Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.2. No.7 (Juli 2021)
Tema/Edisi : Hukum Pidana (Bulan Ketujuh)
https://jhlg.rewangrencang.com/

KERJA SAMA INDONESIA DENGAN ASEAN MENGENAI *CYBER SECURITY* DAN *CYBER RESILIENCE* DALAM MENGATASI *CYBER CRIME*

(INDONESIA'S COOPERATION WITH ASEAN ON CYBER SECURITY AND CYBER RESILIENCE IN TACKLING CYBER CRIME)

Kristiani Virgi Kusuma Putri

Fakultas Hukum Universitas Brawijaya

Korespondensi Penulis : virgii_kp@student.ub.ac.id

Citation Structure Recommendation :

Putri, Kristiani Virgi Kusuma. *Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.2. No.7 (Juli 2021).

ABSTRAK

Dibalik kelebihannya, *Cyber Space* juga memiliki sisi gelap tertentu yang mendukung adanya kejahatan-kejahatan, seperti penipuan, informasi teroris, pedofilia, dan lain-lain. Dalam mengatasi hal tersebut, pemerintah Indonesia telah melakukan serangkaian upaya yang salah satunya adalah dengan menerbitkan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 11 Tahun 2008 Informasi dan Transaksi Elektronik. Namun, berdasarkan hasil penelitian, dari keenam negara ASEAN, yaitu Singapura, Malaysia, Indonesia, Filipina, Thailand, dan Vietnam, hanya Indonesia yang tidak memiliki undang-undang keamanan siber secara khusus. Tetapi di samping itu, dalam menangani keamanan dan ketahanan siber, Indonesia masih secara aktif melakukan kerja sama internasional seperti bergabung dengan ASEAN.
Kata Kunci: ASEAN, Indonesia, Kejahatan Siber

ABSTRACT

Behind the advantages, cyberspace is also has a certain dark side that supports the existence of crimes, such as fraud, terrorist information, pedophilia, and others. In dealing with this, the Indonesian government has made several efforts, one of which is by enacting Law Number 36 of 1999 about Telecommunications and Law Number 11 of 2008 about Information and Electronic Transactions. However, based on research results, from the six ASEAN countries, which are Singapore, Malaysia, Indonesia, Philippines, Thailand, and Vietnam, only Indonesia does not have a specific cybersecurity law. But besides that, in overcoming cybersecurity and resilience, Indonesia is still actively engaged in international cooperation such as joining ASEAN.
Keywords: ASEAN, Indonesia, Cyber Crime

A. PENDAHULUAN

Di era globalisasi, *Cyber Space* (ruang siber/dunia maya) telah menjadi kebutuhan pokok bagi manusia yang dapat menghubungkan orang terlepas dari jarak yang dimiliki. *Cyber Space* sendiri adalah era baru yang dibawa oleh internet.[1] *Cyber Space* merupakan hal yang nyata meskipun tidak berwujud. Hal tersebut dikarenakan bentuknya berupa dunia virtual, yaitu dunia tanpa batas. Inilah yang dimaksud dengan *Borderless World*, yaitu ketika ruang siber tidak perlu mengenali perbatasan negara, yang mana hal tersebut dapat menghilangkan dimensi ruang, waktu, dan tempat.[2] Berkaitan dengan *Cyber Space* itu sendiri, Bruce Sterling pernah berpendapat sebagai berikut:[3]

> *"Although it is not exactly "real," "cyberspace" is a genuine place. Things happen there that have very genuine consequences. This "place" is not "real," but it is serious, it is earnest. Tens of thousands of people have dedicated their lives to it, to the public service of public communication by wire and electronics."*

Dibalik kelebihannya, c*yber space* juga memiliki sisi gelap tertentu misalnya seperti akses pornografi. Menurut pengamatan yang dilakukan oleh Barrett, bahwa internet memang mengandung hal-hal yang terlarang dan tidak menyenangkan.[4] Hal tersebut juga mendukung adanya kejahatan-kejahatan seperti penipuan, pertukaran informasi terorisme, pedofilia, pembajakan perangkat lunak, peretasan komputer, dan lain-lain.

