Diskusi Ilmiah Komunitas Hubungan Internasional
Vol. 4 No. 4, Desember 2024, Hal 134-146
ISSN 2828-1853 (Online)

Pengembangan Keamanan Siber Indonesia melalui ASEAN Regional Forum (ARF)

Visvanathan Gabriel Matrix Baruna Vivekananda[1)], A.A. Bagus Surya Widya Nugraha[2)], Penny Kurnia Putri[3)]

[1,2,3)] Hubungan Internasional/Fakultas Ilmu Sosial dan Ilmu Politik/Universitas Udayana.

Abstrak

Ekspansi yang pesat dalam dunia digital telah mengantarkan kita ke era baru keterhubungan global, menawarkan peluang tanpa batas sekaligus menghadirkan tantangan keamanan yang signifikan. Penelitian ini menyelidiki perjalanan Indonesia dalam meningkatkan postur keamanan sibernya melalui ASEAN Regional Forum (ARF). Di dunia di mana ancaman siber melampaui batas-batas negara dan berdampak pada aktor negara dan non-negara, Indonesia mengakui pentingnya menjaga keamanan nasionalnya di dunia maya berdasarkan *White Defence Paper*, yang mengakui bahwa *cyberspace* menjadi domain kelima dalam dunia perang. Berdasarkan data sekunder, ditemukan hasil analisis bahwa momentum kepemimpinan Indonesia dalam ARF berpotensi meningkatkan pengembangan keamanan siber negara. Hal ini didasarkan atas berbagai agenda dan kemitraan yang berada dalam ARF, berdampak secara langsung maupun tidak langsung terhadap pengembangan keamanan siber Indonesia. Pengembangan keamanan siber yang dihasilkan melalui ARF terhadap keamanan nasional Indonesia berdasarkan klasifikasi Choucri dalam keamanan siber berdampak terhadap dua kategori ancaman siber berdasarkan Choucri. Hal ini ditunjukkan dalam 1) Ancaman siber terhadap infrastruktur yang didapatkan dari program *Cyber and Critical Tech Cooperation Program & ASEAN Cyber Capacity Development Project* dan 2) Terorisme siber yang didapatkan dari program *ASEAN Cyber Capability and Capacity Development Project*. Indonesia selama kepemimpinan dalam ARF mampu memanfaatkan *platform* ARF dalam mendukung pengembangan keamanan siber negara.

Kata-kunci: keamanan siber, keamanan nasional, ASEAN Regional Forum

Abstract

The rapid expansion of the digital world has ushered in a new era of global connectedness, offering limitless opportunities while presenting significant security challenges. This research investigates Indonesia's journey in improving its cybersecurity posture through the ASEAN Regional Forum (ARF). In a world where cyber threats transcend national boundaries and impact both state and non-state actors, Indonesia recognises the importance of maintaining its national security in cyberspace based on the White Defence Paper, which acknowledges that cyberspace is becoming the fifth domain of war. Based on secondary data, it is analysed that the momentum of Indonesia's leadership in the ARF has the potential to increase the country's cybersecurity development. This is based on various agendas and partnerships within the ARF, which have direct and

indirect impacts on Indonesia's cybersecurity development. The development of cybersecurity generated through the ARF on Indonesia's national security in cybersecurity has an impact on two categories of cyber threats based on Choucri. This is shown in 1) Cyber threats to infrastructure obtained from the Cyber and Critical Tech Cooperation Programme & ASEAN Cyber Capacity Development Project and 2) Cyber terrorism obtained from the ASEAN Cyber Capability and Capacity Development Project programme. Indonesia has been able to utilise the ARF platform to enhance the development of the country's cybersecurity during its leadership in the ARF.

***Keywords**: cyber security, national security, ASEAN Regional Forum*

Kontak Penulis
Visvanathan Gabriel Matrix Baruna Vivekananda
Hubungan Internasional, Fakultas Ilmu Sosial & Ilmu Politik, Universitas Udayana
Jl. Wirasatya VI No.105, 80224
Telp: 082144135958 Fax: -
E-mail : barunavivekananda@student.unud.ac.id

PENDAHULUAN

Latar Belakang Masalah

Pengaruh besar dari globalisasi mendorong perubahan besar dalam dinamika di Kawasan Asia Tenggara, ASEAN mulai menjalin kemitraan akibat efek globalisasi yang menjadi konsekuensi nyata bagi ASEAN, salah satunya dalam teknologi informasi dan komunikasi (Lesmana et al., 2017). Keamanan siber menjadi permasalahan yang krusial dalam ranah hubungan internasional di tengah perkembangan teknologi melalui internet dan teknologi komunikasi lainnya (Kshetri, 2013, Nye, 2010). Meningkatnya ancaman siber menyebabkan keresahan global yang berpotensi mengganggu pertumbuhan ekonomi, stabilitas politik, dan keamanan nasional (Gartzke & Lindsay, 2020). Menurut Center for Strategic and International Studies, kejahatan siber mengakibatkan kerugian ekonomi sebesar $1,5 milyar setiap tahunnya (Lewis, 2018). Berbagai kemudahan dan canggihnya kemajuan dalam teknologi informasi dan komunikasi (TIK), menghadirkan sisi positif dan juga negatif dalam keamanan siber (Putri et al., 2017).

Wilayah Asia Tenggara pun tidak terhindarkan dari ancaman Serangan siber berprofil tinggi. Pada tahun 2017, *ransomware WannaCry* mengakibatkan terinfeksi ribuan computer di Indonesia (Mashita, 2018). Serangan siber pada dasarnya memiliki berbagai bentuk, ekspresi, pemikiran yang dilakukan sengaja atau tidak sengaja oleh seluruh pihak dengan berbagai motif dan tujuan (Maskun, 2021, hal. 134). Kegiatan ini pun dapat mengancam kedaulatan suatu negara, keutuhan wilayah, dan keselamatan suatu bangsa karena berpotensi mengancam objek vital dan non-vital negara. Akhir tahun 2017 menunjukkan terdapat sekitar 100 juta orang yang dikategorikan sebagai pengguna internet di Indonesia (Suwidharma et al., 2023 dalam Internet World State, 2019).

