Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan, 2020, Vol 1 (2): 118-129
ISSN: 2722-2853. Homepage: govsci.fisip-unmul.ac.id

DOI: https://doi.org/10.54144/govsci.v1i2.12

Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber

Indonesia's international cooperation: strengthening national security in the field of cyber security

Afifah Fidina Rosy
Sebelas Maret University
Email Correspondence: afrosyfidina@gmail.com

Abstract
This research analyses the development of cyber security capacity and international cooperation in cyber security carried out by Indonesia with other countries. Research results show that the development of Indonesian cyber security has been strengthened by the establishment of National Cyber and Crypto Agency. It is also found that Indonesian cyber diplomacies have yielded cooperation with other countries to strengthen cyber security as part of national security. They have been carried out bilaterally or multilaterally, and can be categorized as cooperative security based on common goals, i.e. to prevent the rise of threats to national security.

Keywords: *cyber security, cyber crime, security, internet, cooperative security, cooperation.*

Pendahuluan

Dunia internasional kini telah mencapai era baru dimana isu non-tradisional semakin mendapatkan perhatian dari aktor-aktor hubungan internasional. Semakin berkembangnya isu-isu global tersebut merupakan konsekuensi dari adanya globalisasi dimana tidak adanya batasan pasti dalam penyebaran informasi di dunia. Keadaan tersebut membawa pada perubahan pola interaksi dari aktor-aktor hubungan internasional yang tidak hanya terjadi antara negara dengan negara, namun juga negara dengan aktor non-negara. Perubahan yang ada diikuti oleh penemuan dan pengembangan teknologi yang semakin maju, salah satunya berupa penemuan internet sebagai media penyebaran informasi dan komunikasi.

Sejak pertama kali muncul, sedikit banyak internet telah membawa perubahan pada berbagai aspek kehidupan manusia. Perubahan tersebut tak hanya memiliki dampak positif seperti dipermudahnya interaksi dan penyebaran informasi antar aktor hubungan internasional yang semula

terhambat jarak dan wilayah, tetapi juga memiliki dampak negatif bagi penyebaran informasi itu sendiri di dalam internet. Lebih lanjut, dampak negatif dari internet adalah munculnya kejahatan siber *(cyber crime).* Kejahatan siber melibatkan jaringan internet yang terhubung dengan hampir seluruh komputer di seluruh dunia. Selain itu, kejahatan ini dapat menyebabkan ketidakamanan data dan dokumen yang dikoneksikan melalui server internet. Sehingga, dalam konteks lebih luas kejahatan ini dapat mengganggu keamanan suatu negara.

Kejahatan siber dapat mengganggu dan menjadi ancaman bagi keamanan nasional suatu negara dikarenakan saat ini banyak negara yang sudah mengkoneksikan data-data dan kontrolnya terhadap beberapa sektor melalui internet atau daring (*online)*. Karena luasnya jenis kejahatan siber yang dapat terjadi di internet, hingga kini belum ada klasifikasi dan pengertian pasti dari kejahatan siber itu. Namun, kejahatan siber saat ini telah mendapatkan perhatian internasional sebagai salah satu kejahatan transnasional. Dapat dilihat dari diidentifikasikannya kejahatan siber sebagai salah satu dari *New Emerging Crimes* pada Konferensi Anggota PBB tentang Kejahatan Transnasional Terorganisir (*Conference of States Parties UNTOC)* pada tahun 2010. Senada dengan penetapan oleh PBB tersebut, Julian Droogan menyatakan bahwa kejahatan siber telah berkembang menjadi salah satu ancaman utama dari kesejahteraan masyarakat di seluruh dunia[1]. Dengan demikian, hal ini membuktikan bahwa keamanan yang ditujukan untuk mencegah dan menangani kejahatan siber perlu dikembangkan dan menjadi fokus baru keamanan nasional negara.

Indonesia adalah negara yang penggunaan internetnya termasuk sangat tinggi. Hal tersebut terbukti dari hasil studi yang bekerjasama dengan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2019 yang menunjukkan bahwa dari total 264 juta penduduk Indonesia, terdapat 171,17 juta jiwa atau 64,8 persen masyarakat yang telah terhubung ke internet.[2] Dengan penggunaan internet yang begitu tinggi dari masyarakat, ancaman terjadinya kejahatan siber tentu juga akan sangat tinggi. Oleh karena itu, diperlukan upaya peningkatan keamanan siber oleh Pemerintah Indonesia sebagai bagian dari penjagaan keamanan nasional.

