# PERAN ASEANAPOL DALAM MENGHADAPI KEJAHATAN SIBER (STUDI KASUS: PENCURIAN DATA TERHADAP NEGARA ANGGOTA ASEAN)

**SKRIPSI**

*Diajukan sebagai salah satu syarat memperoleh gelar sarjana pada Departemen Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Hasanuddin*


**OLEH**

**VANISSA NUGRAH AULIA**

**E061191067**

**DEPARTEMEN ILMU HUBUNGAN INTERNASIONAL**

**FAKULTAS ILMU SOSIAL DAN ILMU POLITIK**

**UNIVERSITAS HASANUDDIN**


**2023**

**HALAMAN JUDUL**

**SKRIPSI**

# PERAN ASEANAPOL DALAM MENGHADAPI KEJAHATAN SIBER (STUDI KASUS: PENCURIAN DATA TERHADAP NEGARA ANGGOTA ASEAN)

**Disusun dan diajukan oleh**

**VANISSA NUGRAH AULIA**

**E061191067**

*Diajukan sebagai salah satu syarat memperoleh gelar sarjana pada*

*Departemen Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik*

*Universitas Hasanuddin*

**DEPARTEMEN ILMU HUBUNGAN INTERNASIONAL**

**FAKULTAS ILMU SOSIAL DAN ILMU POLITIK**

**UNIVERSITAS HASANUDDIN**

# HALAMAN PENGESAHAN

JUDUL : PERAN ASEANAPOL DALAM MENGHADAPI KEJAHATAN SIBER (STUDI KASUS : PENCURIAN DATA TERHADAP NEGARA ANGGOTA ASEAN)

N A M A : VANISSA NUGRAH AULIA

N I M : E061191067

DEPARTEMEN : HUBUNGAN INTERNASIONAL

FAKULTAS : ILMU SOSIAL DAN ILMU POLITIK

Makassar, 23 Juni 2023

Mengetahui :

| Pembimbing I, | Pembimbing II, |
|---|---|
| **Seniwati, S.Sos, M.Hum, Ph.D** | **Nurjannah Abdullah, S.IP, MA** |
| NIP. 197602022000122003 | NIP. 19890103201903201O |

Mengesahkan :
Ketua Departemen Hubungan Internasional,

**Prof. Drs. H. Darwis, MA., Ph.D.**
NIP. 196201021990021003

## PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

| | |
|---|---|
| Nama | : Vanissa Nugrah Aulia |
| NIM | : E061191067 |
| Program Studi | : Ilmu Hubungan Internasional |
| Jenjang | : S1 |

Menyatakan dengan sebenar-benarnya bahwa skripsi yang saya tulis dengan judul: **"PERAN ASEANAPOL DALAM MENGHADAPI KEJAHATAN SIBER (STUDI KASUS: PENCURIAN DATA TERHADAP NEGARA ANGGOTA ASEAN)"**

Merupakan hasil karya saya sendiri dan bukan merupakan pengambilalihan tulisan atau pemikiran orang lain. Apabila dikemudian hari terbukti dan dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini merupakan hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, 11 Juli 2023


Vanissa Nugrah Aulia

# KATA PENGANTAR

Bismillahirrahmanirrahim, Puji syukur penulis panjatkan atas kehadirat Allah SWT dan shalawat kepada bagina Rasulullah SAW atas segala Rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir ini sebagai salah satu syarat untuk mendapatkan gelar sarjana pada Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin. Skripsi ini tentunya terselesaikan dengan baik atas bantuan, dukungan, dan doa dari berbagai pihak. Oleh karena itu, penulis menyampaikan ucapan terima kasih yang mendalam kepada:

1. Orang tua penulis Ayah **Ir. Sirwan Jaya Razak M.Si** dan Ibu **Hj. Siti Saedah S.Pd**. yang penulis cintai dan sayangi, terima kasih atas dukungan dalam bentuk kasih sayang dan finansial. Serta dengan setia mendengar keluh kesah selama proses skripsi ini dibuat. Untuk adik-adik penulis **Farraz Aprillah Fahrani** dan **Muh. Fadel Alfatwa**, terima kasih sudah menjadi adik yang baik dan pengertian melalui *comfort chat* dan *late-night call*.
2. **Nenek Aji Hj. Hudiyah, Nenek Almh. Hj. Siti Saenab, Papa Tua Alm. H. Djafar BA, dan Nenek Ota Alm. H. Abdul Razak**, penulis persembahkan skripsi ini untuk kalian karena *legacy* yang kalian tinggalkan mempermudah penulis dalam beberapa hal.
3. Dosen pembimbing skripsi **Ibu Seniwati, S.Sos, M.Hum, Ph.D dan Kak Nurjannah Abdullah, S.IP, MA** atas waktu, tenaga, serta proses edukasi yang diluangkan untuk membimbing penulis dalam menyelesaikan skripsi.
4. Ketua Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Hasanuddin, **Bapak Prof. Drs. H. Darwis, MA., Ph.D**, Sekretaris Departemen **kak Aswin Baharuddin, S.IP, MA**, jajaran dosen **Bapak Drs. Patrice Lumumba, M.A., Drs. H.M. Imran Hanafi, M.A., M.Ec., Bapak Dr. Adi Suryadi B, M.A., Bapak Drs.**

**H. Husain Abdullah, M.Si., Bapak Drs. Munjin Syafik Asy'ari, M.Si., Bapak Muh. Nasir Badu, S.Sos, M.Hum, Ph.D, Bapak Burhanuddin, S.IP., M.So., Bapak Agussalim, S.IP., MIRAP., Bapak Ishaq Rahman, S.IP., M.Si., Ibu Puspasrida Syahdan, S.Sos., M.Si., Kak Muh. Ashry Sallatu, S.IP., M.Si.**, terima kasih atas ilmu yang dibagikan kepada penulis, penulis berharap melalui ilmu yang penulis dapatkan dari berkuliah dapat penulis gunakan untuk hal-hal yang positif dan bermanfaat bagi penulis dan bagi orang banyak. Para staff Departemen **Ibu Rahmawati, SE., dan Pak Ridwan** terima kasih atas bantuan yang diberikan kepada penulis dalam mengurus seluruh administrasi perkuliahan hingga masa akhir pengurusan skripsi dan kelulusan.

5. Keluarga besar penulis **Om Sano** dan **Tante Qiqi**, terima kasih sudah mau menjadi kakak sekaligus orang tua selama penulis kuliah di Makassar. **Om Jasar, Tante Mina, Om Hasbir, Tante Lina, Tante Asty**, yang sudah mendukung penulis baik secara langsung maupun tidak langsung. Dan, seluruh sepupu-sepupu; **Kakak Joshua, Leo, Aflah, Ufal, Bagas** atas dukungan kepada penulis melalui afirmasi semangat dan antar jemput bandara.
6. **Mutia, Tiara, dan Iin**, terima kasih karena sudah menemani penulis dari masa SMA hingga saat ini. Terima kasih karena sudah percaya pada penulis atas apa yang penulis lakukan, *I wish you guys here witness this chapter of my life*. Untuk **Ajeng**, *only me and Allah who know how much you meant to me, thank you for always listen to me, believe in me, and endless support for whatever I did*.
7. **Sophee, Wiwit, dan Dilla**, terima kasih sudah mau menemani penulis selama 4 tahun masa perkuliahan, terima kasih karena sabar mendengarkan penulis marah dan sedih, terima kasih atas hal-hal lucu yang kalian lakukan untuk menghibur penulis.

8. **Indra dan Fira**, terima kasih atas memori yang akhir-akhir ini yang dibuat, *personally* hal ini spesial bagi penulis. *Thank you* sudah hadir disaat penulis merasa kesepian.
9. **Olaf, Vina, Nia, Dina, Samantha, Reza JKT, Geo, June, Kezia, Tsamara, Reysita, Deborah, Maya**, menyadarkan penulis bahwa penulis memiliki teman angkatan. *Thank you* besar *guys*.
10. Teman-teman UNHAS MUN Community, **Kak Aldy, Kak Ica, Kak Dopes, Kak Joko, Kak Naila, Daffa, Nandiv, Faje, Ica Karisma, Regina, Nanda, Amirah, Salsa Solo, Cikal**, terima kasih sudah menjadi tempat pertama yang percaya penulis untuk menjalankan tanggung jawab organisasi.
11. Orang yang pernah membantu penulis dalam menyelesaikan skripsi ini, **Kak Ryan di ASEAN Youth Organization**. **Orang-orang baru** yang penulis temui selama masa penulisan skripsi ini yang memberikan inspirasi, ilmu, dan stress.
12. ***Playlist* "jedag jedug tiktok yg menggairahkan semangatmu!" dan beberapa bacaan** yang menjadi salah dua hiburan penulis selama proses penulisan skripsi ini.
13. Dan, untuk penulis Vanissa Nugrah Aulia. *Yup we did it* walaupun terseok-seok karena harus membagi fokus dari magang, *volunteer*, dan organisasi *you will always nail it*. *Good luck with life and future endeavors*.

## Abstrak

Vanissa Nugrah Aulia, E061191067 dengan judul skripsi "Peranan ASEANAPOL Dalam Menghadapi Kejahatan Siber (Studi Kasus: Pencurian Data Terhadap Negara Anggota ASEAN)" di bawah bimbingan Ibu Seniwati, S.Sos, M.Hum, Ph.D selaku pembimbing I dan Nurjannah Abdullah, S.IP, MA pembimbing II pada Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin.

