PERBANDINGAN UPAYA ASEAN DAN EU DALAM KEAMANAN SIBER DI REGIONAL

Disusun dan Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh Gelar Sarjana Sosial (S.Sos) Strata-1

SKRIPSI

Oleh:

Muhammad Thobroni Rahadiansyah
201910360311125

Program Studi Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Muhammadiyah Malang
2024

PERBANDINGAN UPAYA ASEAN DAN EU DALAM KEAMANAN SIBER REGIONAL

Diajukan Oleh :

MUHAMMAD THOBRONI RAHADIANSYAH
201910360311125

Telah disetujui
Pada hari Kamis 15 Agustus 2024

Pembimbing I

Dedik Fitra Suhermanto, M.Hub.Int

Wakil Dekan I

Najamuddin Khairur Rijal, S.IP.,M.Hub.Int

Ketua Program Studi
Hubungan Internasional

Prof. Gonda Yumitro, M.A., Ph.D.

SKRIPSI

Dipersiapkan dan disusun oleh :

MUHAMMAD THOBRONI RAHADIANSYAH
201910360311125

Telah dipertahankan di depan Dewan Penguji Skripsi
dan dinyatakan
L U L U S
Sebagai salah satu persyaratan untuk memperoleh gelar
Sarjana (S-1) Hubungan Internasional
Pada hari Kamis 15 Agustus 2024
Di hadapan Dewan Penguji

Dewan Penguji :

1. **Ruli Inayah Ramadhoan, M.Si** ( )
2. **Muhammad Fadzryl Azmy,M.A** ( )
3. **Dedik Fitra Suhermanto M.Hub.Int** ( )

Mengetahui,
Wakil Dekan I Fakultas Ilmu Sosial dan Ilmu Politik

Najamuddin Khairur Rijal, S.IP.,M.Hub.Int

BERITA ACARA BIMBINGAN SKRIPSI

Nama : Muhammad Thobroni Rahadiansyah

NIM : 201910360311125

Program Studi : Hubungan Internasional

Fakultas : Fakultas Ilmu Sosial dan Ilmu Politik

Judul Skripsi : Perbandingan Upaya ASEAN dan EU dalam Keamanan Siber di Regional

Pembimbing : Dedik Fitra Suhermanto, M.hub.Int

Kronologi Bimbingan:

Tanggal	Paraf Pembimbing	Keterangan
23 Oktober 2023		Pengjuan Judul
27 Oktober 2023		Revisi Pendahuluan
30 Oktober 2023		Revisi Teori
3 November 2023		Revisi Pembahasan
6 November 2023		Penentuan Kesimpulan
10 November 2023		ACC TA
28 November 2023		Penandatanganan ACC oleh Dosen Pembimbing

Malang, 20 Januari 2024

Menyetujui,

Dedik Fitra Suhermanto, M.Hub.Int

UNIVERSITAS MUHAMMADIYAH MALANG
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
Jurusan : Ilmu Kesejahteraan Sosial * Ilmu Pemerintahan * Ilmu Komunikasi * Sosiologi * Hubungan Internasional
Jl. Raya Tlogomas No. 246 Telp. (0341) 460948, 464318-19 Fax. (0341) 460782 Malang 65144 Pes. 132

SURAT PERNYATAAN

Yang bertandatangan di bawah ini:

Nama : Muhammad Thobroni Rahadiansyah
NIM : 201910360311125
Jurusan : Hubungan Internasional
Fakultas : Ilmu Sosial dan Ilmu Politik
UNIVERSITAS MUHAMMADIYAH MALANG

Dengan ini menyatakan dengan sebenar-benarnya bahwa

1. Tugas Akhir dengan Judul :"Perbandingan Upaya ASEAN dan EU Dalam Keamanan Siber di Regional "adalah hasil karya saya, dan dalam naskah tugas akhir ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu Perguruan Tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, baik sebagian ataupun keseluruhan, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka

2. Apabila ternyata di dalam naskah tugas akhir ini dapat dibuktikan terdapat unsur- unsur PLAGIASI, saya bersedia TUGAS AKHIR INI DIGUGURKAN dan GELAR AKADEMIK YANG TELAH SAYA PEROLEH DIBATALKAN, serta diproses sesuai dengan ketentuan hukum yang berlaku.

3. Tugas akhir ini dapat dijadikan sumber pustaka yang merupakan HAK BEBAS ROYALTY NON EKSKLUSIF.

Demikian pernyataan ini saya buat dengan sebenar-benarnya untuk dipergunakan sebagaimana mestinya.

Malang, 20 Januari 2024

Muhammad Thobroni Rahadiansyah

ABSTRAK

Muhammad Thobroni Rahadiansyah, 2024, 201910360311125, Universitas Muhammadiyah Malang, Fakultas Ilmu Sosial dan Ilmu Politik, Program Studi Hubungan Internasional, Perbandingan Upaya ASEAN dan EU dalam Keamanan Siber di Regional, Dosen Pembimbing : Dedik Fitra Suhermanto, M.Hub.Int

Di masa teknologi yang maju ini, banyak negara yang memindahkan sistem kerjanya secara online, namun terdapat permasalahan mengenai keamanan siber yang muncul ketika terjadi perubahan sistem. Agar banyak negara yang mulai menyadari pentingnya keamanan siber, dalam konteks penelitian ini penulis mencoba membandingkan upaya keamanan siber di kawasan ASEAN dengan kawasan Uni Eropa dalam menekan kerja sama lintas batas dan pembentukan kelembagaan sebagai kunci untuk mencapai tujuan tersebut. mampu menciptakan kebijakan keamanan siber yang efektif di tingkat regional dan nasional. Dalam penelitian ini metode yang digunakan adalah deskriptif untuk menjelaskan dan menganalisis suatu permasalahan atau persoalan yang terjadi. Dalam penelitian ini, penulis menggunakan teori liberalisme institusional dalam mencoba menjelaskan upaya kerja sama yang dilakukan kawasan ASEAN dan Uni Eropa dalam mengatasi masalah ancaman siber. Studi ini juga menemukan adanya perbandingan dan persamaan dalam upaya kedua kawasan dalam mengatasi ancaman siber di kawasan ASEAN dan Uni Eropa.

Kata Kunci: ASEAN, Perbandingan, Kerja Sama, Keamanan Siber, Uni Eropa

Menyetujui,
Pembimbing,

Dedik Fitra Suhermanto, M.Hub.Int

Malang, 20 Januari 2023
Peneliti,

Muhammad Thobroni Rahadiansyah

ABSTRACT

Muhammad Thobroni Rahadiansyah, 2024, 201910360311125, University of Muhammadiyah Malang, Faculty of Social and Political Science, Internasional Relation Study Program, Comparison of ASEAN and EU Efforts on Cybersecurity in the Region, Advisor I: Dedik Fitra Suhermanto, M.Hub.Int

In this time of advanced technology, many countries have moved their work systems online, but there are problems about cybersecurity that arise when the system changes occur. So that many countries are starting to realize the importance of cybersecurity, in the context of this research the author tries to compare cybersecurity efforts in the ASEAN region with the European Union region in suppressing cross-border cooperation and the formation of institutions as a key to being able to create effective cybersecurity policies at regional and national levels. In this research, the method used is descriptive to explain and analyze a problem or issue that occurs. In this research, the author uses the theory of institutional liberalism in trying to explain the cooperation efforts made by the ASEAN region and the European Union in overcoming the problem of cyber threats. This study also found that there are comparisons and similarities in the efforts of the two regions to overcome cyber threats in the ASEAN region and the European Union.

Keyword: ASEAN, Comparation, Cooperation, Cyber Security, European Union

Approved,
Advisor,

Dedik Fitra Suhermanto, M.Hub.Int

Malang, 20 January 2023
Researcher,

Muhammad Thobroni Rahadiansyah

KATA PENGANTAR

Assalamu'alaikum Warrahmatullahi Wabarakatu

Puji Syukur kehadirat Allah Subhanahu wa Ta'ala yang telah memberikan nikmat dan karunia-Nya yang luar biasa kepada hamba-hambanya. Shalawat serta salam semoga selalu tercurah kepada junjungan Nabi besar Muhammad SWT yang telah membawa cahaya Islam kedalam dunia ini dan menjadi penutan bagi setiap umatnya hingga akhir zaman. Setelah melewatinya proses kerja keras, penyusunan skripsi berjudul "***PERBANDINGAN UPAYA ASEAN DAN EU DALAM KEAMANAN SIBER DI REGIONAL***" akhirnya bisa terselesaikan. Selain sebagai syarat mendapatkan gelar SI, penulis berharap skripsi ini dapat bermanfaat bagi semua pihak yang berkepentingan dan dapat megembangkan ilmu pengetahuan khususnya pada ilmu hubungan internasional. Oleh karena itu, penulis ingin mengungkapkan rasa terimakasih kepada pihak-pihak yang telah memberikan dukungan dan doanya yang diberikan kepada penulis sehingga penulis mampu menyelesaikan skripsi ini pada waktunya. Beberapa pihak tersebut antara lain:

1. Kepada ibu tercinta Ira Puspita yang terus memberikan dukungan dan doa serta tidak lelah memberikan kepercayaanya untuk penulis sehingga penulis dapat menyelesaikan studi Hubungan Internasional di Fakultas Ilmu Sosial dan Politik Universitas Muhammadiyah Malang.
2. Adik tersayang Elvina Hera Ruslita , terimakasih telah mendukung dan penyemangat bagi penulis sehingga skripsi dapat terselesaikan.
3. Dedik Fitra Suhermanto, M.Hub.Int. selaku dosen pembimbing yang telah memberikan tenaga, pikiran dan waktunya dalam membimbing penulis dengan penuh kesabaran. Terimakasih atas ilmu yang telah diberikan kepada penulis.
4. Seluruh jajaran dosen Program Studi Hubungan Internasional Universitas Muhammadiyah Malang dan staff dari tim Laboratorium Hubungan Internasional Universitas Muhammadiyah Malang yang telah memberikan ilmu kepada penulis sebagai mahasiswa.
5. Kepada keluarga besar ibu dan saudara-saudara tercinta yang tanpa lelah memberikan dukungan, doa dan motivasi bagi penulis sehingga penullis dapat menyelesaikan skripsi ini.

6. Teman-teman Basecamp saya yang selalu memberikan semangat dan keceriaan, setiap tawa dan canda kalian membuat proses ini menjadi semakin ringan dan menyenangkan sehingga penulis dapat menjalani setiap langkah dalam menyelesaikan skripsi ini dengan tanpa beban.
7. Semua pihak yang tidak dapat disebutkan diatas yang telah membantu dengan segala budi dan amal baiknya selama ini. Penulis menyadari bahwa skripsi ini masih banyak kekurangan dan jauh dari kata sempurna. Oleh karena itu dengan segala kerendahan hati, penulis mengharapkan saran dan kritik yang membangun agar menjadikan skripsi ini lebih baik kedepannya.

Terima Kasih

Wassalamu‘alaikum Warrahmatullahi Wabarakatu

Malang, 20 Januari 2024

Muhammad Thobroni Rahadiansyah

DAFTAR ISI

LEMBAR PERSETUJUAN.....**i**
LEMBAR PENGESAHAN.....**ii**
BERITA ACARA BIMBINGAN SKRIPSI.....**iii**
SURAT PERNYATAAN.....**iv**
ABSTRAK.....**v**
KATA PENGANTAR.....**vii**
PLAGIASI.....**xi**
A. Latar Belakang Masalah.....**2**
B. Teori Liberalisme Institutional.....**6**
C. Konsep Keamanan Siber.....**8**
D. Metode Penelitian.....**10**
E. Pembahasan.....**11**
Upaya keamanan siber di kawasan ASEAN.....11
Upaya keamanan siber di kawasan Uni Eropa.....15
Analisis upaya keamanan siber di kawsan ASEAN dan Uni Eropa dalam Liberalisme Institusionalis.....20
F. Kesimpulan.....**24**
Daftar Pustaka.....**26**

UNIVERSITAS MUHAMMADIYAH MALANG

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

HUBUNGAN INTERNASIONAL
hi.umm.ac.id | hi@umm.ac.id

SURAT KETERANGAN
Nomor : E.5.a/194/HI/FISIP-UMM/IX/2024

Yang bertanda tangan di bawah ini, Ketua Program Studi Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Muhammadiyah Malang, menerangkan bahwa mahasiswa:

Nama	:	**Muhammad Thobroni Rahadiansyah**
NIM	:	**201910360311125**
Judul Skripsi	:	Perbandingan Upaya ASEAN dan EU dalam Keamanan Siber di Regional
Dosen Pembimbing	:	1. Dedik Fitra Suhermanto, M. Hub.Int.

telah melakukan cek plagiasi pada naskah Skripsi sebagaimana judul di atas, dengan hasil sebagai berikut:

	BAB I
	15%
Similarity	2%

**) Similarity maksimal 15% untuk setiap Bab.*

Demikian surat keterangan ini dibuat untuk dipergunakan sebagai syarat pengurusan bebas tanggungan di UPT. Perpustakaan UMM.

