BAB VI
KESIMPULAN & SARAN

6.1 Kesimpulan

Penggunaan dan tingkat ketergantungan penggunaan teknologi komunikasi dan informasi di suatu negara berbanding lurus dengan potensi risiko dan ancaman terhadap kepentingan nasional suatu bangsa. Indonesia saat ini sedang dalam tahap awal mengembangkan peraturan dan strategi keamanan siber nasional yang komprehensif. Meski pemerintah telah mengeluarkan beberapa peraturan terkait, peraturan tersebut nyatanya belum menghubungkan semua instansi pemerintah dan komunitas resmi lainnya dengan pihak swasta yang terlibat dalam keamanan siber di Indonesia. Penguatan kebijakan berupa undang-undang diperlukan untuk memperjelas, memperkuat domain siber sebagai bagian dari domain kedaulatan Indonesia dan memberikan landasan hukum yang dapat menjangkau tingkat ancaman siber yang kompleks, dinamis, dan multidomain. Hukum harus mampu mengkolaborasikan kewenangan, kekuatan dan seluruh pemangku kepentingan terkait mengingat penanganan sifat ancaman siber yang sangat kompleks, dinamis dan multidomain terhadap keamanan, pertahanan, dan kepentingan nasional Indonesia. Selain itu, pemerintah harus segera menyelaraskan peraturan perundang-undangan yang terkait dengan pertahanan, keamanan, dan kepentingan nasional, seperti ketentuan mengenai infrastruktur/objek vital negara.

Dalam hal penanganan tidak dapat dipungkiri Amerika jauh lebih sukses daripada Indonesia dan hal tersebut bukanlah suatu kejutan dikarenakan hal tersebut sudah selayaknya terjadi. Amerika Serikat dilihat dari sudut apapun merupakan negara yang lebih superior, termasuk dalam ruang siber. Memahami ini, LoI antara Indonesia dan Amerika Serikat pun terealisasi, bertujuan untuk memberikan kerangka kerja guna mendorong kerja sama dan peningkatan kapasitas di ruang siber antara kedua negara. Ini memiliki ruang lingkup kerja sama di beberapa bidang, termasuk diskusi tentang pengembangan strategi siber nasional, kemampuan manajemen insiden nasional, kapasitas dan kerjasama kejahatan siber, kemitraan multi-stakeholder, promosi kesadaran keamanan siber, dan kerja sama di tempat-tempat regional terkait lainnya yang sesuai. Keseriusan Indonesia dalam menangani ancaman siber mulai terlihat serius saat Pemerintah Indonesia

membentuk Badan Siber dan Sandi Negara (BSSN) melalui Peraturan Presiden Nomor 53 Tahun 2017. Pembentukan badan ini merupakan upaya pemerintah untuk menjaga keamanan siber Indonesia sebagai salah satu bidang Pemerintah yang perlu didorong dan diperkuat untuk meningkatkan pertumbuhan ekonomi nasional dan mewujudkan ketahanan nasional. Dikarenakan penanganan siber di Indonesia sangatlah jauh jika dibandingkan dengan apa yang dilakukan Amerika seperti mulai dari lembaga penanganan, mekanisme kerja dan sampai kepada payung hukum yang ada. Jelas Amerika sebagai negara maju dan juga yang lebih dulu memahami pentingnya keamanan siber memiliki sistem yang lebih muktahir dibandingkan Indonesia sebagai negara berkembang, jadi penting bagi Indonesia untuk terus berkaca dan mencoba mempelajari apa yang diimplementasikan di Amerika.

Tepat dengan terbentuknya BSSN, Indonesia juga mulai melakukan banyak kerjasama dengan berbagai negara seperti Inggris, Australia, Amerika Serikat, China dll untuk membahas isu siber. Setelah melakukan wawancara dengan seorang diplomat kemlu, Dengan diterbitkannya Letter of Intent (LoI) yang berisikan kerjasama dalam ruang siber antara Amerika Serikat dengan Indonesia diharapkan dapat membantu perkembangan penanganan isu siber di Indonesia, dan aktivitas yang diharapkan dalam kerjasama ini adalah *Transfer of Knowledge, Transfer of Technology* dan Pertukaran data/informasi sensitive. Tak hanya itu pendekatan dalam memahami kemanan siber di dunia juga terbagi kedalam dua hal yaitu *Sovereignty as a Rule* dan *Sovereignty as a Principal.* Dari ketiga MoU dan LoI tersebut, kita dapat melihat dengan jelas perbedaan yang signifikan dalam pendekatan kedaulatan yang dicanangkan oleh negara-negara tersebut. Dalam MoU antara Indonesia dengan AS, dan antara Indonesia dengan Inggris, misalnya, kedua negara tidak secara khusus menyebut soal kedaulatan dan bahkan masalah lain terkait kedaulatan. Di sini, kita dapat menyimpulkan secara eksplisit bahwa baik AS maupun Inggris mendukung *Sovereignty as a Principal*. Sebaliknya, LoI antara Indonesia dan China dengan jelas menyoroti pentingnya kedua negara untuk saling menghormati kedaulatan satu sama lain di dunia maya dan yurisdiksi. Dari LoI ini kita dapat melihat pendekatan China pada kedaulatan yang tampaknya mendukung posisi *Sovereignty as a Rule*. Indonesia juga cenderung mendukung posisi kedaulatan sebagai aturan yang menjunjung tinggi prinsip penghormatan terhadap

