JPW (Jurnal Politik Walisongo) – Vol 6, No 1 (2024), 73-83
ISSN: 2503-3190 (p); 2503-3204 (e)
DOI: 10.21580/jpw.v6i1.19442

Kebijakan Luar Negeri Indonesia Melalui Diplomasi Siber Asean Regional Forum (ARF): Sanksi-Sanksi Dan Peran Indonesia

Kadek Nadya Ananda Putri

Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Udayana, Indonesia

Abstract

The rapid development of the technology and information industry requires individuals to be able to adapt to technological sophistication. Through technology, people can easily access the internet anywhere and anytime. As a result of the development of the internet, its reach is increasingly wider, ultimately bringing positive and negative impacts. One of the negative impacts that results is cybercrime which is detrimental to life. Thus, Indonesia together with ASEAN formed a regional forum to combat the issue of cyber-crime in the region. The aim of this research is to analyse the form of policy implemented by Indonesia in the results of the ASEAN Regional Forum diplomacy and Indonesia's role in cyber diplomacy. This research uses descriptive qualitative research methods by collecting literary sources such as journals, books and websites. The results of this research found that Indonesia's role in the ASEAN Regional Forum is very influential, and Indonesia shows its existence in proposing various proposals related to cyber security. The ASEAN Regional Forum cyber diplomacy also explained that there are three forms that can be taken, such as Confidence Building Measures, Preventive Diplomacy, and Conflict Resolution Mechanism. Thus, it can be concluded that the role of Indonesia's involvement in the ARF is not merely to be a participant, but to be able to provide suggestions that are included in the future work plan. Also, Indonesia has laws to deal with perpetrators and acts of domestic cyber-crime.

Pesatnya perkembangan industri teknologi dan informasi menuntut individu untuk dapat beradaptasi dalam kecanggihan teknologi. Melalui teknologi, masyarakat dapat dengan mudah mengakses internet dimanapun dan kapanpun. Akibat dari perkembangan internet yang semakin luas jangkauannya, pada akhirnya membawa dampak positif dan negatif. Dampak negatif yang dihasilkan salah satunya yaitu kejahatan siber yang merugikan kehidupan. Dengan demikian, Indonesia bersama dengan ASEAN membentuk forum regional untuk memerangi isu kejahatan siber dalam kawasannya. Tujuan dari penelitian ini adalah untuk menganalisis bentuk kebijakan yang diterapkan Indonesia dalam hasil diplomasi ASEAN Regional Forum dan peran Indonesia dalam diplomasi siber. Penelitian ini menggunakan metode penelitian kualitatif deskriptif dengan mengumpulkan sumber-sumber literatur seperti jurnal, buku, dan *website*. Hasil dari penelitian ini ditemukan bahwa peran Indonesia dalam ASEAN Regional Forum sangat berpengaruh dan Indonesia memperlihatkan eksistensinya dalam mengusulkan berbagai usulan terkait keamanan siber. Diplomasi siber ASEAN Regional Forum pun menerangkan bahwa terdapat tiga bentuk yang dapat dilakukan, seperti *Confidence Building Measures, Preventive Diplomacy,* dan *Conflict Resolution Mechanism*. Dengan demikian dapat disimpulkan bahwa, peran keterlibatan Indonesia dalam ARF tidak semata-mata hanya menjadi peserta saja, tetapi mampu memberikan usulan yang dimasukan dalam *workplan* kedepannya. Serta, Indonesia memiliki undang-undang dalam menangani pelaku dan tindakan kejahatan siber domestiknya.

Keywords: Diplomasi Siber, Peran Indonesia, Kebijakan Luar Negeri, ASEAN Regional Forum

Pendahuluan

Arus perkembangan globalisasi sangat dinamis dari waktu ke waktu. Pesatnya perkembangan yang disebabkan oleh globalisasi ini menyebabkan teknolgi semakin massif keberadaannya. Penggunaan smartphone, gadget, serta barang elektronik lainnya menandakan bahwa kecanggihan dan kemassifan dari keberadaan teknologi ini yang pada akhirnya menuntut individu untuk bisa beradaptasi. Kemasifan teknologi tidak hanya berdampak bagi industri-industri tekstil atau industri otomotif saja, tetapi berdampak lebih luas bagi interaksi internasional. Luasnya pengaruh teknologi ini sebab adanya ketidakterbatasan "dunia" globalisasi.

Istilah "globalisasi" sebetulnya sudah ada sejak tahun 1930-an dan juga menjadi "buzzword" atau frasa yang popular pada tahun 1990-an (James dan Stege, 2014). Lebih lanjut, menurut McGrew (2005) turut memberikan pandangan bahwa globalisasi dapat dipahami melalui sebuah proses yang ditandai dengan beberapa hal, seperti: (1) Stretching atau peregangan aktivitas dalam bidang sosial, politik, budaya, serta ekonomi yang melampaui batas-batas nasional negara. (2) Growing Magnitude atau pesatnya keterhubungan (interconnectedness) dalam berbagai aspek kehidupan. (3) The Accelerating Pace atau kecepatan laju interaksi global yang diiringi oleh perkembangan transportasi dan komunikasi. (4) The Growing, Extensity, and Velocity atau bertambahnya perluasan, intensitas, serta kecepatan interaksi global.