Malang, 26 Agustus 2024
Ka. Prodi HI,

Prof. Gonda Yumitro, M.A., Ph.D

Kampus I
Jl. Bandung 1 Malang, Jawa Timur
P: +62 341 551 253 (Hunting)
F: +62 341 460 435

Kampus II
Jl. Bendungan Sutami No 188 Malang, Jawa Timur
P: +62 341 551 149 (Hunting)
F: +62 341 582 060

Kampus III
Jl. Raya Tlogomas No.246 Malang, Jawa Timur
P: +62 341 464 318 (Hunting)
F: +62 341 460 435
E: webmaster@umm.ac.id

PERBANDINGAN UPAYA ASEAN DAN EU DALAM KEAMANAN SIBER DI REGIONAL

Muhammad Thobroni Rahadiansyah

Program Studi Hubungan Internasional

Fakultas Ilmu Sosial dan Politik, Universitas Muhammadiyah Malang

Email:Thobyra@gmail.com

Abstract

Dalam era teknologi yang maju ini, banyak negara telah memindahkan sistem kerja mereka ke dalam jaringan daring, namun muncul berbagai masalah terkait keamanan siber seiring dengan perubahan sistem tersebut. Oleh karena itu, banyak negara mulai menyadari pentingnya keamanan siber. Dalam konteks penelitian ini, penulis mencoba membandingkan upaya keamanan siber di kawasan ASEAN dengan kawasan Uni Eropa dalam menekan kerjasama lintas batas dan pembentukan institusi sebagai kunci untuk menciptakan kebijakan keamanan siber yang efektif di tingkat regional dan nasional. Metode yang digunakan dalam penelitian ini adalah deskriptif untuk menjelaskan dan menganalisis masalah atau isu yang terjadi. Penulis menggunakan teori liberalisme institusional untuk menjelaskan upaya kerjasama yang dilakukan oleh kawasan ASEAN dan Uni Eropa dalam mengatasi masalah ancaman siber. Penelitian ini juga menemukan adanya perbandingan dan kesamaan dalam upaya kedua kawasan tersebut untuk mengatasi ancaman siber.

Keywords: *ASEAN; Komparasi; Kerjasama; Keamanan Siber; Uni Eropa*

A. Latar Belakang Masalah

Pada era kemajuan teknologi saat ini, banyak teknologi yang memberikan kemudahan dalam melakukan pekerjaan, salah satunya adalah teknologi digital yang pada saat ini mengalami perkembangan yang sangat pesat. Teknologi digital merupakan teknologi yang dapat dioperasikan dengan sedikit manusia dan berdasarkan sistem komputer (Kundang K Juman, n.d.). Dengan adanya teknologi dan Inovasi yang cepat berkembang, diperlukan pemahaman mengenai ancaman siber di segala aspek, terutama pada aspek pemerintahan, karena memegang kunci penting dalam keberlangsungan bernegara. Selain itu dengan adanya teknologi yang semakin maju ini, dapat memberikan kemudahan terhadap mengolah dan menyimpan data, sehingga banyak negara pada saat ini mulai untuk melakukan perubahan dari metode konvensional menjadi metode yang lebih modern dalam mengolah data. Peralihan yang dilakukan oleh negara-negara yang ada merupakan respon dari bentuk perkembangan zaman yang saat ini semakin pesat, serta seluruh negara mulai untuk mengintegrasikan sistem mereka agar mudah memberikan pelayanan terhadap masyarakat yang ada. Saat ini adanya teknologi digital dapat memberikan pengaruh terhadap keberlangsungan ekonomi, penyimpanan data, dan integritas antar negara di kawasan. Dengan adanya beberapa pengaruh tersebut dapat memberikan kemudahan negara dalam mengatur dan menjalankan negara dalam aspek nasional maupun internasional. Namun dengan adanya teknologi yang maju ini, tidak hanya memberikan keuntungan namun juga memberikan kerugian terhadap penggunaanya, seperti mulai munculnya *"Cybercrime"* yang marak terjadi pada tahun 2020. Munculnya kejahatan siber tidak hanya sebatas *phising* dan *pencurian data*, melainkan memiliki banya variasi di dalamnya sperti *carding, ddos attack, hacking, ransomware,* dan *cyber bullying* (Sekar & Purwani, 2023).

Kejahatan siber merupakan bentuk risiko yang berkembang, disebabkan oleh perkembangan teknologi dan informasi. Pada sektor siber ruang dan dimensi yang menjadi masalah telah berbeda, karena kejahatan siber dilakukan di ruang siber atau *cyberspace*. Merupakan ruang maya yang terbentuk dari jaringan computer dan system informasi yang saling terhubung dengan global. Secara sederhana ruang siber adalah ruang yang mencakup Internet, jaringan antar computer, perangkat lunak dan semua aktivitas digital yang terjadi di dalam ruang siber tersebut. Ruang siber menjadi tempat untuk *anonymus* melakukan pertukaran Informasi, komunikasi, dan berbagai kegiatan lainnya yang bersifat maya. Didalam ruang siber sendiri tidak ada Batasan pada sektor informasi dan pengguna, serta pada platform ruang siber ini menyediakan media sosial, *e-commerce,* transaksi keuangan, dan bahkan sampai

Pendidikan. Ruang siber pada dasarnya memberikan begitu banyak manfaat dan potensi perkembangan yang baik namun disisilain ruang siber juga dapat memberikan ancaman terhadap keamanan negara, mulai dari sekala yang kecil hinga kepada sekala yang besar (Kementrian Pertahanan Republik Indonesia, 2014).

Pada tahun 2020 di kawasan ASEAN saja, banyak data informasi yang hilang disebabkan pencurian data yang menimbulkan kerugian sebesar 3.86 juta USD. Terjadinya serangan siber ini disebabkan oleh kurangya sumber daya manusia yang mengetahui mengenai system keamanan siber atau rendahnya kapabilitias masyarakat mengenai keamanan siber. Namun masalah tersebut tidak bisa hanya masalah yang timbul oleh masyarakat melainkan juga ada kesalahan dalam pemerintah yang masih belum peduli terhadap pengamanan data dari individu. Selain itu pemerintah juga belum memiliki kapabilitas yang lebih dalam mengatasi masalah keamanan siber di tingkat regional maupun nasional. Dengan adanya serangan siber ini memberikan dampak yang buruk terhadap ekonomi negara dan masalah mengenai keamanan data dari sebuah negara. Pencurian data yang dilakukan merupakan salah satu bentuk ancaman siber yang dapat menyerang individu dan dapat menyebabkan pemerasan dan pemalsuan identitas. Dengan adanya masalah ini negara-negara anggota ASEAN mulai sadar mengenai bagaimana keamanan siber ini penting. Namun pendekatan yang dilakukan oleh setiap negara memiliki perbedaan sehingga negara anggota ASEAN mulai untuk membentuk sebuah forum yang membahas mengenai keamanan siber di tingkat regional maupun nasional (Anshori & Ramadhan, 2019).

Berbeda dengan negara di kawasan ASEAN, Uni Eropa mulai concern terhadap masalah keamanan siber ini sejak tahun 2004, yang disebabkan karena adanya tantangan baru terhadap keamanan yang mulai bergeser pada sector digital. Selain adanya perubahan keamanan pada sektor digital terdapat masalah mengenai serangan siber yang dilakukan oleh para kelompok hacker tertentu seperti menyebar virus *ransomware, phising,* dan *hacking*. Pada tahun 2020 terdapat peningkatan dalam serangan *ransomware* sebanyak 35 kali serangan dalam rentang waktu empat bulan.(ENISA, 2022) Sehingga Uni Eropa merespon dengan mulai membentuk sebuah badan keamanan jaringan dan informasi di Eropa dengan nama *European Network and Information Security Agency* (ENISA). Pembentukan Lembaga ENISA merupakan sebagai bentuk kepedulian Uni Eropa dalam megatasi masalah keamaman siber yang dirasa telah mulai memberikan dampak negative terhadap keberlangsungan system yang ada di kawasan Uni Eropa. Lembaga ini memiliki tugas sebagai salah satu lembaga yang memberikan saran terhadap keamanan siber bagi negara anggota Uni Eropa (Markopoulou et

al., 2019). Selain dibentuknya Lembaga pengawas Uni Eropa juga mencoba untuk membentuk satuan khusus di dalam Interpol mereka dengan membentuk *European Cybercrime Centre* yang bertugas menangani apabila terdapat kasus serangan terhadap ruang siber atau *cyberspace*. Sehingga bisa dikatakan bahwa *European Cybercrime Centre* adalah sebagai tim cepat tanggap atau tim respon apabila terdapat serangan yang dilakukan pada sektor *cyberspace* (Vendius, 2022).

Disislain kawasan ASEAN memiliki pertumbuhan pengguna teknologi internet yang besar, pada tahun 2017 pengguna internet di kawasan ASEAN sebesar 380 juta pengguna dan terus mengalami peningkatan penggunanya. Dengan adanya penigkatan pengguna internet ini banyak serangan siber yang terjadi terhadap system pemerintahan maupun pada sektor swasta dan sektor public serangan yang terjadi mencakup seperti ransomware dan pencurian data. Berdasarkan data yang telah dikeluarkan oleh Interpol mengenai serangan siber di kawasan ASEAN, ransomware memiliki serangan yang signifikan hal in di buktikan dengan terdeteksinya 2,7 juta ransmoware yang tersebar di kawasan ASEAN dalam rentang waktu tiga kuartal waktu pertama pada tahun 2020. Negara-negara di Kawasan ASEAN menanggapi masalah keamanan siber dengan berbagai Langkah kebijakan. Setiap negara anggota memiliki pendekatan yang berbeda dalam mengatasi masalah keamanan siber. Meskipun terdapat Kerjasama *ASEAN Ministerial Conference on Cybersecurity* (*AMCC*) masih terdapat perbedaan kebijakan didalam pendekatan kemanan siber yang dilakukan setiap negara (Goals, 2020).