kedaulatan negara di dunia maya, sebagaimana diatur dalam MoU atau LoI tentang kerja sama keamanan siber antara Indonesia dengan negara-negara lain di luar AS dan Inggris.

Memiliki hubungan kerjasama siber dengan negara kuat, tentunya juga akan memperkuat dan meningkatkan kapasitas siber Indonesia. Hal ini juga menjadi strategi Indonesia untuk mendapatkan akses teknologi siber terkini dari AS melalui *experience and knowledge sharing* sebagai salah satu area kerjasama. Sejauh ini kerjasama yang paling sering dilaksanakan adalah berbagi informasi dan juga pelatihan. Terkait cyberterrorism yang juga menjadi cakupan kerjasama, BSSN berkolaborasi bersama dengan Badan Nasional Penanggulangan Terorisme (BNPT). Sebagai informasi, kerjasama RI-AS di bidang siber juga dapat menjadi acuan untuk lintas kooperasi antar instansi pemerintah. Antara BSSN dan Kedutaan AS telah memiliki semacam mekanisme *information sharing* terkait ancaman siber yang ada dan yang akan ada, kemudian melaksanakan program *capacity building*, dan strategic dialogue di bidang keamanan siber yang melibatkan entitas keamanan siber di masing-masing negara. Dimana sebagai contoh terdapat banyak pelatihan baik melalui webinar dan intensive training yang salah satu nya terdapat di BINUS guna meningkatkan kapasitas, AS juga pernah membantu RI pada saat website resmi KPU dibajak dengan kontek *Information Sharing*, Sedangkan untuk perkara Cyberterrorism, AS telah banyak melakukan pertemuan dan juga *transfer of knowledg*e guna meningkatkan pemahaman Indonesia. Setelah semua analisa yang telah dilakukan, penulis dapat menarik kesimpulan bahwa implementasi kerjasama ruang siber antara Indonesia dan Amerika Serikat untuk meningkatkan kapasitas penanganan *cyberterrorism* di Indonesia dapat dinilai kurang maksimal. Pendapat yang diberikan oleh penulis pun didukung oleh Direktorat Strategi Keamanan dan Siber BSSN dimana dikatakan bahwa signifikansi dari implementasi kerjasama yang dilakukan belumlah semaksimal yang diharapkan. Program *capacity building* dan *information sharing* yang dinilai sebagai aspek terepenting dalam kerjasama ini belum dapat dijalankan seperti yang dihirapkan karena BSSN masih terkendala masalah komunikasi dengan pihak Amerika Serikat atau khususnya FBI. Masalah komunikasi ini muncul dikarenakan BSSN untuk berkomunikasi dengan pihak AS harus melalui kedutaan terlebih dahulu sebelum akhirnya disampaikan kepada

pihak terkait, jalur komunikasi ini dinilai tidak efektif dikarenakan membutuhkan waktu lama untuk terealisasi yang menyebabkan baik program *capacity building* maupun *information sharing* terlibat kendala dan pada akhirnya berimbas pada implementasi penanganan ancaman *cyberterrorism*. Penulis beranggapan bahwa seharusnya Indonesia dan AS harusnya memiliki mekanisme komunikasi yang cepat dan secara langsung seperti halnya dalam kerjasama siber yang dilakukan oleh Jepang dan AS dimana komunikasi bukanlah sebuah kendala.

Pada intinya, kerjasama yang terikat oleh LoI ini penting bagi perkembangan siber Indonesia sebagai negara yang sedang menata sistem keamanan sibernya. Dengan mempelajari sistem keamanan siber dari negara maju seperti AS, Indonesia dapat mengambil banyak pelajaran. Meskipun belum terlihat besar kecilnya kontribusi kerjasama ini, BSSN meyakini bahwa pada akhirnya nanti hasil dari bentuk kerjasama akan selalu berada pada upaya untuk menghadirkan ruang siber yang aman dan stabil. Hal tersebut menjadi tugas BSSN sebagai leading sektor urusan keamanan siber Indonesia dan elaborator entitas terkait siber lainnya. Selain itu yang patut diapresiasi adalah penanganan ancaman cyberterrorism yang ditangani oleh BSSN dan BNPT sudah dapat terbilang efektif dikarenakan dapat secara konkrit mendeteksi ancaman yang ada, hal ini tentunya tidak dapat dipisahkan dari seringnya BNPT melakukan komunikasi langsung dengan pihak Amerika Serikat.