Indonesia merupakan anggota yang aktif dalam berbagai forum PBB, termasuk dalam Konferensi Anggota PBB tentang Kejahatan Transnasional Terorganisir yang telah menetapkan lima kejahatan baru yang harus mendapat perhatian, termasuk kejahatan siber yang dapat terjadi lintas batas negara. Dari sisi Indonesia sendiri, tergolong rentan terhadap kejahatan-kejahatan tersebut dikarenakan letaknya yang strategis dan masyarakatnya

[1] Droogan, J. (2010). Asian Transnational Security Challenges: Emerging Trends, Regional Visions. The Council for Asian Transnational Threat Research.

[2] Yudha Pratomo. (16 Mei 2019). APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa. diakses pada 20 Mei 2020 melalui https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa

yang banyak dan beragam. Sehingga, Pemerintah Indonesia melakukan upaya pencegahan dengan menaruh perhatian khusus terhadap kejahatan lintas negara baru dan berkembang yang telah ditetapkan, serta mengintensifkan kerjasama internasional untuk melindungi kepentingan dan kedaulatan nasional Indonesia.[3] Dalam hal ini, Indonesia mengupayakan peningkatan keamanan siber dengan cara bekerjasama dengan negara lain, baik melalui kerjasama bilateral maupun regional.

Berdasarkan uraian latar belakang pertanyaan yang diajukan, penulis merumuskan pernyataan masalah yang dihadapi dalam penelitian ini yaitu Bagaimanakah kerjasama yang dilakukan oleh Indonesia dalam bidang keamanan siber dengan negara lain untuk memperkuat keamanan nasional.

Dalam penelitian ini, penulis melakukan tinjauan pustaka dari beberapa sumber literatur dan penelitian terdahulu yang mendukung dan berkaitan dengan penelitian ini. Jurnal pertama yang berhubungan dengan penelitian ini adalah Jurnal yang ditulis oleh Bambang Supriyadi yang berjudul, "Persepsi Bersama Indonesia-Australia dalam Hibah Dana dan Peralatan Investigasi Cyber Crime dari Australia Kepada Indonesia" yang diterbitkan pada tahun 2017 dan dimuat di *Journal of International Relations* Universitas Diponegoro, Volume 3, Nomor 1, Tahun 2017, hal. 140-149 . Jurnal ini membahas mengenai faktor-faktor yang mempengaruhi kebijakan yang diambil oleh Australia dalam menyediakan pembiayaan dan peralatan investigasi kejahatan kepada Indonesia yang dianalisis dengan konsep *collective identity* teori konstruktivisme yang didasari atas persepsi terhadap ancaman dalam menjelaskan behavior negara. Dalam jurnal ini penulis memiliki kesimpulan bahwa kerjasama kolektif dilakukan oleh Indonesia dan Australia dalam peningkatan keamanan siber dan penanganan kejahatan siber karena adanya persamaan persepsi sebagai negara yang sama-sama menghadapi ancaman siber terlepas dari hubungan diplomatik antara Indonesia dan Australia mengalami pasang surut. Jurnal ini penting bagi penelitian saya karena dalam jurnal ini dipaparkan oleh penulis bahwa kesamaan kepentingan dan persepsi terhadap ancaman dapat memicu adanya kerjasama bahkan dalam bidang keamanan dengan negara rival sekalipun. Sehingga, hal ini sejalan dengan konsep yang akan saya gunakan dalam penelitian saya.

Jurnal kedua yang berhubungan dengan penelitian saya adalah Jurnal yang ditulis oleh Hidayat Chusnul Chotimah berjudul, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara" yang diterbitkan pada tahun 2019 dan dimuat dalam Jurnal Politica Vol. 10 No. 2 November 2019. Jurnal ini membahas tentang pembentukan Badan Siber dan Sandi Negara sebagai pihak yang berfokus pada aspek keamanan siber maupun diplomasi siber negara dengan mempertimbangkan tingginya penggunaan internet dan posisi strategis

[3] Kemenlu. (7 April 2019). Kejahatan Lintas Negara. diakses pada 20 Mei 2020 melalui https://kemlu.go.id/portal/id/read/89/halaman_list_lainnya/kejahatan-lintas-negara

Indonesia dalam persepsi negara-negara major power di bidang siber yang dianalisis dengan konsep keamanan siber dan diplomasi siber. Di dalam jurnalnya, penulis juga memaparkan peran BSSN dalam menjalin kerjasama di bidang siber seperti kerjasama yang dilakukan dengan Australia, Kerajaan Inggris Raya, Kerajaan Belanda, Amerika Serikat, dan menjalin kerjasama di tingkat regional melalui *ASEAN's Cooperation on Cyber Security and Against Cyber crime* dan juga *ASEAN Cyber Capacity Program (ACCP)*. Sehingga, jurnal ini penting bagi penelitian saya karena adanya pemaparan mengenai kerjasama yang dilakukan oleh Indonesia dalam bidang keamanan siber yang dilakukan untuk menjaga keamanan dan kedaulatan siber Indonesia sehingga dapat memperkuat data bagi penelitian saya.