Perkembangan globalisasi yang pesat membawa dampak bagi kehidupan nasional dan global. Bagi sebagian masyarakat menganggap globalisasi ini membawa pengaruh yang positif karena memudahkan aktivitas kita untuk berkomunikasi, mencari informasi jarak jauh, dan juga memudahkan kita melakukan hal yang yang bersifat lintas batas negara. Akan tetapi, dibalik semua manfaat positif tersebut, nyatanya ada pula dampak negatif yang mungkin kerap sekali kita mengabaikannya. Globalisasi dapat membawa dampak negatif bagi kehidupan bangsa kita seperti, perilaku masyarakat yang individualis, kesehatan yang menurun sebab paparan sinar radiasi dari gadget, kadar polusi yang semakin bertambah, bahkan globalisasi juga memengaruhi tingkat keamanan siber nasional sehingga diperlukannya peningkatan sekuritisasi negara.

Kecanggihan penggunaan barang elektronik yang kita gunakan saat ini dapat dengan mudah disalahgunakan oleh beberapa oknum, seperti tindakan peretasan, pencurian data, kejahatan malware yang menyebabkan kerugian pada masyarakat. Kerugian-kerugian ini juga berkaitan dengan dampak dari internet. Ruang lingkup internet menjadi jejaring yang luas dalam kehidupan global. Adanya internet ini membawa individu ke dalam suatu ruang yang disebut dengan "cyberspace" atau dunia maya. Cyberspace merupakan sebuah bentuk dunia yang bersifat "imajiner" dan mempermudah setiap individu untuk melakukan aktivitas sosialnya dengan gaya yang baru, yaitu dalam bentuk AI (Artificial Intelligence). Menurut Kementerian Pertahanan (2014, hal.5) cyberspace adalah ruangan atau dunia komunikasi berbasis perangkat keras seperti komputer dengan realitas yang unik, dalam hal ini realitas yang dimaksud adalah realitas virtual. Ruang siber juga membawa efek negatif dalam penerapannya. Adanya kemudahan untuk mengakses internet dapat mempersuasi masyarakat untuk bertindak kriminal. Tindakan kriminal dalam ruang siber disebut dengan kejahatan siber atau cybercrime.

Tindakan kejahatan siber belakangan ini telah menyerang sebagian besar negara. Canggihnya teknologi, dan dinamika kehidupan menyebabkan kejahatan siber merajalela. Kejahatan siber atau cybercrime merupakan tindakan ilegal yang dilakukan melalui pemanfaatan teknologi informasi dan komunikasi (TIK). Target dalam operasional ilegal ini adalah teknologi atau jaringan itu sendiri. Secara sederhana, cybercrime ini menggunakan teknologi atau (TIK) dengan target sasaran teknologi milik orang lain. Meningkatnya kejahatan siber dalam dunia global disebabkan oleh beberapa faktor-faktor mulai dari faktor eksternal maupun faktor

internal. Penyebab yang berasal dari faktor eksternal antara lain seperti, kecanggihan fitur-fitur teknologi, situ-situs jaringan yang memudahkan para peretas untuk beroperasional, penegakkan hukum yang lemah, penawaran-penawaran pekerjaan yang ilegal seperti hacking untuk mendapatkan hasil upah yang tinggi, dan lainnya. Sedangkan, faktor internal dapat terjadi karena kesenjangan sosial dan ekonomi individu sehingga para pelaku dapat melakukan tindakan kriminal untuk mendapatkan upah, dan lainnya.

Heinl mengemukakan bahwa potensi dari ancaman siber ini paling banyak dilakukan di negara-negara seperti ASEAN pada tahun 2012-2013, khususnya yang menjadi target adalah penyerangan pada website atau situs-situs resmi milik pemerintahan (Heinl, C. H., 2013 hal 137). Informasi dan data-data dari pemerintahan ini sangat bernilai tinggi, sebab itu tindakan peretasan kerap sekali terjadi di lingkungan pemerintahan, tetapi tidak berarti bahwa cybercrime tidak dapat memasuki lingkungan masyarakat itu sendiri. Menurut informasi dari Kementerian Pertahanan (2014, hal.14), dampak-dampak dari tindakan penyerangan siber ini dapat berupa adanya penyalahgunaan informasi, pengendalian sistem dengan cara remote, kerugian finansial, kekerasan, konflik, dan data-data yang disalahgunakan. Dampak dari kejahatan siber ini sangat berbahaya karena dapat mengintai segala tindak tanduk yang kita lakukan melalui teknologi dan kejahatan siber ini bersifat sangat luas hingga global.

Bentuk-bentuk dari kejahatan siber atau cybercrime ini memiliki banyak jenis yang dapat kita temui secara umum, seperti: spionage, carding, cyber terrorism and cybersquatting, data forgery, illegal content, unauthorized access, offense against, infringements of privacy, cyber phishing, cyber ransomware, SIM swap, skimming crime dan masih banyak lagi bentuk-bentuk kejahatan siber (I Nyoman & Wayan, 2018:5). Dengan berbagai macam jenis-jenis cybercrime yang mengganggu stabilitas kehidupan membuat banyak pihak pemerintahan terutama pemerintah global semakin aware terhadap tindakan illegal ini, sehingga dibutuhkannya peningkatan upaya keamanan baik di di tingkat nasional, regional, maupun global. Kesadaran akan pentingnya sekuritisasi atau peningkatan keamanan dalam bidang siber membuat negara-negara di ASEAN (Association of Southeast Asian Nations) semakin mengupayakan berbagai cara untuk memerangi kasus kejahatan siber di kawasannya. Dengan demikian ASEAN membentuk sebuah Diplomasi Forum Regional untuk membahas isu-isu kejahatan siber yang menyerang Kawasan negara-negara anggotanya. ASEAN Regional Forum ini merupakan satu-satunya forum di tingkat pemerintahan yang dihadiri oleh seluruh negara-negara besar di kawasan Asia Pasifik dan kawasan lainnya (Kemlu, 2019). Dalam perundingan diplomasi siber yang dilakukan, Indonesia menunjukkan eksistensi dan keterlibatannya dalam ARF serta mengusung berbagai macam ide untuk memerangi kasus kejahatan siber serta hasil usulan tersebut akan dirundingkan dan hasil resminya akan dimasukkan dalam agenda resmi dari ARF.