Penelitian ini bertujuan untuk menganalisis peran ASEANAPOL dalam menghadapi kejahatan siber terhadap negara anggota ASEAN dan berfokus pada pencurian data yang terjadi di Indonesia, Singapura, dan Filipina dengan menggunakan konsep kejahatan siber dan organisasi internasional. Dengan menggunakan jenis penelitian pendekatan kualitatif melalui data yang dikumpulkan dengan menggunakan studi literatur sebagai teknik pengumpulan data, kebutuhan penilitan terhadap data dan informasi diperoleh dari jurnal, buku, artikel ilmiah, dan dokumen pendukung seperti dokumen resmi pemerintah dan lembaga internasional lainnya melalui *internet*. Pada bagian pertama dari penelitian ini menganalisis ASEANAPOL sebagai salah satu organisasi internasional di Asia Tenggara, kemudian, analisis terhadap kerugian yang dihadapi negara anggota ASEAN ketika pencurian data terjadi, dan kesiapan negara anggota ASEAN dalam menghadapi pencurian data. Pada bagian selanjutnya, penelitian ini menganalisis peran ASEANPOL dalam menghadapi pencurian data terhadap negara anggota ASEAN dengan berfokus pada bagaimana ASEANAPOL menjadi forum untuk membuat kebijakan atau program mengenai kejahatan siber, ASEANAPOL mempengaruhi kebijakan domestik negara, dan kontestasi kekuatan negara di forum ASEANAPOL. Kemudian, penelitian ini juga menganalisis peluang dan tantangan yang dihadapi oleh ASEANAPOL dalam menghadapi kasus pencurian data yang terjadi di negara anggota ASEAN. Hasil dari penelitian ini menunjukkan bahwa ASEANAPOL sebagai garda terdepan dalam menghadapi kejahatan siber di Asia Tenggara belum memenuhi fungsinya dan belum benar-benar dapat mengatasi kasus pencurian data yang terjadi di Indonesia, Singapura, dan Filipina.



***Kata Kunci*** ***:*** *ASEANAPOL, Kejahatan Siber, Pencurian Data, ASEAN, Organisasi Internasional, Indonesia, Singapura, Filipina.*

***Abstract***

*Vanissa Nugrah Aulia, E061191067 with the title of thesis "The Role of ASEANAPOL in Dealing with Cybercrime (Case Study: Data Breaching Against ASEAN Member States)" under the guidance of Mrs. Seniwati, S.Sos, M.Hum, Ph.D as first supervisor and Nurjannah Abdullah, S.IP, MA as second supervisor at the Department of International Relations, Faculty of Social and Political Sciences, Hasanuddin University.*

*This study aims to analyze ASEANAPOL's role in dealing with cybercrime against ASEAN member states and focuses on data breaching that occurred in Indonesia, Singapore, and the Philippines using the concept of cybercrime and international organizations. By using a qualitative type of research approach through data collected using literature studies as a data collection technique, research needs for data and information obtained from journals, books, scientific articles, and supporting documents such as official government documents and other international institutions through the internet. In the first part of this study analyzes ASEANAPOL as one of the international organizations in Southeast Asia, then, analysis of the losses faced by ASEAN member countries when data breaching occurs, and the readiness of ASEAN member states in facing data breaching. In the next section, this study analyzes the role of ASEANPOL in dealing with data breaching against ASEAN member states by focusing on how ASEANAPOL becomes a forum for making policies or programs regarding cybercrime, ASEANAPOL influences countries' domestic policies, and contestation of state power in the ASEANAPOL forum. Then, this study also analyzes the opportunities and challenges faced by ASEANAPOL in dealing with data breaching cases that occur in ASEAN member countries. The results of this study show that ASEANAPOL as the frontline in dealing with cybercrime in Southeast Asia has not fulfilled its function and has not really been able to overcome data breach cases that occur in Indonesia, Singapore, and the Philippines.*

***Keywords*** ***:*** *ASEANAPOL, Cybercrime, Data Breaching, ASEAN, International Organization, Indonesia, Singapore, The Philippines.*

DAFTAR ISI

# BAB I

# PENDAHULUAN

## A. Latar Belakang

Pada Juli 2016, Vietnam diserang siber oleh kelompok peretas Tiongkok “1937CN” yang membajak layar informasi penerbangan dan sistem suara di bandara Noi Bai dan Tan Son Nhat, yang mengakibatkan hilangnya kontrol lokal, dan menyiarkan propaganda anti-Vietnam dan Filipina (Raska & Ang, 2018). Kelompok peretas APT32, juga dikenal sebagai OceanLotus yang dicurigai memiliki hubungan dengan pemerintah Vietnam, membobol komputer ASEAN sebelum KTT para pemimpin regional di ibukota Filipina, Manila. Grup ini juga menyusup ke situs kementerian atau lembaga pemerintah di Laos, Kamboja dan Filipina dengan membuat kode berbahaya ke komputer yang ditargetka (Raska & Ang, 2018). Dengan salah satu kasus yang terjadi di Vietnam dan Filipina, negara anggota ASEAN seperti Indonesia, Malaysia, Filipina, Vietnam, dan Singapura menjadikan pencurian data sebagai salah satu kejahatan yang sangat beresiko bagi industri bisnis dan politik dalam negeri.

Kelompok peretas APT32 juga menargetkan beberapa institusi pemerintah Kamboja seperti kementerian luar negeri, kementerian lingkungan, layanan sipil dan urusan sosial, dan polisi nasional Kamboja. Selain Kamboja, kelompok peretas APT32 juga menargetkan negara anggota ASEAN lainnya yaitu Filipina dan Vietnam yang berdampak pada portal angkatan bersenjata dan kantor presiden Filipina, portal beberapa kelompok, individu, dan media

non-pemerintah Vietnam, hingga portal milik beberapa perusahaan minyak Tiongkok (Reuters, 2017). Kelompok peretas yang juga menargetkan institusi pemerintah menjadi salah satu bukti bahwa isu keamanan siber di Asia Tenggara sangat membutuhkan perhatian dan tindakan.

Adanya kasus yang terjadi di beberapa negara Asia Tenggara ini, juga dipengaruhi oleh penggunaa internet di Asia Tenggara. Pada tahun 2019 *Google* mencatat penggunaan internet di Asia Tenggara mencapai 360 juta, menjadikan Asia Tenggara menjadi salah satu wilayah dengan pertumbuhan ekonomi tercepat karena didukung dengan koneksi internet yang tinggi dan ketersediaan internet pada masyarakat. Pengunaan ini kemudian meningkat 40 juta pengguna baru pada tahun 2020 ketika pandemi Covid-19 terjadi, sehingga jumlah pengguna internet di Asia Tenggara meningkat hingga 400 juta pengguna atau setara dengan 70% populasi penduduk Asia Tenggara. Akibat dari mobilisasi yang terjadi saat pandemi, penduduk di Asia Tenggara mulai terbiasa dengan seluruh kegiatan dilakukan di *cyberspace*. Sehingga pada tahun 2021, terjadi kenaikan pengguna baru sebanyak 40 juta menjadikan pengunaan internet di Asia Tenggara menembus 440 juta atau setara dengan 75% populasi di Asia Tenggara memiliki akses terhadap *internet* (Google et al., 2021). Meningkatnya pengunaan internet menjadi faktor kunci adanya pencurian data terjadi dan masyarakat yang lebih rentan terhadap kejahatan yang bersifat siber.

Dengan berkembangnya penggunaan *internet* pada saat bersamaan juga membuka potensi kejahatan siber, akibatnya kurangnya akuntabilitas menjadikan *Internet* sebagai sarana penyebaran ujaran kebencian, kekerasan

ekstremisme. Kejahatan siber juga meningkat dengan lebih dari 7.000 pencurian yang mengungkap lebih dari 15 miliar data, pada tahun 2019 (United Nations, 2021). Meningkatnya penggunaan *internet* negara-negara di Asia Tenggara membuat resiko serangan siber semakin tinggi yang dapat menyebabkan pencurian atau kegagalan sistem, korban dari pencurian data bukan hanya merugikan individu, melainkan negara dan perusahaan juga ikut dirugikan dengan total biaya yang sangat besar. Negara-negara ASEAN menjadi target kebocoran atau pencurian data karena kebanyakan dari negara anggota ASEAN memiliki infrastruktur siber yang tidak aman dan sangat mudah untuk dieksploitasi (Raska & Ang, 2018). Peningkatan pengguna internet dinilai tidak dibarengi dengan infrastruktur siber yang baik sehingga ASEAN menjadi sasaran empuk untuk menjadi target kejahatan siber.

Banyaknya kasus pencurian data yang terjadi di Asia Tenggara menyebabkan kerugian yang dirasakan negara anggota ASEAN sebesar 2,62 juta US Dollar dan rata-rata data yang terekspos adalah 22.5000 pada tahun 2019 (Lago, 2020). Tahun 2020 juga merupakan peringatan bagi banyak negara di Asia Tenggara untuk berinvestasi dalam pembangunan infrastruktur siber mereka. Banyak bisnis sangat terpengaruh oleh pandemi, insiden siber juga menyebabkan kerugian finansial yang besar karena hilangnya aktivitas bisnis sehingga membuat banyak perusahaan dan bisnis bangkrut. Pencurian data merupakan salah satu resiko terbesar dalam pembangunan ekonomi negara, kerugian rata-rata yang disebabkan oleh adalah 3,86 juta US Dollar dan waktu rata-rata untuk mengidentifikasi dan mengatasi pelanggaran ini sekitar 280 hari

(Tan et al., 2021). Kemudian pada tahun selanjutnya, (Leesa-Nguansuk, 2022) menuliskan, ASEAN dirugikan sebanyak 2,87 juta US Dollar kenaikan ini memungkinkan berdampak pada kenaikan harga barang dan jasa.

Pencurian data bukan saja merugikan negara, bisnis, dan individu dalam bidang ekonomi, tetapi pencurian data berpotensi menggunakan data yang terekspos untuk melakukan pencucian uang, penipuan dan memungkinkan untuk tujuan kejahatan terorganisir, termasuk tindakan korupsi, perdagangan manusia, penyelundupan migran, dan bahkan terorisme (United Nations Office on Drugs and Crime, 2022). Dalam mengahadapi berbagi bentuk kejahatan siber, ASEAN pada tahun 2017 mendeklarasikan komitmen ASEAN dalam menghadapi kejahtan siber di kawasan melalui *ASEAN Declaration to prevent and combat cybercrime* (The Association of Southeast Nations, 2017) yang berisi tentang *framework* yang dapat dilakukan salah satunya dengan memanfaatkan ASEANAPOL dan kerjasama dengan berbagai lembaga internasional. Untuk menghadapi kejahatan transnasional—selain memiliki kebijakan dan strategi dalam bidang keamanan siber—ASEAN memiliki lembaga kepolisian yaitu ASEANAPOL.

