



**Universitas Katolik Parahyangan Fakultas Ilmu Sosial dan
Ilmu Politik**

Program Studi Ilmu Hubungan Internasional

Terakreditasi A

SK BAN –PT NO: 3095/SK/BAN-PT/Akred/S/VIII/2019

**Kebijakan Pemerintah Indonesia dalam Keamanan Siber Nasional
Tahun 2017-2020: Upaya Penanganan Kasus Night Fury Interpol.**

Skripsi

Diajukan untuk Ujian Sidang Jenjang Sarjana Program Studi Ilmu

Hubungan Internasional

Oleh

Joshua Cahyo Putra Djami

2017330125

Bandung

2021



**Universitas Katolik Parahyangan Fakultas Ilmu Sosial dan
Ilmu Politik
Program Studi Ilmu Hubungan Internasional**

Terakreditasi A

SK BAN –PT NO: 3095/SK/BAN-PT/Akred/S/VIII/2019

**Kebijakan Pemerintah Indonesia dalam Keamanan Siber
Nasional Tahun 2017-2020:
Upaya Penanganan Kasus Night Fury Interpol.**

Skripsi

Diajukan untuk Ujian Sidang Jenjang Sarjana Program Studi Ilmu
Hubungan Internasional

Oleh

Joshua Cahyo Putra Djami
2017330125

Pembimbing

Sapta Dwikardana, Ph. D.

Bandung
2021

Fakultas Ilmu Sosial dan Ilmu Politik
Jurusan Hubungan Internasional
Program Studi Ilmu Hubungan Internasional



Tanda Pengesahan Skripsi

Nama : Joshua Cahyo Putra Djami
Nomor Pokok : 2017330125
Judul : Kebijakan Pemerintah Indonesia dalam Keamanan Siber Nasional Tahun 2017-2020: Upaya Penanganan Kasus Night Fury Interpol.

Telah diuji dalam Ujian Sidang jenjang Sarjana
Pada Rabu, 27 Januari 2021
Dan dinyatakan **LULUS**

Tim Penguji

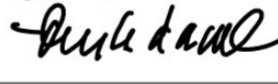
Ketua sidang merangkap anggota

Mireille Marcia Karman, M.Litt.

: 

Sekretaris

Sapta Dwikardana, Ph.D.

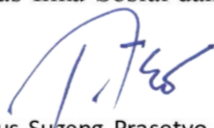
: 

Anggota

Dr. Atom Ginting Munthe

: 

Mengesahkan,
Dekan Fakultas Ilmu Sosial dan Ilmu Politik


Dr. Pius Sugeng Prasetyo, M.Si

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

Program Studi Ilmu Hubungan Internasional



Tanda Persetujuan Skripsi

Nama : Joshua Cahyo Putra Djami
Nomor Pokok : 2017330125
Judul : Kebijakan Pemerintah Indonesia dalam Keamanan Siber
Nasiona tahun 2017-2021: Upaya Penanganan Kasus *Night
Fury* Interpol .

Menyetujui untuk
diajukan pada Ujian
Sidang jenjang Sarjana
Bandung, 25 Januari
2021

Pembimbing,

Sapta Dwikardana, Ph.D.

Mengetahui
Ketua Program Studi Ilmu Hubungan Internasional

Ratih Indraswari, S.IP., M.A.

LEMBAR PERNYATAAN

Nama : Joshua Cahyo Putra Djami
NPM : 2017330125
Jurusan / Program Studi : Ilmu Hubungan Internasional
Judul : Kebijakan Pemerintah Indonesia dalam Keamanan Siber Nasional Tahun 2017-2020: Upaya Penanganan Kasus *Night Fury* Interpol.

Dengan ini menyatakan bahwa rancangan penelitian ini merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain. Adapun karya atau pendapat pihak lain yang dikutip, ditulis sesuai dengan kaidah penulisan ilmiah yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila kemudian hari diketahui bahwa pernyataan ini tidak benar.

Bandung, 12 Januari 2021



Joshua Cahyo Putra Djami

ABSTRAK

Nama : Joshua Cahyo Putra Djami
NPM : 2017330125
Judul : Kebijakan Pemerintah Indonesia dalam Keamanan Siber Nasional Tahun 2017-2020: Upaya Penanganan Kasus *Night Fury* Interpol

Perkembangan Teknologi dan Informasi di Indonesia telah meningkatkan efisiensi penyelenggaraan urusan negara baik di sektor politik, ekonomi, sosial dan lain-lain. Salah satu inovasi yang sudah diimplementasikan di Indonesia adalah implementasi konsep *Big Data* dalam transaksi ekonomi. Fenomena ini memunculkan ancaman-ancaman keamanan siber yang berasal dari luar dan dalam batasan negara. Penelitian ini membahas bagaimana upaya kerja sama sebagai bentuk upaya penanganan serangan siber Internasional dinamai kasus *Night Fury* antara Interpol dan Indonesia mempengaruhi kebijakan keamanan siber masyarakat Indonesia dalam skala nasional. Pergeseran fokus kebijakan pemerintahan Indonesia terhadap Keamanan Siber di Indonesia mendorong untuk dibentuknya kerja sama Interpol dan POLRI untuk bekerja sama melalui Direktorat Tindak Pidana Siber (Dittipidsiber). Untuk menganalisis kebijakan pemerintahan Indonesia terkait keamanan siber, *Copenhagen School* akan digunakan dalam penelitian ini sebagai *grand theory* dengan memberikan fokus utama terhadap isu keamanan non-tradisional melalui teori sekuritisasi, dan menggunakan konsep arena organisasi internasional sebagai teori pendukung untuk menganalisis kerusakan dari kasus ini terhadap kebijakan keamanan siber. Dalam penelitian ini, ditemukan bahwa adanya kegagalan kerja sama Interpol dan POLRI untuk memitigasi dampak kerusakan dari kasus *Night Fury*. Penelitian ini akan berusaha untuk menemukan pengaruh penanganan kasus tersebut terhadap metode pengembangan kebijakan keamanan siber nasional di Indonesia dan berkontribusi terhadap diskusi metode pendekatan terbaik terkait keamanan siber.