Berdasarkan uraian latar belakang diatas penulis merumuskan masalah yang dihadapi penelitian ini, yaitu bagaimanakah peran Indonesia dalam diplomasi keamanan siber dan sanksi-sanksi yang diterapkan kepada pelaku keamanan siber. Dengan demikian penelitian ini dimaksudkan untuk menjawab pokok permasalahan tersebut serta meninjau dan menganalisis organisasi internasional seperti ASEAN terlibat dalam diplomasi keamanan siber melalui ARF dan juga penelitian ini akan melibatkan hukum internasional yang diberikan terhadap pelaku kejahatan siber.

Tinjauan Pustaka

Penelitian ini menggunakan penelusuran beberapa literatur yang membahas mengenai diplomasi Indonesia dengan ASEAN dalam memerangi kejahatan siber dan membandingkan beberapa literatur yang menjadi tinjauan yang masih belum banyak jurnal membahas mengenai diplomasi Indonesia dengan ASEAN.

Pertama, jurnal yang berjudul *"ASEAN Regional Forum: Realizing Regional Cyber Security In ASEAN Region"* karya Bima Yudha Wibawa M. dan Diah Apriani Atika S. pada tahun 2015, yang menjelaskan mengenai upaya untuk meningkatkan keamanan siber di Kawasan ASEAN melalui forum regional dengan menawarkan 3 mekanisme, diantaranya: *Confidence Building Measure (CBM),* yang berfungsi untuk memperkuat kepercayaan dari masing-masing anggota ARF *(ASEAN Regional Forum)* untuk pengembangan keamanan siber, lalu ada *Preventive Diplomacy* yang bertujuan untuk tindakan preventif, dan terakhir ada *Conflict Resolution* yang bertujuan untuk menyesuaikan dalam hukum, tetapi sedang dalam tahap pengembangan. Jurnal ini dikemas dengan menggunakan prinsip dari ASEAN itu sendiri dan membahas mengenai adanya mekanisme kerja sama bilateral terkait keamanan siber. Penelitian yang ditulis oleh jurnal ini hanya menjelaskan mengenai konsep keamanan kawasan dan mekanisme ersama saja tanpa mempertimbagkan bentuk sanksi yang diberikan terhadap pelaku kejahatan siber yang merajalela.

Kedua, Jurnal yang berjudul *"Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber"* yang ditulis oleh Afifah Fidiana Rosy tahun 2020, yang menjelaskan mengenai upaya memperkuat keamanan siber dalam tingkat nasionalnya melalui diplomasi dan kerja sama bilateral maupun multilateral. Penelitian tersebut kurang memberikan paparan tentang peran yang dapat ditawarkan oleh Indonesia dalam proses kerja sama bilateral maupun multilateral.

Melalui kedua literatur tersebut, peneliti menawarkan kebaruan yang belum dijelaskan dalam beberapa jurnal diatas. Maka dari itu, peneliti mencoba untuk menjelaskan sanksi-sanksi yang ditetapkan oleh ARF kepada pelaku kejahatan siber serta peran Indonesia dalam diplomasi *ASEAN Regional Forum* tersebut.

Kerangka Teoritis

Model Kebijakan Luar Negeri Graham T. Allison

Untuk menjawab pertanyaan-pertanyaan penelitian, penulis menggunakan salah satu teori kebijakan luar negeri yang diusung oleh Graham T. Allison dalam bukunya yang berjudul "Essence of Decision: Explaining The Cuban Missile Crisis) yang dipublikasikan pada tahun 1971. Dalam bukunya, Allison menjelaskan bahwa proses pengambilan kebijakan luar negeri dibagi menjadi tiga paradigma untuk menganalisis, diantaranya:

1. RAM (Rational Actor Model)

Model Aktor Rasional ini menjelaskan bahwa dalam proses pengambilan keputusan, actor internasional akan memutuskan dengan segala bentuk-bentuk pertimbangan yang menggunakan kalkulasi intelektual, rasio atau akal sehingga sebagai actor ia akan mendapatkan konsekuensi dengan keuntungan yang tinggi dan kerugian yang rendah. Kalkulasi untung-rugi dan menang-kalah akan menjadi bentuk pertimbangan Kembali agar proses pengambilan kebijakan dapat dibentuk dengan matang dan aplikatif.

2. Model Proses Organisasi (The Organizational Process)

Pada model ini lebih menekankan pada bagaimana kebijakan diambil melalui berbagai proses dan prosedur dalam organisasi yang sesuai dengan SPO (Standard Procedure Operating) yang ada pada organisasi tersebut. Hasil dari pengambilan keputusan dapat berupa bentuk output dari proses organisasi yang melibatkan aktor di dalamnya.

3. Model Politik Birokrasi (Bureaucratic/Governmental Politics)

Model ini menekankan pada proses pengambilan keputusan yang di dalamnya

melibatkan pihak-pihak yang berkepentingan. Pihak ini merujuk pada birokrat. Para birokratik bertanggung jawab pada proses perumusan kebijakan. Model politik birokrasi ini merujuk pada bentuk-bentuk kompromi, koordinasi, deliberasi, juga kompleksitas yang terjadi dalam proses pengambilan kebijakan.