Seluruh dunia sudah lama prihatin dengan adanya kejahatan siber (*Cyber Crime*). Hal tersebut terbukti dari salah satu topik yang dibahas dalam kongres ke-10 Persatuan Bangsa-Bangsa (PBB), yaitu *Prevention of Crime and the Treatment of Offenders* di Wina, Austria pada tahun 2000, yang mana pembahasannya terkait dengan kejahatan jaringan komputer. Tetapi, tidak setiap negara anggota memiliki aturan mengenai kejahatan siber serta tidak seluruh negara ikut prihatin dengan masalah *Cyber Crime* (hanya negara maju dan beberapa negara berkembang saja).

---

[1] A. Mahzar, *Spiritualitas Cyberspace: Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia*, Penerbit Mizan, Bandung, 1999, p.9.

[2] O. W. Purbo, *Perkembangan Teknologi Informasi dan Internet di Indonesia*, Kompas, 2000, p.50.

[3] Bruce Sterling dalam Muhamad R. dan Yanyan M., *Cybersecurity Policy and Its Implementation in Indonesia*, Journal of ASEAN Studies, Vol.4, No.1 (2016), p.61.

[4] N. Barrett, *Digital Crime: Policing the Cybernation*, Kogan, London, 1997, p.21.

Hal ini tergantung pada seberapa berkembangnya suatu negara hukum dan seberapa besar perhatiannya terhadap kemajuan teknologi. Seperti yang diungkapkan pada Kongres PBB di Wina sebagai berikut[5]:

> "Alasan kurangnya perhatian terhadap kejahatan siber mungkin disebabkan dari rendahnya tingkat partisipasi negara dalam komunikasi elektronik internasional, rendahnya tingkat pengalaman penegakan hukum, dan rendahnya perkiraan kerugian masyarakat atas kejahatan siber."

Sebagai negara berkembang, Indonesia mengalami sedikit ketertinggalan dalam hal penjagaan dan perkembangan teknologi informasi.[6] Padahal, penggunaan teknologi informasi untuk tujuan destruktif merupakan ancaman bagi sebuah pertahanan nasional. Ancaman tersebut bisa dalam bentuk militer ataupun non-militer. Ancaman militer terhadap pertahanan nasional adalah ancaman terhadap pertahanan dan keamanan. Sedangkan ancaman non-militer terhadap pertahanan negara adalah ancaman terhadap ideologis, politik, ketahanan ekonomi, sosial, dan budaya. Cepat atau lambat, eksistensi kemajuan teknologi akan mempengaruhi berbagai bidang kehidupan manusia, baik itu bidang sosial, bidang budaya, maupun bidang politik.[7]

Sarjana hukum Ari Purwadi[8] juga membenarkan hal tersebut ketika ia mengatakan bahwa dia percaya teknologi mewakili sistem nilai tertentu. Karena teknologi itu sendiri pada dasarnya adalah produk sosial budaya masyarakat. Secara umum, unsur itu bisa diidentifikasi sebagai sumber potensial ancaman yang terdiri dari sumber internal dan eksternal, baik kegiatan intelijen, gangguan investigasi, organisasi ekstremis, peretas, kelompok kejahatan terorganisir, persaingan, permusuhan, konflik, dan juga teknologi.[9]

---

[5] United Nations Office on Drugs and Crime, *Crimes Related to Computer Networks - Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (April 10 2000) diakses dari United Nations Office on Drugs and Crime: https://www.unodc.org/document.

[6] M. Nur, *Dilema Pengembangan Infrastruktur Informasi Indonesia*, Info Komputer, Vol.12, No.8 (1998), p.34.

[7] J. Sudarsono, *Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial Politik*, Masyarakat Jurnal Sosiologi, FISIP UI-Gramedia, Jakarta, 1992, p.4.

[8] A. Purwadi, *Kebutuhan Akan Perangkat Hukum Perjanjian di Bidang Alih Teknologi*, Hukum dan Pembangunan, Vol.3, Tahun XXIII (1993), p.234.

[9] Kementerian Pertahanan Republik Indonesia, *A Road Map to Cyber Defense National Strategy*, KEMENHAN, Jakarta, 2013, p.24.