Kata Kunci: Sekuritisasi, *Big Data*, Interpol, Keamanan Siber, Kasus *Night Fury*, Kerja sama Internasional, Skimming, Web-Skimming.

ABSTRACT

Name : Joshua Cahyo Putra Djami
NPM : 2017330125
Title : Indonesian Government Policy on National Cybersecurity in 2017-2020:
Interpol Cooperative Efforts in Handling Night Fury Case.

The development of technology and information in Indonesia has increased the efficiency of the administration of state affairs in the political, economic, social and other sectors. One of the innovations that have been implemented in Indonesia is the implementation of the Big Data concept in economic transactions. The phenomenon of security and security threats originating from outside and within state boundaries. This study discusses how to work together as a form of international disaster management efforts called the Night Fury case between Interpol and Indonesia which affects the management of Indonesian society on a national scale. The shift in the focus of the Indonesian government's policy towards Cybersecurity in Indonesia encourages the formation of cooperation between Interpol and POLRI to work together through the Directorate of Cyber Crime (Dittipidsiber). To analyze Indonesian government policies related to system security, the Copenhagen School will be used in this study as a large theory by giving a main focus on non-traditional issues through securitization theory, and using the concept of the international organization arena as a supporting theory to analyze the damage from this case to cybersecurity policy. In this study, it was found that there was a failure in cooperation between Interpol and POLRI to mitigate the impact of the damage from the Night Fury case. This research will attempt to find the implications of the case's efforts in handling cyber security towards Indonesia's cyber security policies development and contributes to the discussion of the most optimal way to approach cyber security.

Keywords: Securitization, Big Data, Cybersecurity, Interpol International Cooperation, Night Fury Case, Skimming, Web-Skimming.

KATA PENGANTAR

Puji syukur dan terima kasih penulis panjatkan kepada Tuhan Yang Maha Esa. Atas berkat, rahmat dan perlindunganNya, penulis dapat melewati proses dan menyelesaikan penelitian ini dengan baik dan tepat waktu. Penelitian ini membahas mengenai Pengaruh Ancaman Siber terhadap Kebijakan Keamanan Siber Nasional melalui Kasus *Night Fury* Interpol dalam bentuk kerja sama pada tahun 2017 hingga tahun 2019. Temuan-temuan dalam penelitian ini diharapkan dapat menjadi penjelas atas pengaruh kerja sama sebagai penanganan kasus ancaman baru dalam pengembangan kebijakan keamanan siber. Namun, penulis menyadari bahwa penelitian ini belum sempurna dan masih membutuhkan perbaikan. Maka, terkait dengan penelitian ini, penulis menyambut dengan baik segala kritik dan saran/masukan yang bersifat membangun. Namun, dibalik segala kekurangan penelitian ini, penulis berharap agar penelitian ini dapat bermanfaat bagi banyak pihak.

Terimakasih yang ingin saya sampaikan ditujukan kepada Tuhan Yesus Kristus, karena kasih karunia-Nya seluruh penulisan ini tidak akan terjadi dan terlaksana. Saya mengucapkan teima kasih kepada seluruh anggota keluarga saya, terutama keluarga inti saya. Kepada Ayah saya Bapak David Djami dan Ibu saya Alice Risma Tambunan Djami, yang sudah memberikan dukungan dan semangat terhadap segala upaya studi saya. Saya juga hendak mengucapkan terima kasih kepada kakak dan adik saya, Jessica Serah Djami dan Jeovanca Livni Djami. Tanpa

dukungan dan kata-kata motivasi yang diberikan oleh kedua saudara saya, saya tidak akan mampu menyelesaikan skripsi ini. Saya juga hendak berterimakasih kepada dosen pembimbing saya, Mas Sapta Dwikardana yang sudah mau membimbing dan mengarahkan karya tulis skripsi ini. Saya juga mengucapkan seluruh anggota jurusan Hubungan Internasional Universitas Katolik Parahyangan selaku almamater saya yang telah menjadi tempat saya menuntut ilmu selama 3,5 tahun. Saya mengucapkan terima kasih kepada segala kolega-kolega saya di Jurusan Hubungan Internasional Universitas Katolik Parahyangan.

Saya juga hendak berterima kasih kepada sesama mahasiswa Hubungan Internasional: Ramandika Pudji Prakoso, Iqmal Sunny Saputra, Nur Muhammad Sulthan, Jonathan Prasetyo, dan Alex Wibisono selaku individual yang selalu membantu saya dalam perkuliahan dan mendukung saya dalam menyusun karya tulis ini. Saya juga ingin mengucapkan terima kasih kepada Claudia Karin, Sabila Elsa Cerelia, Audrey Dea Azzahra, Vanessa Phoebe, Tazkhia Kimi, dan Inelya Zeafira yang sudah membantu saya dalam menyusun skripsi dan memberikan bantuan panduan alur sidang skripsi saya. Saya juga mengucapkan terima kasih kepada kakak-kakak tingkat yang membantu saya di masa perkuliahan, Alm. Aghiya Khrisna Nugraha, Santi Rebecca, dan Carol Wetik yang sudah membantu membimbing saya. Penulis juga berterima kasih kepada seluruh teman-teman alumni SMA Regina Pacis penulis yang berkuliah di Universitas Katolik Parahyangan yang sudah membantu dan mendukung saya dalam proses pelaksanaan kuliah dan skripsi ini. Penulis juga hendak mengucapkan terima kasih kepada Interpol sebagai organisasi internasional

dimana penulis pernah menjadi pegawai magang dan mendapatkan informasi yang dibutuhkan untuk melengkapi skripsi ini.