Menurut National *Cyber Security Index* (NCSI), COVID-19 menjadi momentum kejahatan siber di Indonesia, salah satunya pemberitahuan COVID-19 pemerintah Indonesia sebanyak 18,000 kasus dengan sejumlah 60-70% berkaitan dengan isu COVID-19 (Amarullah et.al., 2021). Tren peningkatan ancaman siber dapat dilihat pada **Tabel 1**. Serangan siber umumnya menyasar sistem elektronik yang bergantung pada teknologi dan jaringan yang dapat menjadi ancaman terhadap objek vital negara. Maka, diperlukan keamanan siber yang mumpuni di Indonesia dan *cyberspace* menjadi domain kelima yang sebagai medan perang (Kementerian Pertahanan RI, 2015).

Grafik 1. Trafik Anomali Internet Indonesia Tahun 2018-2022

Sumber: Diolah dari berbagai sumber

Sebagai satu *economic powerhouse*, Indonesia memiliki peran yang krusial dalam menjaga keamanan siber di wilayahnya (Rahman & Anwar, 2020). Indonesia tergabung dan menjadi salah satu *founding father* dalam *ASEAN Regional Forum* (ARF), isu keamanan siber sejak 2012 mengadopsi "*Statement on Cooperation in Ensuring Cyber Security*". ARF mendorong negara anggota dalam berpartisipasi dan implementasi undang-undang keamanan siber sesuai kondisi nasional negara. *Platform* ini menjadi ideal bagi Indonesia dalam meningkatkan keamanan siber negara mengingat Indonesia memegang posisi yang strategis sebagai kepemimpinan ARF periode 2023.

Pada tahun 2023, momentum Indonesia dalam kepemimpinan ASEAN turut berkontribusi

terhadap kemanan siber Indonesia melalui kemitraan maupun agenda dalam ARF, salah satunya adalah *ARF Defence Officials Dialogue* (ARF DOD) di Dili, Timor Leste, yang diwakilkan oleh Dirjen Strahan Mayjen TNI, Bambang Trisnohadi, sebagai ketua Delegasi RI. Pertemuan ini membahas agenda *blue economy*, kerja sama pasca COVID-19, serta pemanasan global. Kegiatan ini menunjukkan ARF sebagai *platform* yang ideal bagi Indonesia dalam meningkatkan keamanan siber melalui *framework* yang berada dalam ARF

Tinjauan Pustaka

Penelitian ini telah mengikuti perkembangan yang membahas tema serupa dan memperkaya topik keamanan siber Indonesia dan *ASEAN Regional Forum*. Penelitian ini mengkaji tiga literatur yang relevan untuk dijadikan referensi dalam tulisan.

Penelitian ini meninjau literatur pertama yang berjudul "*Cyber Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with It* karya Maskun dkk. (2021) menjelaskan tata kelola kemanan siber *Association of Southeast Asian Nations* (ASEAN) yang berargumen tantangan keamanan siber serta tata kelola dalam melindungi kepentingan nasional dalam ruang siber. *Cyber Security Governance* dan tata Kelola siber telah menjadi isu utama dalam ASEAN yang menghasilkan kerangka keamanan siber. Maka, dibutuhkan kooperasi regional antara anggota ASEAN dalam menangani ancaman siber.

Literatur kedua dari Kristiani Putri (2021) yang berjudul "*Kerja Sama Indonesia dengan ASEAN mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime*" menganalisis kerja sama Indonesia melalui *ASEAN* dalam menanggulangi *cybercrime* yang mengancam keamanan nasional, stabilitas ekonomi, serta kesejahteraan sosial. Putri menekankan pentingnya memandang *cybercrime* sebagai isu yang krisis mengancam keamanan nasional, stabilitas ekonomi, dan kesejahteraan sosial. Ia berargumen bahwa ancaman siber telah menjadi kompleks sehingga dibutuhkan upaya kolaborasi antar negara, utamanya ASEAN dalam menyelesaikan permasalahan ini.

Selanjutnya, literatur dari Bima Yudha Wibawa Manopo dan Diah Apriani Atika Sari (2015) yang berjudul "*ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN*" membahas mengenai peran penting ARF dalam mempromosikan keamanan dan stabilitas regional, termasuk dalam ranah keamanan siber. Dalam beberapa tahun terakhir, ancaman siber berpotensi melemahkan perkembangan dan stabilitas ekonomi ASEAN. Literatur ini menekankan ASEAN untuk memperkuat kerangka institusional untuk keamanan siber, salah satunya mengembangkan *cyber security working group* dalam ARF untuk memfasilitasi pertukaran antara negara anggota dalam pengembangan pedoman dalam keamanan siber.

Berdasarkan ke-3 kajian literatur ini, peneliti berupaya menunjukkan kebaruan dalam penelitian, yang dapat ditinjau sebagai berikut. Pertama, penelitian ini menunjukkan momentum yang dimanfaatkan Indonesia dalam pengembangan keamanan sibernya melalui ARF, baik dalam kemitraan maupun program terkait keamanan siber. Kedua, peneliti menggunakan tiga konsep, yaitu *Power in International Organisations* (IOs), keamanan nasional, dan keamanan siber.

Barkin (2013) mendefinisikan *IOs* sebagai organisasi antar-pemerintah yang inklusif, berlawanan dengan NGOs dan korporasi. IOs merupakan organisasi yang didirikan berdasarkan kesepakatan antar negara. Kekuatan atau *power* suatu negara dapat bersumber dari beberapa hal dan diaplikasikan melalui cara-cara tertentu, dalam hal ini *power*

bersumber dari kekuatan strukturan antar-negara dalam suatu organisasi internasional. Lebih lanjutnya, *power* dapat diaplikasikan melalui penentuan agenda, negosiasi, pembentukan perspektif prosedur dan birokrasi. Dalam *Power in IOs*, terdapat empat kategori *power* yang diaplikasikan suatu negara.