Jurnal ketiga yang berhubungan dengan penelitian saya adalah jurnal yang ditulis oleh Bima Yudha Wibawa Manopo dan Diah Apriani Atika Sari yang berjudul, "ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN Region" yang diterbitkan pada tahun 2015 dan dimuat dalam jurnal Belli ac Pacis. Vol. 1. No.1 Juni 2015. Jurnal ini membahas mengenai peran ASEAN Regional Forum dalam mewujudkan *regional cyber security* dan juga penanganan kejahatan siber di ASEAN yang dianalisis menggunakan konsep keamanan kawasan. Dalam jurnal ini penulis mendapatkan kesimpulan bahwa penanganan kejahatan siber di dalam ASEAN Regional Forum adalah melalui *Confidence Building Measures*, *Preventive Diplomacy*, dan *Conflict Resolutions*. Langkah-langkah kerjasama dalam meningkatkan keamanan siber regional tersebut dilakukan dengan memperhatikan prinsip-prinsip yang dimiliki ASEAN. Jurnal ini juga membahas mengenai adanya mekanisme kerjasama bilateral terkait keamanan siber di dalam ASEAN regional forum yang dapat dilakukan dengan negara maju di luar anggota ASEAN untuk meningkatkan keamanan siber masing-masing negara dan turut mengembangkan . Hal tersebut tentu penting bagi penelitian saya, karena dapat menjadi penguat bahwa adanya kerjasama yang dilakukan oleh negara di ASEAN dengan negara lainnya dalam hal peningkatan keamanan siber sebagai bagian dari keamanan nasional.

Metode Penelitian

Ilmuwan hubungan internasional dalam berbagai literatur menyepakati bahwa keamanan adalah sebuah "*Contested Concept".* Hal ini keamanan merupakan sebuah kondisi yang terbebas dari ancaman militer atau dengan kata lain berarti adanya kemampuan suatu negara untuk melindungi negara-bangsanya dari serangan militer yang berasal dari lingkungan eksternal.[4] Keamanan nasional adalah kebutuhan dasar bagi suatu bangsa untuk melindungi dan menjaga kepentingan nasional.

Faktor utama yang menjadi dasar konsep keamanan nasional suatu bangsa adalah kebutuhan untuk memenuhi kepentingan nasional. Keamanan

[4] Helga Haftendorn (1991). The Security Puzzle: Theory, Building and Discipline in International Security. Dalam intenational studies quarterly. vol .35 no. 1 hlm 3-17

nasional memiliki tujuan untuk memelihara dan mempertahankan eksistensi negara selain dari tujuannya untuk menjaga dan melindungi negara.Konsep keamanan menekankan peran pemerintah dalam melindungi integritas teritorial negara dari ancaman yang datang dari luar maupun dari dalam negeri.[5] Dalam hubungan internasional kontemporer, keamanan nasional yang diupayakan untuk melindungi kepentingan nasional tidak lagi hanya mencakup isu tradisional. Hal tersebut seperti yang diutarakan oleh pakar keamanan internasional, Barry Buzan bahwa, "Keamanan tidak hanya meliputi aspek militer dan aktor negara semata melainkan akan meliputi aspek-aspek non militer dan melibatkan pula aktivitas-aktivitas aktor non-negara.[6]

Lebih lanjut, Buzan menulis artikel terkait dimensi dalam keamanan nasional yang meliputi lima aspek, yakni; (1) Keamanan politik yang menyangkut jaminan untuk mempertahankan hak politik dan kebebasan untuk mempertahankan rezim politik, (2) Keamanan militer yang menyangkut kebebasan dari ancaman intervensi militer pihak eksternal, (3) Keamanan ekonomi yang menyangkut jaminan akses terhadap segala sumber daya dan aktivitas pasar global untuk mencapai kesejahteraan sosial, (4) Keamanan masyarakat yang menyangkut kebebasan dari segala bentuk konflik horizontal baik karena alasan identitas maupun sumber daya dan ekonomi, (5) Keamanan lingkungan yang menyangkut jaminan terbebas dari kerusakan lingkungan hidup yang dapat mengakibatkan berbagai bencana kemanusiaan.[7] Dengan demikian berdasarkan pendekatan tersebut, sektor militer dalam konsep keamanan nasional bukanlah aspek satu-satunya. Sementara itu, keamanan nasional juga akan mencakup secara luas dan menyeluruh sektor politik, ekonomi, masyarakat, dan lingkungan baik dari level individu dalam negara, nasional, regional, maupun internasional.