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	xi
DAFTAR AKRONIM	xiii
BAB I	1
PENDAHULUAN	1
1.1 LATAR BELAKANG MASALAH	1
1.2. IDENTIFIKASI MASALAH	11
1.2.1. Deskripsi Masalah	11
1.2.2. Pembatasan Masalah	13
1.2.3. Perumusan Masalah	14
1.3 TUJUAN DAN KEGUNAAN PENELITIAN	15
1.3.1. Tujuan Penelitian.....	15
1.3.2. Kegunaan Penelitian	16
1.4 KAJIAN LITERATUR	16
1.5 KERANGKA PEMIKIRAN	26
1.6. TEKNIK PENGUMPULAN DATA	30
1.6.1. Metode Penelitian	30
1.6.2 Teknik Pengumpulan Data	32
1.7 SISTEMATIKA PEMBAHASAN	32
BAB II	35
KERJA SAMA TERKAIT KEBIJAKAN KEAMANAN SIBER INDONESIA- INTERPOL	35
2.1 INTERPOL SEBAGAI AKTOR INTERNASIONAL DI INDONESIA	36
2.1.1 Profil Organisasi Interpol di Indonesia	36
2.1.2 Peran Organisasi Interpol dalam upaya Pemeliharaan Keamanan di Indonesia	41

2.2 KEBIJAKAN DAN PERJANJIAN LUAR NEGERI TERKAIT KEAMANAN SIBER DI INDONESIA.....	48
2.2.1 Pemeliharaan Keamanan Siber berdasarkan Kebijakan Pemerintah Indonesia	48
2.2.2 Respon terhadap Ancaman Siber Indonesia berdasarkan UU dan Perjanjian Luar Negeri	52
2.3 KERJA SAMA AKTOR INTERNASIONAL DAN PERANNYA DALAM KEAMANAN SIBER NASIONAL	56
2.3.1 ASEAN <i>Cyber-Desk</i> , Interpol, Tipidsiber dan Sektor Pribadi : Kerja sama Internasional Indonesia.	56
2.3.2 Kesesuaian Peran Interpol di Kasus <i>Night Fury</i> dengan Undang-Undang Keamanan Siber di Indonesia:	59
BAB 3.....	64
SEKURITISASI INTERPOL DALAM MENANGANI KASUS NIGHT FURY INTERPOL	64
3.1 KASUS NIGHT FURY INTERPOL: ANCAMAN INTERNASIONAL TERHADAP KEAMANAN NASIONAL INDONESIA	68
3.1.1 Kronologi dan Modus Operandi <i>Magecart</i> : Kejahatan di Ruang Terbuka	68
3.1.2 Analisis Kerusakan dan Korban Kejahatan Siber.....	74
3.1.3 Mitigasi dan Penanggulangan Kerugian Tindak Kejahatan Pelaku Kasus <i>Night Fury</i> Interpol.....	78
3.2 IMPLEMENTASI TEORI SEKURITISASI: KEBIJAKAN KEAMANAN SIBER DI KASUS NIGHT FURY INTERPOL.....	79
3.2.1 Analisis Upaya Penanganan Kasus <i>Night Fury</i> Interpol melalui Sekuritisasi	79
3.2.2 Kegagalan Respon Kasus <i>Night Fury</i> dalam proses Sekuritisasi	84
3.2.3 Pengaruh Proses Sekuritisasi untuk PengembanganKeamanan Siber Nasional	88
BAB IV	95
KESIMPULAN	95
DAFTAR PUSTAKA	99

DAFTAR AKRONIM

ASEAN	<i>Association of South East Asian Nations</i>
ATM	<i>Automated Teller Machine</i>
BSSN	Badan Siber dan Sandi Nasional
CPU	<i>Central Processing Unit</i>
Ditpid Siber	Direktorat Tindak Pidana Siber
Divhubinter	Divisi Hubungan Internasional
ICPO-Interpol	<i>The International Criminal Police Organization</i>
IPTEK	Ilmu Pengetahuan Teknologi
ISP	<i>Internet Service Provider</i>
JS-Sniffer	<i>Java Script Sniffer</i>
MLA	<i>Mutual Legal Assistance</i>
POLRI	Kepolisian Republik Indonesia
PBB	Perserikatan Bangsa-Bangsa
TIK	Teknologi Informasi dan Komunikasi
NCB	<i>National Crime Bureau</i>
USD	<i>United States Dollar</i>
UU	Undang Undang
SGD	<i>Singapore Dollar</i>