Negosiasi merupakan salah satu *power* yang digunakan negara, dalam hal ini negara dengan *power* yang lebih kuat cenderung memenangkan negosiasi atau memperoleh suara dalam forum multirateral (Barkin, 2013). Kedua, penentuan agenda menjadi *power* yang diaplikasikan negara dalam forum multilateral atau agenda internaisonal lainnya. Mengindentifikasi penerapan *power* ini dapat dikatakan sulit, namun dapat mengidentifikasi penggunaan *power* melalui kemampuan negara dalam menentukan agenda apa yang akan dibahas dan tidak dibahas. Ketiga, pembentukan perspektif, negara menggunakan *power* dalam membentuk pandangan orang terhadap isu tertentu. Nye (dalam Barkin, 2013) menyebutkan hal ini sebagai "*soft-power*". Keempat, prosedur dan birokrasi, Barkin (2013) menilai bahwa negara dapat mengekspresikan *power* dalam organisasi internasinal melalui keikutsertaannya dalam menciptakan prosedur atau birokrasi yang disebut dengan *institutional power*. Pada dasarnya, negara menempatkan orang pada posisi tertentu dalam struktur birokrasi organisasi internasional yang berjalan selaras dengan kepentingannya.

Selain itu, menurut Choucri (2012), mendefinisikan keamanan nasional sebagai keamanan negara dalam empat dimensi keamanan, yaitu: eksternal, internal, keamanan lingkungan, dan keamanan siber. Choucri berargumen bahwa keempat dimensi tersebut sebagai suatu kesatuan dan keamanan negara terwujud Ketika empat dimensi tersebut terjamin. Penelitian ini berfokus dalam dimensi keamanan siber yang diartikan sebagai kemampuan negara untuk melindungi dirinya dan institusi dari ancaman, spionasi, kejahatan dan penipuan, pencurian identitas dan e-transaksi desktruktif lainnya di ranah siber.

Keamanan siber menjadi salah satu dimensi dari keamanan nasional dan dapat mengancam negara (Choucri, 2012). Keamanan siber merupakan salah satu bentuk dari ancaman asimetris atau *asymmetric threats* yang diartikan sebagai asimetri di antara dua pihak dan taktik yang digunakan oleh pihak yang lebih lemah untuk membuat kekuatan pihak yang lebih kuat tidak berarti (Mark, 2021). Lebih lanjut, Choucri mengklasifikasi beberapa bentuk ancaman siber terhadap keamanan nasional yang dibagi dalam empat jenis, yaitu: 1) *militarization of cyberspace*, 2) *cyber warfare*, 3) *cyber threats to infrastructure*, dan 4) *cyber terrorism*.

Keberadaan *cyberspace* tidak hanya mendatangkan ancaman, tetapi juga kerja sama dan inovasi institusional. Choucri percaya bahwa negara akan melakukan kerja sama dalam dua scenario. Pertama, negara ingin merai kepentingan yang tidak dapat diraih jika diperjuangkan seorang diri. Kedua, negara-negara memiliki kesamaan kondisi dan ingin menanggulangi permasalahan bersama. Selaras dengan pendapat Choucri, Ksherti (2016) menilai bahwa negara saling bersaing dan membentuk aliansi dalam mengembangkan kemampuan pertahanan siber dan Serangan siber untuk mencapai keunggulan di ranah *cyberspace*.

Keamanan siber sangat bergantung sangat bergantung pada kemampuan negara dalam melindungi *cyberspace* dan kapasitasnya dalam mengatasi ancaman siber secara kolektif maupun individu (Gijsbers & Veenendaal, 2011). Pada dasarnya, *cyberspace* atau ruang siber merupakan domain yang terintegrasi dengan aktor publik dan swasta, sipil, militer, aktor

nasional dan internasional yang beroperasi secara simultan dan saling ketergantungan.

Tujuan Penelitian

Berdasarkan rumusan masalah dan tinjauan pustaka, tujuan penelitian ini adalah menunjukkan Pengembangan keamanan siber Indonesia melalui *ASEAN Regional Forum* (ARF), utamanya signifikansi kepemimpinan Indonesia dalam ARF periode 2023.

METODE

Jenis penelitian yang diterapkan adalah kualitatif. Dalam penelitian kualitatif, terdapat data dan teori yang menjadi unit, data diperoleh diliteraturkan, diinventarisasi, kualifikasi, kemudian diuraikan dengan fakta-fakta yang ada dan disusun dalam tulisan (Neuman, 2014).

HASIL DAN PEMBAHASAN

Kondisi Keamanan Siber ASEAN dan Indonesia

ASEAN telah melihat potensi ekonomi dalam ruang digital sejak 1996, ke-7 negara anggota membahas mengenai peluang serta tantangan dalam internet (Noor, 2020). Pada tahun 2019, perekonomian Asia Tenggara mencapai $100 milyar dan 90% dari 360 juta pengguna internet terhubung melalui perangkat seluler (Google, Temasek, Bain & Company, 2019). Inisiatif ambisius dari ASEAN dalam domain dunia maya ditunjukkan dalam *ASEAN ICT Masterplan* 2020, *Masterplan on ASEAN Connectivity*, dan *ASEAN Smart Cities Network*.

Visi ASEAN dalam mewujudkan konsolidasi di ruang siber dalam struktur ASEAN di Tingkat Kementerian membahas isu keamanan siber dalam *ASEAN Regional Forum* (ARF), *ASEAN Defence Ministers' Meeting*, *ASEAN Ministerial Meeting on Transnational Crime*, *ASEAN Digital Ministers' Meeting*, dan *ASEAN Ministerial Conference on Cybersecurity*. ASEAN memiliki tiga pilar, yaitu *ASEAN Political-Security Community (APSC)*, ASEAN Economic Community (AEC), dan ASEAN Socio-Cultural Community (ASCC). Permasalahan keamanan siber bersinggungan dengan salah satu pilar ASEAN, yaitu APSC, dan ASEAN Regional Forum berada di bawah pilar tersebut. Berdasarkan *Global Security Index* pada tahun 2020, di Asia Tenggara, Singapura memegang peringkat pertama dari segi tingkat keamanan siber (Estiyovionita & Sitamala, 2022).