ASEANAPOL memiliki beberapa program yang bertujuan untuk meningkatkan kapabilitas ASEANAPOL dalam menghadapai kejahatan di kawasan khususnya bentuk kejahatan yang baru seperti kejahatan siber. Salah satunya dengan bekerjasama dengan *Australian Federal Police* mengadakan sebuah program dengan tujuan bekerjasama dengan mitra penegak hukum di ASEAN dan untuk membantu mengembangkan keterampilan investigasi

kejahatan siber terutama di bidang *online sexual exploitation of children* (Anas, 2022). ASEAN juga bekerjasama dengan organisasi regional seperti Uni Eropa, khususnya pada bidang terorisme, kejahatan terorganisir, dan keamanan siber hal ini dikarena adanya kesamaan ancaman yang dirasakan oleh Uni Eropa dan negara-negara Asia. Namun, dilain sisi hubungan ini terbatas karena adanya perbedaan budaya atau definisi tentang suatu isu seperti prinsip perlindungan data (khususnya berkaitan dengan akses internet terbuka) (Kirchner et al., 2021). Fungsi ASEANAPOL dinilai masih bersifat diplomatik, ketika ASEAN berkomitmen untuk bekerjasama dalam memerangi kejahatan siber organisasi regional seperti Uni Eropa masih mempertanyakan hal-hal mendasar mengenai keamanan siber yang belum dilaksanakan oleh ASEANAPOL dan ASEAN laksanakan (Bossong & Holmes, 2021). Terlepas dari sifatnya yang masih diplomatik, kerjasama yang dilakukan ASEANAPOL menunjukkan keseriusan dalam menghadapi kejahatan siber di kawasan.

Secara umum, kejahatan siber diartikan sebagi pelanggaran yang dilakukan di dunia maya, dan pelanggaran yang bergantung pada *internet* untuk mendukung kejahatan yang dilakukan. Pada level internasional, ada sejumlah perjanjian dan konvensi dengan cakupan yang berbeda-beda yang membahas tentang masalah kejahatan siber, namun, tidak ada instrumen hukum PBB tentang kejahatan siber. Pada akhirnya tahun 2019, Majelis Umum PBB mengadopsi resolusi tentang "*countering the use of information and communications technologies for criminal purposes*", dan memperkenalkan komite *ad hoc*. *Ad hoc* berfungsi untuk mengelaborasi konvensi internasional

tentang kejahatan siber yang komprehensif dan melalui resolusi PBB ini dapat menjadi langkah pertama untuk menciptakan perjanjian internasional baru tentang kejahatan siber (UN Regional Information Centre for West Europe, 2022). Cakupan dan definisi kejahatan siber yang masih berbeda-beda menjadi faktor yang membuat kejahatan siber cukup sulit untuk dihadapi oleh negara atau bahkan sebuah organisasi regional.

Sifatnya yang transnasional, menjadikan kejahatan siber pada dasarnya mengharuskan negara memberlakukan undang-undang untuk menyelaraskan definisi kriminalitas dan meningkatkan kerjasama antar negara (Chang, 2020). *The Council of Europe* menjadi lembaga internasional pertama yang menjadikan kejahatan siber sebagai sebuah ancaman model baru bagi negara anggota Uni Eropa, sehingga pada 2001 Council of Europe mengadakan *Convention on Cybercrime* atau biasa dikenal dengan *Budapest Convention* yang menghasilkan sebuah perjanjian multinasional yang berisi tentang sarana untuk menuntut pelaku kejahatan siber dan upaya-upaya penting lainnya untuk mengatur *cyberspace* dan infrastruktur siber masing-masing negara (Council of Europe Portal, 2022). Konvensi Budapest didukung oleh Perserikatan Bangsa-Bangsa (PBB), karena pada konvensi ini negara-negara *non-council* juga ikut berpartisipasi, sehingga konvensi Budapest dianggap sebagai perjanjian internasional, bukan regional.

Resolusi 56/121, Majelis Umum PBB mencatat bahwa kerjasama organisasi internasional dan regional dalam memerangi *hi-technology crime*, dan menekankan bahwa pentingnya sebuah perjanjian internasional yang

membahas tentang kejahatan siber (Chang, 2020). Dengan sifatnya yang transnasional dan dukungan seperti PBB, Uni Eropa, dan berbagai negara kejahatan siber dinilai memerlukan kerjasama dari berbagai pihak.

Berdasarkan uraian di atas, penulis akan menganalisis lebih dalam kebijakan ASEAN dengan memanfaatkan ASEANAPOL dalam menghadapi kejahatan transnasional yang bermunculan pasca berkembangnya penggunaan *internet* saat pandemi covid-19 dan setelah pandemi covid-19 dan menganalisis apakah ASEANAPOL efektif untuk mengurangi pencurian data di kawasan. Maka dari itu, penulis akan menganalisi dan mengidentifikasi permasalahan yang telah dipaparkan sebelumnya dengan judul penelitian **Peran ASEANAPOL dalam menghadapi kejahatan siber (studi kasus: pencurian data terhadap negara anggota ASEAN)**.

## B. Rumusan Masalah

Berdasarkan pada pembahasan yang penulis telah uraikan dalam latar belakang, maka penulis akan membatasi judul dengan berfokus pada pencurian data terhadap lembaga pemerintahan, bisnis, dan perusahaan yang beroperasi di 3 negara anggota ASEAN yaitu **Indonesia, Singapura, Filipina**. Pada penelitian ini juga, penulis akan berfokus pada **dampak pencurian data (*data breaching*) terhadap kondisi ekonomi dan politik Indonesia, Singapura, Filipina dari tahun 2017 sampai 2022**. Dengan Batasan masalah tersebut, berikut merupakan rumusan masalah yang akan dibahas dalam penulisan ini:

1. Bagaimana peran ASEANAPOL dalam menghadapi kejahatan siber khususnya pencurian data terhadap negara anggota ASEAN?
2. Bagaimana peluang dan tantangan ASEANAPOL dalam menghadapi kejahatan siber khususnya pencurian data negara anggota ASEAN?

## C. Tujuan Penelitian

1. Untuk menganalisis peran ASEANAPOL dalam menghadapi kejahatan siber khususnya pencurian data terhadap negara anggota ASEAN
2. Untuk menganalisis peluang dan tantangan ASEANAPOL dalam menghadapi kejahatan siber khususssnya pencurian data negara anggota ASEAN

## D. Manfaat Penelitian

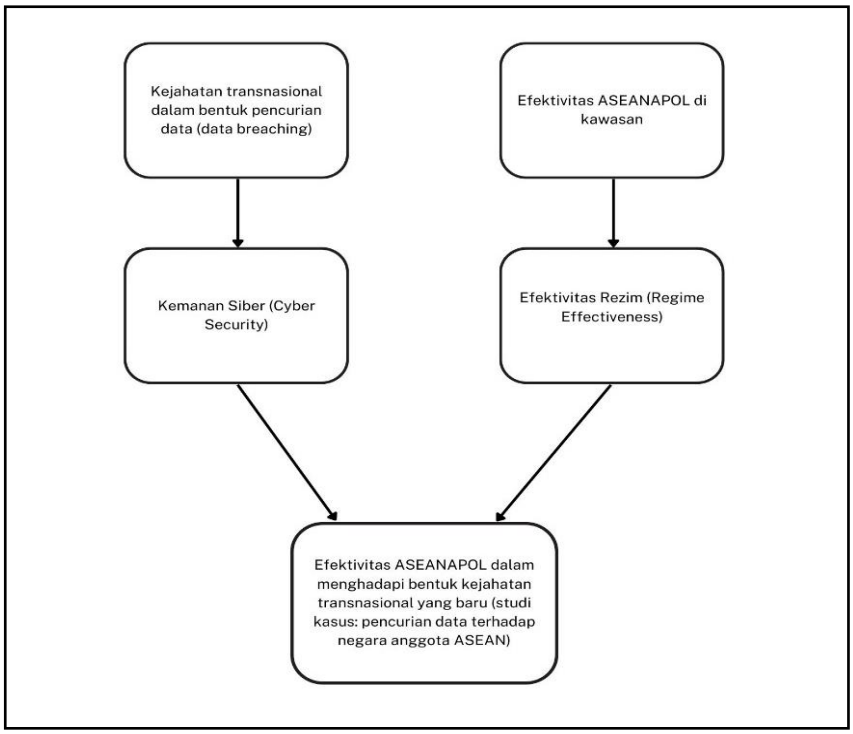
1. Bagi penulis penilitian ini diharapkan dapat menambah pemahaman mengenai peran ASEANAPOL dalam menghadapi pencurian data terhadap negara anggota ASEAN
2. Bagi akademisi, penulis berharap hasil penelitian ini dapat dijadikan sumber informasi dan referensi yang jelas bagi mahasiswa Ilmu Hubungan Internasional dan disiplin ilmu lain yang berkaitan dengan tema penilitian

## E. Kerangka Konsep

Untuk menjawab pertanyaan penelitian penulis akan menggunakan konsep *Cybersecurity* untuk menjelaskan pencurian data atau *data breaching* sebagai kejahatan yang mengancam keamanan siber negara, dan konsep *Regime*

*Effectiveness* untuk menganalisis efektivitas ASEANAPOL dalam menghadapi pencurian data di kawasan.

*Gambar 1. Kerangka Konsep*



a. Kejahatan Siber (*Cybercrime*)

Memasuki dunia yang semakin berkembang dan pesatnya arus informasi, kini dunia memasuki area yang baru dalam hubungan internasional yaitu *cyberspace* atau dunia maya. Definisi mengenai *cyberspace* diberbagai negara berbeda-beda termasuk definisi *cyberspace* dalam perspektif organisasi atau lembaga internasional. Definisi dunia maya atau *cyberspace* dapat dilihat dalam dokumentasi pertahanan negara, dan ketika dibandingkan definisi ini akan menggambarkan *interest* sebuah negara terhadap *cyberspace* (Medeiros & Goldoni, 2020). *The dictionary of Military and Associated Terms* (United States Department of Defense, 2021) mendefinisikan *cyberspace* sebagai sebuah *global domain* dalam lingkup informasi yang terdiri dari infrastruktur teknologi informasi yang saling bergantungan, termasuk *internet*, jaringan telekomunikasi, sistem komputer, dan *embedded processors and controllers*, hingga data penduduk. Berkembangnya *cyberspace* dan aksesnya yang bekerja dan terhubung ke dalam jaringan dengan menggunakan perangkat pintar, skala dan variasi serangan siber meningkat secara eksponensial.