Diplomasi Siber

Diplomasi merupakan bagian penting dari instrumen interaksi suatu negara dalam hubungan internasional dan memiliki tujuan untuk mencapai kepentingan nasional. Menurut Bull (1977, hal. 156) sebagai salah satu tokoh dari mazhab English school memandang bahwa konsep diplomasi ini dipandang sebagai sesuatu perilaku dari hubungan antara negara dengan entitas dalam ker ja sama politik internasional yang dilakukan oleh beberapa aktor resmi dengan cara yang damai. Diplomasi melibatkan berbagai macam jenis dari perilaku aktor-aktor internasional. Tetapi, keberhasilan atau kegagalan dari proses diplomasi ini bergantung pada kemampuan dari para representasi negara seperti diplomat untuk mengenali dinamika power. Wight (1979) memandang bahwa diplomasi dapat diartikan sebagai upaya yang digunakan untuk menyesuaikan arus kepentingan nasional yang saling bertentangan antara actor satu dengan lainnya melalui negosiasi dan juga proses kompromi. Terdapat lima fungsi dari diplomasi ini, diantaranya: pertama, diplomasi digunakan untuk memberikan fasilitas berkomunikasi dalam politik dunia. Kedua, diplomasi digunakan untuk menegosiasikan suatu perjanjian Bersama. Ketiga, diplomasi digunakan untuk mengumpulkan informasi dan intelijen dari negara lainnya. Keempat, diplomasi digunakan untuk menghindari adanya gesekan dari hubungan internasional. Kelima, diplomasi digunakan untuk ersam keberadaan Masyarakat dalam suatu negara (Bull, 2002). Sedangkan menurut Hans J. Morgenthau, dijelaskan bahwa definisi diplomasi adalah “Diplomacy is the promotion of the national interests by peaceful means” (Setiawan, 2016, hal. 04). Morgenthau mendefinisikan diplomasi dalam 2 arti, yaitu arti luas dan arti sempit. Diplomasi dalam arti luas didefinisikan dalam menyangkut perumusan dan pelaksanaan politik luar negeri dari tingkatan yang tinggi hingga rendah. Sedangkan, diplomasi dalam arti sempit memiliki arti bahwa diplomasi menjadi suatu cara Dimana hubungan resmi antar pemerintah terjadi. Merujuk pada pengertian diplomasi, terdapat bentuk-bentuk diplomasi, salah satu bentuk diplomasi yang dilakukan Indonesia untuk menjaga keamanan negaranya adalah diplomasi siber (cyber diplomacy). Diplomasi siber dapat dikatakan sebagai upaya untuk memfasilitasi komunikasi, menegosiasi, mengumpulkan informasi intelijen dari negara lain dan menghindari gesekan siber. Lalu, diplomasi siber juga dapat dikatakan sebagai upaya diplomatik untuk mengamankan terkait ruang siber negara (Hamonangan & Assegaf, 2020). Cyber diplomacy dalam perundingannya melibatkan diplomasi, resolusi, perjanjian, dan kebijakan siber. Diplomasi siber dapat dilakukan oleh aktor-aktor negara maupun aktor non-negara. Cyber diplomacy dapat dilakukan melalui kementerian luar negeri dan kedutaan yang berlokasi di suatu negara.

Organisasi Internasional

Organisasi internasional merupakan wadah untuk melakukan pola kerjasama yang bersifat lintas batas negara, dan didasari pada struktur organisasi yang jelas serta memiliki tupoksi atau tugas pokok dan fungsi yang berkelanjutan demi mencapai tujuan yang disepakati secara bersama. Menurut Clive Archer, organisasi internasional (OI) memiliki tiga peran utama dalam sistem internasional, diantaranya:

1. Sebagai Instrumen

Organisasi internasional ini digambarkan sebagai instrumen bagi para aktor untuk mencapai tujuan tertentu dan sebagai sarana bagi aktor untuk berdiplomasi.

2. Sebagai Arena

Organisasi internasional dikatakan sebagai arena maksudnya adalah sebagai tempat berkumpul, berdiskusi, berdebat, serta bekerja sama dalam membahas suatu tujuan kepentingan bersama. Dalam praktiknya, organisasi internasional harus bersifat netral dan tidak boleh memihak aktor manapun.

3. Sebagai Aktor

Organisasi internasional sebagai aktor adalah bahwa organisasi internasional ini bersifat independen dan dapat bertindak tanpa adanya pengaruh dari pihak luar manapun.

ASEAN Regional Forum (ARF)

ARF merupakan salah satu forum regional yang diusung oleh ASEAN dalam membahas isu-isu internasional. ARF juga merupakan salah satu program yang berada di bawah koordinasi Dewan Masyarakat Politik dan Keamanan ASEAN (ASEAN Political-Security Community). Anggota dari ARF yang terlibat sebanyak 26 negara dan 1 entitas dari Uni Eropa (dengan total keseluruhan sebanyak 27 negara). Negara-negara yang terlibat adalah 10 negara ASEAN, yaitu Indonesia, Brunei Darussalam, Malaysia, Kamboja, Thailand, Laos, Myanmar, Filipina, Singapura, Vietnam. Lalu ada 10 mitra ASEAN, yaitu Amerika Serikat, Australia, Kanada, India, Republik Rakyat Tiongkok, Selandia Baru, Jepang, Rusia, Korea Selatan, dan Uni Eropa. Serta terdapat 7 negara kawasan, seperti Bangladesh, Korea Utara, Mongolia, Pakistan, Papua Nugini, Sri Lanka, dan Timor Leste). Penyebutan untuk keanggotaan ARF adalah peserta (participant). ASEAN Regional Forum dibentuk pada tahun 1994 sebagai wadah konsultasi dan dialog mengenai hal-hal politik dan keamanan di kawasan serta membahas dan menyamakan pandangan antarnegara peserta ARF guna untuk meminimalisir ancaman terhadap stabilitas dan keamanan kawasan (Kemlu, 2019).