Berdasarkan konsep yang dipaparkan di atas, menunjukkan bahwa telah terjadi perluasan makna dari isu keamanan tradisional menuju isu keamanan non-tradisional. Sehingga, kajian keamanan nasional perlu dikembangkan hingga sampai pada ranah analisis interaksi antar aktor terkait sektor keamanan. Hal tersebut dikarenakan adanya *grey area* yang diartikan sebagai adanya ancaman terhadap keamanan dan stabilitas baik nasional maupun internasional yang muncul akibat terjadinya proses interaksi aktor negara dan non-negara. Sehingga, semakin beragam fenomena global yang muncul dan hal tersebut termasuk ancaman keamanan nasional dengan memanfaatkan kemajuan teknologi informasi. Dengan demikian, mulai meluas pula perubahan *behavior* aktor internasional dalam menyikapi fenomena global yang semula selalu dengan pendekatan militer kemudian

[5] (Darmono, 2010: 9)
[6] Buzan, Barry (1997). Rethinking Security after The Cold War dalam Cooperation and Conflict The Nordic Journal of International Studies Vol. 32 no. 1 hlm 5-28
[7] (Buzan, 1991) .'New Patterns of Global Security in Twentieth Century'. International Affairs Vol. 67 No. 31. Halaman 439-451

berganti menjadi pendekatan non-militer dalam menjaga keamanan nasional.[8]

Kaspersky resource center mendefinisikan keamanan siber sebagai sebuah praktek yang dilakukan untuk melindungi komputer, server, perangkat mobile, sistem elektronik, jaringan internet, dan data dari serangan yang dapat merusak. Hal tersebut juga diketahui sebagai keamanan teknologi informasi atau keamanan informasi elektronik. Istilah tersebut berlaku untuk konteks yang beragam dan bisa dibedakan menjadi beberapa kategori.[9] Keamanan siber sendiri terdiri dari berbagai macam aspek, seperti kumpulan alat, kebijakan, perlindungan keamanan, pedoman pelaksanaan, pendekatan manajemen resiko, tindakan, serta pelatihan yang kemudian digunakan untuk melindungi ruang siber yang pada dasarnya dibangun atas kepastian hukum, tindakan prosedural, struktur organisasi, *capacity building,* dan kerjasama internasional[10]. Lebih lanjut, keamanan siber merupakan bagian dari mekanisme keamanan yang dilaksanakan untuk melindungi dan meminimalisir gangguan terhadap kerahasiaan, integritas, serta ketersediaan sebuah informasi, yang dalam hal ini secara khusus melalui dunia maya.

Upaya peningkatan keamanan siber yang dilakukan oleh negara merupakan salah satu upaya yang berkaitan dengan tujuan menjaga keamanan nasional. Hal tersebut dikarenakan kebijakan dan strategi pertahanan dan keamanan negara bersifat dinamis dan dapat berubah mengikuti perkembangan fenomena dan isu global yang berpotensi menjadi ancaman nasional. Secara spesifik, keamanan siber kini telah mulai menjadi perhatian dan strategi keamanan negara-negara di dunia. Perubahan strategi keamanan negara yang merambah dunia maya disebabkan semakin berkembang dan meluasnya kejahatan siber dengan memanfaatkan perkembangan teknologi informasi dan komunikasi saat ini. Hal ini juga dikarenakan dalam beberapa sektor, negara telah menggunakan jaringan internet sebagai basis dari kontrolnya sehingga akan menjadi kelemahan apabila tidak terdapat kebijakan terkait keamanan siber yang melindungi.

Kejahatan siber memiliki banyak ragam baik yang berada pada level individu, kelompok kecil, maupun kelompok kejahatan terorganisasi yang menyerang dan melakukan kejahatannya secara sistematis. Berikut beberapa contoh kejahatan siber (*cyber crime)* yang menjadi perhatian dalam keamanan siber;(1) *Unauthorized Access to Computer System and Service* Kejahatan ini dilakukan dengan masuk secara ilegal ke dalam sistem jaringan komputer. Modus operasi ini biasanya dilakukan dengan maksud untuk pencurian informasi penting dan rahasia, (2) *Illegal Contents* yakni

[8] Perwita, Prof. A. A. B. (2008). Dinamika Keamanan dalam Hubungan Internasional dan Implikasinya Terhadap Indonesia. Hlm 13