Dengan kinerja yang saling berhubungan, pelanggaran keamanan siber dapat berdampak negatif bagi performa ekonomi sebuah negara (Corallo et al., 2020). Bukan hanya ekonomi, kejahatan siber juga berdampak pada sosial politik pada sebuah negara, (Lacy & Prince, 2018) mengemukakan bahwa beberapa ancaman terhadap

keamanan siber dimasa depan yang dihasilkan dari meningkatnya keterhubungan masyarakat melalui *cyberspace*, beberapa tantangannya merupakan masalah "tradisional" – pelecehan, *grooming and recruitment*, pencurian identitas dan penipuan – dilakukan dengan teknologi baru. Dunia maya menjadi salah satu tempat kecemasan warga negara sebagai individu menjadi masalah keamanan nasional yang baru dan memiliki tingkat bahaya yang sama dengan ancaman keamanan yang tradisional. *Internet* membawa dampak yang tinggi bahkan bagi negara-negara maju yang memiliki infrastruktur siber terbaik. Hal ini menjadi sebuah ancaman yang baru dan kerentanan terhadap keamanan negara, termasuk spionase komersial, pelanggaran data, intrusi ke dalam jaringan pemerintah, ancaman terhadap infrastruktur fisik, dan campur tangan pada pemilu (Branch, 2020).

Perkembangan teknologi jauh lebih cepat dan tidak didukung oleh kemampuan negara, organisasi atau sebuah lembaga untuk memperkirakan dampaknya terhadap sistem politik, sosial dan ekonomi. Oleh karena itu, pelaksanaan peraturan norma dan proses tata kelola yang bertujuan untuk menghadapi dampak perkembangan teknologi ini seringkali lebih lambat daripada perkembangan teknologi itu sendiri. Hal ini mempengaruhi kebanyakan negara, konektivitas semakin berkembang jauh lebih cepat daripada kemampuan pemerintah, industri, dan masyarakat sipil untuk mengembangkan kapasitas teknis dan kebijakan untuk memanfaatkan konektivitas yang tinggi dan

kesiapan infrastuktur siber untuk menghadapi ancaman yang muncul dari konektivitas yang tinggi (Calderaro & Craig, 2020).

Hingga awal tahun 2000-an keamanan siber sangat jarang dibahas dalam isu keamanan nasional, sampai pada akhirnya Amerika Serikat dengan pengaruhnya menggunakan terminologi keamanan siber dan *cyberspace* yang mempengaruhi kebijakan militer AS tentang keamanan siber (Branch, 2020). Dengan penggunaan terminologi keamanan siber yang mempengaruhi kebijakan sebuah negara terhadap keamanan nasional, *cyberspace* menjadi ruang politik yang diperebutkan, dibentuk oleh perbedaan kepentingan, norma dan nilai. Akibat politisasi ini, para aktor negara, lembaga internasional, dan organisasi internasional memasuki dimensi politik yang baru. Oleh karena itu, penggunaan sumber daya diplomatik dan kinerja fungsi diplomatik yang kemudian digunakan untuk mengamankan kepentingan nasional terkait dengan dunia maya atau *cybersapce*.

Kepentingan tersebut umumnya diidentifikasi pada *national cyberspace* atau strategi *cybersecurity*, yang seringkali menjadi referensi pada agenda diplomasi. Isu utama dalam agenda diplomasi *cyberspace* meliputi *cybersecurity*, *cybercrime*, *confidence-building*, kebebasan ber-*internet*, dan tata kelola *internet* (Barrinha & Renard, 2017). Hal ini menjadikan isu keamanan siber mejadi sebuah isu yang di-sekuritisasi (*hypersecuritization*), sehingga menciptakan diskusi yang beragam tentang masa depan keamanan nasional termasuk

keamanan siber yaitu *the cyber catastrophist, the digital realist, and the techno-optimist*.

*The cyber catastrophist* menunjukkan bahwa bencana digital ada mulai kelihatan dampaknya– dan sering kali diremehkan dalam wacana ancaman geopolitik. Beberapa *cyber catastrophist* juga melihat bencana digital yang mengakibatkan keruntuhan sosial, ekonomi, dan infrastruktur yang serupa dengan kekerasan yang dimungkinkan oleh senjata pemusnah massal. Berdasarkan *Global Trends 2030: Alternative worlds* sebuah laporan dari *the National Intelligence Councils* tentang masa depan keamanan dan ekonomi global menyatakan bahwa potensi peningkatan kekuatan senjata nuklir oleh Rusia, Pakisatan, Iran, dan Korea Utara dibarengi dengan adanya peluang penggunaan serangan siber. Melalui laporan ini membuktikan adanya anggapan bahwa keamanan siber atau *cyberweapon* pada level yang sama dengan senjata pemusnah massal, yang berpotensi menjadikan isu ini di-sekuritisasi yang memasukkan aktor non-negara sebagai kontributor potensial terjadinya bencana digital (Lacy & Prince, 2018).

Oleh karena itu, *cyber catastophist* menyarankan agar aktor negara, lembaga dan organisasi internasional, hingga individu perlu mewaspadai peningkatan ancaman terhadap keamanan siber. Dan yang paling penting adalah menganggap serius kemungkinan bencana digital dan banyaknya dampak yang disebabkan, kemudian melibatkan

organisasi dan lembaga internasional untuk mengamankan dan melindungi keamanan siber (Lacy & Prince, 2018).

Untuk mengonter pernyataan dari *cyber catastrophist*, *the digital realist* menilai bahwa visi tentang peristiwa bencana masa depan yang terjadi di *cyberspace* hanya untuk menciptakan produk budaya populer. Selain itu, akan ada beberapa pihak yang mendapatkan manfaat ekonomi dari ekonomi politik keamanan siber yang diciptakan oleh ancaman dan ketidakamanan baru. Beberapa pakar juga menyatakan tentang bagaimana beberapa organisasi, bisnis, dan lembaga pemerintah menjadi semakin skeptis tentang beberapa skenario bencana yang digunakan dalam promosi materi untuk solusi dan alat siber yang ingin dijual (Lacy & Prince, 2018).

Thomas Rid berpendapat bahwa sangat bermasalah untuk membicarakan kemungkinan perang siber, para aktor internasional tidak mungkin terlibat dalam konflik di mana instrumen siber merupakan "senjata" utama. Perang adalah penggunaan kekerasan untuk mencapai tujuan politik atau ekonomi tertentu melalui teknik yang membuat musuh tidak berdaya, apabila kemungkinan penggunaan cyberweapons pada situasi perang tidak akan sebanding kemampuannya dengan penggunaan senjata yang lebih tradisional. Namun, tidak berarti bahwa siber konflik, kejahatan siber, dan gangguan yang berasal dari *cyberspace* tidak menimbulkan masalah pada kepentingan nasional. Dampak negatif yang berasal dari siber pada kepentingan dan keamanan

nasional, umumnya tidak berdampak pada kematian dan kehancuran fisik. Tantangan bagi kemanan nasional khususnya bidang militer adalah bagaimana memanfaatkan kecepatan, keamanan, efisiensi, dan efektivitas biaya siber tanpa menciptakan kelemahan baru bagi keamanan nasional (Lacy & Prince, 2018).

Pada dasarnya, *cyberspace* hanyalah salah satu dari masalah yang terjadi di dalam kehidupan bernegara, argumen bahwa *cyberspace* menjadi ancaman bagi keamanan negara hanya bersifar ekonomi. Oleh karena itu, *digital realist* menekankan fokus pada pengembangan strategi keamanan siber dan keamanan siber secara defensif dan ofensif. Di lain sisi, beranggapan bahwa menyamakan senjata siber sebagai sebuah "*gamechanger*" akan menciptakan skenario destruktif seperti yang telah dikemukakan *cyber catastrophist* (Lacy & Prince, 2018).

Beberapa beranggapan bahwa perkembangan teknologi yang terjadi pada kehidupan manusia saat ini merupakan bagian dari sistem politik yang dimana masyarakat diberikan kebebasan dan hak untuk mengembangkan sesuatu, oleh karena itu, dengan perkembangan teknologi yang baru dapat meningkatkan sektor-sektor lain seperti Kesehatan, komunikasi, ekonomi, dan keamanan. *The techno-optimist* percaya bahwa jika masyarakat mengembangkan institusi dan budaya politik yang tepat, dunia dapat melanjutkan proses mengatasi bencana dan bahaya yang disebabkan oleh perkembangan teknologi. Dengan populasi dunia yang hampir seluruhnya menganut sistem demokrasi

liberal juga tidak menjadikan semua hal sempurna, tetapi masyarakat liberal memiliki mekanisme kritik dan refleksi yang memungkinkan adanya perbaikan dimasa yang akan datang. Kevin Kelly menilai keamanan siber dan berbagi dampak didalamnya merupakan sebuah proses lingkaran yang akan terus berputar (*circle of new good provoking new bad which provokes new good which spawns new bad is just spinning us in place, only faster and faster*) (Lacy & Prince, 2018).

Oleh karena itu, *techno-optimist* berfokus pada pengembangan infrastruktur siber yang dapat dimulai dengan riset dan edukasi, karena kebanyakan bencana siber disebabkan oleh kesalahan yang dapat diperbaiki. Dalam hal perang siber, *techno-optimist* percaya hal ini akan diatasi dengan adanya pengembangan teknologi yang baru, tetapi *techno-optimist* khawatir dengan cara negara menggunakan teknologi baru untuk melakukan pengawasan dan pengendalian populasi. Khususnya dalam hal militerisasi internet, kemungkinan komunikasi, edukasi, dan mobilisasi menjadi terbatas sehingga potensi kebebasan yang dimiliki masyarakat dikontrol ketat. Bagi *techno-optimist*, politik keamanan siber harus difokuskan untuk melindungi keamanan warga negara ancaman yang diciptakan oleh negara itu sendiri (Lacy & Prince, 2018).