Dalam penelitian ini penulis melakukan kajian literatur riview terhadap Beberapa studi sebelumnya mengenai beberapa penelitian terdahulu tentang isu keamanan siber di berbagai kawasan regional dan global. Beberapa studi memiliki fokus terhadap analisis kebijakan, namun pada studi lain berfokus pada teknologi mengenai penanganan keamanan siber. Namun, dalam studi yang menitik beratkan terhadap studi komparatif penanganan keamanan siber di kawasan secara khusus kawasan ASEAN dengan Eropa masih sedikit. Penelitian pertama yang dilakukan oleh Xuechen Chen dan Yifan Yang, mengenai studi komparasi terhadap pendekatan EU dan ASEAN dalam *Cyber Governance* memiliki kesimpulan bahwa pendekatan yang dilakukan oleh kedua kawasan tersebut memiliki pendekatan berdasarkan norma yang berlaku di kawasan seperti kawasan UE yang menjadi pioner terhadap keberlangusngan tata kelola siber di kawasan maupun global. Namun berbeda dengan pendekatan yang dilakukan oleh ASEAN, mereka memiliki fokus untuk melakukan budaya diplomasi unik yang dilakukannya dan memegang teguh prinsip sentralitas di kawasan ASEAN.(Chen & Yang, 2022). Namun,

penelitian terdahulu mengenai *Cyber Security* di kawasan ASEAN yang dilakukan oleh Fikry dan Rizki dengan judul Kepentingan Singapura pada keamanan siber di Asia Tenggara dalam singapore Internasional *Cyber week* memiliki kesimpulan yang sama dengan menjelaskan bahwa negara-negara di kawasan ASEAN harus membentuk kesadaran dan norma terhadap keamanan siber di Asia Tenggara.(Anshori & Ramadhan, 2019) Berbeda dengan penelitian yang dilakukan oleh Kai Lin Tay, penelitian yang dilakukan menggunakan metode perbandingan yang membandingkan bagaimana keamanan siber di kawasan Eropa dengan kawasan Amerika, sehingga dapat menemukan pendekatan yang cocok di kawasan ASEAN (Tay, 2023). Namun perbedaan pendapat yang dilakukan oleh penelitian Lennon Chang menyebutkan bahwa ASEAN tidak memiliki concern terhadap keaman siber hal ini di buktikan dengan adanya negara anggota yang masih belum memiliki kebijakan yang kuat dalam menangani kasus kejahatan siber seperti Myanmar dan Kamboja (Chang, 2017).

Selain beberapa studi tersebut terdapat studi yang dilakukan oleh Bima Yudha dan Diah Apriani dengan judul "*ASEAN Regional forum: Realizing Regional Cyber Security in ASEAN region*" dengan menjelaskan bagaimana terwujudnya keamanan siber di kawasan ASEAN. Pada penelitian tersebut ditemukan data bahwa keamanan siber di kawasan ASEAN dapat terjadi apabila terdapat perjanjian didalam *Treaty of amity* dalam berlangsungnya keamanan siber di kawasan ASEAN. Selain itu negara di kawasan ASEAN juga dapat membangun kerjasama bilateral antar negara anggota ASEAN agar terwujudnya keamanan siber di kawasan ASEAN (Yudha et al., 2015). Namun perbedaan kesimpulan dikemukakan oleh Iqbal Ramadhan yang menyimpulkan bahwa kerangka kerjasama keamanan siber di kawasan ASEAN dapat terjadi apabila dapat memanafaatkan fungsi dari sekertariat jendral dan forum-forum regional yang penting, sehingga sub-organisasi memiliki peran penting dalam mempromosikan kerangka keamanan siber di kawasan ASEAN(Ramadhan, 2022). Trine Thygesen Vendius melakukan peneilitian serupa dengan menggunakan rumusan masalah berbeda dengan menitik beratkan terhadap bagaimana *European Cybercrime Center* (EC3) upayanya dalam keberlangsungan keamaman siber di kawasan Eropa dalam membentuk regulasi mengenai keamanan siber dapat lebih jelas dan dapat mencegah kejahatan siber seperti pencurian data, dan serangan Ddos (Vendius, 2022). Didalam penelitian yang sama Alya Fathia Fitri memiliki kesimpulan yang berbeda bahwa keamanan siber di kawasan Uni Eropa dapat terwujud apabila melakukan kerjasama intra-regional (Luzern, 2017). Selain itu, penelitian yang dilakukan oleh Lazlo Kovacs pada tahun 2018 memiliki fokus terhadap strategi yang tepat terhadap keamanan siber di Uni Eropa dan Nato. Berdasarkan data yang telah ditemukan oleh

Lazlo, strategi yang dilakukan oleh Uni Eropa telah berhasil memberikan pengaruh terhadap keamanan dan memiliki tujuan yang jelas mengenai keamanan siber yang diharapkan oleh anggota Uni Eropa. Berdasarkan data yang telah ditemukan oleh Lazlo dan Aisyah tersebut menjelaskan bahwa penerapan regulasi yang dilakukan oleh Uni Eropa memiliki kemajuan yang bertahap dan tidak dapat dilakukan secara sempurna dalam waktu singkat. Walaupun dengan adanya kendala waktu dalam mengimplementasikan kebijakan mengenai keamanan siber yang dilakukan, negara negara anggota di kawasan Uni Eropa masih menganggap bahwa keamanan siber merupakan salah satu bentuk ancaman dari globalisasi yang harus diselesaikan, karena dapat memberikan pengaruh terhadap keamanan suatu negara dan keamanan suatu kawasan (Kovács, 2018).

Dengan mengacu pada data penelitian yang terdahulu mengenai keamanan siber di kawasan ASEAN dan Uni Eropa, terlihat bahwa masih sedikit penelitian yang membahas mengenai perbedaan dan persamaan dalam upaya keamanan siber yang dilakukan oleh kawasan ASEAN dan Uni Eropa. Penelitian ini bertujuan untuk membandingkan bagaimana upaya yang dilakukan oleh kawasan tersebut dalam menangani masalah keamanan siber di kawasan regional dengan lebih mendalam. Dengan membandingkan pandangan dari studi sebelumnya, penelitian ini diharapkan dapat memberikan tambahan pengetahuan yang lebih lengkap mengenai bagaimana respon ASEAN dan Eropa dalam menghadapi keamanan siber. Faktor faktor kunci yang telah teridentifikasi dalam mempengaruhi pendekatan yang dilakukan oleh kedua kawasan tersebut nantinya dapat digunakan sebagai parameter dalam membandingkan pendekatan yang dilakukan. Pada penelitian ini di harapkan memiliki manfaat dan relevansi dalam konteks hubungan internasional, temuan didalam penelitian ini dapat memberikan dasar yang kuat dalam membentuk kerjasama yang lebih mendalam mengenai keamanan siber di wilayah ASEAN dan Eropa. Selain itu penelitian ini juga dapat memberikan bantuan terhadap panduan dan norma-norma internasional yang berkaitan dengan keamanan siber, serta memberikan arah terhadap negara dalam menentukan arah kebijakan mengenai keamanan siber. Berdasarkan penjabaran latar belakang masalah penelitian yang ada, maka dapat disusun rumusan masalah “Bagaimana perbandingan Upaya yang dilakukan oleh kawasan ASEAN dan kawasan Eropa dalam mengatasi masalah keamanan siber ?”.

B. Teori Liberalisme Institutional

Liberalisme Institutional merupakan sebuah prespektif yang mulai muncul pasca perang dunia ke-2, para kaum liberalisme memiliki pandangan mengenai bagaimana perilaku

negara dapat menciptakan perdamaian dengan melakukan kerjasama dan diplomasi. Pandangan liberalisme berangkat pada tiga aspek inti yang pertama liberalisme memmiliki pandangan bahwa pada dasarnya manusia memiliki sifat yang baik dan positif yang berasal dari pemikiran mereka. Kemudian yang kedua kaum liberalis memiliki kepercayaan bahwa hubungan internasional dapat bersifat kooperatif dibandingkan dengan konfliktual. Selanjutnya yang ketiga adalah adanya asumsi adanya kemajuan terhadap setiap aspek yang ada, sehingga kaum liberalis secara tidak langsung juga mendukung modernisasi yang terjadi di setiap negara yang ada, dengan adanya modernisasi di setiap negara dapat memberikan perluasan dalam aspek kerjasama yang akan dilakukan (Doering, 2013). Menurut pendapat yang dikeluarkan oleh Robert o Keohane bahwa Liberal Institusionalisme dengan dibentuknya suatu institusi Internasional dapat memberikan dorongan dalam proses kemajuan Bersama di antara negara anggota, Intitusi Internasional juga dapat dijadikan sebagai wadah penampungan dari kepentingan-kepentingan setiap negara anggota. Institusi internasional dapat memberikan aturan terhadap Tindakan suatu negara. Teori ini berpendapat bahwa negara dapat diatur oleh power supranasional, sehingga dengan adanya institusi internasional dapat memberikan kemajuan terhadap Kerjasama antar negara dan dapat menciptakan perdamaian. Dengan terbentuknya institusi internasional dapat memberikan hubungan timbal balik yang menguntungkan. Selain itu pandangan Institusionalisme ini menekankan bahwa Lembaga-lembaga ini dapat memberikan keseimbangan kekuatan dan mencegah konflik Melalui kerjasam dan diplomasi yang dilakukan. Dengan adanya pendekatan ini Kerjasama internasional dapat terjalin apabbila ada Lembaga-lembaga yang memfasilitasi dialog antar negara yang ada. Pendekatan ini sering digunakan untuk menjelaskan fenomena Kerjasama dan penyelesaian konflik dalam dinamika global saat ini (Febiola, 2018). Didalam penelitian ini teori ini digunakan untuk menganalisis bagaimana kawasan ASEAN dan Uni Eropa dalam menyelesaikan masalah keamanan siber dengan melakukan kerjasama.

Penggunaan teori liberalisme institusional pada penelitian ini sesuai dengan upaya yang dilakukan oleh kawasan ASEAN dan Uni Eropa dalam mengatasi ancaman siber yang terjadi didua kawasan tersebut. Kerjasama yang dilakukan merupakan bukti bahwa negara sejatinya dapat berdamai apabila negara tersebut memiliki sebuah institusi yang memberikan ruang terhadap negara-negara untuk mengutarakan kepentingan mereka. Selain itu dengan

adanya institusi tersebut dapat memberikan ruang terhadap negara untuk saling berdiskusi dan tidak menaruh curiga terhadap negara karena adanya saling keterbukaan. Selain itu Kerjasama yang dibangun dapat dikontrol dan dijalankan sesusai dengan kepentingan bersama. Dengan adanya isntitusi yang ada dapat memberikan cakupan yang luas terhadap Kerjasama yang akan di ambil (Asiyah, 2019).

Sedangkan menurut Jackson dan Sorensen institusi memiliki dua sifat yaitu institusi yang bersifat secara global seperti liga bangsa-bangsa (LBB) dan persatuan bangsa-bangsa (PBB), dan yang kedua bersifat regional seperti Uni Eropa dan ASEAN. Para pengamat liberalisme institusional memiliki peran penting dalam meningkatkan Kerjasama yang terjadi antara negara-negara. Berdasarkan argument diatas maka adanya institusi internasional maupun regional dapat mengatur negara-negara untuk mencapai kepentingan Bersama dengan menyetujui aturan yang telah di sepakati Bersama. Selain itu actor yang berperan penting menurut kaum liberalisme Institusional adalah negara karena melakukan Kerjasama regional dan selalu megupayakan Kerjasama untuk mencapai kepentingan nasional mereka. Institusi internasional yang memiliki kepercayaan mampu untuk melakukan peningkatan terhadap kerjasama diantara negara anggota dan memiliki cakupan Kerjasama yang lebih luas. Dengan adanya perluasan cakupan dalam Kerjasama dapat memberikan dampak yang lebih tehadap memenuhi kebutuhan kepentingan nasional (Adi Kusuma, 2022).

C. Konsep Keamanan Siber

Munculnya keamanan siber tidak dapat terlepas dari beberapa konsep yang telah muncul seperti *Cyber*, *Cyberwar*, dan *Cyberspace.* Semua konsep yang telah disebutkan tadi memiliki keterikatan terhadap ranah digital yang saling terkoneksikan dengan sebuah internet. Istilah *Cyber* sendiri muncul pada tahun 1948 yang berasal dari kata *Cybernetics* yang memiliki makna sebuah studi tentang pesan yang dapat mengendalikan mesin dan rakyat. Namun pada masa itu *Cybernetics* memiliki sebuah tujuan untuk pengiriman pesan pada perang dunia kedua dan sebagai bentuk komputasi komputer pasca perang dunia ke-dua. Konsep keamanan siber sebagai salah satu bentuk sekuritas dimulai pada tahun 1991, yang ditemukan di dalam sebuah laporan *Computer Science and Telecommunications Board (CSTB).* Di dalam laporan tersebut menjelaskan mengenai perlindungan terhadap pengungkapan yang tidak diinginkan, manipulasi, dan kerusakan data. Beragamnya serangan siber di dunia *cyberspace*,

memunculkan banyak tindak kejahatan yang berbentuk digital. Jika kejahatan tersebut mulai berubah menjadi sebuah serangan terhadap suatu sistem maka dibutuhkan upaya pengamanan dalam menyelesaikan masalah serangan tersebut. Sehingga pada dasarnya *Cybersecurity* merupakan salah satu bentuk upaya pengamanan terhadap sumberdaya teknologi informasi dalam mencegah terjadinya *Cybercrime* (Chotimah, 2019).