Indonesia sebagai salah satu *founding father* ASEAN menyadari Pembangunan nasional berawal dari kondisi regional yang aman (Khanisa & Farhana, 2018). Bagi Indonesia, *ASEAN* menjadi *cornerstone* dalam politik luar negeri Indonesia, yang ditunjukkan dalam keterlibatan dalam *ASEAN Regional Forum* dalam isu keamanan siber. Dalam isu ini, Indonesia menerbitkan UU Nomor 36 Tahun 1999 tentang Telekomunikasi dan UU Nomor 11 Tahun 2008 Informasi dan Transaksi yang menjadi landasan dalam merumuskan kebijakan dan regulasi terkait keamanan informasi (Putri, 2021). Kebijakan keamanan siber dan strategi Indonesia telah berlandaskan pada UUD 1945 alinea ke-4 dalam melaksanakan ketertiban dunia dan melindungi segenap bangsa. Hal ini diperkuat dengan UU No. 3 Tahun 2022 tentang Pertahanan Negara yang bertujuan untuk melindungi kedaulatan negara, keutuhan wilayah, serta keselamatan segenap bangsa dari segala bentuk ancaman (Nugraha, 2016).

Sejak tahun 2015, Indonesia dikategorikan sebagai negara dengan perkekonomian berkembang dengan GDP sebesar $753,99 milyar dan penggunaan internet yang meningkat dari 88,1 juta pada tahun 2014 menjadi 139 juta (AAPJI, 2014 dalam Nugraha, 2016). Pengembangan Teknologi dan Informasi Komputer (TIK) Indonesia sejak saat itu menunjukkan perkembangan yang pesat didukung dengan momentum pengguna *Twitter*

dan *Facebook* yang terbesar di dunia. Dalam Buku Putih Pertahanan Indonesia, menunjukkan Indonesia mengakui keamanan global dan keadaan strategis yang memengaruhi pertahanan nasional. Pedoman negara ini menjadi *guidelines* dalam menentukan strategi utama keamanan nasional yang stabil. Dengan perkembangan ini, Indonesia tidak terhindarkan dari ancaman di ruang siber.

Berdasarkan pelanggaran data di Indonesia tahun 2021-2022 yang dihimpun dari laporan BSSN dan artikel lainnya, setidaknya terdapat 21 pelanggaran data *major* yang mengancam data pemerintahan, data penduduk, maupun terhadap laman resmi pemerintah. Pada 15 Juli 2021, terdapat kebocoran data penduduk Indonesia sebanyak 1,3 juta penduduk Indonesia. Pihak yang melakukan Serangan siber ini tidak diketahui dan kejadian ini merugikan Kementerian Kesehatan RI, aplikasi e-HAC, dan penduduk Indonesia. Data pelanggaran data di Indonesia dari tahun 2021-2022, serangan siber dalam bentuk kebocoran data dari masyarakat Indonesia

ASEAN Regional Forum (ARF) dalam Keamanan Siber

ASEAN Regional Forum (ARF) menunjukkan komitmen dalam memberantas kejahatan siber melalui kerangka forum multilateral yang formal dengan mendorong dialog, konsultasi, mempromosikan Pembangunan kepercayaan dan diplomasi preventif di Kawasan ASEAN (CCDCOE, 2013). Perjalanan ARF dalam keamanan siber mulai diimplementasikan pada tahun 2006 dalam pertemuan di Malaysia dan kembali ditekankan pada tahun 2012 dalam pertemuan di Malaysia dan kembali ditekankan pada tahun 2012 di Phnom Penh dengan mengeluarkan *"ARF Statement on Cooperation in Ensuring Cyber Security"*. Keamanan siber menjadi agenda yang diperkuat kembali dalam ARF dalam pertemuan ARF ke-19 di Kamboja, dimana para Menteri mengadopsi *"Statement on Cooperation in Ensuring Cyber Security"*. Pertemuan ini memvalidasi dan memperkuat dorongan dalam meningkatkan koperasi dalam keamanan siber. Pedoman ARF dalam menanggulangi keamanan siber terlihat dalam *ASEAN Cooperation on Cybersecurity and against Cybercrime* (Estiyovionita & Sitamala, 2022).

ASEAN Regional Forum memiliki lima *work streams*, di antaranya: kontra terorisme dan kejahatan transnasional, keamanan teknologi informasi dan komunikasi (TIK), bantuan bencana, keamanan maritim, serta non-proliferasi dan perlucutan senjata (ARF, n.d.). Sejak tahun 2020, ARF telah mengadopsi ARF *Ha Noi Plan Action II (2020-2025)* sebagai dokumen panduan menyeluruh untuk lima aliran kerja ARF. *Work streams* yang berhubungan dalam keamanan siber melalui *Ha Noi Plan Action II (2020-2025)* berkomitmen untuk mempromosikan dan mengembangkan lingkungan TIK yang terbuka, aman, stabil, mudak diakses dan lingungan yang damai dalam mencegah konflik dan dengan mengembangkan kepercayaan, keyakinan dan kerja sama di antara negara anggota ARF.

Kemitraan Keamanan Siber Indonesia melalui ASEAN Regional Forum

Keketuaan ASEAN periode 2023 memberikan kesempatan bagi Indonesia dalam memimpin forum-forum yang relevan terhadap AEAN, salah satunya adalah *ASEAN Regional Forum* (ARF). Pertemuan ARF ke-30 pada 14 Juli 2023 di Jakarta, diketuai oleh Indonesia yang dipimpin oleh Menteri Luar Negeri RI, Retno, L.P Marsudi. ARF telah menghasilan pengembangan progresif terhadap keamanan siber melalui dokumen *Chairman's Statement* atau pernyataan ketua, dalam hal ini dari Indonesia (ASEAN, 2023).