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Integrasi internet ke dalam kehidupan masyarakat umum sudah dilakukan secara otomatis dan dilakukan dengan tingkat kecepatan yang tinggi, menyebabkan pengumpulan dan perkembangan data menjadi hal yang cepat untuk dilakukan. Berangkat dari fenomena tersebut, maka munculah konsep *Big Data*.¹ *Big Data* adalah data yang terdiri dari variasi informasi yang lebih luas dan hadir dalam volume yang meningkat dan dengan kemampuan memproses informasi dengan kecepatan yang semakin tinggi. Dilengkapi dengan volume dan kecepatan yang meningkat, konsep ini menjelaskan sebuah ruang besar dan luas yang terdiri dari data yang berkembang dalam suatu sumber yang dapat diakses oleh pihak tertentu. Pengembangan TIK (Teknologi Informasi dan Komunikasi) yang dinamakan *Big Data* adalah akumulasi aset informasi bervolume luas, berkecepatan tinggi, dan memiliki berbagai macam variasi yang membutuhkan bentuk pemrosesan informasi inovatif yang hemat biaya yang memungkinkan peningkatan wawasan, pengambilan keputusan, dan otomatisasi proses pengambilan keputusan.²

¹Sistem Aplikasi Satuan Kerja. "Big Data: Apa Itu Dan Mengapa Itu Penting." Sas.com, 2020.

² Andrews, Evan. "Who Invented the Internet?" HISTORY. HISTORY, Desember 18, 2013. <https://www.history.com/news/who-invented-the-internet>.

Hal ini merupakan teknologi yang berkembang dari adanya integrasi internet dalam kehidupan sehari-hari secara perlahan-lahan. Inovasi ini memiliki ciri-ciri yang melekat pada implementasinya. *Big Data* pada umumnya memiliki bentuk akumulasi data yang cepat, volume data yang luas, memiliki jangkauan bervariasi, memiliki nilai atau berharga dan terverifikasi sebagai informasi yang valid. Dari kelima ciri karakteristik ini, TIK seketika mampu menjadi perangkat yang mempermudah pihak pemerintah dan perusahaan-perusahaan berbasis *Big Data* untuk menggunakan akumulasi data ini agar dapat digunakan untuk meningkatkan performa layanan yang telah mereka sediakan. Dari segala ciri-ciri karakteristik perkembangan TIK ini, yang menjadi kunci bagi kelima karakteristik ini adalah penggunaannya dalam kehidupan masyarakat Indonesia. Apabila suatu layanan dilengkapi dengan beberapa ciri tersebut namun tidak digunakan untuk meningkatkan 'otomatisasi' dari sebuah sistem yang digunakan dalam suatu proses, maka akumulasi data tersebut tidak dapat dikategorikan sebagai layanan TIK. Maka tidak semua pihak modern dapat dikatakan sebagai perusahaan yang menggunakan *Big Data*.

Perusahaan *Big Data* adalah perusahaan yang menggunakan sistem dari akumulasi data sebagai layanan utama untuk menjalankan fungsi tertentu.³ Negara-negara di dunia; termasuk Indonesia, sudah mulai menyadari bahwa perkembangan industri secara perlahan mulai terintegrasi dalam media digital dalam bentuk data-data. Data-data ini kemudian dikumpulkan dan disusun sedemikian rupa untuk

³ Oracle Administrator. "What Is Big Data? |Oracle." Oracle.com, 2020. <https://www.oracle.com/big-data/what-is-big-data.html>.

membentuk rangkaian informasi mengenai individu-individu yang menggunakan internet yang menjadi suatu sumber yang dapat menyimpan data-data tersebut. Data ini dikumpulkan secara otomatis apabila seseorang mendaftarkan dirinya untuk menggunakan suatu jenis layanan yang disediakan oleh baik pihak pemerintahan maupun pihak layanan pribadi. *Big Data* sudah diimplementasikan dalam berbagai jenis layanan di Indonesia. Indonesia sudah mulai membuka akses kepada berbagai jenis layanan yang berbasis dengan TIK. Implementasi ini datang dalam berbagai aspek dan tidak terlihat semata-mata sebagai perangkat yang digunakan pihak-pihak dan bahkan dampak dari *Big Data* sudah diadopsi dalam penyelenggaraan aktivitas pemerintahan dan hal-hal yang bersangkutan dengan kepentingan negara yang dijalankan baik di dalam maupun diluar Indonesia.⁴ Kedua pihak yang terkena dampak dari TIK sebagai suatu inovasi juga mengalami ancaman bahaya yang datang dari kejahatan yang dapat difasilitasi dengan kehadiran teknologi tersebut. Sebelum membahas dampak yang diberikan oleh penggunaan TIK, definisi tetap harus diberikan untuk menjaga konsistensi makna dari topik pembahasan yang dianalisa dalam makalah ini. Dalam pelaksanaan kegiatan suatu layanan yang berasal baik dari sebuah perusahaan maupun suatu instansi pemerintah, pihak penyelenggara berurusan dengan dinamika kehidupan masyarakat transnasional.⁵

⁴ Gang Hoon Kim, Silviana Trimi, and Ji Hyong Chung, "Big Data Applications in the Government Sector: A Comparative Analysis among Leading Countries," 2014, Electronics and Telecommunications Research Institute. Diakses 12 Oktober 2020.

⁵ Ibid.

Sebelum memahami makna dari ancaman transnasional terhadap masyarakat nasional, tahap awal memahami istilah tersebut adalah untuk memahami definisi yang tetap dari konsep ancaman 'Transnasional' harus dipahami terlebih dahulu.⁶ Transnasionalisme dalam konteks definisi makna katanya memiliki makna yang merujuk kepada aktor pelaksana kegiatan ekonomi internasional sudah tidak terbatas oleh perbatasan atau area tertentu. Namun dalam konteks hubungan internasional, transnasionalisme adalah objek penelitian sosial ilmiah dan fenomena sosial yang berasal dari interkonektivitas yang meningkat antara orang-orang yang semakin tumbuh dan berkembang setelah munculnya keberadaan internet dan signifikansi peran ekonomi dan sosial terlepas dari batas-batas wilayah antara negara-negara.⁷ Dengan kata lain, dapat dikatakan bahwa peningkatan signifikansi aktor-aktor non-negara sebagai pemeran hubungan internasional merupakan esensial dalam isu-isu transnasional dalam ruang pembahasan hubungan internasional. Berangkat dari pemahaman tersebut, maka dapat dikatakan bahwa masyarakat transnasional datang dari hadirnya internet sebagai fasilitas umum yang digunakan sehari-hari.