Keamanan siber sendiri dapat di definisikan sebagai sebuah Tindakan dalam melindungi data yang bersifat kerahasiaan, ketersediaan, dan keutuhan informasi yang diproses. Keamanan siber merupakan suatu isu yang memunculkan banyak perdebatan, salah satunya adalah keamana siber membutuhkan pendekatan yang tepat untuk diatasi karena memiliki ruang yang berbeda. Namun ada pendapat lain yang menjelaskan bahwasanya keamanan siber merupakan bentuk lain dari politik yang memilki akar keapada kondisi anarkis yang memiliki keutamaan untuk membantu diri sendiri dalam memenuhi kebutuhan yang berasal dari kekuatan (Anshori & Ramadhan, 2019).

Keamanan siber ditujukan pada isu keamanan dalam informasi di dalam pemerintah, organisasi, dan adanya ururan individu yang saling terhubung dengan internet. Keamanan siber memiliki cakupan dengan segala bentuk yang berhubungan dengan pengawasan computer, monitoring, sampai control yang harus dilalui. Kemanan siber pada saat ini tidak lagi berada di wilayah teknologi saja melainkan telah masuk kedalam ancaman terhadap keamanan nasional maupun regional. Perkembangan teknologi informasi telah membentuk perubahan secara signifikan dalam menjelaskan mengenai konsep keamanan, pada saat ini ruang interaksi keamanan tidak hanya pada sektor fisik melainkan telah masuk ke dalam sektor maya. Sehingga negara harus mengikuti perkembangan dalam megatasi ancaman keamanan pada dunia maya ini. Konsep keamaman siber ini pada saat ini telah ditetap kan sebagai salah satu wilayah yang harus negara jaga keamanannya sama halnya dengan daerah teritoral negara secara fisik. Pada saat ini serangan siber tidak hanya tertuju pada institusi public saja melainkan sampai menyerang institusi pemerintahan (Triwahyuni & Wulandari, 2016).

Sedangkan menurut pendapat dari siagian di dalam jurnalnya yang berjudul “Peran keamanan siber dalam mengatasi konten negatif guna mewujudkan ketahanan informasi nasional” ,Keamanan siber merupakan system yang memiliki peran untuk memberikan perlindungan terhadap system informasi dan ancaman siber. Didalam keamanan siber terdapat tiga komponen utama yang dirancang untuk memandu kebijkan keamamn dalam sebuah jaringan dan institusi yaitu: Confidentiality, Integrity, Availability. Tiga komponen tersebut

merupakan tujuan utma dalam konsep keamanan siber. Sehingga pada dasarnya keamanan siber adalaha sebuah metode atau cara untuk menangkal ataupun meminimalisir tingkat resiko terjadinya ancaman siber (Siagian et al., 2017).

.

D. Metode Penelitian

Pada penelitian ini, peneliti mencoba menggunakan jenis penelitan deskriptif yang digunakan untuk dapat menjelaskan dan menganalisa suatu masalah atau isu keamanan terutama, keamanan siber di kawasan ASEAN dan Uni Eropa, yang menjadi topik utama dalam penelitian ini. Penelitian deskriptif merupakan salah satu bentuk penelitian yang menggambarkan suatu fenomena dengan data yang akurat dan di teliti secara sistematis. Penelitian deskriptif ini dilakukan tanpa melakukan manipulasi terhadap variable data yang ada, sehingga penelitian ini lebih memiliki fokus terhadap mengumpulkan dan menganalisis data dengan tujuan menjelaskan sebuah karakteristik mengenai keamanan siber yang dilakukan di kawasan ASEAN dan kawasan Uni Eropa (Syafrida, 2021). Penelitian ini menggunakan metode kualitatif untuk melihat bagaimana perbandingan upaya keamanan siber di kawasan ASEAN dan Uni Eropa. Metode penelitian Kualitaitf memiliki penekanan terhadap proses analisis dinamika hubungan antar fenomena yang di amati, dengan berdasarkan logika (Balakrishnan & Forsyth, 2019). Data pendukung yang digunakan pada penelitian ini menggunakan studi literatur terhadap jurnal, buku, data report dari instansi terkait, dan web institusional yang terkait, terutama data yang memiliki fokus terhadap upaya keamanan siber di kawasan ASEAN dan Uni Eropa, implementasi teknologi keamanan, dan kerjasama antar negara. Studi literatur yang digunakan dapat memberikan landasan teoritis dan juga dapat memberikan pemahaman yang utuh mengenai konsep dan teori yang di gunakan, seperti konsep keamanan siber dan teori liberalisme isntitusional. Proses pengumpulan data memerlukan telaah mendalam megenai pengumpulan data tersebut yang nantinya dapat memberikan penjelasan yang komperhensif. Dengan adanya beberapa data dari berbagai sumber, peneliti berharap dapat melakukan analisis yang lebih mendalam dan nantinya akan di telaah guna mendapatkan data yang sesuai dan di butuhkan oleh peneliti, sehingga mendapatkan hasil yang dapat menjelaskan perkembangan keamanan siber di kawasan ASEAN dan Uni Eropa.

Pada penelitian ini terdapat dua variable yang pertama adalah variable dependen atau variabel unit Analisa, yang memiliki fungsi sebagai variabel yang di amati. Sedangkan variable

yang kedua adalah variable independen atau yang sering disebut sebagai unit eksplanasi, yang memiliki pengaruh terhadap perilaku variable dependen atau pada unti Analisa. Dengan melakukan perician terhadap kedua varibel tersebut bertujuan untuk memberikan gambaran yang komperhensif dan mendalam terhadap hubungan variable dependen dan variable independent (Mas'oed, 1994). Didalam penelitian ini,memiliki fokus unit analisa yang digunakan adalah keamanan siber, yang pada saat ini memiliki concern dari negara negara karena adanya perubahan dinamika keamanan yang pada saat ini telah menjadikan ruang siber sebagai salah satu aspek yang penting dalam keberlangsungan keamanan suatu negara maupun kawasan. Sedangkan untuk unit eksplanasi pada penelitian ini adalah upaya keamanan siber yang dilakukan oleh kawasan ASEAN dan Uni Eropa. Pengambilan variable kedua ini menjadi landasan untuk dapat memahami bagaimana kebijakan, inisiatif, dan kerajasama yang dilakukan oleh masing-masing kawasan di bidang keamanan siber. Dengan melihat varibel pertama dan kedua maka peneliti menggunakan level Analisa data berupa Korelasionis karena hubungan dari kedua variable tersebut setara dan tidak lebih besar. Level analisis korelasionis merupakan sebuah hubungan antara variable dependen dan independent yang memiliki pengaruh terhadap dampak yang dilakukan, namun korelasionis memiliki level yang setara atau tidak ada yang lebih besar maupun lebih kecil (Mas'oed, 1994).

E. Pembahasan

Upaya keamanan siber di kawasan ASEAN

Organisasi ASEAN merupakan organisasi kerjasama regional di kawasan Asia Tenggara yang didirikan pada tahun 1967 yang memiliki tujuan untuk menjaga perdamaian dan keamanan di kawasan Asia Tenggara. Saat ini ASEAN memiliki 11 anggota utama yang terdiri dari Indonesia, Malaysia, Thailand, Filipina, Brunei Darussalam, Vietnam, Myanmar, Kamboja, Laos, Singapura, dan Timor Leste. Organisasi ini memiliki tiga pilar utama dalam keberlangsungan organisasi tersebut yaitu *ASEAN Political Security (APSC), ASEAN Economic Community (AEC),* dan *ASEAN Socio-Cultural Community (ASCC)* (Estiyovionita & Sitamala, 2022). Didalam konteks penelitian ini yang mencoba untuk membahas mengenai keamanan siber maka pembahasan tersebut masuk kedalam pilar ASEAN yang pertama yaitu *ASEAN Political Security (APSC)*. Sehinngga dengan adanya pilar tersebut dapat diketahui bahwa upaya keamanan siber di kawasan memiliki arah yang sejalan dengan keberlangsungan keamanan di kawasan ASEAN. Pada dasarnya negara negara anggota di ASEAN telah merancang strategi khusus dalam menemukan formula di dalam keamaman siber yang cocok

bagi anggota ASEAN karena negara anggota ASEAN memiliki kekurangan dan kelebihan mereka masing-masing.

Negara anggota di kawasan ASEAN memiliki beberapa rangka kegiatan dalam mencoba memperkuat keamanan siber di kawasan mereka. Beberapa kegiatan yang dilakukan oleh negara anggota ASEAN adalah dengan menjadikan *ASEAN regional forum (ARF)* sebagai salah satu platform untuk negara anggota terutama di kawasan Asia-Pasifik untuk dapat melakukan pertukaran informasi dengan negara mitra dialog ASEAN yang terdiri dari Australia, Kanada, China, Jepang, Korea Selatan, Selandia Baru, Rusia, Amerika Serikat, dan Uni Eropa. Tujuan utama dari adanya ARF adalah untuk membangun kepercayaan dan kerajasama regional dengan mengendepankan upaya dialog untuk mencegah ancamanan non-tradisional ataupun ancaman yang berada di ruang siber. Selain terdapat kerajasama regional terdapat Kerjasama yang dilakukan oleh anggota negara ASEAN yaitu membentuk *ASEAN ministrial conference on cybersecurity* (AMCC). Berbeda dengan ARF, ruang lingkup yang di ambil dari AMCC ini adalah memiliki focus terhadap isu-isu keamanan siber, serta jangkuan Kerjasama yang dilakukan hanya sebatas dengan negara anggota ASEAN saja. Forum ini menjadi salah satu bentuk awal keseriusan negara-negara anggota ASEAN dalam menanggapi keamanan siber di kawasan mereka. AMCC sendiri telah dilaksanakan sebanyak enam kali yang dimana pada pertemuan terakhir negara anggota ASEAN mulai membahas pentingnya perlindungan infrastruktur informasi dari ancaman keamanan siber yang di timbullkan oleh *ransomeware*. Sehingga di dalam conferecence tersebut negara anggota ASEAN menyambut baik pembaharuan terhadap strategi keamanan siber di ASEAN, diharapkan pembaaharuan tesebut dapat mmeberikan acuan terhadap penanggulangan keamanan siber di setiap negara angota ASEAN (ASEAN Cybersecurity Cooperation Strategy, 2021).

Selain adanya pembentukan forum yang menangani masalah keaamanan siber di kawasan ASEAN, beberapa negara anggota ASEAN telah melakukan pembentuk badan yang mengurus keamanan siber di dalam negeri. Salah satu contoh adalah negara Indonesia yang membentuk Badan Siber dan Sandi Negara (BSSN). Lembaga tersebut muncul karena adanya peraturan persiden nomor 53 di tahun 2017. Lembaga tersebut dibentuk langsung oleh pemerintah dengan bertanggung jawab secara langsung kepada presiden serta bertujuan untuk menciptakan iklim siber nasional yang aman. Dengan terbentuknua Lembaga tersebut negara Indonesia memiliki tim respon dalam menghadapi masalah keamanan siber dan menjadi pengbung informasi antara nasional dengan forum regional. (Rahmadiani et al., 2019). Selain itu negara pelopor keamanan siber di kawasan ASEAN yaitu Singapura juga memiliki badan keamanan siber di dalam negeri mereka sendiri yang Bernama *Cyber Security Agency* (CSA)

badan tersebut dibentuk pada tahun 2015 untuk megawasi dan mengkoordinasi kegiatan keamanan siber di dalam negeri Singapura (Vu, 2016).