Pernyataan Ketua ARF 2023 menyatakan beberapa poin mengenai penguatan keamanan

siber regional yang relevan dengan keamanan nasional Indonesia. Maka, Indonesia dalam pertemuan ke-30 ARF mendukung adanya kemitraan regional maupun implementasi norma-norma yang menguatkan keamanan siber regional (ASEAN, 2023). Poin dalam pernyataan Indonesia sebagai ketua ARF 2023 menjadi relevan bagi pengembangan keamanan siber Indoneia, dikarenakan keamanan infrastruktur kritikal TIK serta keamanan ruang siber menjadi poin utama dalam *Defence White Paper* Indonesia tahun 2015 (Kementerian Pertahanan RI, 2015). Berikut adalah dua poin yang merangkum atensi forum ARF ke-30 dalam isu keamanan siber, yaitu (1) penguatan keamanan teknologi, informasi dan komunikasi, serta (2) penguatan keamanan ruang siber.

Pertemuan ARF ke-30 mendukung adanya penguatan keamanan TIK melalui pemanfaatan forum-forum yang relevan dengan keamanan TIK regional. Dukungan ini tertuju pada forum ARF Inter-Sessional Meeting on Security of and in the Use of ICTs (ISM on ICTs Security) yang secara berkala telah menyediakan ruang bagi anggota ARF untuk membahas perlindungan infrastruktur kritikal TIK. Selain itu, pertemuan ARF ke-30 juga mendukung koordinasi antara ARF dengan forum relevan untuk mendorong penguatan TIK melalui: *ASEAN Digital Ministers Meeting (ADGMIN)*, *ADMM-Plus, ASEAN Ministerial Meeting on Transnational Crime (AMMTC)*, dan *ASEAN Ministerial Conference on Cybersecurity (AMCC) on matters pertaining to ICTs Security* (ASEAN, 2023). Dengan demikian, koordinasi antar-forum tersebut dapat meningkatkan pengembangan keamanan siber melalui peningkatan perlindungan infrastruktur TIK kritikal regional.

Kedua, yaitu penguatan keamanan siber. Pertemuan ARF ke-30 juga menyadari pentingnya meningkatkan keamanan di ruang siber, sehingga pertemuan tersebut menyatakan antusiasme dalam mengimplementasikan ASEAN Regional Action Plan on the Implementation on the UN GGE Norms of Responsible State Behaviour in Cyberspace. Pertemuan tersebut menyadari adanya keselarasan antara norma tersebut dengan ASEAN Cybersecurity Cooperation Strategy 2021-2025 (ASEAN, 2023). Adanya itikad dalam mengimplementasikan norma perilaku negara di dalam ruang siber adalah pengembangan keamanan siber, yaitu penguatan keamanan di ruang siber regional.

Indonesia juga berpartisipasi aktif dalam forum ARF dan forum relevan lainnya yang secara spesifik membahas isu-isu mengenai keamanan siber. Salah satu dari forum tersebut adalah *ASEAN Regional Forum Senior Officials' Meeting* (ARF SOM). Indonesia menempatkan Sidharto Reza Suryodipuro, Direktur Jendral Kerja Sama ASEAN di bawah Kementrian Luar Negeri RI pada tanggal 14 Juni 2023 sebagai delegasi dalam *ARF Senior Officials' Meeting*. Dalam kesempatan ini, Indonesia mengusulkan untuk membahas perkembangan *ARF Ha Noi Plan of Action II*, pertukaran pandangan atas isu regional dan internasional yang termasuk keamanan siber, *counter-terrorism* dan kejahatan transnasional. Hal ini menjadi relevan untuk memperkuat keamanan siber secara regional maupun nasional.

Berdasarkan data yang dihimpun dari rekam jejaknya, dari tahun 2015 hingga 2022, setidaknya terdapat 17 kemitraan yang terjalin antara Indonesia dengan negara lainnya sebagai penerima manfaat dari program tersebut. Saat ini terdapat empat kerja sama yang masih berjalan hingga Oktober 2023, yaitu *Critical and Emerging Technology (CET) Standards for Safety, Security and Trade, Singapore Cybersecurity Centre for Excellence*, *ASEAN Cybercrime Operations Desk*, dan *Singapore-United States Third Country Training Programme (TCTP) Cybersecurity Workshops*. Hal ini menunjukkan bahwa

Indonesia dalam ranah keamanan siber bukan sebagai *lead actor* di ARF.

Indonesia juga menjalankan kemitraan berupa lokakarya yaitu ARF ICTs Security Workstream pada tahun 2022 bersama Australia. Salah satu mitra kerjasama ASEAN yang memanfaatkan ARF untuk mengembangkan keamanan siber dalam rentang tahun 2015 - 2022 adalah Australia. Kemitraan ini yang dilakukan antara ASEAN dengan Australia menargetkan jalur keamanan teknologi dan informasi ARF, atau ARF ICTs Security Workstream. Kemittraan Kerjasama ini direalisasikan melalui adanya lokakarya implementasi sebelas program sukarela dan norma perilaku negara yang bertanggung jawab di dunia maya pada Maret 2022, dimana Indonesia dan Australia menjadi co-host atau tuan rumah dari lokakarya tersebut (ASEAN, 2022).

Kemitraan keamanan siber antara ASEAN dan Australia melalui ARF juga direalisasikan melalui dukungan finansial terhadap ketahanan siber di Asia Tenggara. Australia memberikankan pendanaan sebesar AUD 74 juta untuk Program kemitraan Teknologi Kritis, atau Cyber and Critical Tech Cooperation Program yang mendukung penggunaan internet secara terbuka, bebas dan aman untuk mendorong pertumbuhan ekonomi, melindungi keamanan nasional dan mempromosikan stabilitas internasional (ASEAN, 2022).