Metode Penelitian

Penulis menggunakan metode penelitian kualitatif deskriptif. Metode ini digunakan karena dapat mencakup berbagai isu sosial dan memberikan pemahaman terhadap berbagai fenomena sosial. Penelitian jenis kualitatif deskriptif ini mampu memberikan penjelasan, serta menganalisis dengan kompleks. Menurut Creswell, penelitian kualitatif dijelaskan sebagai berikut:

"Qualitative research begins with assumptions and the use of interpretive/theoretical frameworks that inform the study of research problems addressing the meaning individuals or groups ascribe to a social or human problem" (Creswell, 2013, hal. 44).

Penelitian ini menggunakan Teknik pengumpulan data sekunder dengan merujuk pada berbagai jurnal, buku, artikel, dan literatur dari website terkait. Penjabaran metode kualitatif deskriptif ini disajikan dalam bentuk penjelasan berupa kata-kata dan bukan berupa angka.

Hasil dan Pembahasan

Isu keamanan tradisional bukan lagi menjadi fokus utama dunia internasional. Isu-isu keamanan non-traditional berhasil mencuri perhatian pemerintah global belakangan ini. Salah satunya isu keamanan siber. Dalam menanggapi isu kejahatan siber yang sifatnya merugikan kehidupan sosial dan negara, Indonesia dan berbagai negara kawasan regional seperti ASEAN melakukan perundingan diplomasi untuk mencari upaya mengatasi isu keamanan kawasannya. ASEAN membentuk forum regional yang dinamakan ASEAN Regional Forum (ARF). Dalam pertemuan Tingkat Menteri ke-27 ASEAN pada tahun 1994, para menteri luar negeri menyetujui bahwasanya "ARF could become an effective consultative Asia-Pacific Forum for promoting open dialogue on political and security cooperation in the region. In this context, ASEAN should work with its ARF partners to bring about a more predictable and constructive pattern of relations in the Asia Pacific" (Kemlu, 2019).

Menurut data dari Kemlu (2019) pembentukan dari ARF ini memiliki tujuan sebagai berikut:

1. Mendorong dialog dan konsultasi yang konstruktif mengenai isu-isu politik serta keamanan yang menjadi perhatian bersama di kawasan.
2. Memberikan kontribusi nyata bagi upaya pembangunan rasa saling percaya (confidence-building) dan diplomasi preventif (preventive diplomacy) di lingkungan kawasan Asia Pasifik.
3. Mendorong Kerjasama yang menumbuhkan budaya damai, toleransi, saling memahami dan beradab. ARF diharapkan dapat mendukung upaya untuk menciptakan lingkungan yang kondusif bagi Pembangunan yang berkelanjutan dan bagi kemajuan yang bermanfaat bagi kehidupan.

Model Proses Organisasi

Model Proses Organisasi (The Organizational Process) digunakan oleh aktor-aktor organisasi pemerintahan maupun non-pemerintahan untuk berunding sesuai prosedur organisasi dalam menemukan output (Allison, 1971). Dalam diplomasi siber yang dilakukan Indonesia pada ARF memiliki pendekatan yang bersifat evolusioner dan berlangsung dalam tiga tahapan, yaitu:

1. Confidence Building Measures

Upaya untuk membangun kepercayaan anggota yang mengedepankan dialog dan konsultasi. Menurut Menlu RI Retno Marsudi, pendekatan "tit for tat" telah menghambat krisis kepercayaan dan juga kerja sama yang mendalam (Portal Informasi Indonesia, 2023). Maka dari itu, dibutuhkannya Pembangunan kepercayaan masing-masing anggota dalam kawasan untuk dapat bekerja sama.

2. Preventive Diplomacy

Mekanisme pencegahan konflik yang lebih responsive dalam menghadapi tantangan dari ancaman keamanan di kawasan.

3. Conflict Resolution Mechanism

Merumuskan resolusi konflik yang dapat menjaga stabilitas negara kawasan.

Berdasarkan konsep proses organisasi, Keputusan ARF ini diambil melalui consensus setelah melalui berbagai macam bentuk konsultasi antar para peserta ARF. Sejak berdirinya di Bangkok pada tahun 1994, ARF telah mengalami evolusi, seperti:

1. Pemajuan dan peningkatan kepercayaan antarnegara peserta.
2. Pengembangan diplomasi pencegahan.
3. Elaborasi mengenai pendekatan pencegahan konflik. (Kemlu, 2019).

Menanggapi kasus kejahatan siber dan tindakan keamanan siber, ARF mengadakan sesi dialog mengenai isu-isu militeristik, pertahanan, juga keamanan secara rutin melalui ARF Defense Official Dialogue, ARF Security Policy Conference, ARF Heads of Defense Universities/College, Institutions Meeting. Adapun area kerja sama yang menjadi pokok bahasan ARF, yaitu:

1. Penanggulangan bencana (disaster relief)
2. Kontra-terorisme dan kejahatan lintas batas negara (Counter-terrorism and transnational crime).
3. Keamanan maritim (maritime security)
4. Non-proliferasi dan perlucutan senjata (Non-proliferation and disarmament)
5. Teknologi informasi dan komunikasi (Information and communication technologies).