6.2 Saran

Dalam konteks hukum, pengembangan keamanan siber berarti ketersediaan dokumen kebijakan keamanan sebagai dokumen standar yang dirujuk orang ketika menjalankan seluruh proses terkait keamanan informasi. Pengembangan dan penguatan kebijakan keamanan siber di Indonesia harus diintegrasikan dengan strategi nasional untuk membangun ekosistem keamanan siber nasional yang telah disiapkan oleh pemerintah. Strategi nasional tersebut meliputi upaya hukum dan upaya teknis, seperti standar operasional penataan organisasi, lembaga manajemen keamanan siber, peningkatan kapasitas sumber daya manusia dan upaya peningkatan kerjasama internasional. Sangat penting untuk membangun dan memperkuat landasan hukum internal atau legislasi nasional Indonesia terlebih dahulu sebelum membangun politik luar negeri Indonesia tentang keamanan siber

di tingkat internasional. Seperti yang telah dijelaskan sebelumnya mengenai kondisi keamanan siber di Indonesia, beberapa tantangan utama bagi perkembangan industri keamanan siber di Indonesia antara lain rendahnya kesadaran masyarakat akan isu siber, budaya insiden keamanan siber yang tidak terlaporkan, karena organisasi yang terkena dampak. lebih memilih kerahasiaan daripada risiko tantangan hukum dan kerusakan reputasi, kurangnya peralatan dan teknologi standar untuk memperkuat keamanan siber, relatif rendahnya jumlah praktisi keamanan siber profesional dan skala peningkatan keterampilan yang diperlukan, kualitas yang bervariasi dari beberapa infrastruktur telekomunikasi dan TIK , dan kecepatan internet yang rendah, dan anggaran TIK yang terbatas baik di sektor swasta maupun pemerintah.

Keberadaan inisiasi kerjasama ruang siber antara Amerika Serikat dan Indonesia merupakan hal yang seharusnya menjadi jawaban dari permasalah keamanan siber yang dialami. Namun setelah penandatanganan kerjasama tersebut yaitu pada tahun 2018 sampai sekarang yaitu 2022 yang berarti kerjasama sudah terjalin selama 3 tahun. Melihat fakta yang terjadi selama 4 tahun tersebut, tidak ada perkembangan besar yang signifikan terjadi terhadap keamanan siber Indonesia yang seharusnya menjadi tujuan kerjasama. Realita yang terjadi adalah keamanan siber Indonesia tidak jauh berkembang setelah 4 tahun sejak penandatanganan kerjasama. Penulis memberikan menarik kseimpulan bahwasanya kerjasama ruang siber antara Indonesia dan Amerika serikat belum mencapai potensi yang seharusnya, dan hal ini pun telah diakui oleh BSSN sebagai aktor utama dalam kerjasama ini. Kendati sumber daya siber yang dimiliki AS jauh lebih maju dari pada Indonesia, dengan kerjasama diharapkan terjadi peningkatan dari sisi Indonesia sebagai negara berkembang dalam penanganan siber dikarenakan dapat belajar dari AS dan dapat terjadi. Telah diberutahukan bahwa BSSN mengalami masalah dalam menhubungi pihak Amerika Serikat guna melakukan kerjasama dikarenakan BSSN harus melalui kedutaan terlebih dahulu sebelum akhirnya disampaikan kepada pihak AS. Hal seperti ini seharusnya tidaklah terjadi dikarenakan komunikasi merupakan aspek penting dalam sebuah kerja sama, seharusnya Indonesia dan AS memiliki program konkrit seperti hal nya yang dimiliki oleh AS dan Jepang dimana program tersebut membuat kedua negara

saling terintegrasi satu sama lainnya. Untuk persoalan *capacity building*, BSSN sudah melakukan pekerjaan yang cukup tepat dengan beberapa kali melakukan pelatihan tetapi *information sharing* lah yang menjadi masalah karena seperti yang dibahas sebelumnya BSSN masih belum dapat dengan mudah menghubungi pihak AS. Dikarenakan kedua hal tersebut sangat berpengaruh penting dengan penanganan *cyberterrorism*, peningkatan intensitas kerjasama harus segera dilaksanakan karena BNPT sebagai badan penanganan terorisme sudah melakukan pekerjaan dengan efektif dan jika kedua hal tersebut dapat ditingkatkan, perkembangan akan terlihat sangat signifikan.