Pengembangan Keamanan Siber Indonesia tahun 2015-2023 melalui ASEAN Regional Forum (ARF) berdasarkan 4 Jenis Ancaman Keamanan Siber oleh Choucri

Pengembangan keamanan siber di Indonesia pada dasarnya didukung oleh keketuaan dan keanggotaan Indonesia dalam forum keamanan siber yang dijalankan melalui ARF dari tahun ke tahun. Sebagai negara anggota ARF, Indonesia berhasil mengembangkan keamanan siber dengan berpartisipasi dalam kemitraan keamanan siber. Adanya serangkaian strategi keamanan siber, forum-forum keamanan siber dan realisasinya dalam bentuk kemitraan bagi negara anggota ASEAN secara tidak langsung telah membantu pengembangan keamanan siber Indonesia. Selain itu, kepemimpinan Indonesia sebagai tuan rumah maupun ketua ASEAN pada tahun 2023 memberikan momentum untuk memanfaatkan power dalam

Tabel 1. Analisis 4 Jenis Ancaman Keamanan Siber Indonesia melalui *ASEAN Regional Forum* (ARF)

No	Jenis Ancaman	Ancaman	Keterangan
1	*Militarization of Cyberspace*	-	Sejalan dengan pedoman *Defence White Paper Indonesia*
2	*Cyber Warfare*	-	Sejalan dengan pedoman *Defence White Paper Indonesia*
3	*Cyber threats to Infrastructure*	v	Upaya ini tertuang dalam Peraturan Presiden No.82 tentang Perlindungan Infrastruktur Informasi Vital (IIV)
4	*Cyber Terrorism*	v	Kemitraan *ASEAN Cyber Capacity Development Project* diinisiasi oleh INTERPOL melalui ARF

Sumber: Diolah dari berbagai sumber

ARF yang secara tidak langsung mendukung agenda keamanan siber Indonesia.

Pengembangan keamanan siber yang dihasilkan melalui ARF akan dibahas berdasarkan empat jenis ancaman siber yang dapat mengganggu keamanan nasional suatu negara, yaitu: 1) *militarization of cyberspace*; 2) *cyber warfare*; 3) *Cyber threats to infrastructure*; dan 4) *cyber terrorism*, maka kemitraan yang berlangsung melalui ARF akan dikategorikan kembali berdasarkan relevansinya terhadap empat jenis

ancaman keamanan siber menurut Choucri (2012).

Dalam jenis ancaman pertama, *militarization of cyberspace*, Choucri (2012) menilai bahwa militerisasi dunia maya merupakan elemen yang semakin diperlukan untuk menjaga keamanan nasional negara. Sehubungan dengan tujuan tersebut, militerisasi dunia maya dapat dilakukan oleh suatu negara sebagai perpanjangan dari kebijakan pertahanannya. Maka dari itu, ancaman terhadap keamanan nasional akibat militerisasi dunia maya perlu diantisipasi. Hal ini juga menjadi kekhawatiran bagi Indonesia, sehingga isu mengenai militerisasi ruang siber muncul pada pedoman kebijakan pertahanan Indonesia tahun 2015.

Indonesia menyadari bahwa militerisasi ruang siber menjadi isu yang krusial dalam menjaga keamanan nasional. Hal ini teridentifikasi dalam Buku Putih Pertahanan atau *Defense White Paper Indonesia* tahun 2015 sebagai pedoman kebijakan pertahanan Indonesia. Indonesia menilai bahwa penggunaan sistem, peralatan, dan platform berbasis internet cenderung semakin meluas, sehingga menimbulkan potensi kerawanan. Maka, ruang siber ditambahkan sebagai domain kelima pertahanan negara akibat potensinya sebagai medan perang (Kementerian Pertahanan RI, 2015).

Pengembangan keamanan siber Indonesia, dalam hal ini untuk mengantisipasi pemanfaatan ruang siber sebagai medan perang, didukung oleh kemitraan-kemitraan yang dihasilkan melalui ARF. Pada tahun 2019, Indonesia mendukung implementasi norma berperilaku negara yang bertanggung jawab di dunia maya sebagai ketua dari lokakarya (ASEAN, 2022). Selain itu, Indonesia juga mendukung dialog terkait perilaku negara yang bertanggung jawab dalam pemanfaatan teknologi dan informasi sebagai tuan rumah *ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies* pada tahun 2021 (United States Department of State, 2021). Maka dari itu, upaya antisipasi militerisasi dunia siber telah dilakukan dengan memastikan kemitraan terhadap perilaku negara yang bertanggung jawab, sebagaimana disebutkan diatas.

Jenis ancaman kedua, *cyber warfare*. Perang siber sederhananya merupakan serangkaian aktivitas berbasis dunia maya yang dirancang untuk melindungi negara dan kepentingannya. Karakteristik perang siber sendiri dapat diklasifikasi menjadi ofensif atau defensif, sebagaimana perang secara fisik di dunia nyata. Sarana, tujuan, pelaku, agen, dan instrumen perang pun dapat dikatakan sama dalam batasan tertentu (Choucri, 2012).

Sebagaimana disebutkan dalam Buku Putih Pertahanan Indonesia, maka Indonesia memahami adanya ancaman perang siber melalui militerisasi ruang siber (Kementerian Pertahanan RI, 2015). Maka dari itu, Indonesia mendorong adanya kemitraan dalam memastikan perilaku negara yang bertanggung jawab dalam dunia maya. Mengingat bahwa target dari serangan siber umumnya memanfaatkan teknologi informasi dan komunikasi seperti kabel, jaringan, dan sistem telekomunikasi, maka Indonesia mengembangkan keamanan sibernya dengan mengusung ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ASEAN, 2022).