[9] Kaspersky Resource Center. (2020). What is Cyber Security?. Diakses pada 20 Mei 2020 melalui https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[10] Ardiyanti, Handrini. (2014). Cyber Security dan Tantangan Pengembangannya di Indonesia.dapat diakses melalui https://jurnal.dpr.go.id/index.php/politica/article/view/336

memasukan data atau informasi ke internet tentang suatu hal yang tidak benar dan dianggap melanggar hukum atau mengganggu ketertiban publik yang ditujukan kepada individu, kelompok maupun negara, (3) *Data Forgery* yakni memalsukan data pada dokumen penting yang tersimpan di internet. Kejahatan ini ditujukan pada dokumen yang dimiliki lembaga yang layanannya berbasis web data, (4) *Cyber Sabotage and Extortion* yakni kejahatan dengan tujuan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer hingga sistem jaringan komputer yang terhubung dengan internet, (5) *Cyber Espionage* yakni mata-mata terhadap pihak lain melalui fasilitas jaringan internet sebagai media kejahatan. Pada umumnya hal ini dilakukan untuk mendapat dokumen atau data penting pihak tertentu yang tersimpan dalam suatu sistem yang terhubung dengan komputer, (6) *Offense against Intellectual Property* yakni kejahatan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet, (7) *Carding* yakni aksi mencuri nomor kartu-kartu penting milik orang lain dan dipergunakan untuk transaksi perdagangan di internet, (8) *Cracking* Kejahatan di internet yang memiliki ruang lingkup lebih luas, mulai dari aksi balas dendam terhadap instansi tertentu hingga pembajakan hak atas kekayaan intelektual dan penghilangan data melalui jaringan internet.

Konsep keamanan bersama telah mengalami perkembangan selama beberapa dekade terakhir ini. Sejalan dengan perkembangannya tersebut, keamanan bersama atau *cooperative security* dapat diartikan sebagai prinsip strategis yang dimaksudkan untuk mencapai sebuah tujuan melalui kesadaran institusional daripada melalui ancaman baik secara material maupun secara fisik.[11] Dalam pengertian lain, *cooperative security* disebutkan memiliki tujuan utama untuk mencegah perang dan guna mencapainya diperlukan penggeseran perencanaan keamanan negara. Perencanaan keamanan dirubah dari yang semula disiapkan untuk menghentikan atau menghadapi ancaman, menjadi upaya untuk mencegah ancaman tersebut untuk muncul. Dengan demikian, konsep *cooperative security* ini bisa dikatakan berbeda dengan konsep *collective security.*[12]

Perbedaan konsep dengan *collective security* tersebut dapat kembali diartikan sebagai perubahan kebijakan keamanan yang semula didasarkan pada paksaan dan konfrontasi menuju strategi yang dimaksudkan guna mencari solusi atas masalah keamanan melalui sebuah kerjasama bahkan dengan pihak yang memiliki potensi menjadi musuh sekalipun. Sehingga, strategi keamanan yang benar-benar kooperatif seharusnya tidak memiliki unsur paksaan sedikitpun. Strategi dan kerjasama keamanan tersebut tidak

[11] J.E. Nolan et. al., "The Concept of Cooperative Security", in: J.E. Nolan (ed.), Global Engagement, Cooperation and Security in the 21st Century; Brookings, Washington, D.C., 1994, pp. 4-5.

[12] Ashton Carter/William Perry/John D. Steinbrunner, A New Concept of Cooperative Security; Brookings Institution, Washington D.C. 1992; p. 7

ditujukan pada penyelesaian konflik tetapi lebih cenderung pada pencegahan ancaman dan potensi konflik untuk muncul.[13]

Konsep dari *cooperative security* ini menjadi konsep keamanan yang patut diperhitungkan karena banyak hal. Alasan utamanya adalah di era perkembangan global seperti sekarang ini, banyak permasalahan yang berada di luar jangkauan dan kapasitas dari sebuah negara untuk diselesaikan secara tunggal. Tantangan kontemporer yang sudah jelas terlihat dan perlu mendapat perhatian adalah isu-isu transnasional seperti ancaman terorisme, permasalahan lingkungan, migrasi, kejahatan terencana, dan perdagangan obat. Tetapi, bahkan isu keamanan tradisional pun kini telah berubah menjadi kompleks yang menyebabkan terlihat mustahil bagi suatu negara untuk melindungi kepentingan nasionalnya tanpa adanya kerjasama dengan negara lain. Karena itulah, banyak negara yang menjalankan kerjasama berdasarkan konsep dari *cooperative security* ini, dengan catatan seluruh pihak yang bekerjasama sama-sama memiliki kepentingan untuk menjaga keamanan bersama.[14]