Beberapa negara yang membentuk badan keamaman siber di kawasan merupakan salah satu bentuk program yang telah di gagas beberapa negara anggota di dalam rancangan ASEAN *Cybersecurity Cooperation Strategy* 2021-2025. Namun rancangan program tersebut baru 10 persen yang selesai dan sebanyak 74 persen masih dalam tahap berjalan, dan sisanya belum dimulai. Selain itu kawasan ASEAN masih belum memiliki *Computer Emergency Response Team (CERT)*. Namun rancangan ASEAN *Cybersecurity Cooperation Strategy* ini memfokuskan untuk memperkuat Kerjasama dan kapasitas dari Lembaga CERT di setiap negara, sehingga di tingkat regional lembaga tersebut dapat berkoordinasi dengan lembaga di negara lain dalam mengatasi keamanan siber di kawasan ASEAN (BSSN, 2023).

Selain terdapat Kerjasama di dalam regional terdapat Kerjasama regional dengan negara yang lebih maju dalam bidang keamanan siber di kawsan ASEAN. Kerjasama yang dilakukan antara ASEAN denga Korea Selatan merupakan salah satu Kerjasama yang di lakukan oleh ASEAN dalam memperbaiki dan melakukan pelatihan dalam meningkatkan keamanan siber di kawaan ASEAN. Namun Kerjasama ini lebih berfokus terhadap pengangan covid 19 yang pada saat itu terjadi. Akan tetapi Kerjasama tersebut mencakup aspek keamanan siber di kawasan ASEAN, karena adanya perubahan perilaku masyarakat Ketika pandemic yang dimana segala bentuk kegiatan fisik berubah menjadi kegiatan yang dilakukan secara online. Dengan adanya masalah tersebut membuat Kerjasama ASEAN-Korea Selatan mulai memperhatikan juga pentingnya keamanan siber di kawasan ASEAN (Phuong et al., 2021).

Kerjasaman yang di lakukan oleh ASEAN selain dengan Korea Selatan adalah Kerjasama ASEAN-Japan dalam sektor keamanan siber yang Bernama ASEAN-*Japan Cybersecurity Capacity Building Centre*(AJCCBC). Kerjasama ini dibentuk pada tahun 2018 dibawah kendali TELMIN/SOM dan didanai oleh *Japan ASEAN Integration Fund* (JAIF). Tujuan di bentuknya AJCCBC adalah sebagai tempat pelatihan terhadap tenaga kerja keamanan siber selama 4 tahun yang nantinya diharapkan dapat meningkatkan kapasitas para tenaga kerja keamanan siber di negara anggota ASEAN. Selain ASEAN dan Jepang membentuk Lembaga tersebut, mereka juga mulai membentuk forum antara ASEAN dan Jepang yang bertujuan untuk memperkuat kolaborasi pengelolaan keamanan siber. Forum tersebut bernaman *ASEAN-Japan Cybersecurity Working Group Meeting*, forum ini telah melakukan pertemuan mereka yang ketiga di Indonesia pada tahun 2022 dengan sistem *Hybrid*. Forum tersebut merupakan forum regional terbatas yang di khususkan untuk negara anggota

ASEAN dan Jepang sebagai salah satu bentuk fasilitator Kerjasama dan kolaborasi keamanan siber antara ASEAN dengan Jepang (Fathma Ilmi Anindita Iskandar, 2020).

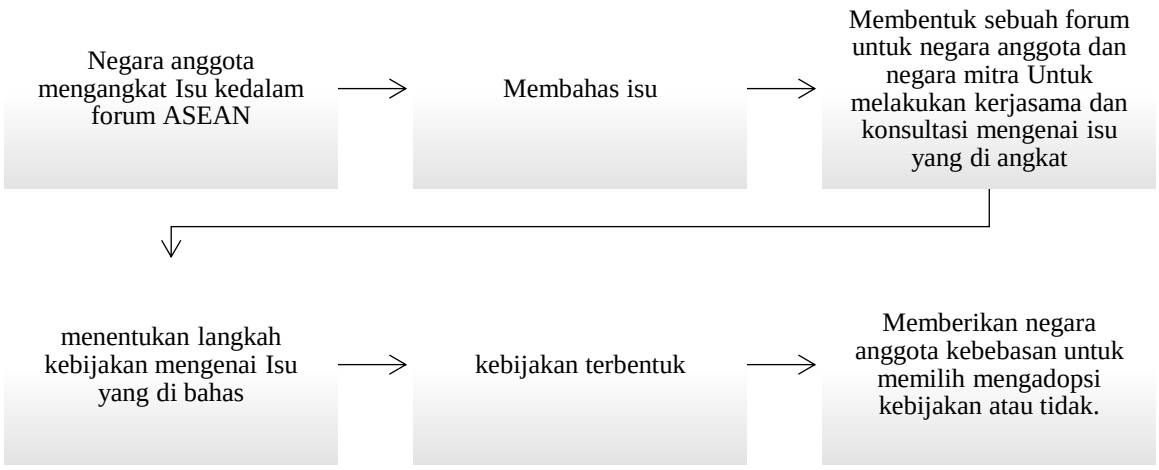
Kerjasama yang dilakukan ASEAN dalam meningkatkan keamanan siber di kawasan banyak dilakukan dengan negara-negara yang telah memiliki kemajuan dalam bidang teknologi. Hal ini di lakukan karena negara anggota ASEAN masih sedikit yang terbilang memiliki pengetahuan mengenai keamanan siber yang lebih maju. Namun di kawasan ASEAN terdapat negara pengagas keamanan siber yang sangat maju dan sangat berambisi untuk meningkatkat keamana siber negara mereka sebagai acuan bagi negara anggota ASEAN yang lain, negara tersebut adalah negara Singapura. Serta masih banyaknya negara di kawasan ASEAN yang melakukan pengamanan siber secara individu tidak secara Bersama yang menimbulkan kurang efektifnya kerangka keamanan siber dan kurang adanya maintenence dalam keberlangsungan Kerjasama keamanan siber di kawasan ASAEN. Selain itu adanya kebijakan open door policy di kawasan ASEAN menimbulkan banyak kepentingan yang berbeda, sehingga memunculkan perbedaan cara penanganan keamanan siber di kawsan ASEAN.

Didalam proses pengambilan keputusan yang dilakukan oleh ASEAN dengan berdasarkan konsultasi dan konsensus. Namun apabila konsensus tersebut tidak dapat tercapai maka Konferensi Tingkat Tinggi ASEAN dapat menentukan keputusan untuk di ambil. Hal ini sesuai dengan yang tertuang didalam piagam perhimpunan bangsa-bangsa Asia Tenggara pada pasal 20 megenai konsultasi dan konsensus. Dengan meilihat isi dari piagam tersebut pengambilan keputusan yang dilakukan di kawasan ASEAN tidak bersifat mengikat namun berdasarkan kekeluargaan yang memberikan ruang terhadap negara anggota untuk dapat menentukan kebijakan yang cocok untuk di angkat atau tidak. Konsep konsensus yang dilakukan oleh ASEAN adalah dengan memberikan ruang terhadap negara anggota untuk dapat mengekspresikan pendapat mereka dengan nyaman. Dengan adanya konsep konsensus ini kawasan ASEAN memberikan prinsip bahwa suara dari setiap negara anggota akan didengar, sehingga mencegah adanya paksaan terhadap pandangan yang berbeda untuk menyesuaikan diri dengan keputusan yang ada. Pada dasarnya konsensus ASEAN adalah sebuah bentuk prinsip mengenai hak kebebasan negara anggota dalam mengungkapkan dan menentukan keputusan mereka sendiri. Dengan penggunaan prinsip konsensus ini ASEAN mengalami masalah dalam pengambilan keputusan yang lama dan mengalami kebuntuan terhadap keputusan yang akan di ambilnya.

Prinsip Konsultasi yang di ambil oleh ASEAN adalah dengan memberikan ruang terhadap negara anggota yang mengalami masalah untuk saling berbagi dan memeberikan

masukan terhadap masalah yang di alami salah satu contohnya adalah *ASEAN Regional Forum* (ARF) yang menjadi salah satu forum bagi negara anggota untuk berkonsultasi dengan sesama negara anggota maupun negara lain dalam menghadapi masalah yang dibahas. Dengan menggunakan prinsip konsultasi ini ASEAN berharap untuk dapat memberikan dampak positif terhadap penyelesaian masalah yang sedang di hadapi oleh negara anggota yang bersifat nasional maupun regional. Untuk lebih jelasnya dapat melihat bagan berikut mengenai bagaimana proses pengambilan kebijakan di ASEAN.

1 Bagan Pengambilan keputusan ASEAN



Upaya keamanan siber di kawasan Uni Eropa

Uni Eropa telah melakukan beberapa upaya yang komperhensif dalam upaya meningkatkan keamanan siber di kawasan Uni Eropa. Salah satu langkahnya adalah dengan membuat kebijakan keamanan siber yang bernama *Network and Information Systems Directive (NIS Directive)*, peraturan ini mewajibkan negara-negara anggota untuk dapat menerapkan kebijakan keamanan siber di negaranya. Dengan adanya peratutan tersebut negara anggota diharapkan dapat melakukan adaptasi terhadap sistem keamanan nasional mereka dengan memastikan beberapa komponen pendorong dalam menjalan kan keamanan siber seperti kesiapsagaan negara-negara anggota, dengan meyakinkan mereka untuk memiliki peralatan yang memadai, kerjasama di antara seluruh negara anggota dengan membentuk grup kerjasama antar negara anggota agar memudah kan pertukaran informasi yang dilakukan, serta

meningkatkan budaya masyarakat mengenai pentingnya keamanan siber. Kebijakan ini mulai menjadi pedoman dalam keamanan siber di setiap negara pada tahun 2018. Tujuan utama dari dibentuknya kebijakan *NIS Directive* untuk memastikan bahwa sector penting dalam penyedia layanan informasi yang bergantung terhadap jaringan dapat mengambil tindakan teknis yang tepat dalam mengelola keamanan jaringan dan sistem informasi (NCSC, 2018). Pada tahun 2023 kerangka kebijakan NIS telah mengalami pembaruan, hal ini disebabkan karena ancaman siber yang terus berkembang sehingga kerangka NIS terdahulu harus mengalami pembaharuan. Pada pembahruan kerangaka NIS mengalami perluasan terhadap cakupan aturan keamanan siber ke sektor dan entitas terbaru. Cakupan yang dicoba untuk di ambil adalah pada sector swasta yang di anggap memiliki peran penting dalam keberlangsungan keamanan suatu negara (European Parliament and the Council of the European Union, 2022).