Selanjutnya, *cyber threats to infrastructure*. Ancaman siber terhadap infrastruktur dapat diklasifikasi dalam dua jenis: (1) ancaman terhadap infrastruktur komunikasi dan informasi; dan (2) ancaman terhadap bentuk-bentuk infrastruktur lainnya yang bergantung kuat pada komunikasi. Internet merupakan tulang punggung yang dapat berimplikasi ke

berbagai sektor, baik itu kerentanan dalam sektor publik maupun swasta (Borchgrave et.al., 2001, dalam Choucri, 2012, hal. 151). Dalam Buku Putih Pertahanan Indonesia menyebutkan bahwa segala sumber daya dan infrastruktur digunakan sebagai upaya pertahanan negara (Kementerian Pertahanan RI, 2015). Upaya ini tertuang dalam Peraturan Presiden No.82 tentang Perlindungan Infrastruktur Informasi Vital (IIV), apabila terganggu akan berakibat negatif terhadap pelayanan publik, kepentingan umum, keamanan dan pertahanan, maupun perekonomian nasional. Dalam Pasal 1 No.4 menyebutkan bahwa keamanan siber merupakan upaya pemerintah yang inovatif dan adaptif bertujuan dalam melindungi segenap lapisan ruang siber, baik itu aset informasi, ancaman dan serangan siber, yang bersifat sosial dan teknis.

Dalam menjamin kemanan infrastruktur jaringan, BSSN berperan penting dan secara aktif melakukan pengamanan pra-pelaksanaan hingga pasca-pelaksanaan kegiatan nasional maupun internasional pada tahun 2022 (BSSN, 2022). Kegiatan seperti ASEAN Para Games 2022, Konferensi Tingkat Tinggi G20, Sidang Tahunan MPR dan DPR, dan kegiatan lainnya, BSSN secara aktif melakukan layanan *Information Technology Security Assessment* (ITSA), monitoring aktivitas lalu lintas jaringan, media sosial, hingga pengamanan jaringan dan sinyal komunikasi (BSSN, 2022, hal. 55-58). Secara spesifik dalam KTT G20, BSSN menjadi leading sector dari ke-17 kegiatan KTT G20 melakukan Vulnerability Assessment (VA) terhadap infrastruktur serta situs-situs yang digunakan dalam kegiatan. Serangan dan kalkulasi yang dilakukan BSSN menemukan terdapat aplikasi berhaya dalam komputer yang digunakan hotel serta anomali trafik di IIX dan International Gateway, sebagai salah satu tempat penyelenggaraan acara KTT G20.

Jenis ancaman terakhir yaitu *cyber terrorism*. Teroris telah memanfaatkan untuk menggunakan ruang siber dan kemampuan mereka dalam dunia maya untuk keuntungan mereka; banyak kelompok yang memiliki kehadiran yang mapan di arena siber, dan pola penggunaan mereka tampak cukup canggih. Dalam beberapa tahun terakhir, mereka memanfaatkan dunia maya untuk beberapa hal, mulai dari perang psikologis, rekrutmen politik, mobilisasi, pelatihan, penggalangan dana, dan bahkan instruksi tentang cara membuat senjata hingga tips perilaku tentang cara melakukan pengawasan, pembunuhan, dan sabotase (Choucri, 2012). Kapabilitas teroris dalam memanfaatkan ruang siber ini tentunya memperkuat potensi adanya terorisme siber.

Terorisme siber dapat dilihat sebagai bentuk perang informasi di mana pesan-pesan politik diekspresikan dengan cara-cara kekerasan. Hal ini diperkuat dengan adanya media berita kabel internasional internasional, terorisme siber, dan situs *web* (dan *blog*) tentang terorisme. Selain itu, keberadaan *hacker* yang dapat dikategorikan sebagai teroris juga semakin menguat. Dihadapkan dengan serangkaian isu tersebut, maka negara cenderung mengerahkan tanggapan berupa kebijakan yang mengatur interaksi dalam hubungan internasional di dunia siber (Choucri, 2012). Namun, terdapat opsi baru bagi Indonesia, yaitu kemitraan dalam merespon terorisme siber melalui ARF.

Kemitraan *ASEAN Cyber Capacity Development Project* diinisiasi oleh INTERPOL melalui ARF pada Januari 2016 dengan tujuan untuk memperkuat kemampuan negara-negara di ASEAN dalam memerangi kejahatan dunia maya dan bekerja sama sebagai sebuah kawasan. Fase pertama (2016 - 2018) dan kedua (2019-2021) telah dilaksanakan dengan mengusung berbagai kegiatan. Beberapa kegiatan yang dilakukan adalah seminar, lokakarya dan pelatihan staf penegak hukum,

yang pada dasarnya ditujukan untuk merespon ancaman-ancaman siber sesuai tren (Cybil, n.d).

Secara tidak langsung, serangkaian kemitraan yang dihasilkan melalui ARF telah mendukung pengembangan keamanan siber Indonesia, yaitu dengan menjaga tindakan negara terhadap militerisasi dunia siber dan meningkatkan kapasitas respon Indonesia terhadap ancaman siber. Serangkaian kerja sama tersebut dapat dirangkum melalui tabel berikut.

PENUTUP

Kemitraan yang dihasilkan melalui ASEAN Regional Forum (ARF) telah berimplikasi terhadap pengembangan keamanan siber Indonesia. Hal ini dapat dilihat berdasarkan empat area keamanan siber sesuai kategorisasi oleh Choucri, yaitu: (1) militerisasi dunia maya; (2) perang siber; (3) ancaman siber terhadap infrastruktur; dan (4) terorisme siber. Pengembangan keamanan siber berupa antisipasi terhadap (1) militerisasi dunia maya dan (2) perang siber teridentifikasi melalui adanya kemitraan antara ASEAN dengan Australia seperti lokakarya mengenai perilaku negara yang bertanggung jawab di dunia maya, serta ASEAN dengan Amerika dialog terkait perilaku negara yang bertanggung jawab dalam pemanfaatan teknologi dan informasi. Selanjutnya, (3) ancaman siber terhadap infrastruktur baik secara fisik maupun siber berkurang melalui *Cyber and Critical Tech Cooperation Program* dan *ASEAN Cyber Capacity Development Project*, sehingga telah mengembangkan keamanan siber bagi infrastruktur. Terakhir, pengembangan dalam merespon (4) keamanan siber diwujudkan melalui kemitraan berupa seminar, pelatihan staf, dan lokakarya dalam merespon terorisme antara ASEAN dengan INTERPOL.

