mendukung sistem keamanan negara dalam ranah siber dan pertumbuhan ekonomi digital, *Cyber Policy Dialogue II* menghasilkan MoU kesepakatan untuk melanjutkan kerjasama dalam urusan siber. *Cyber Policy Dialogue III* dilakukan setelah adanya *Cyber Bootcamp*, pada dialog ini Australia menjelaskan akan pentingnya mekanisme siber internasional dan regional dalam membangun ruang siber yang aman. *Cyber Policy Dialogue* ini berperan penting dalam saling membangun kesadaran dan kapasitas Australia dan Indonesia.

Pada pelatihan Australia melakukan pelatihan terhadap Indonesia melalui *Cyber Bootcamp*, Program *Cyber Bootcamp* dirancang dalam menyatukan keterampilan dan keahlian yang saling melengkapi dari seluruh pemerintah, akademisi dan sektor swasta untuk memberikan program pelatihan yang komprehensif, holistik

dan inovatif kepada Indonesia. *Cyber Bootcamp* merupakan program intensif selama dua minggu di Australia dimana dalam kegiatan ini perwakilan Indonesia mengikuti pelatihan, *workshop*, kunjungan lokasi industri, dan dialog dengan lembaga pemerintah Australia. Dengan adanya program ini Australia berharap Indonesia dapat mengimplementasikan pelatihan dan pembelajaran dalam menangani isu-isu siber nasional yang akan berkontribusi untuk *cybersecurity* yang kuat bagi kawasan regional.

Sehingga dapat disimpulkan bahwa upaya Australia dalam meningkatkan *cybersecurity* melalui diplomasi siber dengan Indonesia merupakan langkah yang sangat penting, hal ini demikian karena Indonesia merupakan mitra internasional yang cocok dalam penerapan *Australia's International Cyber Engagement Strategy 2017* untuk meningkatkan *cybersecurity* nasional maupun *regional* dan peluang siber lainnya.

4.2 Saran

Saran yang dapat penulis sampaikan untuk penelitian selanjutnya adalah penelitian ini hanya terbatas pada tahun 2017 - 2020 sesuai dengan awal adanya dialog antara Australia dan Indonesia hingga durasi awal kesepakatan MoU Australia Indonesia. Penulis menyarankan untuk penelitian selanjutnya dapat memperluas jangkauan tahun-tahun selanjutnya karena MoU Australia dan Indonesia dalam kerjasama siber kedua negara sepakat untuk melanjutkan kerjasama.