Pembahasan

Keamanan siber yang dikembangkan di Indonesia pada awalnya di inisiasi pada tahun 2007. Pengembangan kapasitas keamanan siber diwujudkan dalam kebijakan yang memberikan adanya kepastian hukum. Kebijakan tersebut adalah dikeluarkannya Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007/21 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Peraturan tersebut kemudian mengalami beberapa kali proses revisi yang akhirnya menghasilkan ditetapkannya Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12 /2010. Dalam peraturan tersebut, turut diatur terkait pembentukan *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII), yakni tim yang bertugas untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet.[15] Selain Peraturan Menteri yang telah dikeluarkan, menurut Hasyim Gautama, UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008 dan Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82

[13] Heintz Vetschera. 2007. Cooperative Security: The Concept And Its Application In South Eastern Europe. Vienna: National Defence Academy and Bureau For Security Policy At The Autrian Ministry Of Defence in Co-operation with PfP Consortium Of Defence Academics And Security Studies Institutes. Hlm 33-39

[14]Michael Moodie.(2000). Cooperative Security: Implications for National Security and International Relations dalam Cooperative Monitoring Center Occasional Paper/14. Albuquerque; Sandia National Laboratories. Hlm 5

[15] Ardiyanti, Handrini. (2014). Cyber Security dan Tantangan Pengembangannya di Indonesia.dapat diakses melalui https://jurnal.dpr.go.id/index.php/politica/article/view/336 hlm.99

Tahun 2012 juga merupakan pondasi awal untuk dibangunnya keamanan siber di Indonesia.[16]

Berdasarkan analisis data sistem *monitoring traffic* yang kemudian dilakukan oleh ID-SIRTII, tercatat bahwa insiden serangan di dalam dunia maya mencapai satu juta insiden akibat kelemahan sistem dan aplikasi yang tidak diketahui. Dalam hal ini, institusi pemerintah juga tidak luput dari serangan siber di mana dalam kurun waktu 1998-2009 sebanyak 2.138 serangan telah dialamatkan terhadap website domain milik pemerintah Indonesia. Dalam tingkat global, telah banyak terjadi pula Perang Siber dan bahkan pada tahun 2017 telah ada serangan siber WanaCrypt0r 2.0 atau virus Wanna Cry yang menyebar dan menginfeksi dengan cepat ke seluruh negara di dunia.[17] Hal itu tentu membuat Indonesia mau tidak mau harus semakin aware terhadap isu keamanan siber karena hal tersebut terkait dengan keamanan nasional.

Peristiwa-peristiwa yang terjadi kemudian membuat Indonesia membentuk Badan Siber dan Sandi Negara sebagai institusi pelaksana diplomasi siber yang menangani permasalahan keamanan siber di Indonesia. Sebagai institusi siber nasional, BSSN berperan dalam menjalin koordinasi dan kerjasama antara institusi dan pemangku kepentingan di bidang siber di Indonesia. Institusi tersebut meliputi Kepolisian Republik Indonesia dalam *cyber crime*, TNI/Kementerian Pertahanan dalam *cyber defense*, Kementerian Luar Negeri dalam *cyber diplomacy* dan juga institusi lain dalam kaitannya dengan siber.[18]

Dalam bidang diplomasi siber, BSSN bersinergi dengan KemenLu. Hal tersebut dikarenakan internet bersifat transnasional dan terdapat kemungkinan adanya benturan dengan kepentingan antar negara. Lebih lanjut, internet telah menciptakan dimensi baru pada keamanan informasi yang akhirnya berimplikasi pada hubungan internasional, di mana apapun yang beredar di internet berpotensi untuk menyebar secara bebas dan negara harus beradaptasi dan menyesuaikan arus internet dengan pembuatan kebijakan negara.[19] Oleh karena itu, untuk menciptakan peningkatan keamanan siber Indonesia yang efektif, Pemerintah harus melakukan diplomasi siber berikut ini; (1) kemitraan atau kerjasama internasional dengan negara lain karena adanya ancaman siber yang memiliki kompleksitas dan lintas negara, (2) kerjasama yang melibatkan berbagai unsur di tingkat nasional baik dari kalangan masyarakat maupun swasta, (3) penegasan orientasi politik luar negeri dan diplomasi Indonesia melalui strategi di

[16] Hasyim Gautama.(2011). Penerapan Cyber Security.

[17] Hidayat Chusnul Chotimah. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. Jurnal Politica Vol.10 No. 2. Dapat diakses melalui https://doi.org/10.22212/ jp.v10i1.1447

[18] Badan Siber dan Sandi Negara, Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019, 6-8.