Pengembangan keamanan siber di Indonesia melalui ARF diwujudkan dengan posisi Indonesia baik melalui kemitraan maupun sebagai penerima manfaat. Secara aktif, Indonesia memegang posisi sebagai pemimpin seperti Co-Chair pada yaitu *ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies* tahun 2021. Secara pasif, hal ini diwujudkan dengan posisi Indonesia sebagai penerima manfaat dari kemitraan seperti *ASEAN Cyber Capability and Capacity Development Project* (C3DP). Maka dari itu, dapat disimpulkan bahwa kemitraan yang dihasilkan melalui ARF secara tidak langsung telah mewujudkan pengembangan empat area keamanan siber di Indonesia melalui berbagai program dan agenda dalam ARF, utamanya dalam *work streams* mengenai TIK.

Daftar Pustaka

Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021). *Analyzing Cyber Crimes during COVID-19 TIme in Indonesia* (3rd ed., Hal. 79–82). School of Strategic and Global Study.

ASEAN (2023). *Chairman's Statement: The ASEAN Post Ministerial Conference (PMC) 10+1 Sessions with The Dialogue Partners and Trilateral Meetings*. Jakarta. (Hal. 1-35). Tersedia pada https://asean.org/wp-content/uploads/2023/07/FINAL-Chairmans-Statement-PMC-101-with-DPs-and-Trilateral-.pdf diakses 12 Agustus 2023.

Barkin, J. Samuel. (2013). *International Organization*. Palgrave Macmillan New York. Tersedia pada https://doi.org/10.1057/9781137356734 diakses 20 Mei 2023.

BSSN. (2020). *Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024*.

CCDCOE. (2013). *ASEAN Regional Forum Reaffirming the Commitment to Fight Cyber Crime.* Ccdcoe.org. Tersedia pada https://ccdcoe.org/incyder-articles/asean-regional-forum-reaffirming-the-commitment-to-fight-cyber-crime/ diakses 25 Mei 2023.

Choucri, Nazli. (2012). *Cyberpolitics in International Relations*: Context, Connectivity, and Content. MIT Press.

Gijsbers, K., & Veenendaal, M. (2011). *Protecting the National Interests in Cyberspace*. Georgetown Journal of International Affairs, Hal. 191–196. Tersedia pada https://www.jstor.org/stable/43133829 diakses 10 Agustus 2023.

Google, TEMASEK, & Bain & Company. (2019). e-Conomy SEA 2019. Swipe up and to the right: Southeast Asia's $100 billion Internet economy. *Bain*, hal. 6–64. Tersedia pada https://www.bain.com/globalassets/noindex/2019/google_temasek_bain_e_conomy_sea_2019_report.pdf diakses 10 Agustus 2023.

Kementerian Pertahanan RI. (2015, November). *Defence White Paper*.

Kshetri, N. (2013). *Cybercrime and Cybersecurity in the Global South*. Palgrave Macmillan UK. Tersedia pada https://doi.org/10.1057/9781137021946 diakses 20 Mei 2023.

Lesmana, I. M. A., Sushanti, S., & Resen, P. T. K. (2017). ASEAN Way sebagai Sebuah Paradoks: Kasus Terorisme Kelompok Abu Sayyaf. DIKSHI (Diskusi Ilmiah Komunitas Hubungan Internasional), 1(1). Tersedia pada https://ojs.unud.ac.id/index.php/hi/article/view/33905 diakses 24 Januari 2024.

Lewis, J. (2018). *Economic Impact of Cybercrime- No Slowing Down*. In CSIS. CSIS. Tersedia pada csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf diakses 25 Juni 2023.

Lindsay, J. R., & Gartzke, E. (2020). *Politics by many other means: The comparative strategic advantages of operational domains*. Journal of Strategic Studies, 45(5), Hal. 743–776. Tersedia pada https://doi.org/10.1080/01402390.2020.1768372. diakses 25 Juni 2023.

Maskun, M., Irwansyah, I., Yunus, A., Safira, A., & Lubis, S. N. (2021). *Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with it*. Jambe Law Journal, 4(2), hal. 131–150. Tersedia pada https://doi.org/10.22437/jlj.4.2.131-150 diakses 20 Mei 2023.

Manopo, B. Y. W., & Sari, D. P. (2015). *ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN Region*. Belli Ac Pacis, 1(1), hal. 44–51.

Nugraha, Y. (2016). *The Future of Cyber Security Capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity* (T. Roberts & Dr. A. S. Sastrosubroto, Eds.). University of Oxford.

Nye, J. (2010). *Cyber Power*. In Belfer Center, Belfer Center for Science and International Affairs, Hal. 1–23.

Putri, K. V. K. (2021). *Kerja Sama Indonesia dengan ASEAN mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime*, Hal. 542–552.

Putri, N. T., Fasisaka, I., & Nugraha, A. A. Bagus Surya Widya (2017). Penanganan *Cyber Attacks* oleh Pemerintah Tiongkok melalui Kebijakan *Network Security Tahun 2000*-2015. DIKSHI (Diskusi Ilmiah Komunitas Internasional), 1(1). Tersedia pada https://ojs.unud.ac.id/index.php/hi/article/view/27393/17349 diakses 24 Januari 2024.

Suwidharma, I. P. E., Nugraha, A. A. B. S. W., & Sushanti, S. (2023). Inisiasi Pemerintah Indonesia terkait Isu *Cyber Crime* yang Menghasilkan Kesepakatan *Code of Conduct on Framework of Security Cooperation* dengan Pemerintah Australia. DIKSHI (Diskusi Ilmiah Komunitas Hubungan Internasional), 2(2). Tersedia pada https://ojs.unud.ac.id/index.php/hi/article/view/86757/45197 diakses 24 Januari 2024.