Selanjutnya, berdasarkan analisis yang dilakukan oleh ATKearney menunjukkan bahwa negara-negara di Asia Tenggara yang tergabung dalam ASEAN telah muncul sebagai target utama serangan *Cyber* karena beberapa alasan berikut:[10] Pertama, negara-negara ASEAN terutama Malaysia, Indonesia, dan Vietnam menjadi tempat tuan rumah global untuk blokade utama aktivitas web yang mencurigakan; Kedua, kebijakan kawasan, tata kelola, dan kemampuan keamanan siber relatif rendah; Ketiga, terdapat kekurangan kemampuan dan keahlian yang tumbuh di dalam negeri karena terfragmentasi industri dan kekurangan keterampilan; dan Keempat, persepsi risiko *Cyber* dari korporasi yang dilakukan *Stakeholders* tidak melihat keamanan siber sebagai prioritas bisnis yang mengakibatkan tidak adanya pendekatan holistik terhadap ketahanan siber.

Padahal, harapan dari adanya *Cyber Space* adalah untuk membawa kenyamanan, kebahagiaan, dan kesempatan tak terbatas untuk masyarakat. Namun ketika kejahatan-kejahatan siber mulai berkembang di Asia Tenggara, maka keamanan dan ketahanan siber menjadi hal yang *Urgent* dikarenakan dampak dari permasalahan siber berpotensi merusak atau mengganggu kehidupan, baik itu individu, negara, dan bahkan seluruh dunia.[11] Adapun rumusan masalah yang diangkat dalam paper ini adalah sebagai berikut:

1. Bagaimana kondisi Indonesia dengan ASEAN Mengenai Kebijakan *Cyber Security* dan *Cyber Resilience* dalam mengatasi *Cyber Crime*?
2. Bagaimana konsep kerja sama Indonesia dengan ASEAN mengenai Kebijakan *Cyber Security* dan *Cyber Resilience* dalam upaya untuk mengatasi *Cyber Crime*?

B. PEMBAHASAN

1. Kondisi Indonesia dengan ASEAN Mengenai Kebijakan *Cyber Security* dan *Cyber Resilience* dalam Mengatasi *Cyber Crime*

Keterkaitan antara stabilitas keamanan dan kelancaran pembangunan adalah dasar pendirian Association of Southeast Asian Nations atau disingkat ASEAN.

[10] A.T.Kearney, *Cybersecurity in ASEAN-An Urgent Call to Action*, Penerbit A.T. Kearney Korea LLC, Korea, 2018, p.9.

[11] Y. A. Piliang, dalam M. Slouka, *Ruang yang Hilang: Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan*, Penerbit Mizan, Bandung, 1999, p.14-15.

Indonesia sebagai salah satu negara pionir pendiri ASEAN menyadari bahwa pembangunan di tingkat nasional harus dilandasi oleh kondisi aman dan stabil di tingkat regional.[12] Pemerintah Indonesia telah melakukan serangkaian upaya untuk melindungi dunia siber dari ancaman kejahatan siber. Salah satu upaya pemerintah dalam menjaga keamanan informasi di dunia maya adalah dengan menerbitkan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 11 Tahun 2008 Informasi dan Transaksi sebagai dasar landasan perumusan regulasi dan kebijakan terkait keamanan informasi. Bahkan, Pemerintah Indonesia juga membentuk Badan Siber dan Sandi Nasional (BSSN) yang memiliki tanggung jawab untuk mencegah serangan dunia maya. BSSN juga bekerja untuk memperkuat pertahanan negara terhadap ancaman dunia siber dan meningkatkan kesadaran publik tentang keamanan siber.[13]

Menilik survei kebijakan keamanan dan ketahanan siber dari enam negara ASEAN, dapat diketahui bahwa sebagian besar negara di ASEAN telah membuat beberapa bentuk undang-undang dan kebijakan untuk menangani masalah siber, memberikan tanggung jawab yang terbatas kepada pemilik *Platform*, memerangi *Cyber Crime* dengan memberlakukan peraturan yang menghukum orang yang melakukan kejahatan di internet, dan menjaga data pribadi warga negara dengan membuat peraturan untuk memastikan privasi warga negaranya.