Berdasarkan penjelasan sebelumnya, maka terdapat tiga indikator pada konsep kejahatan siber yang akan diterapkan pada bab pembahasan dan analisis; Menjadikan isu keamanan siber sebagai isu

keamanan nasional, mempengaruhi kebijakan yang diambil oleh negara, dan dengan adanya kekhawatiran akibat dampak perkembangan teknologi, isu keamanan siber di-sekuritisasi sehingga menciptakan diskusi yang beragam tentang masa depan keamanan nasional termasuk keamanan siber yaitu *the cyber catastrophist, the digital realist, and the techno-optimist*.

b. Organisasi Internasional (*International Organization*)

Organisasi internasional merupakan bentuk kerjasama internasional yang dilakukan oleh banyak aktor untuk menyelesaikan sebuah isu atau permasalahan tertentu. Robert Keohane dalam (Milner, 1992) menuliskan bahwa ketika aktor menyesuaikan perilaku mereka atau mengantisipasi referensi dari aktor lain dalam proses kordinasi kebijakan, maka perilaku ini dapat disebut dengan kerjasama. Konsep kerjasama terdiri atas dua elemen penting; 1) mengasumsikan bahwa perilaku masing-masing aktor diarahkan pada beberapa tujuan. Tujuan ini tidak perlu menjadi tujuan yang sama bagi semua aktor yang terlibat, tetapi tujuan ini mengasumsikan perilaku rasional yang dilakukan oleh aktor. 2) Implikasi dari kerjasama adalah memberikan para aktor yang terlibat mendapat keuntungan atau penghargaan atas keterlibatan dalam forum kerjasama.

Dalam paradigma hubungan internasional, aktor akan membentuk sebuah wadah untuk mengakomodasi kerjasama antara

negara ini. Oleh karena itu, organisasi internasional dibentuk oleh aktor salah satunya untuk memenuhi dan mengakomodasi kerjasama yang mereka lakukan (Milner, 1992). Organisasi internasional digunakan menjadi sebuah alat untuk implementasi kebijakan dari aktor dengan kekuatan yang lebih besar dari aktor lain dan menjadi sebuah arena untuk kontestasi dari kebijakan yang telah dihasilkan. Selain kontestasi kebijakan, organisasi internasional juga menjadi arena untuk kontestasi antara *social forces*, ide, dan negara (O'Brien, 2002). Di lain sisi, (Beland & Orenstein, 2013) mengemukakan bahwa organisasi internasional tidak hanya kontestasi kebijakan atau ide, organisasi lebih fleksibel dari hanya sekedar arena untuk kontestasi ide. Organisasi internasional sering menjadi tempat untuk mengembangkan ide-ide baru, hal ini membuat sulit untuk mengkarakterisasi pendekatan kebijakan organisasi internasional sebagai hal yang stabil, kecuali pada periode waktu yang relatif singkat yang dimana memungkin menunjukkan konsistensi ideologi (Beland & Orenstein, 2013). Dengan adanya, organisasi internasional bukan hanya sebagai forum kebijakan, tetapi juga untuk pengembangan ide-ide yang membuat organisasi internasional menjadi lebih fleksibel.

Dalam menganalisis organisasi internasional, konsep paradigma kebijakan sering digunakan untuk menawarkan *analytical leverage* terhadap diskursus dan kebijakan domestik yang mempengaruhi organisasi yang dimaksud. Organisasi internasional tidak konsisten dari

waktu ke waktu dalam preferensi kebijakan, karena organisasi internasional tidak tunduk pada satu kelompok kepentingan atau negara, melainkan sistem terbuka, rentan terhadap berbagai pengaruh dan para aktor yang berkomitmen untuk bersaing dengan gagasan dan paradigma kebijakan sosial. Pandangan organisasi internasional sebagai sistem terbuka ini kontras dengan pandangan realis, yang melihat organisasi internasional melalui lensa dilema "*principal-agent*". Dalam perspektif realis, organisasi internasional adalah "agen" negara-negara nasional. Pengambil keputusan utama berada pada negara-negara yang kuat (Beland & Orenstein, 2013). Oleh karena itu, dalam pandangan realis, arah organisasi internasional biasanya dipengaruhi dari negara-negara yang memiliki pengaruh besar pada organisasi tersebut.

Sedangkan pandangan *liberal internationalist* menyanggah pandangan yang disampaikan oleh realis, *liberal internationalist* berpendapat bahwa organisasi internasional merupakan forum independen sehingga bebas untuk mempromosikan berbagai kerjasama yang dapat dilakukan oleh berbagai negara dengan negara lainnya. Kemudian, beberapa tahun terakhir, *constructivist scholar* memandang organisasi internasional dari sisi ideasional atau *agenda-setting function* yang dapat dilakukan pada organisasi internasional. Bagi konstruktivis fungsi *agenda-setting* pada organisasi internasional dipengaruhi oleh legitimasi yang dimiliki oleh organisasi itu sendiri, seperti; otoritas

rasional-legal yang berasal dari *charters*[1], legitimasi yang didelegasikan kepada organisasi internasional yang diperoleh dari negara, legitimasi moral yang berasal dari misi penting organisasi, dan legitimasi yang didapatkan dari *expert* berdasarkan fokus organisasi internasional yang diterima secara luas (Beland & Orenstein, 2013). Dengan menggunakan pandangan konstruktivis, akan mempermudah sejauh mana peranan organisasi internasional pada isu-isu tertentu karena adanya legitimasi dan fungsi *agenda-setting* yang menjadi parameter awal.

Dengan mempertimbangkan penjelasan yang telah dipaparkan sebelumnya, terdapat dua indicator organisasi internasional untuk diterapkan pada bab hasil dan analisis; Organisasi internasional menjadi sebuah forum kontestasi ide untuk menentukan arah dan tujuan organisasi internasional dalam menghadapi masalah tertentu (*agenda-setting*), dan organisasi internasional juga berperan untuk mempengaruhi kebijakan domestik negara.

## F. Metode Penelitian

a. Jenis Penelitian

Jenis penelitian yang digunakan penulis adalah metode campuran yaitu pendekatan kualitatif. Kualitatif digunakan sebagai analisis deskriptif terhadap peranan ASEANAPOL dalam menghadapi

[1] Dokumen yang menandai terbentuknya sebuah organisasi internasional

pencurian data di kawasan melalui informasi dan data yang diperoleh dari berbagai sumber.

b. Teknik Pengumpulan Data

Penulis mengumpulkan data dengan menggunakan studi literatur sebagai teknik pengumpulan data, kebutuhan penilitan terhadap data dan informasi terkait peran ASEANAPOL dalam menghadapi pencurian data terhadap negara anggota ASEAN diperoleh dengan melalui jurnal, buku, artikel ilmiah, dan dokumen pendukung seperti dokumen resmi pemerintah dan lembaga internasional lainnya melalui *internet*. Apabila dimungkinkan, penulis akan melakukan wawancara terhadap lembaga atau organisasi terkait sebagai salah satu bentuk pengumpulan data primer.

c. Teknik Analisis Data

Setelah semua data dikumpulkan kemudian penulis akan menganalisis data secara kualitatif, dengan menuliskan seluruh data berdasarkan fakta yang terjadi yang kemudian dikaitkan dengan peran ASEANAPOL.

## G. Sistematikan Penulisan

Berikut merupakan uraian sistematika penulisan penelitian yang terbagi ke dalam bab, yaitu:

a. Bab 1 Pendahuluan, penjelasan mengenai latar belakang permasalahan, Batasan dan rumusan masalah, tujuan dan manfaat penelitian, kerangka

konsep, metodologi penelitian, dan ditutup dengan sistematikan penulisan.

b. Bab 2 Tinjauan Pustaka, menjelaskan lebih jauh menengenai konsep yang digunakan dalam penelitian ini.
c. Bab 3 Gambaran Umum, berisi tentang ASEANAPOL sebagai salah satu organisasi internasional yang ada di Asia Tenggara, kesiapan negara anggota ASEAN dalam menghadapi kejahatan siber, dan kerugian yang dihadapi negara anggota ketika pencurian data terjadi.
d. Bab 4 Analisis dan hasil penelitian, bab ini merupakan implementasi dari pertanyaan rumusan masalah dengan menggunakan operasional variabel.
e. Bab 5 Kesimpulan, berisi tentang saran kebijakan dan rangkuman hasil penelitian.

# BAB II

# TINJAUAN PUSTAKA

## A. Kejahatan Siber (Cybercrime)

Dunia maya atau *cyberspace* merupakan sebuah infrastruktur teknologi informasi yang saling bergantungan, termasuk *internet*, jaringan telekomunikasi, sistem komputer, dan *embedded processors and controllers*, hingga data penduduk (United States Department of Defense, 2021). Seperangkat infrastruktur ini menjadi rentan terhadap terjadinya kejahatan siber. Sebelum *term* kejahatan siber ditemukan, Donn B. Parker di dalam sebuah artikel memperkenalkan *computer crime* atau kejahatan komputer. Taksonomi Parker mengklasifikasikan kondisi yang termasuk dalam kejahatan komputer, kondisi ini ketika komputer digunakan sebagai (1) objek kejahatan, (2) lingkungan tempat kejahatan terjadi, (3) instrumen untuk melakukan kejahatan, dan (4) simbol kejahatan (Payne, 2020). Pada dekade berikutnya, Hollinger dan Lanza-Kaduce pada tahun 1988 menulis salah satu karya kriminologis tentang kejahatan komputer, dengan fokus pada bagaimana kejahatan komputer dikriminalisasi. Karya ini kemudian menginspirasi terciptanya Konvensi Budapest atau *Budapest Convention* tentang kejahatan siber, yang ditandatangani pada tahun 2001 dan dianggap sebagai salah satu perjanjian internasional terpenting untuk mempromosikan tanggapan kolaboratif terhadap kejahatan yang terjadi pada dunia maya.