Peran dan Kepentingan Nasional Indonesia Dalam ARF

Bentuk-bentuk kejahatan siber kerap sekali mengincar berbagai objek-objek vital dan riskan, terkhususnya dalam hal teknologi dan informasi. Hal ini tentunya memberikan dampak yang negatif dan merugikan. Padahal, jika saja ruang siber ini diaplikasikan secara benar dan tepat, hal ini akan memiliki dampak positif untuk keberlangsungan perekonomian negara serta pemajuan digitalisasi. Dengan perkembangan industri yang semakin pesat, keamanan siber sangat diketatkan untuk melindungi bagian-bagian vital negara. Dengan melalui peningkatan siber dalam diplomasi dan kerja sama internasional ASEAN Regional Forum. Melalui ARF, Indonesia dapat menunjukkan eksistensinya dalam berkomitmen, serta memperlihatkan kemampuan untuk menyelesaikan permasalahan. Kerja sama ini menjadi media dalam memperlihatkan kontribusi dari Indonesia dalam menjaga dan mempertahankan tindakan keamanan dan

kedamaian dunia. Menurut K.J Holsti (1988), kepentingan nasional Indonesia dapat diidentifikasikan dalam 3 hal, yaitu:

1. Core values: Sesuatu yang paling vital yang menyangkut eksistensi suatu negara.
2. Middle-range objectives: Hal ini menyangkut kebutuhan ekonomi suatu negara.
3. Long-range goals: Sesuatu yang sifatnya ideal, seperti persoalan perdamaian dan ketertiban dunia.

Peran Indonesia dalam ARF menggambarkan bahwa upaya dari Indonesia berhasil untuk memenuhi kepentingan nasionalnya melalui prinsip eksternal, yaitu kerja sama dan diplomasi dengan negara-negara kawasan ataupun organisasi internasional. Keikutsertaan Indonesia dalam forum regional ASEAN menegaskan bahwa Indonesia memandang ancaman dari kejahatan siber (cyber crime) merupakan situasi yang perlu mendapatkan perhatian yang khusus karena hal ini mengancam kedaulatan negara dan keamanan nasional negara (Jackson & Sorensen, 2013).

Diplomasi Indonesia Dalam Bidang Siber

Diplomasi siber merupakan instrumen dalam melakukan negosiasi serta menjalin kerja sama antarnegara terkhususnya dalam bidang keamanan siber. Meningkatkan keamanan siber tidaklah mudah. Menurut kaum liberalis, suatu aktor tidaklah dapat berdiri sendiri, mereka memerlukan dukungan dan bantuan untuk bekerja sama dengan aktor lainnya dalam mencapai kepentingan bersama. Maka dari itu, Indonesia dalam meningkatkan keamanan siber negaranya membutuhkan kerja sama dengan negara kawasan ataupun internasional. Hal ini berkaitan dengan bagaimana bentuk diplomasi Indonesia di dalam ARF. Di dalam forum internasional ASEAN Regional Forum, Indonesia menggunakan diplomasi siber sebagai instrumen utamanya mencapai kepentingan nasional. Melalui perundingan tersebut, Indonesia dapat mengembangkan kapasitas keamanan wilayahnya sekaligus berkontribusi pada stabilitas keamanan lingkup kawasan. Indonesia melalui ARF meluncurkan beberapa poin terkait keamanan siber, diantaranya:

1. Point of Contact

Bentuk capaian Indonesia salah satunya melalui bentuk kontak poin dari perwakilan negara-negara yang berada di lingkup ASEAN maupun regional yang memiliki persoalan yang sama yaitu cybersecurity. Kontak poin ini diusung oleh Indonesia sebagai cara untuk memudahkan proses diplomasi dalam penanganan kejahatan siber, maupun hal-hal lain yang memiliki tujuan yang sama. Kontak poin yang tidak sebatas nama instansi, atau nomor instansi saja, tetapi juga nomor pribadi seperti e-mail, serta nomor telepon pribadi pejabat yang memiliki kewenangan besar. Cara ini merupakan salah satu cara yang dapat memudahkan Indonesia untuk mendapatkan hasil yang maksimal karena proses diplomasi dan komunikasi dapat dilaksanakan lebih mudah. Usulan kontak poin ini merupakan usulan resmi dan orisinil dari Indonesia. Gagasan ini kemudian disepakati dan dituang dalam dokumen resmi ASEAN Regional Forum Workplan on Security of and in the Use of Information and Communications Technologies (ICT's). Kontak poin ini digunakan untuk memudahkan identifikasi pelaku kejahatan siber.

2. Capacity Building Melalui Study Group

Belum ada kebijakan regional yang menyangkut keamanan siber. Hal ini membuat Indonesia mengusung dan mempromosikan keperluan keamanan siber dalam Tingkat regional. Indonesia menyarankan untuk Menyusun kurikulum terkait siber. Lalu Indonesia juga mengusulkan pembentukan study group untuk menganalisis, mengkaji, dan merumuskan kurikulum tersebut. Study group mencakup diadakannya hal-hal seperti workshop, seminar, dan pelatihan di tingkat regional tentang penanganan siber. Indonesia dengan delegasi Rusia dalam study group itu mulai membentuk simulasi penanganan insiden siber (David & Arwin, 2016:17).

3. Internet Protocol Version 4 (Ipv4) Upgrade (Ipv6).

Indonesia mengusulkan untuk seluruh negara-negara ASEAN untuk melakukan transisi terhadap penggunaan Ipv4 menuju

Ipv6. Hal ini merupakan Solusi untuk peningkatan sistem keamanan internet. Ipv6 memiliki sistem keamanan yang lebih baik daripada Ipv4. Namun, usulan yang dilakukan oleh Indonesia saat itu tidak mendapat respons yang memuaskan. Hal ini dikarenakan bahwa delegasi yang dikirim merupakan seseorang yang kurang menguasai bidang cyber (David & Arwin, 2016:12).