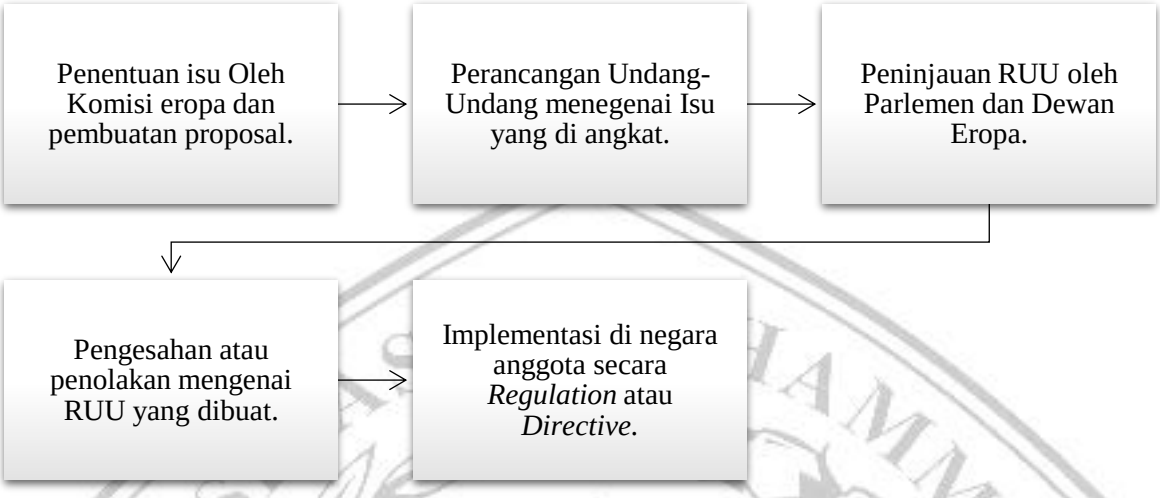
Didalam kebijakan NIS ini membagi dua kategori dalam perusahaan, yang pertama adalah perusahaan operator layanan penting dan yang kedua adalaah penyedia layanan digital. Didalam pembagian dua kategori tersebut untuk memudahkan memilah sector apa saja yang dapat mempengaruhi keamanan suatu negara. Dalam proses kerja kerangka NIS tidak bekerja sendiri melainkan membutuhkan satu Lembaga nasional untuk menjadi pengawas dalam penerapan kerangka NIS ini. Didalam kerangka NIS ini juga mendorong Kerjasama antar negara anggota dengan memfasilitasi pertukaran informasi dan koordinasi respon dalam mengatasi ancaman siber di kawasan. NIS dapat dikatakann sebagai sebuah fondasi yang solid bagi seluruh negara anggota Uni Eropa dalam mengatasi masalah ancaman siber terutama di kawasan Uni Eropa. Kerangka kebijakan NIS tidak dapat berjalans sendiri melainkan mambutuhkan Lembaga yang nantinya dapat mengkontrol dan mengawasi dalam perkembangan kebijakan. Fondasi yang solid ini yang nantinya akan memberikan kemudahan dalam menjalankan kebijakan keamanan siber di kawasan Uni Eropa. Kebijakan NIS ini merupakan suatu bentuk kebijakan yang bersifat dinamis, hal ini di buktikan dengan adanya pembeahruan yang dilakukan guna memberikan kebijakan yang baik terhadap system keamanan siber bagi negara anggota Uni Eropa. Dengan adanya evaluasi yang berjalan di dalam kebijakan NIS ini, dapat membantu memastikan bahwa kebijakan akan tetap relevan dan efektif dalam mengatasi masalah keamaman siber di tingkat regional maupun nasional (Markopoulou et al., 2019).

Didalam proses pengambilan sebuah keputusan untuk di jadikan sebuah kebijakan di kawasan Uni Eropa, dibutuh kan empat lembaga utama dalam prosesnya yaitu : Parlemen Eropa, Dewan Eropa, Dewan Uni Eropa, dan Komisi Eropa. Didalam proses pengambilan keputusan tersebut harus melewati sebuah standar yang bernamakan *codecesion progress.*

Tahap awal dari proses ini adalah dengan penyusunan sebuah proposal yang dilakukan oleh Komisi Eropa, dan yang nantinya proposal tersebut akan di diskusikan oleh Parlemen Eropa dan menyetujui rancangan undang-undang atau kebijakan tersebut. Didalam proses tersebut Komisi Eropa harus menemukan dampak negatif maupun posisitif terhadap kebijakan yang di ajukan, serta Komisi Eropa juga harus mendiskusikan kebijkan baru tersebut dengan pihak-pihak yang bersangkutan.

Setelah melalui proses tersebut Parlemen Eropa, Dewan Eropa dan Dewan Uni Eropa akan berdiskusi masing-masing untuk menyetujui atau tidaknya kebijkan tersebut. Parlemen Eropa nantinya akan memberikan pengajuan amandemen dan melakukan voting mengenai amandemen yang akan dilakukan. Sedangkan untuk Dewan Eropa dan Dewan Uni Eropa akan memeriksa kebijakan tersebut setelah amandemen serta akan menyetujui sebuah kesepakatan politik. Setelah tahap ini selesai melakukan voting oleh Parlemen, maka status dari kesepakatan politik yang telah di setujui oleh dewan akan berubah menjadi formal common Position. Didalam tahap tersebut merupakan penentuan dalam penyetujuan atau penolakan terhadap proposal yang di ajukan. Kemudian Dewan dan Parlemen akan membaca usulan yang di ajukan oleh Komisi dan membahas pengajuan tersebut. Namun jika tidak ada kesepakatan di antara dua lembaga tersebut maka akan dilakukan pembacaan kedua. Proposal yang dilakukan pembacaan kedua tersebut nantinya akan di tinjau ulang dan di revisi yang melibatkan Dewan dan Komisi. Setelah komite memiliki kesepakatan terhadap proposal tersebut, maka proposal yang telah di setujui akan dikirimkan kepada Parlemen dan Dewan yang nantinya akan diadakan pembacaan ketiga yang akan menghasilkan sebuah hukum kebijakan. Didalam tahap ini Parlemen dan Dewan berhak untuk mengajukan amandemen untuk yang kedua kalinya. Namun apabila kebijakan tersebut ditolak oleh Parlemen maka kebijakan tersebut tidak akan di adopsi, sedangkan apabila kebijakan tersebut di setujui maka akan di adopsi menjadi undang-undang yang sah dengan dipublikasikan di jurnal official Uni Eropa yang nantinya akan diterapkan di hukum nasional negara anggota. Uni Eropa memiliki tiga jenis legilisasi utama yaitu *Regulation,* yang merupakan hukum yang berlaku dan mengikat semua negara anggota setelah dipublikasikan oleh Komisi Eropa. *Directive,* bentuk hukum yang mengikat negara-negara anggota Uni Eropa atau kelompok negara anggota dengan memberikan flesibelitas terhadap kebijakan yang diterapkan di negara anggota dapat berbeda namun dengan tujuan yang sama. *Decision,* didalam tipe ini kebijakan bersifat mengikat namun hanya kepada negara anggota yang di tunjuk untuk melakukan kebijakan tersebut. Untuk lebih jelasnya dapat melihat bagan berikut mengenai proses pengambilan kebijakan oleh Uni Eropa.

2 Bagan Proses Pengambilan Keputusan Uni Eropa



Uni Eropa pada saat ini memiliki kepedulian terhadap perlindungan data dari masyarakatnya sehingga Uni Eropa membentuk sebuah kebijakan yang bernama *General Data Protection Regulation* (GDPR). Kebijakan ini merupakan peraturan privasi data yang berlaku di kawasan Uni Eropa. GDPR berfungsi untuk memberikan perlindungan terhadap hak privasi individu mengenai pengolahan data pribadi pada sektor informasi dan jaringan. Hak yang ditekankan pada kebijkan ini adalah pemberian individu untuk mengetahui apakah data mereka telah diproses, adakah data yang di akeses dan juga pemberian hak untuk penghapusan data individu. Pembentukan kebijakan GDPR ini merupakan salah satu bentuk kebebasan individu yang dijunjung oleh Uni Eropa. Sehingga pemberian akses terhadap data individu merupakan salah satu dari hak yang dimiliki oleh masyarakatnya (Sudibyo, 2020).

Selain pembentukan kerangka terhadap penanganan keamanan siber, Uni Eropa juga melakukan pembentuk badan keamanan jaringan dan informasi yang bernama *European Union Agency for Network and Information Security* (ENISA). Pembentukan badan ini dimulai pada tahun 2004 dengan berdasarkan peraturan (EC) No 460/2004. ENISA melakukan peran aktif dalam menjamin keamanan jaringan dan informasi tingkat tinggi di Uni Eropa. ENISA memiliki misi untuk meningkatkan kesadaran mengenai keamanan jaringan serta mengembangkan budaya keamanan jaringan informasi di kalangan masyarakat, konsumen, perusahaan, dan organisasi sektor public yang berada di kawasan Uni Eropa. ENISA memiliki kontribusi terhadap keamanan jaringan dan informasi dengan Melalui penerbitan rekomendasi,

dukungan terhadap kebijakan pembuatan kebijakan, dan kolaborasi langsung dengan tim oprerasional di seluruh Uni Eropa (European Union Agency for Cybersecurity., 2022).

ENISA memiliki peran penting dalam meningkatkan kapasitas keamanan siber di kawasan Uni Eropa. Badan ini juga memberikan dukungan program pelatihan untuk tenaga professional pada sector keamanan siber. Program pelatihan tersebut dilakukan bertujuan untuk membantu mengembangkan ketrampilan tenaga kerja yang diperlukan untuk melawan ancaman siber yang terus berkembang di setiap waktu. Selain memberikan pelatihan badan ENISA juga memberikan pendalaman dalam pemahaman mengenai kerangka hukum dan kebijakan yang terkait dengan keamanan siber di negara anggota Uni Eropa. Dengan memberikan pemahaman yang cukup ENISA juga dapat melakukan bantuan terhadap implementasi aturan keamanan siber di negara anggota Uni Eropa maupun tingkat regional (ENISA, 2022).

Dalam perkembangannya ENISA tidak hanya sebagai Lembaga yang berfungsi untuk memberikan panduan teknis saja, melainkan pada saat ini ENISA menjadi pusat penelitian yang memberikan pembaharuan terhadap resiko ancaman keamanan siber di Uni Eropa. Sehingga ENISA juga memiliki peran sebagai pengumpul informasi mengenai ancaman siber yang nantinya akan di berikan kepada negara anggota dan dewan Uni Eropa untuk nantinya dapat dilakukan pencegahan terhadap ancaman siber yang terjadi, sehingga ENISA juga menjadi dasar dalam pengambilan keputusan yang strategis dalam menangani keamanan siber. Dengan fokus ENISA sebagai Lembaga yang meningkatkan kapasitas, pertukaran informasi, dan pengembang kebijakan di Uni Eropa, dapat menjadi salah satu Lembaga sentral dalam mendukung keamanan siber di kawasan Uni Eropa, serta membantu menentukan arah bagi negara-negara anggota Uni Eropa dalam mengatasi keamanan siber nasional. Lembaga ini menjadi salah satu pengambilan keputusan yang penting karena didalamnya terdapat tenaga kerja yang berasal dari negara anggota Uni Eropa, sehingga setiap kebijakan yang akan di ambil akan mendapatkan saran dari badan ENISA ini. Peran ENISA juga signifikan terhadap kebijakan keamanan siber di kawasan Uni Eropa, sehingga badan ini menjadi pusat sentral dari keamanan siber di kawasan Uni Eropa. Upaya yang dilakukan oleh ENISA menghasilkan banyak kebijakan dan program kerja yang nantinya akan memberikan dampak terhadap keberlangsunngan pembentukan Lembaga respon dalam mengatasi keamaman siber di setiap negara anggota (European Commission, 2023).

Upaya yang dilakukan oleh Uni Eropa dalam keamanan siber tidak hanya terbatas kepada pembuatan kebijakan dan pembuatan Lembaga pengawas, melainkan terdapat kerajasama yang dilakukan oleh kawasan Uni Eropa dengan kawasan Amerika dan ASEAN.

Kerjasama yang dilakukan dengan Amerika bernama *U.S-UE Cyber Cooperation* yang dimulai pada tahun 2014. Didalam Kerjasama ini Amerika dan Uni Eropa banyak melakukan penandatangan Kerjasama dalam menangani ancaman siber. Penandatanganan Kerjasama ini diharapakan dapat meningkatkan keamana pada sektor siber yang pada saat itu dirasa memiliki potensi yang dapat menyebabkan ancaman terhadap keamanan negara. Point-point yang di bahas di dalam kerangka Kerjasama tersebut adalah perkembangan dunia maya internasional, promosi dan perlindungan Hak Asasi Manusia di dunia maya, dan peningkatan kapasitas *Cybersecurity* di negara-negara anggota. Didalam Kerjasama ini muncul kerangka Kerjasama yang memberikan pelatihan terhadap pemerintah dan swasata dalam mengembangkan keamanan siber yang berfokus terhadap pemerintah dan perusahaan sawasta yang mendalami bidang informasi dan teknologi. Selain itu Kerjasama ini juga membantu meningkatkan respon terhadap insiden ancamana keamanan siber yang dialami oleh individu maupun perusahaan. Kerjasama ini juga menekannkan perlindungan infrastruktur yang penting pada sector informasi dan komunikasi (Ardiansyah, 2014).