	Openness of the Platform	**Cybercrime Prevention**	**Privacy**
Indonesia	Judicial System	No Specific cybersecurity laws; Information and Electronic Transaction Act (Law of the Republic of Indonesia No. 11 of 2008)	Data Protection Regulation (2016) -Personal Data Protection (Draft)
Malaysia	Notice and takedown	Computer Crime Act 1997	Personal Data Protection Act 2010 (PDPA).
Philippines	Judicial System	Cybercrime Prevention Act (2012)	Data Privacy Act (2012)
Singapore	Notice and takedown	COMPUTER MISUSE ACT (1993, amended 2017)	The Data Privacy Act of 2012
Thailand	Judicial System	Computer-Related Crime Bill (2007, amended 2017))	Sector specific approach such as National Health Service Act -Personal Information Protection Act (Draft)
Vietnam	Judicial System	Law on Cyber Information Security (Law No. 86/2015/QH13)	Law on Cyber Information Security (Law No. 86/2015/QH13)

Tabel 1. Kebijakan *Cyber Crime* di 6 Negara ASEAN
(Sumber: Jirapon Sunkpho, dkk.)

[12] Khanisa dan Faudzan Farhana, *Keamanan Maritim Asean dalam Perspektif Ekonomi Politik Indonesia*, Penerbit LIPI Press, Jakarta, 2018, p.1.

[13] Jirapon Sunkpho, dkk., *Cybersecurity Policy in ASEAN Countries*, Information Institute Conferences, Las Vegas, NV, 2018, *p.*4.

Dari tabel tersebut dapat diketahui bahwa tingkat perkembangan aturan yang diterapkan oleh setiap negara memiliki fungsi yang berbeda-beda. Dalam hal keterbukaan *platform*, hanya Singapura dan Malaysia yang memiliki prosedur *Notice and Takedown*. Sementara Indonesia, Filipina, Thailand, dan Vietnam tidak memiliki aturan bagi pemegang hak (pelapor) untuk secara langsung menegakan hukum dengan melindungi hak ciptanya melalui sistem *Notice and Takedown* tersebut. Sebagai gantinya, pemegang hak dalam melindungi hak ciptanya harus melalui tindakan hukum yang disebut dengan "Sistem Peradilan".[14]

Contohnya seperti pada tahun 2017, Etry Mike dalam penelitiannya menemukan beberapa situs dan *website* yang secara ilegal melakukan tindakan memperbanyak buku yang sebenarnya belum memiliki versi elektronik, tapi sudah dapat diunduh di beberapa situs tertentu. Contohnya buku karya Ahmad Fuadi berjudul Negeri 5 Menara yang dapat diunduh di www.rajaebookgratis.com secara gratis dan tentu saja tidaklah resmi. Kemudian kumpulan buku karya Raditya Dika yang dapat pula diunduh pada *blog* pribadi dengan alamat http://ferdhika.uni.me/2012/03/kumpulanebook-novelradityadika.html, yang mana kumpulan buku tersebut juga dapat diunduh secara gratis.[15] Hal tersebut tentu saja sangat merugikan para penulis yang mana mereka tidak dapat menerima royalti apapun terhadap karya mereka yang telah dibajak tersebut. Selain itu apabila penulis ingin mengajukan gugatan terhadap pelaku, maka dibutuhkan tenaga dan waktu yang ekstra dalam mengatasi hal tersebut.

Dari keenam negara ASEAN yang diteliti, hanya Indonesia yang tidak memiliki undang-undang keamanan siber secara khusus. Aturan di Indonesia hanya mengandalkan UU ITE. Begitu juga mengenai masalah perlindungan data pribadi, dimana Thailand dan Indonesia menjadi negara yang tidak memiliki hukum secara spesifik mengenai perlindungan data pribadi. Sehingga apabila terjadi pelanggaran data pribadi, maka hal tersebut diselesaikan oleh hukum dan dengan keputusan yang berbeda-beda. Namun, baik Thailand maupun Indonesia saat ini sedang dalam proses menyusun undang-undang perlindungan data pribadi.