Masyarakat transnasional memiliki ciri utama yang ditekankan pada makalah ini yaitu interkonektivitas yang melampaui masyarakat yang sebelumnya tidak memiliki internet. Masyarakat transnasional meliputi berbagai macam kalangan yang menggunakan internet hanya sebagai alat rekreasi, perangkat asistensi yang

⁶ Vertovec, Steven. 'Transnationalism and Identity'. *Journal of Ethnic and Migration Studies*. 2001 pp. 27.

⁷ Graham, Pamela. 'Reimagining the Nation and Defining the District: Dominican Migration and Transnational Politics'. *Caribbean Circuits: New Directions in the Study of Caribbean Migration*, Center for Migration Studies: Patricia Pessar. 1997 pp 5-11.

digunakan untuk mempermudah manusia di abad ke-21 menjalankan fungsi-fungsi rumit dan disederhanakan, atau bahkan menjadi tonggak untuk berbagai macam sistem yang diandalkan oleh instansi besar; bahkan di level pemerintahan. Ragam demografis yang terdiri dari berbagai representasi kalangan ini menjadi objek utama dalam mengamati fenomena perkembangan teknologi. Fenomena ini, walaupun dialami oleh berbagai macam kalangan, namun memberikan sebuah dampak yang terbagi secara merata kepada para pengguna maupun para objek yang dijadikan data yang terdapat di dalam instansi-instansi yang menggunakan inovasi interkoneksi tersebut, yaitu risiko yang dihadapi oleh berbagai macam kalangan ini dan bahaya yang mengikuti inovasi ini.⁸

Walaupun dalam suatu perkembangan dalam skala apapun, inovasi selalu memiliki dampak positif, namun bukan berarti dampak positif tersebut tidak disertai dengan risiko dan bahkan dengan dampak negatif.⁹ Banyak bagian dari masyarakat yang tidak mengerti tentang dampak-dampak yang mengikuti inovasi dan kegunaannya yang sekilas terlihat begitu aman untuk digunakan. Masyarakat Transnasional yang semakin memiliki akses mudah untuk menggunakan layanan-layanan berskala multinasional yang disediakan oleh pihak-pihak tertentu. Terjadi banyak peristiwa yang merupakan dampak dari kehadiran TIK sebagai jembatan yang mendukung interkoneksi masyarakat modern. Ancaman-ancaman keamanan non-

⁸ Ibid.

⁹ Klaus Peter Schulz, "The Nature of Innovation and Implications on Innovation Management," Department of Innovation Research and Sustainable Resource Management, Chemnitz University of Technology, Germany. Diakses pada September 2021.

tradisional mulai bermunculan dengan adanya TIK. Hal tersebut menyebabkan masyarakat transnasional menyebabkan para pengguna layanan TIK menjadi semakin apatis terhadap ancaman-ancaman dan tidak lagi mencoba untuk mengedepankan literasi layanan berbasis TIK. yang dapat merugikan mereka. Ketidaksadaran masyarakat menjadi faktor pertimbangan bagi pihak-pihak yang memiliki tujuan kriminal untuk dijadikan sasaran korban kejahatan. Kejahatan-kejahatan yang dimaksud adalah kejahatan seperti *skimming* dan pencurian akses data pribadi.. Kejahatan-kejahatan ini biasanya dilakukan oleh pihak pelaku yang sudah mengetahui kebiasaan dan memantau aktivitas korban terlebih dahulu agar mampu untuk menjamin korban dapat dirugikan. Ini merupakan contoh dari bahayanya inovasi tersebut.¹⁰

Skimming adalah kejahatan yang sering terjadi melalui fasilitas yang diadakan oleh TIK, *Skimming* adalah pencurian informasi pribadi yang pernah digunakan dalam transaksi normal. Pencuri dapat memperoleh nomor kartu korban menggunakan metode dasar seperti fotokopi tanda terima atau metode yang lebih canggih seperti menggunakan perangkat elektronik kecil (*skimmer*) untuk menggesek dan menyimpan ratusan nomor kartu korban. Ini merupakan sedikit dari berbagai macam ancaman yang muncul akibat kurangnya pemahaman masyarakat transnasional terhadap layanan yang mereka gunakan sehari-hari. Makalah ini bertujuan untuk menganalisa bagaimana Internet memberikan paparan dan akses bagi individu yang belum memiliki pengetahuan dan pembekalan yang tepat untuk

¹⁰ Ibid.