Analisis upaya keamanan siber di kawsan ASEAN dan Uni Eropa dalam Liberalisme Institusionalis

Banyak upaya yang telah di lakukan oleh kawasan ASEAN dan kawasan Uni Eropa, berdasarkan pandangan dari teori Liberalisme Institutionalis menjelaskan bahwa kebanyakan upaya yang dilakukan oleh kedua kawasan tersebut merupakan Kerjasama, hal ini di dukung dengan adanya reaksi dari negara-negara yang mengangkat isu mengenai masalah keamanan siber yang kemudian di bawa kedalam forum atau institusi yang memfasilitasi interaksi antar negara. Dengan adanya institusi yang memfasilitasi kepentingan dari negara-negara, menjadikan negara lebih sering melakukan Kerjasama dalam mengatasi masalah yang mereka alami. Sehingga konfliktual yang terjadi dapat dikurangi, dan rasa saling curiga dari suatu negara akan berkurang. Pada dasarnya negara membutuhkan peran dari negara lain untuk menyelesaikan polemik masalah yang terjadi di tingkat regional maupun nasional (Dugis, 2018).

Dengan melihat upaya yang dilakukan oleh kedua kawasan tersebut dan penjabaran mengenai liberalisme institutionalis, bisa di ketahui bahwa kedua kawasan tersebut menggunakan pendekatan yang sama dalam mengatasi keamanan siber di kawasan. Pendekatan yang dilakukan adalah dengan melakukan Kerjasama dan pembentukan institusi dalam menampung kepentingan dari setiap negara terutama pada sector keamanan siber di

kawasan ASAEN dan Uni Eropa baik tingkat regional maupun pada tingkat nasional. Bentuk dari institusi yang di bentuk juga memiliki kemiripan yaitu berbentuk sebuah forum dan badan pengawas. Di ASEAN forum yang di gunakan adalah *ASEAN Ministrial Conference on Cybersecurity* (AMCC) dan *ASEAN Regional Forum* (ARF) kedua forum tersebut terbentuk atas kerjasama yang dilakukan secara regional dan internasional dan bentuk kolektifitas negara anggota ASEAN yang mengalami masalah keamanan siber. Disisi lain kawasan Uni Eropa memiliki *European Union Agency for Cybersecurity* (ENISA) yang terbentuk dari kebijakan langsung dari komisi eropa yang nantinya kebijakan tersebut wajib untuk di implementasikan di setiap negara anggota Uni Eropa. Ketiga Lembaga tersebut memiliki kontribusi dalam keberlangsungan pembuatan kebiijakan keamanan siber di kawsan ASEAN dan Uni Eropa, dengan menampung informasi dan menyebarkan kepada negara anggota agar dapat memperbaharui keamanan siber di tingkat regional maupun nasional.

Dengan melihat upaya di atas dapat diketahui terdapat perbedaan dalam mengidentifikasi isu keamanan siber, sehingga pendekatan yang dilakukan oleh kedua kawasan berbeda. Pendekatan yang dilakukan Uni Eropa dalam mengidentifikasi adalah dengan melakukan pendekatan *top-down*. Pendekatan *top-down* merupakan salah satu bentuk pendekatan yang menjadikan pembentuk kebijakan sebagai aktor utama dalam terbentuknya suatu kebijakan dan juga dalam pengimplementasiannya dilakukan secara tersentralisir (Nurainina, 2018). Sehingga didalam kebijakan keamanan siber yang di ambil oleh Uni Eropa bersifat *top-down* yang dimana dewan didalam Uni Eropa mengambil isu global dan menganggap itu sebuah ancaman yang kemudian memunculkan sebuah kebijakan keamanan siber yang nantinya mewajibkan negara-negara anggota untuk melakukan implementasi terhadap kebijakan yang telah dibuat tersebut.

Berbeda dengan kawasan Uni Eropa, kawasan ASEAN mengidentifikasi masalah yang ada di satu negara, yang kemudian negara tersebut membawa isu tersebut kedalam forum regional seperti ASEAN dengan melalui proses konsensus. Proses yang dilakukan ini dapat memberikan penetuan arah kebijkan yang tepat terhadap negara anggota, karena adanya perbedaan kekuatan dan kelemahan yang dialami oleh setiap negara anggota. Hal ini di buktikan dengan beberapa negara anggota memiliki perbedaan dalam melakukan implementasi kedalam sistem pemerintahan mereka. Seperti contoh yang dilakukan oleh negara Indonesia memilih menggunakan sistem judicial, yang dimana sistem tersebut merupakan pemberian tanggung jawab terhadap pemilik platform untuk mengatasi masalah siber yang di hadapinya. Berbeda dengan negara Singapura, negara tersebut menggunakan sistem *notice and takedown*, sistem tersebut memberikan hak secara langsung terhadap platform yang mengalami serangan

siber untuk dapat menegakkan hukum dan memberikan perlindungan secara langsung terhadap data pribadi masyarakatnya. Dengan adanya perbedaan ini dapat diketahui bahwa pengimplementasian yang dilakukan oleh setiap negara anggota memiliki perbedaan, sehingga membutuhkan waktu yang lebih lama untuk dapat membuat kebijakan mengenai keamanan siber di kawasan ASEAN. Selain itu adanya perbedaan kepentingan dari suatu negara dapat memberikan pengaruh terhadap kebijakan yang nantinya akan di ambil (Kristiani, 2021). Selain masalah Implementasi yang dirasa kurang masih terdapat satu masalah lain dalam perkembangan keamanan siber di kawasan ASEAN yaitu kurangnya pembentukan badan keamanan siber di dalam dewan ASEAN maupun institusional baru yang dapat lebih memfokuskan terhadap keamanan siber di kawasan ASEAN. Namun institusional yang baru juga harus memiliki maintence dan pengawasan yang baik karena kawasan ASEAN hanya melakukan sebagaian dari kerangka Kerjasama yang telah di setujui. Dengan adanya dampak negatif dalam pengimplementasian kebijakan keamanan siber di kawasan ASEAN menimbulkan keterlambatan dalam penanganan keamanan yeng menyebabkan ketidak merataan implementasi yang dilakukan oleh ASAEN terhadap negara anggota.

Dalam upaya keamanan siber di kawasan Uni Eropa dan ASEAN terdapat Kerjasama lintas batas yang dilakukan seperti adanya Kerjasama kawasan dengan negara lain dalam mengatasi dan meningkatkan kapabilitas keamanan siber di dua kawasan tersebut. Dengan adanya Kerjasama lintas batas ini dapat memberikan ruang bagi negara anggota dan negara mitra untuk dapat melakukan dialog dan Kerjasama yang efektif dalam mengatasi masalah ancaman siber di kawasan tersebut. Dengan adanya Kerjasama lintas batas ini dapat menciptakan lingkungan yang mendukung untuk pertukaran Informasi dan melakukan koordinasi dalam mengatasi masalah secara Bersama. Selain itu adanya Lembaga ENISA memberikan dampak terhadap terkoordinasinya informasi dan bentuk kebijakan yang bersifat sentralisttis (European Union Agency for Cybersecurity., 2022).

Lembaga yang telah dibentuk oleh kedua kawasan tersebut memiliki daya adaptasi yang tinggi hal ini dilakukan untuk dapat memberikan penyesuaian terhadap perubahan ancaman siber yang marak terjadi di dua kawasan tersebut. Adapatasi yang dilakukan juga merupakan salah satu upaya menampung kepentingan dari negara anggota yang memiliki perbedaan dalam mengatasi keamanan siber mereka. Namun perbedaan ini dapat di angkat kedalam forum yang telah dibuat sebelumnya oleh kawasan ASAEN dan Uni Eropa. Sehingga keamanan siber akan terjadi maintence guna memperbaiki kebijakan yang tidak relevan pada saat ini.

Perbandingan upaya keamanan siber di kawasan ASEAN dan Uni Eropa memiliki respon yang serupa dalam mengatasi tantangan keamanan siber yang berkembang setiap waktunya. Kedua kawasan tersebut menyadari bahwa dalam mengatasi masalah yang mengalami perkembembangan membutuhkan Kerjasama lintas batas dan membetuk sebuah institusi sebagai sarana dan fondasi dalam mencapai keamanan siber yang lebih efektif. Langkah yang di lakukan oleh ASEAN dengan membentuk *ASEAN Ministrial Cocference on Cybersecurity* (AMCC) dan adanya partisipasi dalam *ASEAN Regional Forum* (ARF) memperlihatkan bagaimana komitmen untuk menjalin kolaborasi dalam menghadapi ancaman siber. Disisi lain Uni Eropa juga melakukan upaya yang mirip dengan ASEAN guna melawan ancaman siber Melalui pembentukan *European Union Agency for Cybersecurity* sebagai Lembaga sentral dalam memberikan bantuan teknis, penelitian lebih lanjut, dan memfasilitasi pertukaran informasi antara negara anggota. Fokus yang sama dihadapi oleh kedua kawasan tersebut dalam ancaman keamanan siber menimbulkan peningkatan kapasitas keamanan siber dan pembentukan kebijakan yang dilakukan dengan melalui kerjasama sebagai kunci untuk mengatasi masalah yang berkembang dengan cepat. Dengan dibentuknya lembaga di kawasan ASEAN dan Uni Eropa dapat menciptakan sebuah platform baru yang dapat menampung kepentingan dari negara anggota, sehingga dapat terciptanya strategi baru dalam mengatasi keamanan siber pada tingkat nasional maupun regional. Langkah yang dilakukan oleh kedua kawasan tersebut merupakan bentuk dari pentingnya Kerjasama dalam setiap uapaya peneyelesaian masalah ditingkat regional maupun nasional. Selain itu kedua kawasan tersebut menggunakan kebijakan *open door policy* yang menjadikan adanya hubungan timbal balik komunikasi di dalam forum, sehingga dapat terjalin Kerjasama yang saling menguntungkan dan tidak menimbulkan keuntungan di satu sisi saja. Hal ini di perkuat dengan adanya setiap kebijakan keamanan siber membentuk sebuah forum yang nantinya menjadi sebuah fasilitas negara anggota regional dapat mengutarakan kepentingan mereka dalam pemebentukan sebuah kebijakan terutama pada sektor kebijakan keamanan siber di kawasan. Namun forum yang ada harus menjadi penghubung informasi yag baik agar dapat terjalin Kerjasama yang baik antar negara anggota.

Namun dalam proses penetapan isu dari kedua kawasan tersebut terdapat perbedaan yang sangat signifikan. Perbedaan yang terlihat adalah kawasan Uni Eropa yang melakukan pendekatan *top-down* dalam mengidentifikasi isu keaman siber ini sampai dengan kepada system implementasi kebijakan. *System top-down* yang dilakukan adalah dengan melakukan pembahasan mengenai isu global yang dilakukan oleh dewan yang nantinya akan menghasilkan kebijakan dengan mewajibkan untuk di implementasikan di setiap negara anggota. Hal ini

dapat memberikan dampak terhadap negara anggota yang masih belum mampu untuk mengikuti atau mengimplementasikan kebijakan yang telah dibuat tersebut. Berbeda dengan pendekatan yang dilakukan oleh kawasan ASEAN, dalam mengidentifikasi isu kawasan ASEAN menggunakan pendekatan yang *bottom-up*. Pendekatan tersebut lebih mengidentifikasi isu berdasarkan negara-negara anggota yang mengalami sehingga negara anggota memajukan isu tersebut kedalam forum karena di anggap telah memberikan dampak negatif terhadap negara anggota, sehingga dalam mengidentifikasi isu yang muncul harus membutuhkan negara untuk mengusung kedalam forum terlebih dahulu. Dengan adanya negara yang terlebih dahulu harus mengusung maka membutuhkan waktu yang cukup lama dalam menemukan formula kebijakan dan Langkah yang cocok untuk mengatasi isu tersebut. Dengan diketahuinya perbedaan dan persamaan ini di harapkan dapat memberikan tolak ukur dalam membandingkan keamanan siber di kawasan ASEAN dan Uni Eropa.