---

[14] Jirapon Sunkpho, dkk., *Cybersecurity Policy in ASEAN Countries*, Information Institute Conferences, Las Vegas, NV, 2018, *p.*4.

[15] Etry Mike, *Perlindungan Hukum Hak Kekayaan Intelektual Terhadap Tindakan Pelanggaran Pembajakan Buku Elektronik Melalui Media Online*, Al-Imarah: Jurnal Pemerintahan dan Politik Islam, Vol.2, No.2 (2017), p.140.

Sedangkan negara Vietnam menjadi satu-satunya negara ASEAN yang memiliki pengaturan hukum komprehensif yang menangani keamanan dan perlindungan data pribadi dalam satu hukum tunggal (terkodifikasi).[16]

Masalah tersebut harus ditangani di antara negara-negara ASEAN dengan berkolaborasi dan berbagi informasi yang akan menjadi aspek penting dalam keamanan dan ketahanan siber. Tanpa kolaborasi, ekosistem keamanan dan ketahanan siber akan mudah untuk diblokade.[17] Karena *Cyber Crime* merupakan kejahatan lintas batas negara yang diklasifikasikan sebagai kejahatan luar biasa. Sehingga, penting untuk memiliki perjanjian multilateral sebagai langkah untuk mengatasinya, baik di tingkat regional maupun di tingkat internasional.[18]

2. Kerja sama Indonesia dengan ASEAN Mengenai Kebijakan *Cyber Security* dan *Cyber Resilience* dalam Mengatasi *Cyber Crime*

Cyber Security adalah keamanan informasi yang diterapkan ke komputer atau jaringan. Tujuannya untuk membantu pengguna mencegah penipuan atau mendeteksi segala upaya penipuan dalam sistem berbasis informasi. Keamanan siber juga sebagai bentuk upaya untuk melindungi informasi dari serangan siber. Serangan siber pada operasi informasi ialah semua tindakan yang disengaja untuk mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Tindakan ini dapat berbentuk gangguan fisik atau gangguan aliran logis sistem Informasi. Sedangkan keamanan siber nasional adalah sebuah istilah yang digunakan untuk keamanan siber yang berhubungan dengan aset / sumber daya suatu negara.[19]

Cyber Resilience sebagai ketahanan nasional ialah konsepsi pengembangan kekuatan siber melalui pengaturan dan penyelenggaraan kesejahteraan dan keamanan yang seimbang, serasi, dan selaras dalam seluruh aspek kehidupan secara utuh dan terpadu berlandaskan UUD NRI 1945 dan wawasan nusantara. Dengan kata lain, konsepsi ketahanan siber nasional merupakan pedoman untuk meningkatkan keuletan dan ketangguhan bangsa yang mengandung kemampuan mengembangkan kekuatan siber dengan pendekatan kesejahteraan dan keamanan.

---

[16] Jirapon Sunkpho, dkk., *Op.Cit*., p.5.

[17] Tan Aaron, *Navigating ASEAN's Patchy Cyber Security Landscape*, diakses dari http://www.computerweekly.com/feature/Navigating-ASEANs-patchy-cyber-security-landscape.

[18] Muhamad R. dan Yanyan M., *Cybersecurity Policy and Its Implementation in Indonesia*, Journal of ASEAN Studies, Vol.4, No.1 (2016), p.64.

[19] M. Boisot, *Knowledge Assets: Securing Competitive Advantage in the Information Economy*, OUP Oxford, Oxford, 1998, p.18.

Tujuan nasional keamanan dan ketahanan siber adalah untuk perlindungan, dominasi, dan kontrol data dan informasi. Keamanan dan ketahanan siber nasional berkaitan erat dengan operasi informasi yang melibatkan berbagai pihak seperti militer, pemerintah, badan usaha milik negara, perusahaan, akademisi, sektor swasta, individu, dan dunia internasional. Kelangsungan operasi informasi tidak hanya mengandalkan keamanan dunia siber itu sendiri. Hal tersebut juga tergantung pada keamanan fisik yang terkait dengan semua elemen fisik seperti gedung *Data Center*, bencana sistem pemulihan, dan media transmisi.