Dalam perkembangan studi kejahatan siber, para ahli mencoba untuk mendefinisikan kejahatan siber. Tetapi, sampai saat ini tidak ada definisi universal mengenai kejahatan siber itu sendiri, oleh karena itu (Payne, 2020), menuliskan bahwa mendefinisikan kejahatan siber merupakan hal yang penting karena; (1) cara individu mendefinisikan kejahatan siber akan menentukan perkiraan tingkat kejahatan siber; (2) definisi kejahatan siber akan berdampak pada konsekuensi (atau respon individu) terhadap perilaku tertentu; (3) definisi kejahatan siber berimplikasi pada cara kriminolog mencoba menjelaskan pelanggaran siber; (4) definisi akan memandu strategi intervensi yang digunakan untuk menanggapi jenis perilaku kejahatan; (5) definisi akan memandu strategi pencegahan yang digunakan untuk mencegah perilaku kejahatan; (6) definisi akan menentukan jenis penelitian metodologi yang digunakan untuk mempelajari perilaku; dan (7) definisi akan menentukan bagaimana para akademisi mengajarkan tentang perilaku.

Beberapa akademisi dan ahli mulai mencoba memperkenalkan *terms* yang berhubungan dengan kejahatan siber dan batasan konsep dari *terms* yang telah diperkenalkan. Namun beberapa *terms* yang diperkenalkan sama sekali tidak memiliki definisi yang pas dengan konsep kejahatan siber yang sesungguhnya (Payne, 2020).

*Tabel 1 Konsep yang Berhubungan Dengan Kejahatan Siber* (Payne, 2020)

| | **Definisi** | **Mengapa *terms* ini diperkenalkan** | **Batasan konsep** | **Akademisi dan Ahli** |
|---|---|---|---|---|
| *Computer Crime* | | Peneliti, akademisi, dan pembuat kebijakan memahami bahwa Perilaku baru yang terkait dengan penggunaan komputer mengakibatkan terjadinya tindakan kriminal | Seiring berkembangnya teknologi, dan jumlah perangkat terhubung ke Internet memiliki meningkat, kejahatan setelah terbatas untuk komputer dapat dilakukan tanpa komputer melalui penggunaan perangkat teknologi lainnya | Hollinger and Lanza-Kaduce (1988) Richardson (2008) |
| *Digital Crime* | Setiap kegiatan kriminal yang melibatkan penggunaan komputer dan jaringan atau perangkat digital lainnya | Para peneliti dan praktisi, yaitu, ahli forensik, mengakui bahwa kejahatan dapat berkomitmen menggunakan digital teknologi, terlepas dari apakah komputer digunakan | Frasa berpotensi membatasi jenis-jenis pelanggaran yang mungkin disertakan pada mereka yang memerlukan tingkat komputer kecanggihan yang sebenarnya tidak diperlukan untuk sebagian besar pelanggaran komputer | Gogolin (2010) Kanellis (2006) Taylor et al. (2014) |
| *Electronic Crime* | Sebagai tindakan ilegal yang dilakukan dengan menggunakan komputer atau Media elektronik | Para peneliti menggunakan bahasa yang digunakan untuk menangkap Strategi komunikasi | Karena anggota masyarakat telah berubah, penggunaan "elektronik" dianggap kadaluarsa, | Etter (2001) Grabosky (2006) |

| | | | | |
|---|---|---|---|---|
| | | (misalnya, email) yang sejajar Penggunaan komputer | dengan banyak anak muda sekarang menghindari surat elektronik | |
| *Internet Crime* | aktivitas ilegal apa pun yang melibatkan satu atau beberapa komponen Internet, seperti situs web, obrolan kamar, dan/atau email. Kejahatan internet melibatkan penggunaan Internet untuk berkomunikasi pernyataan palsu atau penipuan kepada konsumen. Kejahatan ini mungkin termasuk, tetapi tidak terbatas pada, skema biaya di muka, non-pengiriman barang atau jasa, peretasan komputer, atau skema pekerjaan / peluang bisnis | Frasa lain menyiratkan level keahlian untuk melakukan pelanggaran, ketika banyak pelanggaran hanya dilakukan "melalui" atau "di" Internet | Frasa tersebut berpotensi mengecualikan kejahatan-kejahatan yang terjadi secara independen dari Internet tetapi tetap saja didorong oleh teknologi siber | Jewkes and Yar (2010) Taylor and Quayle (2003) Wall (2013) |
| *Network Crime* | tidak hanya. . . suatu bentuk intersepsi data, tetapi juga melibatkan penyusupan ke dalam jaringan untuk mendapatkan akses tidak sah ke data, atau bahkan | Penulis (khususnya insinyur) ingin menarik perhatian pada fakta bahwa kejahatan terjadi melalui jaringan yang menghubungkan berbagai | Banyak kejahatan dunia maya terjadi yang sangat tidak ada hubungannya dengan jaringan komputer, tetapi lebih tondo dengan perilaku pengguna komputer | Adeyemi et al. (2013) Wang (2012) |

| | | | | |
|---|---|---|---|---|
| | mengubah data, menghancurkan data, memanfaatkan sumber daya jaringan secara tidak sah, dll | Perangkat teknologi | | |
| *Technocrime* | *Technocrime* mencakup berbagai kejahatan yang dilakukan dalam teknologi sistem | Penulis menarik perhatian pada koneksi antara teknologi dan kejahatan, khususnya di dalam konteks tempat kerja | Dengan menarik perhatian ke teknologi, istilahnya menyiratkan bahwa kejahatan itu terjadi karena teknologi ketika sebagian besar Pelanggaran siber didorong oleh faktor manusia | Friedrichs (2009) Leman-Langois (2008) Steinmetz and Nobles (2017) |
| *Virtual Crime* | Kejahatan virtual mengacu pada kejahatan yang dilakukan dalam pengaturan realitas virtual atau game virtual | Kasus pengadilan telah meninjau apakah kejahatan dapat dilakukan di dunia maya, termasuk dalam game Pengaturan | Sementara beberapa pelanggaran mungkin dilakukan di dunia maya, ini tetap menjadi Pengecualian | Brenner (2001) Lastowka and Hunter (2004) |

Selain itu, beberapa lembaga seperti *The International Criminal Police Organization* mengartikan kejahatan siber sebagai segala bentuk kejahatan yang terjadi di dalam komputer dan sistem informasi yang tujuannya untuk mengakses perangkat secara illegal atau menolak akses yang dilakukan oleh pengguna sebenarnya (The International Criminal Police, 2017). Di sisi lain, perusahaan multinasional yang bergerak dibidang siber, Kaspersky menuliskan kejahatan siber merupakan aktivitas kriminal yang menargetkan atau menggunakan komputer, jaringan komputer, atau perangkat jaringan. Kebanyakan pelanggaran dan kejahatan siber dilakukan oleh *cybercriminal* atau *hacker* dalam bentuk perseorangan ataupun berkelompok yang ingin menghasilkan uang atau profit. Namun, terkadang kejahatan siber bertujuan untuk merusak komputer atau jaringan karena alasan selain keuntungan yaitu bersifat politis atau personal. Beberapa kejahatan siber dilakukan secara terorganisir, menggunakan teknik canggih dan sangat terampil secara teknis (Kaspersky, 2022).

Bagi sebuah negara atau organisasi internasional definisi kejahatan siber secara spesifik terletak pada dokumen resmi atau berada dalam undang-undang dan hukum yang berlaku di dalam beberapa negara (Indonesia, Singapura, Filipina). Dalam sistem perundang-undangan Indonesia, kejahatan siber diatur dalam UU nomor 11 tahun 2008 artikel 27 sampai 37 yang kemudian disempurnakan dalam UU nomor 19 tahun 2016. Pada artikel 30 ayat 3 (Republik Indonesia, 2008), pemerintah Indonesia dengan spesifik menuliskan

pelanggaran yang dilakukan dengan cara menerobos, melampaui, atau menjebol sistem pengamanan termasuk pelanggaran siber.

Berdasarkan *National Crime Prevention Council* Singapura, kejahatan siber merupakan segala bentuk criminal yang berhubungan dengan penggunaan komputer. Kemudian kejahatan siber diatur *the Computer Misuse Act 1993* dan diamandemen menjadi *the Computer Misuse and cybersecurity (Amendment) Act 2017* (Kin et al., 2022; National Crime Prevention Council, 2022).

Pemerintah Filipina, di lain sisi, mendefinisikan kejahatan siber atau juga biasa disebut kejahatan komputer merupakan penggunaan komputer sebagai instrumen untuk tujuan ilegal lebih lanjut seperti melakukan penipuan perdagangan pornografi anak, pelanggaran kekayaan intelektual, mencuri identitas atau pelanggaran privasi. Untuk menghadapi kejahatan siber yang terjadi, pemerintah Filipina mengadopsi *Cyber Prevention Act 2012*, dengan tujuan utama adalah untuk menghukum tindakan seperti *cybersex*, pornografi anak, pencurian identitas dan beberapa pelanggaran siber lainnya (Gravion & Villanueva, 2021).

Seiring perkembangannya, kejahatan siber seringkali disamakan dengan kejahatan terorganisir atau tindakan kejahatan terorganisir dilakukan dengan menggunakan komputer dan internet sehingga dianggap sebagai kejahatan siber, sehingga kedua tindak kriminal ini sering dihubungkan. Namun nyatanya, kejahatan terorganisir dan kejahatan siber menjadi dua hal yang berbeda dan tidak menutup kemungkinan kejahatan terorganisir dapat terjadi di dunia maya. Oleh karena itu, untuk melihat peran kejahatan terorganisir di dunia maya

sangat penting untuk membedakan kedua fenomena ini, (1) *organized cybercriminal* merupakan seseorang atau kelompok yang melakukan kejahatan siber yang didefinisikan di dalam hukum, (2) kejahatan terorganisir "tradisional" merupakan kelompok yang melakukan operasinya secara *online*, yang secara bersamaan juga melakukan aktivitasnya secara *offline* dan menggunakan *internet* sebagai fasilitas kejahatan (Lavorgna, 2020).