[19] Nicholas Westcott. (July 2008). Digital Diplomacy: The Impact of the Internet on International Relations. Research Report 16, hlm 14.

bidang siber melalui BSSN sebagai pelaksana fungsi diplomasi siber maupun keamanan siber dalam upaya mencapai ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber, dan keamanan siber pada ekonomi digital.[20]

Dalam memperkuat keamanan nasional melalui keamanan siber yang efektif, Indonesia bekerjasama baik dalam ranah bilateral maupun multilateral. Dalam ranah bilateral, Indonesia melakukan kerjasama dengan Kementerian Luar Negeri Belanda dan Kerajaan Inggris Raya pada tahun 2018 yang mencakup *information sharing* dalam bidang hukum, perundang-undangan, kebijakan nasional, dan strategi kebijakan manajemen di ranah siber, penguatan kapasitas dan perbantuan kelembagaan serta pengembangan teknologi di bidang keamanan siber melalui jejaring dan program pelatihan dan pendidikan, dan elaborasi upaya bersama dalam membangun ketahanan terhadap serangan siber dan perlindungan terhadap aset vital di ranah siber dan juga hal-hal teknis yang mendukung kerjasama. Di tahun yang sama, Indonesia juga telah bekerjasama dalam konsep siber dan digital lebih luas dengan Australia yang mencaku perihal ekonomi digital, serta dengan Amerika Serikat. Kerjasama-kerjasama tersebut bertujuan untuk memajukan kerjasama dan pembangunan kapasistas di ruang siber dalam bidang-bidang seperti diskusi tentang pengembangan strategi ruang siber nasional, kemampuan manajemen insiden nasional, kapasitas dan kerjasama penanggulangan kejahatan siber.

Dalam ranah multilateral, Indonesia bersama dengan ASEAN melalui ASEAN Regional Forum (ARF) dan ASEAN *Political-Security Community* (APSC) memiliki kesepakatan untuk peningkatan kerjasama dalam hal ancaman non tradisional, yang secara khusus berfokus pada persoalan kejahatan transnasional dan lintas batas. Kemudian, pada tahun 2006 ARF membentuk *ARF on cybersecurity initiatives* terkait pembahasan kejahatan siber di ASEAN yang dituangkan dalam *ASEAN's Cooperation on Cybersecurity and against Cybercrime*. Keikutsertaan Indonesia pada ARF ini dapat memberikan keuntungan berupa kontak poin *(point of contact)* dengan negara-negara di luar anggota yang bekerjasama melalui kerangka kerja ARF. Yang akhirnya dapat mempermudah proses diplomasi siber Indonesia, termasuk dalam penanganan insiden siber.

Kerjasama yang dilakukan oleh Indonesia di bidang keamanan siber baik dalam ranah bilateral maupun multilateral ini dapat dikategorikan sebagai bentuk *cooperative security.* Hal tersebut dikarenakan antara pihak-pihak yang melakukan kerjasama tidak ada yang berada di bawah paksaan dan membentuk kerjasama berdasarkan tujuan yang sama dalam mewujudkan keamanan negaranya. Selain itu, adanya persepsi yang sama antara pihak-pihak dalam kerjasama yang terjadi tidak ada kondisi *zero-sum*

[20] Indra Rosandry, "Merajut Diplomasi Siber Indonesia", Kamis, 22 November 2018, diakses pada 21 Mei 2020 melalui https://mediaindonesia.com/read/detail/199360-merajut-diplomasi-siber-indonesia

seperti dalam game theory yang apabila satu pihak mendapatkan keuntungan, maka pihak lain tidak mendapatkan keuntungan *(zero).* Hal tersebut dikarenakan seluruh pihak yang tergabung dalam *cooperative security* dalam bidang keamanan siber ini sama-sama mendapat keuntungan baik berupa informasi, bantuan peralatan, maupun keuntungan lainnya dalam upaya penanganan ancaman terhadap keamanan nasional yang sama-sama dihadapi, yakni kejahatan siber.

Kesimpulan

Sejak adanya penemuan dan penggunaan internet secara global di seluruh dunia, mulai muncul ancaman non-tradisional baru bagi keamanan nasional negara, yakni berupa kejahatan siber. Karena adanya ancaman yang kemudian pada tahun 2010 ditetapkan oleh PBB sebagai salah satu jenis *new emerging crimes* dalam Konferensi Anggota PBB tentang Kejahatan Transnasional Terorganisir (*Conference of States Parties UNTOC)* tersebut, negara-negara di dunia mulai memberikan perhatian dan melakukan pengembangan dalam hal keamanan siber.