4. Pembentukan Badan yang Bertanggung Jawab Mengenai Cyber security Oleh Masing-Masing Negara.

Indonesia telah membentuk Badan Siber dan Sandi Negara (BSSN) yang bersifat resmi dan khusus dalam menangani bidang siber serta sandi negara. BSSN ini bertugas dalam bidang deteksi, identifikasi, proteksi, pemantauan, penanggulangan, pemulihan, evaluasi, pengendalian, persandian, diplomasi siber, dukungan mitigasi, pusat kontak siber, serta penanggulangan insiden dan serangan siber.

Dalam usulan diplomasi keamanan siber yang diusung Indonesia dalam ASEAN Regional Forum, telah dicapai hasil bahwa 2 susulan diterima dan disepakati oleh forum yang dituangkan dalam ASEAN Regional Workplan on Security and in the Use of Information and Communications Technologies (ICT's).

Undang-Undang Indonesia Terhadap Keamanan Siber Negara

Sanksi-sanksi yang diberikan pada pelaku kejahatan siber secara khusus diatur oleh undang-undang negara masing-masing. Indonesia dalam menegakkan hukum dalam memberantas cybercrime memiliki Undang-Undang yang mengatur mengenai peretasan sistem. Di Indonesia, peretasan ini dimuat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) (Kominfo, 2015). Tindak pidana bagi pelaku kejahatan siber di Indonesia diatur dalam pada pasal 30 ayat 1, ayat 2, dan atau ayat 3 UU No. 11/2008. Pada ayat 1 berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun". Kemudian ayat 2 berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik". Terakhir, ayat 3 berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan" (Kominfo, 2015).

Lalu ada juga pasal 32 ayat 1 UU No. 11/2008 yang berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transaksi, merusak, menghilangkan, hingga memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik" (Kominfo, 2015).

Dan diatur juga dalam pasal 22 huruf B UU No. 36/1999 yang berbunyi " Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi; dan atau akses ke jasa telekomunikasi; dan atau akses ke jaringan telekomunikasi khusus" (Kominfo, 2015).

Kesimpulan

Perkembangan globalisasi sangat bersifat dinamis. Globalisasi selalu mengikuti arah kehidupan masyarakat. Pesatnya perkembangan globalisasi menyebabkan teknologi semakin massif keberadaannya. Sebagian masyarakat dunia mengira teknologi ini membawa dampak yang positif bagi kehidupan sosial. Namun, nyatanya dampak yang dihasilkan juga mengerikan dan negative. Adanya teknologi membuat kita semakin mudah untuk berinteraksi melalui jaringan internet. Berinteraksi dari jarak jauh, hingga dapat melakukan transaksi jarak jauh pula. Lebih lanjut, adanya keluasan dan ketidakterbatasan penggunaan internet menyebabkan hadirnya ancaman tersendiri, salah satunya adalah kejahatan siber atau cybercrime.pemerintah global saat ini sangat mendorong dan memfokuskan pada tingkat keamanan non-tradisional yang sifatnya tidak terasa dan low politics. Indonesia dalam menanggapi isu kejahatan siber ini tidak tinggal diam. Bersamaan dengan

perkembanganya, Indonesia melakukan diplomasi dengan negara-negara ASEAN dan negara kawasan Asia Pasifik yang bernama "ASEAN Regional Forum". ARF merupakan wadah dan tempat berkumpulnya, serta berkomunikasi untuk merundingkan isu-isu persoalan keamanan dalam area kawasan regional ASEAN.

ARF dihadiri oleh sekitar 27 peserta. ARF ini memiliki beberapa tujuan didalamnya, seperti mendorong kerja sama, mendorong kontribusi, serta mendorong dialog antarnegara yang terlibat dalam perundingan diplomasi tersebut. Kerja sama yang dilakukan oleh forum ARF ini dapat kita analisis melalui model proses organisasi, yaitu salah satu proses pengambilan kebijakan yang diusung oleh Graham T. Allison. Dalam hal ini, ARF memang melakukan beberapa proses yang sesuai dengan konsensus dan prinsip dari ASEAN itu sendiri. Hasil dan pembahasan dari ARF membuahkan 3 bentuk tahapan, diantaranya Confidence Building Measures (CBM) yang berfokus pada upaya untuk meningkatkan rasa saling percaya antarnegara kawasan. Preventive Diplomacy yaitu melakukan pencegahan konflik secara responsive. Serta Conflict Resolution Mechanism yaitu mekanisme untuk merumuskan solusi-solusi dalam upaya menjaga stabilitas keamanan nasional. Selanjutnya, dalam forum ARF pun membahas mengenai keamanan siber yang menjadi isu panas. Dalam hal ini, Indonesia mengusulkan beberapa ide atau solusi untuk menangani persoalan kejahatan siber, seperti Point of Contact, Capacity Building Study Group, Upgrade IPv4 to IPv6, dan Pembentukan Badan Siber. Usulan yang diajukan oleh Indonesia membuah respon dalam forum. 2 ide usulan Indonesia diterima dan dituangkan dalam Workplan ICT's. Tidak hanya menyediakan upaya untuk mencegah kejahatan siber saja, tetapi Indonesia dalam praktik hukum domestiknya memiliki Undang-Undang yang mengatur kejahatan dan keamanan pribadi, yaitu Undang-Undang ITE. Dalam undang-undang tersebut, terdapat pasal-pasal yang menjelaskan segala tindakan apa saja yang tergolong dalam kejahatan siber. Dengan demikian, kebijakan luar negeri Indonesia dan diplomasi siber yang dilakukan dalam ASEAN Regional Forum menjawab seluruh pertanyaan dalam rumusan masalah.