Dari penelitian yang ada tentang jaringan kejahatan siber (yang mungkin dapat dibandingkan secara virtual dengan kelompok kejahatan terorganisir), dapat disimpulkan bahwa pelaku kejahatan siber yang terorganisir seringkali tidak memenuhi definisi hukum standar kejahatan terorganisir (sesuai dengan hukum yang ada, misalnya, dalam Konvensi Palermo) atau definisi yang diungkapkan oleh beberapa akademisi, sekalipun kejahatan tersebut berbahaya dan beresiko tinggi. Namun, melihat jenis kegiatan kriminal yang dilakukan, penjahat siber tidak dapat dengan mudah dikonseptualisasikan sebagai kejahatan terorganisir. Tergantung pada negara tempat mereka diadili, sebagian besar kasus yang dianalisis tidak memenuhi ambang hukum persyaratan hukuman minimum untuk dianggap "cukup serius", oleh karena itu, diberi label sebagai kejahatan terorganisir (Lavorgna, 2020). Dalam beberapa kasus, beberapa jenis kejahatan siber tidak (belum) diakui sebagai salah satu kegiatan yang dicakup oleh undang-undang anti-kejahatan terorganisir.

Meningkatnya laporan dan berita yang menuliskan kejahatan terorganisir mulai melakukan operasinya secara *online*, argumen ini tidak sepenuhnya benar karena tidak didukung dengan bukti yang kuat. Tidak

menutup kemungkinan peluang untuk melakukan kejahatan siber menarik bagi beberapa kelompok kejahatan terorganisir tradisional (terutama bagi mereka yang menjalankan aktivitas perdagangan manusia berskala besar, karena dunia maya tanpa batas dapat mengurangi jarak menjadi nol, menghubungkan penjual dan pembeli). Di sisi lain, tidak semua kelompok kejahatan terorganisir mengubah modus operasi mereka secara signifikan karena dunia maya, dengan mengandalkan struktur peluang sosial ekonomi yang berbeda, berbagai kelompok memang memiliki kapasitas adaptasi yang berbeda terhadap kemungkinan dan tantangan baru yang disediakan oleh *internet* (Lavorgna, 2020). Oleh karena itu, perbedaan antara kejahatan terorganisir dan kejahatan siber sangat penting dibutuhkan peran pemerintah dalam level nasional dan organisasi atau lembaga pada level regional untuk menentukan perbedaan kedua tindak kriminal ini, mengingat perkembangan teknologi yang semakin luas memperburam batasan aktivitas daring (dalam jaringan) dan luring (luar jaringan).

Hingga awal tahun 2000-an keamanan siber sangat jarang dibahas dalam isu keamanan nasional, sampai pada akhirnya Amerika Serikat dengan pengaruhnya menggunakan terminologi keamanan siber dan *cyberspace* yang mempengaruhi kebijakan militer AS dalam mencapai keamanan siber (Branch, 2020). Dengan penggunaan terminologi keamanan siber yang mempengaruhi kebijakan sebuah negara terhadap keamanan nasional, *cyberspace* menjadi ruang politik yang diperebutkan, dibentuk oleh perbedaan kepentingan, norma dan nilai. Akibat politisasi ini, para aktor negara, lembaga internasional, dan

organisasi internasional memasuki dimensi politik yang baru. Oleh karena itu, penggunaan sumber daya diplomatik dan kinerja fungsi diplomatik digunakan untuk mengamankan kepentingan nasional terkait dengan *cybersapce*.

Kepentingan tersebut umumnya diidentifikasi sebagi *national cyberspace* atau strategi *cybersecurity*, yang seringkali menjadi referensi pada agenda diplomasi. Isu utama dalam agenda diplomasi *cyberspace* meliputi *cybersecurity*, *cybercrime*, *confidence-building*, kebebasan ber-*internet*, dan tata kelola *internet* (Barrinha & Renard, 2017). Hal ini menjadikan isu keamanan siber mejadi sebuah isu yang di-sekuritisasi (*hypersecuritization*), sehingga menciptakan diskusi yang beragam tentang masa depan keamanan nasional termasuk keamanan siber yaitu *the cyber catastrophist, the digital realist, and the techno-optimist*.

*The cyber catastrophist* menunjukkan bahwa bencana digital mulai kelihatan dampaknya– dan sering kali diremehkan dalam wacana ancaman geopolitik. Beberapa *cyber catastrophist* juga melihat bencana digital yang mengakibatkan keruntuhan sosial, ekonomi, dan infrastruktur yang serupa dengan kekerasan yang dimungkinkan oleh senjata pemusnah massal. Berdasarkan *Global Trends 2030: Alternative worlds* sebuah laporan dari *the National Intelligence Councils* tentang masa depan keamanan dan ekonomi global menyatakan bahwa potensi peningkatan kekuatan senjata nuklir oleh Rusia, Pakistan, Iran, dan Korea Utara dibarengi dengan adanya peluang penggunaan serangan siber. Melalui laporan ini membuktikan adanya anggapan bahwa keamanan siber atau *cyberweapon* pada level yang sama dengan senjata

pemusnah massal, yang berpotensi menjadikan isu ini di-sekuritisasi yang memasukkan aktor non-negara sebagai kontributor potensial terjadinya bencana digital (Lacy & Prince, 2018). Oleh karena itu, *cyber catastophist* menyarankan agar aktor negara, lembaga dan organisasi internasional, hingga individu perlu mewaspadai peningkatan ancaman terhadap keamanan siber. Kemudian, yang paling penting adalah menganggap serius kemungkinan bencana digital dan banyaknya dampak yang disebabkan, kemudian melibatkan organisasi dan lembaga internasional untuk mengamankan dan melindungi keamanan siber.

Untuk menepis pernyataan dari *cyber catastrophist*, *the digital realist* menilai bahwa visi tentang peristiwa bencana masa depan yang terjadi di *cyberspace* hanya untuk menciptakan produk budaya populer. Selain itu, akan ada beberapa pihak yang mendapatkan manfaat ekonomi dari ekonomi politik keamanan siber yang diciptakan oleh ancaman dan ketidakamanan baru. Beberapa pakar juga menyatakan tentang bagaimana beberapa organisasi, bisnis, dan lembaga pemerintah menjadi semakin skeptis tentang beberapa skenario bencana yang digunakan dalam promosi materi untuk solusi dan alat siber yang ingin dijual (Lacy & Prince, 2018). Thomas Rid pada (Lacy & Prince, 2018) berpendapat bahwa sangat bermasalah untuk membicarakan kemungkinan perang siber, para aktor internasional tidak mungkin terlibat dalam konflik di mana instrumen siber merupakan “senjata” utama. Perang adalah penggunaan kekerasan untuk mencapai tujuan politik atau ekonomi tertentu melalui teknik yang membuat musuh tidak berdaya, apabila

kemungkinan penggunaan *cyberweapons* pada situasi perang tidak akan sebanding kemampuannya dengan penggunaan senjata yang lebih tradisional.

Namun, tidak berarti bahwa siber konflik, kejahatan siber, dan gangguan yang berasal dari *cyberspace* tidak menimbulkan masalah pada kepentingan nasional. Dampak negatif yang berasal dari siber pada kepentingan dan keamanan nasional, umumnya tidak berdampak pada kematian dan kehancuran fisik. Tantangan bagi kemanan nasional khususnya bidang militer adalah bagaimana memanfaatkan kecepatan, keamanan, efisiensi, dan efektivitas biaya siber tanpa menciptakan kelemahan baru bagi keamanan nasional (Lacy & Prince, 2018). Pada dasarnya, *cyberspace* hanyalah salah satu dari masalah yang terjadi di dalam kehidupan bernegara, argumen bahwa *cyberspace* menjadi ancaman bagi keamanan negara hanya bersifar ekonomi. Oleh karena itu, *digital realist* menekankan fokus pada pengembangan strategi keamanan siber dan keamanan siber secara defensif dan ofensif.

Di lain sisi, beranggapan bahwa menyamakan senjata siber sebagai sebuah "*gamechanger*" akan menciptakan skenario destruktif seperti yang telah dikemukakan *cyber catastrophist* (Lacy & Prince, 2018). Beberapa beranggapan bahwa perkembangan teknologi yang terjadi pada kehidupan manusia saat ini merupakan bagian dari sistem politik yang dimana masyarakat diberikan kebebasan dan hak untuk mengembangkan sesuatu, oleh karena itu, dengan perkembangan teknologi yang baru dapat meningkatkan sektor-sektor lain seperti Kesehatan, komunikasi, ekonomi, dan keamanan. *The techno-optimist* percaya bahwa jika masyarakat mengembangkan institusi dan budaya

politik yang tepat, dunia dapat melanjutkan proses mengatasi bencana dan bahaya yang disebabkan oleh perkembangan teknologi. Dengan populasi dunia yang hampir seluruhnya menganut sistem demokrasi liberal juga tidak menjadikan semua hal sempurna, tetapi masyarakat liberal memiliki mekanisme kritik dan refleksi yang memungkinkan adanya perbaikan dimasa yang akan datang. Kevin Kelly pada (Lacy & Prince, 2018) menilai keamanan siber dan berbagi dampak didalamnya merupakan sebuah proses lingkaran yang akan terus berputar.

Oleh karena itu, *techno-optimist* berfokus pada pengembangan infrastruktur siber yang dapat dimulai dengan riset dan edukasi, karena kebanyakan bencana siber disebabkan oleh kesalahan yang dapat diperbaiki. Dalam hal perang siber, *techno-optimist* percaya hal ini akan diatasi dengan adanya pengembangan teknologi yang baru, tetapi *techno-optimist* khawatir dengan cara negara menggunakan teknologi baru untuk melakukan pengawasan dan pengendalian populasi. Khususnya dalam hal militerisasi internet, kemungkinan komunikasi, edukasi, dan mobilisasi menjadi terbatas sehingga potensi kebebasan yang dimiliki masyarakat dikontrol ketat (Lacy & Prince, 2018). Bagi *techno-optimist*, politik keamanan siber harus difokuskan untuk melindungi keamanan warga negara ancaman yang diciptakan oleh negara itu sendiri.