Indonesia sebagai negara yang penggunaan internetnya sangat tinggi dan dalam beberapa sektor layanan pemerintahan telah dikontrol melalui daring, maka turut mengembangkan keamanan sibernya. Keamanan siber di Indonesia mulai dikembangkan pada tahun 2007, dan kemudian diperkuat dengan pembentukan BSSN yang menjadi ujung tombak dalam ranah siber di Indonesia. Selain melakukan upayanya secara terkoordinir dengan lembaga pemerintahan lain di dalam negeri, Indonesia juga melakukan diplomasi siber ke luar. Diplomasi itu melibatkan kerjasama dengan negara lain terkait peningkatan keamanan siber sebagai bagian dari keamanan nasional. Indonesia melakukan kerjasama baik dalam ranah bilateral maupun multilateral, yang dapat dikategorikan dalam konsep *cooperative security* berdasarkan tujuan yang sama yakni untuk mencegah munculnya ancaman terhadap keamanan nasional.

Daftar Pustaka

Ardiyanti, H. 2014. *Cyber Security dan Tantangan Pengembangannya di Indonesi*. Jurnal DPR RI. From https://jurnal. dpr.go.id/index .php/politica /article /view/336

Badan Siber dan Sandi Negara. 2018. *Rencana Strategis Badan Siber dan Sandi Negara Tahun* 2018-2019. 6-8.

Bima Yudha Manopo, D. A. 2015. *ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN Region*. Belli ac Pacis. Vol. 1. No.1 , 44-51.

Buzan, B. 1991. *New Patterns of Global Security in Twentieth Century*. International Affairs Vol. 67 No. 31, 439-451.

Buzan, B. 1997. *Rethinking Security after The Cold War*. The Nordic Journal of International Studies Vol. 32 no. 1, 5-28.

Carter, A., Perry, W., & Steinbrunner, J. D. 1992. *A New Concept of Cooperative Security.* Washington D.C: Brookings Institution.

Chotimah, H. C. 2019. *Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara*. Jurnal Politica Vol.10 No. 2.

Darmono, L. B. 2010. *Konsep dan Sistem Keamanan Nasional Indonesia.* Jurnal Ketahanan Nasional XV No. 1.

Droogan, J. 2010. *Asian Transnational Security Challenges: Emerging Trends, Regional Visions.* The Council for Asian Transnational Threat Research.

Gautama, H. 2011. *Penerapan Cyber Security*. From http://kemhubri .dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf

Haftendorn, H. 1991. *The Security Puzzle: Theory, Building and Discipline in International Security*. Intenational studies quarterly. vol.35 no.1, 3-17.

Kaspersky Resource Center. 2020. *What is Cyber Security?* Retrieved May 21, 2020 from Kaspersky.com: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kementrian Luar Negeri. 2019, April 7. *Kejahatan Lintas Negara*. Retrieved May 20, 2020 from Kemenlu.go.id: https:// kemlu.go.id/ portal/id /read/89/halaman_list_lainnya/kejahatan- lintas-negara

Midhio, I Wayan, Yono Reksoprodjo, and Hamzah Zaelani. 2018. *Pembangunan Kapasitas Cyber Security Di Negara Asean:Analisis Komparatif Terhadap Brunei Dan Indonesia*. Jurnal Prodi Perang Asimetris Volume 4, Nomor 1.

Moodie, M. 2000. *Cooperative Security: Implications for National Security and International Relations.* Albuquerque: Sandia National Laboratories.

Nolan, J. 1994. The Concept of Cooperative Security; Global Engagement, Cooperation and Security in the 21st Century. Washington D.C: Brookings.

Perwita, P. A. 2008. *Dinamika Keamanan dalam Hubungan Internasional dan Implikasinya Terhadap Indonesia*. 13.

Pratomo, Y. 2019 (Mei 16). *APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa.* Retrieved May 20, 2020 from Kompas News: https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa

Rosandry, I. 2018 (November 22). *Indra Rosandry,Merajut Diplomasi Siber Indonesia*. From Media Indonesia: https:// mediaindonesia.com/ read /detail/199360 -merajut-diplomasi-siber-indonesia

SOFIA TRISNI, R. I. 2017. *Peningkatan Keamanan Siber Asean Melalui Kerja Sama Keamanan Siber Dengan Australia.* ASEAN Studies Center Universitas Andalas.

Supriyadi, B. 2017. *Persepsi Bersama Indonesia-Australia Dalam Hibah Dana dan Peralatan Investigasi Cyber Crime dari Australia Kepada Indonesia.* Journal of International Relations, Volume 3, Nomor 1, 140-149.

Vetschera, H. 2007. *Cooperative Security: The Concept And Its Application In South Eastern Europe*.

Westcott, N. 2008. *Digital Diplomacy: The Impact of the Internet on International Relations*. Research Report 16, 14.