Tata kelola keamanan dan ketahanan siber di Indonesia sudah memiliki sistem dan strategi yang dilakukan oleh instansi pemerintah dan juga pejabat masyarakat. Kebijakan keamanan dan ketahanan siber telah dikoordinasikan oleh Kementerian Komunikasi dan Informatika (Kominfo). Dalam sistem dan strategi keamanan dan ketahanan siber tersebut, terdapat tiga organisasi pemerintah yang terlibat dalam keamanan dan ketahanan siber di Indonesia yaitu Keamanan Informasi Tim Koordinasi, Direktorat Keamanan Informasi, dan *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII).[20]

Sehubungan dengan hal tersebut selain peran nasional, juga diperlukan peran kerja sama internasional untuk mendukung implementasi keamanan dan ketahanan siber yang sukses. Kerja sama internasional adalah hubungan yang dilakukan oleh suatu negara dengan negara lainnya yang bertujuan untuk memenuhi kebutuhan rakyat dan untuk kepentingan negara-negara di dunia. Kerja sama internasional, yang berpedoman pada politik luar negeri meliputi kerja sama di bidang politik, sosial, pertahanan keamanan, kebudayaan dan ekonomi.[21] Sampai saat ini, peran kerja sama internasional tetap dilakukan secara sektoral baik oleh lembaga, komunitas, maupun entitas sesuai dengan fungsinya. Mereka melakukan kerja sama tersebut melalui bergabung dengan asosiasi internasional. Salah satu strategi aliansi Indonesia dalam kebijakan keamanan dan ketahanan *Cyber* adalah melalui penyelenggaraan kerja sama dengan ASEAN untuk menangani keamanan dan ketahanan *Cyber*.

---

[20] Muhamad R. dan Yanyan M., *Cybersecurity Policy and Its Implementation in Indonesia*, Journal of ASEAN Studies, Vol.4, No.1 (2016), p.67.

[21] Yanuar Ikbar, *Metodologi & Teori Hubungan Internasional*, Penerbit PT Refika Aditama, Bandung, 2014, p.273.

ASEAN sendiri merupakan salah satu kawasan dengan pertumbuhan tercepat di dunia dengan populasi 634 juta jiwa (100 juta jiwa lebih banyak dari Uni Eropa). Hal ini menjadikan ASEAN sebagai pasar terpadat ketiga di dunia dan dengan Pendapatan Domestik Bruto (PDB) gabungan lebih dari $ 2,55 triliun, menjadikan ASEAN sebagai wilayah dengan ekonomi terbesar ketujuh di dunia.[22] Studi oleh ATKearney menunjukkan bahwa ekonomi digital dapat menambah 1 triliun USD.[23] Namun, "Ekonomi Digital" yang sangat bergantung pada teknologi untuk transaksi bisnis membuka jalan baru ancaman kejahatan siber, seperti penipuan *online*, peretasan, dan distribusi materi yang tidak pantas. Sehingga diperlukan keamanan nasional dan perlindungan infrastruktur informasi.[24]

Hal tersebut adalah salah satu dari komitmen Indonesia dalam mewujudkan tiga pilar ASEAN, yaitu Komunitas Ekonomi ASEAN, Komunitas Sosial Budaya ASEAN, dan Komunitas Keamanan Politik ASEAN. Indonesia juga menjadi salah satu negara yang memprakarsai *Treaty of Amity and Cooperation*. Secara substansial, sesama negara anggota melaksanakan perjanjian tersebut dengan tidak saling menyerang dan menyelesaikan konflik dengan cara yang damai.[25]

Indonesia juga pernah secara konsisten bermitra dengan negara anggota ASEAN di sektor keamanan siber yaitu dengan Malaysia dan Singapura karena keunggulannya dalam pengembangan keamanan *Cyber*. Malaysia mendukung keamanan siber melalui kebijakan, kelembagaan, prasarana, program, dan upaya yang telah dibahas dalam forum kerja sama internasional. Siberoc ialah Institusi yang bertanggung jawab untuk menjalankan fungsi keamanan siber di Malaysia yang mendukung kebijakan keamanan siber dan penerapannya di Indonesia, yang berkoordinasi dengan institusi keamanan informasi Malaysia, seperti *Malaysian Computer Emergency Response Team* (MyCERT). Berikutnya Indonesia juga bekerja sama dengan Singapura yang unggul dalam sumber daya manusianya, yaitu dengan memiliki sejumlah pakar keamanan informasi di ASEAN.[26]