menghadapi kemajuan teknologi yang telah terintegrasi dalam kehidupan secara tepat. Kasus-kasus ini terjadi di ruang yang tidak memiliki batasan atau regulasi absolut berdasarkan region tertentu. Interaksi antar individu/kelompok dapat dilakukan tanpa menghiraukan ruang dan jarak yang harus ditempuh. Kemudahan akses dapat dianggap sebagai masa depan dari pelaksanaan kegiatan hubungan internasional, begitu pula dengan ancaman yang mengikutinya. Hal ini menunjukkan perubahan bentuk interaksi masyarakat global berdasarkan media yang digunakan. Dengan keberadaan *Big Data* sebagai sebuah fasilitas, maka para penyedia layanan berbasis data *online* menggunakan *Big Data* sebagai dasar dari layanan yang disediakan. Para pengguna memberikan informasi atau data yang dimasukkan kedalam internet dan terakumulasi menjadi *Big Data* sebagai Maha data. Akumulasi informasi tersebut kemudian diakumulasi dan diproses melalui serangkaian sistem. Sistem ini dirancang oleh penyedia layanan untuk menjalankan suatu fungsi berdasarkan data yang didapatkan dari *Big Data*.¹¹ Dengan mengumpulkan dan memproses data melalui sebuah sistem otomatis, maka para penyedia layanan memiliki akses terhadap berbagai macam informasi –baik informasi pribadi maupun informasi umum. Informasi tersebut akan bertambah lengkap dan dapat diasosiasikan dengan sumber tertentu yang kelak akan membentuk sebuah identitas virtual. Profil individu menjadi semakin lekat dengan informasi mengenai seorang individu, bukan mengenai individu tersebut secara fisik. Hal ini memudahkan interaksi antar aktor

¹¹ Big Data & Privacy: What's Really Going on With Your Personal Information?
By Mae Rice Container: Built In Year: 2019 URL: <https://builtin.com/big-data/big-data-privacy>
diakses pada 1 Februari 2020.

internasional untuk menjadi semakin intrapersonal. Tiga aspek sekuritisasi yang akan diimplementasikan dalam penelitian ini adalah badan politik (negara), penonton (masyarakat), dan konteks (keamanan siber). Dalam menganalisis menggunakan sekuritisasi, diperlukan adanya kehadiran dari *Speech Act*. *Speech Act* merupakan komponen yang diadopsi dari ilmu kebahasaan dimana praktik dari menyatakan sebuah informasi atau mosi dapat menggerakkan atau mempengaruhi adanya sebuah tindakan. Bagaimana aktor badan politik memberikan pernyataan mengenai sebuah isu yang dianggap sebagai isu keamanan adalah kualifikasi untuk sebuah isu dapat memulai sekuritisasi. Bagaimana masyarakat memberikan respon dan konteks yang mengikuti isu spesifik tersebut dapat dianggap sebagai proses sekuritisasi.

Penelitian ini akan membahas mengenai bagaimana negara melakukan perkembangan siber dan kerja sama organisasi internasional yang menyertainya sebagai sebuah aspek yang menjadi faktor penentu pengambilan kebijakan terkait dengan keamanan siber atau *cyber security* di Indonesia. *Cyber security* di Indonesia berarti keamanan informasi yang diaplikasikan dan dipraktikkan kepada komputer dan jaringannya yang selalu disesuaikan/berubah dengan perkembangan teknologi informasi.¹² Dengan mengenalkan Indonesia dengan sebuah medium dimana mobilitas informasi dapat diakses dengan mudah, secara langsung informasi-informasi yang bersifat esensial dan krusial akan menjadi semakin rawan untuk

¹² CISCO, "Anatomy of an Attack," Cisco, November 2020.

diakses oleh pihak-pihak yang tidak berkepentingan.¹³ Disini letak kecemasan dari pihak penyusun kebijakan. Dengan memberikan ‘ruangan’ bagi aktor hubungan internasional seperti negara, organisasi internasional, dan perusahaan-perusahaan multi-nasional untuk saling berinteraksi pada medium yang sulit untuk dipantau dan dikendalikan oleh hukum dan/atau kebijakan tertentu. Klaus Kultti, Tuomas Takalo and Juuso Toikka, tiga penulis akademis yang merupakan spesialis dalam bidang inovasi, temuan, dan hak paten menyatakan bahwa sifat inovasi tidak dapat diimplementasikan secara menyeluruh dan merata tanpa adanya pengawasan.¹⁴ Prinsip ini dapat tercermin dari literasi internet yang belum merata. ‘Keamanan adalah sebuah isu penting’ merupakan pernyataan yang masih harus didasari dengan sebuah teori untuk meyakinkan beberapa kelompok demografis yang tidak memiliki literasi teknologi yang cukup.¹⁵

Teori yang akan digunakan pada karya tulis ini adalah teori sekuritisasi atau ‘*securitization theory*’ yang merupakan teori turunan dari *Copenhagen School* sebagai *grand theory* yang lahir sebagai *synthesis* dari argument antara teori konstruktivisme dan teori realisme klasik dalam hubungan internasional. Teori ini akan dibahas secara ekstensif dan akan diaplikasikan pada isu kasus *Night Fury Interpol* pada bagian kajian literatur. Dengan memahami definisi, dampak, aspek krusial, fungsi dan ancaman dari dunia siber, maka penelitian ini dapat memulai

¹³ Inside Job/Restaurant card skimming. Journal Register. 2015.
<https://www.theguardian.com/money/2015/aug/14/scammers-target-middle-age-women> diakses pada 20 Maret 2020

¹⁴ Klaus Kultti, Tuomas Takalo, and Juuso Toikka, “Secrecy versus Patenting,” *The RAND Journal of Economics* 38, no. 1 (March 2007): 22–42, <https://doi.org/10.1111/j.1756-2171.2007.tb00042.x>.