## B. Organisasi Internasional (*International Organization*)

Awal tahun 1970an kerjasama yang dilakukan antara negara menjadi sebuah fokus yang dipelajari dalam beberapa bidang akademik seperti ilmu politik, ekonomi, dan diplomasi. Seluruh kegiatan yang hasilnya mencapai kerjasama khususnya dalam bidang ekonomi dan urusan keamanan menjadi sebuah kegiatan yang penting dalam lingkungan politik sebuah negara saat itu (Milner, 1992). Robert Keohane dalam (Milner, 1992) menuliskan bahwa ketika aktor menyesuaikan perilaku mereka atau mengantisipasi referensi dari aktor lain dalam proses kordinasi kebijakan, maka perilaku ini dapat disebut dengan kerjasama. Dalam paradigma hubungan internasional, aktor akan membentuk sebuah wadah untuk mengakomodasi kerjasama antara negara ini. Oleh karena itu, organisasi internasional dibentuk oleh aktor untuk memenuhi dan mengakomodasi kerjasama yang mereka lakukan. Kata "organisasi" merujuk pada lembaga antar-pemerintah pertama kali digunakan dalam perjanjian damai setelah Perang Dunia I.

Perjanjian yang dirancang dari tahun 1960-an hingga 1980-an menyebutkan bahwa penamaan "antar pemerintah" memiliki arti tunggal dan merujuk pada organisasi internasional. Khususnya pada Konvensi Wina tentang Hukum Perjanjian antara Negara dan Organisasi Internasional atau antara Organisasi Internasional menuliskan bahwa "untuk tujuan Konvensi ini (...) 'organisasi internasional' berarti organisasi antar pemerintah" (Golia & Peters, 2020). Maksud dari definisi lama ini adalah untuk mengecualikan organisasi non-pemerintah.

Di lain sisi, definisi kontemporer menetapkan tiga kriteria kumulatif: tujuan dibentuknya organisasi internasional yang dapat berwujud dokumen pendirian, diatur oleh hukum internasional publik, antar-pemerintah (keanggotaan negara), dan kehendaknya sendiri. Berdasarkan perspektif ini, entitas tertentu dapat dikatakan sebuah organisasi internasional hanya jika didirikan (1) oleh instrumen yang diatur oleh hukum internasional, dan jika (2) pendiri dan anggotanya adalah negara (atau badan hukum internasional lainnya), dan (3) jika mampu menghasilkan ─ melalui setidaknya satu organ ─ "kehendak" yang berbeda dari anggotanya (Golia & Peters, 2020).

Selain itu, terminologi organisasi internasional merujuk pada asosiasi negara-negara yang didirikan berdasarkan perjanjian. Dari perjanjian ini memiliki tujuan dari terbentuknya organisasi tersebut memiliki struktur khusus sendiri untuk memenuhi fungsi-fungsi tertentu dalam organisasi. Terbentuknya organisasi internasional didasari oleh perjanjian yang bersifat multilateral, sehingga perjanjian ini terhitung sebagai hukum organisasi internasional. Ratifikasi diperlukan untuk berlakunya perjanjian konstituen organisasi internasional, ditandatangani baik oleh semua negara, sejumlah negara tertentu, atau mayoritas negara.

Adanya organisasi internasional digunakan menjadi sebuah alat untuk implementasi kebijakan dari aktor dengan kekuatan yang lebih besar dari aktor lain dan menjadi sebuah arena untuk kontestasi dari kebijakan yang telah dihasilkan. Selain kontestasi kebijakan, organisasi internasional juga menjadi arena untuk kontestasi antara *social forces*, ide, dan negara (O'Brien, 2002). Di

lain sisi, (Beland & Orenstein, 2013) mengemukakan bahwa organisasi internasional tidak hanya kontestasi kebijakan atau ide, organisasi lebih fleksibel dari hanya sekedar arena untuk kontestasi ide. Organisasi internasional sering menjadi tempat untuk mengembangkan ide-ide baru, hal ini membuat sulit untuk mengkarakterisasi pendekatan kebijakan organisasi internasional sebagai hal yang stabil, kecuali pada periode waktu yang relatif singkat yang dimana memungkin menunjukkan konsistensi ideologi (Beland & Orenstein, 2013).

Sejumlah penulis menunjukkan bahwa proses ideasional dalam organisasi internasional membantu menangani masalah sosial dan ekonomi yang dirancang untuk ditangani oleh kebijakan publik yang dihasilkan nanti. Oleh karena itu, adanya ide-ide yang terbentuk dan dihasilkan dalam organisasi internasional menjadi alasan dan tujuan organisasi dibentuk. Ide-ide ini memberikan panduan tentang penciptaan dan reformasi kelembagaan dan umumnya berfungsi untuk mengurangi ketidakpastian pada saat krisis yang dirasakan. Dengan demikian, ide membantu aktor mendefinisikan kepentingan mereka, yang dibentuk tidak hanya oleh kondisi material tetapi melalui interpretasi kondisi (Beland & Orenstein, 2013). Oleh karena itu, membentuk ide dalam organisasi internasional sangat penting untuk memutuskan arah dan tujuan sebuah organisasi internasional.

Adanya ide-ide dalam organisasi internasional ini menjadi hal krusial untuk mempengaruhi pengembangan kebijakan domestik karena organisasi internasional tidak memiliki hak veto formal atas kebijakan domestik.

Kurangnya hak veto formal membuat cara kerja organisasi internasinoal melalui persuasi, meyakinkan “aktor penting” dalam level domestik untuk mengadopsi preferensi kebijakan baru yang diciptakan pada forum organisasi internasional. Mempertimbangkan hal ini dan batas-batas persyaratan keuangan, proses ideasional adalah cara paling sentral di mana organisasi berusaha untuk membentuk kebijakan domestik (Beland & Orenstein, 2013).

Selain sebagai wadah untuk kontestasi ide dan mempengaruhi kebijakan domestik, beberapa pemikir dalam hubungan internasional berikut juga megungkapkan pendapat mengenai bagaimana penerapan teori hubungan internasional memandang organisasi internasional.

Pemikir *realist* mengungkapkan bahwa organisasi internasional, bukan “aktor” tetapi sebatas “forum” dan umumnya sebuah “instrumen” bagi negara-negara anggota. Realisme menekankan bahwa beberapa organisasi internasional tertentu tidak lebih dari mainan politik kekuasaan dan menjadi sebuah alat untuk ambisi nasional dari negara anggotanya. Namun, realisme gagal menangkap fungsi normal organisasi internasional, output normatif mereka dan fakta bahwa negara-negara biasanya mematuhi kewajiban yang berasal dari keanggotaan mereka, bahkan ketika mereka bertentangan dengan kepentingan strategis mereka sendiri (Golia & Peters, 2020).

Di lain sisi, *Functionalism* menjadi salah satu paradigma terpenting untuk memahami organisasi internasional. Ide fungsionalis yang paling dasar adalah *raison d'être* yaitu pemenuhan tugas (fungsi) tertentu untuk mengatasi masalah-masalah yang menyangkut lebih dari satu negara. Fungsi-fungsi pada

organisasi internasional, pada saat yang sama, menetapkan batasan dan memungkinkan untuk memperluas kekuatan organisasi internasional itu sendiri. Namun, fungsionalisme sampai batas tertentu memperburuk retoris dan ideologis yang membenarkan *ex post* perluasan fungsi dan kekuasaan organisasi. Kemudian, fungsionalisme terpaku pada hubungan antara organisasi dan anggotanya, dan menjadikan lingkungan organisasi menjadi "*blind spot*" terutama individu yang mungkin terpengaruh secara negatif oleh aktivitas organisasi (Golia & Peters, 2020).

Oleh karena itu, fungsionalisme tidak dapat berkontribusi pada akuntabilitas organisasi internasional terhadap individu luar. Secara umum, peningkatan kekuatan organisasi internasional sangat mungkin terjadi, tetapi tidak dibatasi dengan baik oleh fungsionalisme sebagai perangkat teoretis. Oleh karena itu, dapat berkontribusi pada krisis legitimasi organisasi internasional (Golia & Peters, 2020).

Kemudian, beberapa tahun terakhir, *constructivist scholar* memandang organisasi internasional dari sisi ideasional atau *agenda-setting function* yang dapat dilakukan pada organisasi internasional. Bagi konstruktivis fungsi *agenda-setting* pada organisasi internasional dipengaruhi oleh legitimasi yang dimiliki oleh organisasi itu sendiri, seperti; otoritas rasional-legal yang berasal dari *charters*[2], legitimasi yang didelegasikan kepada organisasi internasional yang diperoleh dari negara, legitimasi moral yang berasal dari misi penting

[2] Dokumen yang menandai terbentuknya sebuah organisasi internasional

organisasi, dan legitimasi yang didapatkan dari *expert* berdasarkan fokus organisasi internasional yang diterima secara luas (Beland & Orenstein, 2013). Dengan menggunakan pandangan konstruktivis, akan mempermudah sejauh mana peranan organisasi internasional pada isu-isu tertentu karena adanya legitimasi dan fungsi *agenda-setting* yang menjadi parameter awal.

## C. Penelitian Terdahulu

*Tabel 2. Penelitian Terdahulu*

| Judul Tulisan | Teori | Perbedaan Penelitian |
|---|---|---|
| Cyber Security in East Asia: Governing Anarchy. Oleh Nicholas Thomas (2009) | Sekuritisasi | Penelitian ini berfokus pada keseluruhan Asia dengan tiga level analisis yaitu domestik, regional, dan internasional. Dan penelitian ini mencoba membuktikan bahwa keamanan siber yang bersifat transnasional membuat pemerintah sulit untuk mensekuritisasi ancaman dari *cyberspace* |
| Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). Oleh Iqbal Ramadhan (2020) | Kerjasama Internasional; Organisasi Internasional | Penelitian ini berfokus untuk menganalisis kapabilitas dan willingness ASEAN sebagai dominan power di kawasan untuk meregulasi perlindungan data. |
| Regional Cybersecurity: Moving Towards a Resilient ASEAN Cybersecurity Regime. Oleh Caitríona H. Heinl (2014) | Kerjasama Internasional | Artikel ini menjelaskan masalah keamanan siber yang dihadapi ASEAN dan menguraikan opsi kebijakan yang dapat ASEAN lakukan untuk menciptakan rezim keamanan siber yang lebih tangguh di kawasan. |