DAFTAR PUSTAKA

Allison, G. T. (1971). Essence of Decision: Explaining the Cuban Missile Crisis. Little, Brown & Company Canada.

ASEAN, S. (2020). Sekretariat Nasional ASEAN – Indonesia. Setnasasean.id. https://setnasasean.id/asean-regional-forum-arf

BSSN. (2020). BSSN: Budaya Keamanan Siber Faktor Keberhasilan Diplomasi Indonesia | www.bssn.go.id. https://Www.bssn.go.id. https://www.bssn.go.id/bssn-budaya-keamanan-siber-faktor-keberhasilan-diplomasi-indonesia-2/

Chotimah, H. C., Iswardhana, M. R., & Pratiwi, T. S. (2019). Penerapan Military Confi dence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber. Jurnal Ketahanan Nasional, 25(3), 331. https://doi.org/10.22146/jkn.50344

Fadhillah1, S., Sharon, M., Matakupan2, A., Berlian Mingga3, B., Jakarta, U., Letjen, J., Parman, S., 16, Tomang, K., Grogol, Kota, J., Barat, D., Khusus, I., & Jakarta. (2023). Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes. Journal on Education, 05(04), 16553–16564.

Ferdin Bakker, F., Imigrasi, P., Parama, A., Imigrasi, P., Triana, R., & Politeknik, P. (2020). Peran ASEAN Dalam Menanggulangi Isu-Isu Utama Kejahatan Lintas Negara di Kawasan Asia Tenggara (The Role of ASEAN in Tackling the Main Issues of Transnational Crime in the Southeast Asia Region). | JLBP |, 2(1).

Hamonangan, I., & Assegaff, Z. (2020). Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital. Padjadjaran Journal of International Relations, 1(3), 311–333. https://doi.org/10.24198/padjir.v1i3.26246

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. Jurnal Konstituen, 5(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Kartiko, G. (2013). Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional. Rechtidee, 8(2), 136–153. https://doi.org/10.21107/ri.v8i2.695

Kawitri, T., & Sushanti, S. (2022). Globalisasi: Diemensi dan Implikasinya (Pertama, pp. 1–4). Jejak Pustaka.

Kemlu. (2018a). Asean Regional Forum Arf Ancaman Non Tradisional Jangan Dilupakan | Portal Kementerian Luar Negeri Republik Indonesia. Kemlu.go.id. https://kemlu.go.id/portal/id/list/view/84/asean-regional-forum-arf-ancaman-non-tradisional-jangan-dilupakan

Kemlu. (2018b). Kejahatan Lintas Negara | Portal Kementerian Luar Negeri Republik Indonesia. Kemlu.go.id. https://kemlu.go.id/portal/id/read/89/halaman_list_lainnya/kejahatan-lintas-negara

Kemlu. (2019). Forum Regional Asean Arf | Portal Kementerian Luar Negeri Republik Indonesia. Kemlu.go.id. https://kemlu.go.id/portal/id/read/126/halaman_list_lainnya/forum-regional-asean-arf

Kominfo. (2023). Kominfo Sosialisasikan Soal "Cyber Crimes" dalam UU ITE. Kominfo.go.id. https://www.kominfo.go.id/index.php/content/detail/2467/Kominfo+Sosialisasikan+Soal+%27Cyber+Crimes%27+dalam+UU+ITE/0/sorotan_media

Loqman, L., Rahman, A., Studi, P., Pertahanan, D., & Pertahanan, S. (2020). Implikasi Diplomasi Pertahanan terhadap Keamanan Siber dalam Konteks Politik Keamanan Implications of Defense Diplomacy on Cybersecurity in Context Security Politics. Jurnal Diplomasi Pertahanan, 6(2), 2020.

Nisa, K. (2022). Diplomasi Digital Dan Kedaulatan Siber Dalam Hubungan Internasional: Analisis Komparatif Kedaulatan Digital Indonesia Dan Negara Di Amerika Utara (Kanada Dan Meksiko). Jurnal Studi Diplomasi Dan Keamanan, 14(1), 91–133. https://doi.org/10.31315/jsdk.v14i1.6046

Primawanti, H., & Pangestu, S. (2020). Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association of South East Asian Natiions (ASEAN) Regional Forum. Global Mind, 2(2), 1–15. https://doi.org/10.53675/jgm.v2i2.89

Ramadhan, A. R., & Sari, V. P. (2022). Diplomasi Digital Jepang Terhadap Indonesia Melalui Akun Instagram @Jpnambsindonesia Pada Periode Duta Besar Masafumi Ishii Dalam Upaya Mengelola Citra Jepang. Padjadjaran Journal of International Relations, 4(1), 36. https://doi.org/10.24198/padjir.v4i1.34700

Rosy, A. F. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber. Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan, 1(2), 118–129. https://doi.org/10.54144/govsci.v1i2.12

Salsabilla, A., & Sidik, H. (2023). Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019. Padjadjaran Journal of International Relations, 5(2), 142–164. https://doi.org/10.24198/padjirv5i2.41337

Wargi, S. (2021). Kebijakan Luar Negeri Indonesia di Era Jokowi Melalui Dplomasi Ekonomi Dalam Upaya Untuk Menguasai Pasar Halal Dunia. Indonesian Journal of International Relations, 5(2), 320–341. https://doi.org/10.32787/ijir.v5i2.228

Yudha, B., Manopo, W., Apriani, D., & Sari, A. (2015). ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN Region. Belli Ac Pacis, 1(1).