¹⁵ Ibid.

untuk menjabarkan pandangan dan indikator yang diadopsi oleh pemerintahan Indonesia di tahun 2020 terhadap isu ancaman dan Keamanan Siber Nasional berdasarkan penanganan kasus *Night Fury* Interpol.¹⁶ Selain dari *Copenhagen School* dan teori sekuritisasi yang menyertainya, skripsi ini juga akan menginkorporasikan karya tulis *Cyber Security in East Asia: Governing Anarchy* - Nicholas Thomas untuk menjelaskan keamanan siber di Asia Timur dan ASEAN, dan bagaimana penanganan dan perjanjian internasional yang berlaku di kawasan Asia Tenggara sudah melaksanakan sekuritisasi terhadap isu keamanan siber.

Kasus yang dibahas dalam penelitian ini adalah kasus *Night Fury*. Nama *Night Fury* dipopulerisasikan dari seri film *How to Train Your Dragon* dimana salah satu karakter film tersebut; seekor naga bernama *Toothless*; merupakan bagian dari spesies fiksi naga berjenis '*Night Fury*'.¹⁷ Penekanan yang diberikan oleh karya film ini adalah karakteristik dari naga tersebut yang bergerak cepat dan hampir tidak dapat terdeteksi. Layaknya ancaman yang lahir melalui kejahatan siber dalam kasus ini, senjata yang digunakan berupa *virus malware* memiliki karakteristik yang sama. Karakteristik yang dimiliki oleh virus ini sulit untuk dideteksi secara umum dan diperlukan sumber daya dan kemampuan khusus untuk melacak asal dan keberadaan pengguna nya. Nama ini tidak hanya memudahkan para personel yang bekerja di Divhubinter POLRI – Interpol untuk menjalankan tugasnya.

¹⁶ Muller, J. Indonesia: social network penetration Q3 2019, 20 Februari 2019. <https://www.statista.com/statistics/284437/indonesia-social-network-penetration/> Diakses 25 Februari 2020.

¹⁷ "How to Train Your Dragon (2010)". Box Office Mojo. IMDb. Diakses tanggal December 18, 2010.

1.2. IDENTIFIKASI MASALAH

1.2.1. Deskripsi Masalah

Kemajuan teknologi yang sudah dialami oleh sebagian besar porsi masyarakat menyebabkan kesenjangan dalam literasi mengenai internet beserta dengan regulasi-regulasinya. Internet bukanlah komponen yang baru dalam menjalankan fungsi atau aktivitas sehari-hari. Berdasarkan latar belakang masalah yang sudah dipaparkan, ada beberapa aspek yang menyebabkan ketidakseimbangan dalam pengetahuan mengenai internet. Hal ini disebabkan oleh berlimpahnya tingkat inovasi yang bergerak lebih cepat daripada kemampuan beberapa orang untuk beradaptasi dengan kemajuan-kemajuan tersebut. Sudah dijelaskan bahwa dunia siber dapat lahir karena kapasitas kemampuan komputer untuk menghimpun data secara otomatis. Data-data ini kemudian digunakan sebagai dasar dari bagaimana konten-konten yang disediakan oleh layanan-layanan yang disuguhkan kepada masyarakat Indonesia. Walaupun data-data ini diberikan oleh para pengguna layanan secara sukarela, tidak semua pengguna layanan-layanan berbasis informatika mengerti bahaya dari memberikan data tersebut secara cuma-cuma. Kurangnya pemahaman data yang diberikan, bagaimana data tersebut digunakan, dan risiko yang mengikutinya. Masyarakat transnasional sudah didefinisikan sebagai bagian dari masyarakat dunia yang sudah mampu beraktivitas lintas batas tanpa harus dibatasi dan dibatasi oleh batas-batas antar-negara.

Penelitian ini menganalisis bagaimana masyarakat transnasional di Indonesia mampu beradaptasi terhadap perubahan tersebut. Indonesia merupakan salah satu

negara yang memiliki fasilitas terhadap internet sebagai dampak globalisasi. Indonesia mulai menjadi negara yang dimana pelaksanaan kegiatan negaranya didampingi oleh keberadaan internet sebagai suatu sumber daya. Namun lebih daripada itu, Indonesia sudah mulai mengadopsi pola hidup dari masyarakat dunia revolusi industri 4.0. Maka masyarakat dunia mulai berporos melalui dunia siber sebagai tumpuan dalam menjalankan kehidupan sehari-hari. Internet telah memberikan masyarakat dunia sebuah kesempatan untuk menjadi salah satu alat yang menyelesaikan berbagai macam keluhan dan masalah. Internet mempermudah masyarakat dunia untuk membangun jaringan dan kerjasama antar pihak-pihak di dunia yang sebelumnya dianggap mustahil untuk dilaksanakan. Namun setelah mendapatkan beberapa solusi, muncul kontras dari kegunaan jawaban yang tidak sepadan dengan lahirnya permasalahan yang baru. Masalah ini mencakup keberadaan perangkat TIK yang menjadikan kehidupan masyarakat Indonesia dalam berinteraksi secara transnasional dan ikut berkembang. Perkembangan ini di analisis dalam ranah hubungan internasional. Maka dalam pembahasannya, latar politik mendapatkan peran esensial dalam mengidentifikasi masalah keseimbangan untung dan rugi yang menyertai keberadaan revolusi industri 4.0 tersebut seperti yang sudah dipaparkan dalam paragraf sebelumnya. Maka permasalahan ini akan membahas berdasarkan relevansi perkembangan masalah berdasarkan perkembangan konfliknya dan analisa peristiwa yang dapat ditangani dan diamati.