F. Kesimpulan

Perbandingan upaya keamanan siber di kawasan ASEAN dan Uni Eropa memiliki respon yang serupa dalam mengatasi tantangan keamanan siber yang berkembang setiap waktunya. Kedua kawasan tersebut menyadari bahwa dalam mengatasi masalah yang mengalami perkembembangan membutuhkan Kerjasama lintas batas dan membetuk sebuah institusi sebagai sarana dan fondasi dalam mencapai keamanan siber yang lebih efektif. Langkah yang di lakukan oleh ASEAN dengan membentuk *ASEAN Ministrial Cocference on Cybersecurity* (AMCC) dan adanya partisipasi dalam *ASEAN Regional Forum* (ARF) memperlihatkan bagaimana komitmen untuk menjalin kolaborasi dalam menghadapi ancaman siber. Disisi lain Uni Eropa juga melakukan upaya yang mirip dengan ASEAN guna melawan ancaman siber Melalui pembentukan *European Union Agency for Cybersecurity* sebagai Lembaga sentral dalam memberikan bantuan teknis, penelitian lebih lanjut, dan memfasilitasi pertukaran informasi antara negara anggota. Fokus yang sama dihadapi oleh kedua kawasan tersebut dalam ancaman keamanan siber menimbulkan peningkatan kapasitas keamanan siber dan pembentukan kebijakan yang dilakukan dengan melalui kerjasama sebagai kunci untuk mengatasi masalah yang berkembang dengan cepat. Dengan dibentuknya lembaga di kawasan ASEAN dan Uni Eropa dapat menciptakan sebuah platform baru yang dapat menampung kepentingan dari negara anggota, sehingga dapat terciptanya strategi baru dalam mengatasi keamanan siber pada tingkat nasional maupun regional. Langkah yang dilakukan oleh kedua

kawasan tersebut merupakan bentuk dari pentingnya Kerjasama dalam setiap uapaya peneyelesaian masalah ditingkat regional maupun nasional. Selain itu kedua kawasan tersebut menggunakan kebijakan *open door policy* yang menjadikan adanya hubungan timbal balik komunikasi di dalam forum, sehingga dapat terjalin Kerjasama yang saling menguntungkan dan tidak menimbulkan keuntungan di satu sisi saja. Hal ini di perkuat dengan adanya setiap kebijakan keamanan siber membentuk sebuah forum yang nantinya menjadi sebuah fasilitas negara anggota regional dapat mengutarakan kepentingan mereka dalam pemebentukan sebuah kebijakan terutama pada sektor kebijakan keamanan siber di kawasan. Namun forum yang ada harus menjadi penghubung informasi yag baik agar dapat terjalin Kerjasama yang baik antar negara anggota.

Namun dalam proses penetapan isu dari kedua kawasan tersebut terdapat perbedaan yang sangat signifikan. Perbedaan yang terlihat adalah kawasan Uni Eropa yang melakukan pendekatan *top-down* dalam mengidentifikasi isu keaman siber ini sampai dengan kepada system implementasi kebijakan. *System top-down* yang dilakukan adalah dengan melakukan pembahasan mengenai isu global yang dilakukan oleh dewan yang nantinya akan menghasilkan kebijakan dengan mewajibkan untuk di implementasikan di setiap negara anggota. Hal ini dapat memberikan dampak terhadap negara anggota yang masih belum mampu untuk mengikuti atau mengimplementasikan kebijakan yang telah dibuat tersebut. Berbeda dengan pendekatan yang dilakukan oleh kawasan ASEAN, dalam mengidentifikasi isu kawasan ASEAN menggunakan pendekatan yang *bottom-up*. Pendekatan tersebut lebih mengidentifikasi isu berdasarkan negara-negara anggota yang mengalami sehingga negara anggota memajukan isu tersebut kedalam forum karena di anggap telah memberikan dampak negatif terhadap negara anggota, sehingga dalam mengidentifikasi isu yang muncul harus membutuhkan negara untuk mengusung kedalam forum terlebih dahulu. Dengan adanya negara yang terlebih dahulu harus mengusung maka membutuhkan waktu yang cukup lama dalam menemukan formula kebijakan dan Langkah yang cocok untuk mengatasi isu tersebut. Dengan diketahuinya perbedaan dan persamaan ini di harapkan dapat memberikan tolak ukur dalam membandingkan keamanan siber di kawasan ASEAN dan Uni Eropa

Daftar Pustaka

Buku

Doering, P. D. (2013). *LIBERALISME Penyunting Detmar Doering*. 97. https://rowlandpasaribu.files.wordpress.com/2013/09/detmar-doering-ed-liberalisme.pdf

Mohtar Mas'oed. (1994). *Ilmu hubungan international: disiplin dan metodologi*. PT Pustaka LP3ES.

Syafrida, S. hafi. (2021). *Metodologi Penelitian*.

Jurnal

Adi Kusuma. (2022). *EFEKTIVITAS PROGRAM KERJA SAMA UNAIDS-INDONESIA MELALUI SOSIALISASI TANYA MARLO TERHADAP PEMAHAMAN STATUS HIV/AIDS PADA POPULASI KUNCI DI DKI JAKARTA*.

Anshori, M. F., & Ramadhan, R. A. (2019). Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week. *Padjadjaran Journal of International Relations*, *1*(1), 39. https://doi.org/10.24198/padjir.v1i1.21591

Ardiansyah, M. D. (2014). *KERJASAMA AMERIKA SERIKAT DENGAN UNI EROPA DALAM MENANGANI & MENANGGULANGI CYBERCRIME*. 1–19.

ASEAN Cybersecurity Cooperation Strategy. (2021). https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Asiyah, S. (2019). ASEAN sebagai Organisasi Kawasan Regional Asia Tenggara dan Liberalisme Institusional. *Research Gate*, *June*, 1–5.

Balakrishnan, S., & Forsyth, A. (2019). Qualitative methods. In *The Routledge Handbook of International Planning Education*. https://doi.org/10.4324/9781315661063-13

BSSN. (2023). *BSSN Sebagai Focal Point Indonesia Turut Rumuskan Dokumen Keamanan Siber Tingkat ASEAN Pada the 14th Meeting of Asean Network Security Action Council (ANSAC)*.

Chang, L. Y. C. (2017). Comparative Criminology in Asia. *Comparative Criminology in Asia*, *May*. https://doi.org/10.1007/978-3-319-54942-2

Chen, X., & Yang, Y. (2022). Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. *International Spectator*, *57*(3), 48–65. https://doi.org/10.1080/03932729.2022.2066841

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and

Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Dugis, V. (2018). *Teori Hubungan Internasional ; Perspektif-Perspektif Klasik* (Issue December 2016).

Estiyovionita, K., & Sitamala, A. (2022). ASEAN's ROLE IN CYBERSECURITY MAINTENANCE AND SECURITY STRATEGY THROUGH AN INTERNATIONAL SECURITY APPROACH. *Lampung Journal of International Law*, *4*(2), 81–90. https://doi.org/10.25041/lajil.v4i2.2556

European Parliament and the Council of the European Union. (2022). NIS 2 Directive. *Official Journal of the European Union*, *2022*(November), 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union Agency for Cybersecurity. (2022). *Cyber Europe 2022 : after action report : findings from a PAN-EUROPEAN cyber crisis exercise. December*. https://doi.org/10.2824/385167

Fathma Ilmi Anindita Iskandar. (2020). *Diplomasi siber: kebijakan Jepang dalam mendukung pengembangan kapasitas (capacity building) keamanan siber negara ASEAN = Cyber diplomacy: Japan`s policy to support cybersecurity capacity-building in ASEAN countries*.

Febiola, D. (2018). *PERANAN COMPASSION EAST INDONESIA MELALUI CHILD SPONSORSHIP PROGRAMME DALAM PENGENTASAN KEMISKINAN ANAK DI INDONESIA (Studi Kasus Kecamatan Pontianak Utara*. 1–20.

Goals, A. S. D. (2020). ASEAN Sustainable Development Goals Indicators Baseline Report 2020 The ASEAN Secretariat Jakarta. In *Asean*. www.aseanstats.org

Kementrian Pertahanan Republik Indonesia. (2014). Pedoman Pertahanan Siber. *Pedoman Pertahanan Siber*, *5*, 1–74.

Kovács, L. (2018). Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Academy Review*, *23*(1), 16–24. https://doi.org/10.2478/raft-2018-0002

Kristiani, V. (2021). *Kristiani Virgi Kusuma Putri Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime 543*. https://jhlg.rewangrencang.com/

Kundang K Juman. (n.d.). *Modul Perkuliahan Teknologi Digital Pertemuan sesi 2*.

Luzern, H. (2017). Cyber Security Cyber Security. *CRC Press*, *March*, 69–79. http://dx.doi.org/10.1007/978-981-10-8536-9_8

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law and Security Review*, *35*(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

Nurainina, D. R. (2018). Pendekatan Command Control dalam Kebijakan Pencegahan Penyalahgunaan Narkoba (Studi tentang Implementasi Peraturan Walikota Surabaya Nomor 65 Tahun 2014 Pada Kalangan Pelajar di Kota Surabaya). *Fakultas Ilmu Sosial Dan Ilmu Politik, Universitas Airlangga*, 5–6. http://repository.unair.ac.id/74508/3/JURNAL_Fis.AN.33 18 Nur p.pdf

Phuong, N. T., Agung, A., & Perwita, B. (2021). ASEAN-REPUBLIC OF KOREA DIGITAL PARTNERSHIP : THE IMPERATIVES OF TRANS-REGIONAL COOPERATION IN CONTROLLING COVID-19 Anthony Setiawan Hartono , School of International Relations , President University Corresponding Author : aabanyu.perwita@gmail.com. *Journal of InternatIonal Studies*, *17*, 101–129.

Rahmadiani, A., Mantovani, A. P. K., Hariz, S. U., Haryanto, J., & Aidad, F. F. (2019). Strategi Keamanan Siber Indonesia Rekomendasi Rencana Aksi Dan Implementasi. *Center for Digital Society*, *1*(69), 5–24.

Ramadhan, I. (2022). *ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia*. https://doi.org/10.4108/eai.31-3-2022.2320684

Sekar, M., & Purwani, F. (2023). *Analisis Peran dan Penanggulangan Kejahatan Siber : Studi Kasus Spearphishing*. *1*(1), 33–45.

Siagian, L., Budiarto, A., Strategi, P., Udara, P., & Pertahanan, U. (2017). *Peran keamanan siber dalam mengatasi konten negatif guna mewujudkan ketahanan informasi nasional the role of cyber security in overcome negative contents to realize national information resilience*. 1–18.

Sudibyo, A. (2020). Perlindungan Data Pengguna Internet: Menelaah GDPR Uni Eropa. *Anggota Dewan Pers*, 174–198. https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114454-7688.pdf

Tay, K. L. (2023). ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework. In *The International Institute or Strategic Studies*.

Triwahyuni, D., & Wulandari, T. A. (2016). *JIPSi*. *VI*(1).

Vendius, T. T. (2022). Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene. In *European Journal of Policing Studies* (Vol. 3, Issue 2).

https://doi.org/10.5553/ejps/2034760x2015003002005

Vu, C. (2016). *Policy Report CYBER SECURITY IN SINGAPORE*. *December*.

Yudha, B., Manopo, W., Apriani, D., & Sari, A. (2015). ASEAN REGIONAL FORUM: REALIZING REGIONAL CYBER SECURITY IN ASEAN REGION. In *Belli ac Pacis* (Vol. 1, Issue 1).

Laporan

ENISA. (2022). ENISA Threat Landscape 2022. In *European Union Agency for Cybersecurity* (Issue November). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Commission. (2023). *The EU Cybersecurity Act*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

NCSC. (2018). *NIS Directive Cyber Assessment Framework V2.0*.