---

[22] ASEANstats, *ASEAN Statistical Yearbook 2018*,Penerbit ASEAN, Jakarta, 2018.
[23] A.T.Kearney, *Loc.Cit.*.
[24] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD Digital Economy Papers, No.211 (2012). OECD Publishing, Paris, 2012, *p.*4.
[25] Kementrian Pertahanan Republik Indonesia, *Op.Cit.*, p.58.
[26] Kementrian Pertahanan Republik Indonesia, *Ibid.*, p.17.

Selanjutnya, Indonesia dan ASEAN juga bersama-sama menangani kejahatan siber dengan meningkatkan tingkat keamanan siber di negara anggota. Hal tersebut terbukti melalui partisipasi Indonesia dalam kegiatan ASEAN Forum Regional (ARF). Sejak 2006, ARF berfokus pada ancaman kejahatan siber. ARF pernah membuat pertemuan "*Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space*" di Vietnam pada tahun 2012.[27]

Sebelumnya dalam sebuah konferensi yang diadakan di Kuala Lumpur, Malaysia pada tanggal 13-14 Januari 2011, para peserta sepakat untuk membentuk sebuah komunitas untuk meningkatkan keamanan *Cyber* di wilayah Asia Tenggara. Hasilnya, ASEAN-CERT berhasil didirikan. Selanjutnya di sebuah konferensi di Mactan Cebu, Filipina pada tanggal 15-16 November 2012, semua anggota setuju untuk melanjutkan pengembangan ASEAN-CERT serta setuju untuk mendukung tugas-tugasnya. Akhirnya bersama dengan negara-negara ASEAN lainnya, Indonesia berkomitmen untuk mengembangkan keamanan sibernya dan akan secara konsisten melakukannya.[28]

C. PENUTUP

1. Kesimpulan

Berdasarkan survei kebijakan keamanan dan ketahanan siber dari 6 negara ASEAN, dapat diketahui bahwa sebagian besar negara di ASEAN telah membentuk undang-undang dan kebijakan untuk menangani masalah kejahatan siber. Namun, Indonesia masih memiliki beberapa kekurangan dalam menerapkan kebijakan mengenai kejahatan siber yang antara lain: 1) Dalam hal keterbukaan *platform*, Indonesia tidak memberikan ketentuan hukum bagi pemegang hak untuk secara langsung melindungi hak ciptanya; 2) Indonesia yang tidak memiliki undang-undang keamanan siber khusus, tetapi hanya mengandalkan UU ITE; dan 3) Indonesia juga menjadi negara yang tidak memiliki aturan secara spesifik mengenai perlindungan data pribadi. Masalah yang harus segera ditangani oleh negara-negara ASEAN adalah berkolaborasi dan berbagi informasi sehingga ekosistem keamanan dan ketahanan siber tidak akan mudah untuk diblokade.

---

[27] ASEAN Secretaria, *Cooperation on Cybersecurity and against Cybercrime, Octopus Conference: Cooperation Against Cybercrime*, Council of Europe, Strasbourg, France, 2013, p.20.

[28] ASEAN Secretaria, *Ibid*..

Selain antisipasi domestik, peran kerja sama internasional sangat diperlukan untuk mendukung implementasi keamanan dan ketahanan siber yang sukses. Sampai saat ini, Indonesia pernah melakukan kerja sama beberapa kali dengan ASEAN mengenai penanggulangan terhadap kejahatan siber. Kerja sama tersebut seperti *Treaty of Amity and Cooperation;* mengikuti *ASEAN Forum Regional* (ARF); pengembangan ASEAN-CERT, dan lain sebagainya.

2. Saran

Adapun saran yang dapat diberikan oleh penulis adalah sebagai berikut:

a. Bagi pemerintah:

Pemerintah Indonesia diharapkan dapat segera membuat produk hukum yang mengatur secara spesifik mengenai *Cyber Crime* dan perlindungan data pribadi sebagaimana negara-negara anggota ASEAN lainnya. Serta, pemerintah juga diharapkan dapat memperluas kerja sama internasional dalam hal *Cyber Security* dan *Cyber Resilience* tidak hanya di lingkup Asia Tenggara tetapi juga pada lingkup yang lebih luas lagi.

b. Bagi Masyarakat:

Masyarakat diharapkan untuk selalu mematuhi hukum yang berlaku dan tidak segan untuk melaporkan kepada pihak yang berwajib apabila mengetahui tindakan yang melanggar hukum. Terutama dalam kasus-kasus yang berhubungan dengan *Cyber Crime*.

DAFTAR PUSTAKA

Buku

ASEAN Secretaria. 2013. *Cooperation on Cybersecurity and against Cybercrime, Octopus Conference: Cooperation Against Cybercrime*. (Strasbourg, France: Council of Europe).

ASEANstats. 2018. *ASEAN Statistical Yearbook 2018*. (Jakarta: Penerbit ASEAN).

A.T. Kearney. 2018. *Cybersecurity in ASEAN-An Urgent Call to Action*. (Korea: Penerbit A.T. Kearney Korea LLC).

Barrett, N.. 1997. *Digital Crime: Policing the Cybernation*. (London: Kogan).

Boisot, M.. 1998. *Knowledge Assets: Securing Competitive Advantage in the Information Economy*. (Oxford: OUP Oxford).

Ikbar, Yanuar. 2014. *Metodologi & Teori Hubungan Internasional*. (Bandung: Penerbit PT Refika Aditama).

Kementerian Pertahanan Republik Indonesia. 2013. *A Road Map to Cyber Defense National Strategy*. (Jakarta: KEMENHAN).

Khanisa dan Faudzan Farhana. 2018. *Keamanan Maritim Asean dalam Perspektif Ekonomi Politik Indonesia*. (Jakarta: Penerbit LIPI Press).

Mahzar, A.. 1999. *Spiritualitas Cyberspace: Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia*. (Bandung: Mizan).

Nur, M.. *Dilema Pengembangan Infrastruktur Informasi Indonesia*. Info Komputer. Vol.12. No.8 (1998).

Purbo, O. W.. 2000. *Perkembangan Teknologi Informasi dan Internet di Indonesia*. (Jakarta: Kompas).

Slouka, M.. 1999. *Ruang yang Hilang: Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan*. (Bandung: Penerbit Mizan).

Sudarsono, J.. 1992. *Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial Politik*. (Jakarta: Masyarakat Jurnal Sosiologi, FISIP UI-Gramedia).

Sunkpho, Jirapon. dkk.. 2018. *Cybersecurity Policy in ASEAN Countries*. (Las Vegas, NV*:* Information Institute Conferences).

Publikasi

Mike, Etry. *Perlindungan Hukum Hak Kekayaan Intelektual Terhadap Tindakan Pelanggaran Pembajakan Buku Elektronik Melalui Media Online*. Al-Imarah: Jurnal Pemerintahan dan Politik Islam. Vol.2. No.2 (2017).

OECD. *Cybersecurity Policy Making at a Turning Point: Analysing New Generation of National Cybersecurity Strategies for the Internet Economy*. OECD Digital Economy Papers. No.211 (2012). (Paris: OECD Publishing).

R. Muhamad dan Yanyan M. *Cybersecurity Policy and Its Implementation in Indonesia*. Journal of ASEAN Studies. Vol.4. No.1 (2016).

Purwadi, A.. *Kebutuhan Akan Perangkat Hukum Perjanjian di Bidang Alih Teknologi*. Hukum dan Pembangunan. Vol.3. Tahun XXIII (1993).

Website

Aaron, Tan. *Navigating ASEAN's Patchy Cyber Security Landscape*. diakses dari http://www.computerweekly.com/feature/Navigating-ASEANs-patchy-cyber-security-landscape.

Sumber Hukum

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154. Tambahan Lembaran Negara Republik Indonesia Nomor 3881.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders 2000.