Keamanan siber sebagai sebuah *existential threat* mulai dianggap secara internasional dalam kawasan Asia Tenggara mulai terlihat melalui representasi

Konvensi pertemuan bersama APEC / ASEAN yang membahas mengenai kejahatan dunia maya, yang mengarah pada kerja sama antara *Council of Europe* dan Filipina serta permintaan akses selanjutnya dari negara bagian itu.¹⁸ Indonesia juga mulai meninjau dan merevisi undang-undang kejahatan dunia maya. Berangkat dari pemahaman tersebut dapat dilihat bahwa Indonesia sudah menganggap isu keamanan siber sebagai isu yang memiliki signifikansi untuk dibahas dalam ruang diskusi politik. Namun absensi dari urgensi keamanan siber untuk dikembangkan menyebabkan keamanan siber kembali berada di belakang skala prioritas Indonesia. Namun kasus ini merupakan salah satu dari faktor yang dapat dianggap sebagai *emergency situations* dan kerja sama dengan organisasi internasional, sektor pribadi, dan metode pelacakan dengan sumber daya yang dimiliki oleh pihak-pihak tersebut dapat dianggap sebagai *extraordinary measures*.

1.2.2. Pembatasan Masalah

Pembatasan masalah dalam penulisan ini mencakup lingkup waktu dari tahun 2017 hingga tahun 2020. Pembatasan waktu tersebut disusun berdasarkan pertimbangan tingkat kejahatan perkembangan siber yang pesat dalam kurun waktu tersebut dan kurangnya kajian mengenai literasi masyarakat transnasional yang lemah proporsinya apabila dibandingkan dengan perkembangan tersebut. Kontras dari perkembangan ini memojokkan ruang lingkup penelitian kedalam poros yang dapat

¹⁸ Council of Europe. "Project on Cybercrime: Progress Report," November 30, 2007. Available at <http://www.coe.int> diakses pada 5 Maret, 2008.

diamati dari tahun 2017 hingga 2020. Pembatasan masalah dari 2017-2020 dipilih oleh penulis karena topik yang dibahas pada penelitian ini sangat bergantung pada contoh kasus. Kasus yang dimaksudkan; *Night Fury*, dilaporkan dan diinvestigasi semenjak tahun 2017. Investigasi tersebut berjalan hingga pada tahap penanganan selama 3 tahun hingga awal tahun 2020. Sedangkan topik yang dibahas pada penelitian ini adalah pengaruh penanganan kasus tersebut terhadap topik keamanan siber nasional. Peneliti menemukan bahwa pengaruh tersebut memiliki ekstensi pengaruh hingga tahun 2020. Pembatasan topik dipagari oleh teori sekuritisasi sebagai pembatas argumen, level nasional sebagai tolak ukur ancaman internasional dalam pembahasan kebijakan Indonesia terkait ancaman siber, dan pengaruh dari sisi teori besar *Copenhagen School* sebagai pembatasan pembahasan hubungan internasional. Penelitian ini tidak akan membahas kasus pelanggaran pada level konstitusional/hukum secara spesifik, namun hanya akan memberikan gambaran mengenai dasar kerja sama, upaya penanganan pelanggaran hukum, dan implementasi kebijakan nasional terhadap ancaman internasional. Penelitian ini juga tidak akan membahas bagaimana cara kerja virus dan teknis sistem informatika secara mendalam, namun akan menyinggung tentang bagaimana virus bisa menjadi ancaman internasional.

1.2.3. Perumusan Masalah

Berdasarkan paparan yang sudah diberikan pada poin 1.2.2 permasalahan dari pembahasan karya tulis ini menjadi semakin terkerucut kedalam beberapa komponen

yang menjadi bagian esensial dalam menyelesaikan kontras yang terjadi dalam ranah hubungan internasional. Perumusan masalah pada karya penulisan ini dipaparkan sebagai berikut:

Bagaimana Pengaruh Upaya Kerjasama Penanganan Kasus *Night Fury* Interpol terhadap Keamanan Siber Nasional Masyarakat Indonesia?

Maka dengan pertimbangan tersebut, dapat disimpulkan bahwa masa terbaik untuk memaparkan permasalahan ini adalah waktu dan perspektif yang dapat dianalisa dari tahun 2017-2020 dengan teliti berdasarkan metode penelitian penulisan yang akan dipaparkan secara lebih mendetail dalam bagian metode penelitian.

1.3 TUJUAN DAN KEGUNAAN PENELITIAN

1.3.1. Tujuan Penelitian

Tujuan dari penelitian ini berangkat dari keinginan peneliti untuk menganalisa secara lebih lanjut bagaimana dampak perkembangan Teknologi Informasi dan Komunikasi dapat mempengaruhi perkembangan kebijakan keamanan nasional. Kebijakan Pemerintah Indonesia mengenai keamanan siber sebagai fokus yang mendasar dalam penelitian ini mempunyai implikasi yang tidak memiliki definisi konsensus secara internasional. Dalam lingkungan yang semakin memiliki akses terhadap perangkat internet sebagai alat guna sehari-hari dan ancaman siber muncul sebagai isu keamanan baru dengan kemampuan ancaman di tingkat lintas-batas wilayah negara. Tujuan dari penelitian ini adalah untuk menjawab rumusan masalah:

‘Bagaimana Pengaruh Upaya Kerjasama Penanganan Kasus Night Fury Interpol terhadap Keamanan Siber Nasional Masyarakat Indonesia?’ secara komprehensif.

1.3.2. Kegunaan Penelitian

Kegunaan dari penelitian ini merujuk kepada bagaimana perkembangan teknologi membuat pemahaman tentang risiko layanan siber mampu menyakiti maupun membantu para penggunanya. Perkembangan teknologi ini juga membawa risiko ancaman nasional. Bentuk kriminalitas seperti skimmer web merupakan kejahatan yang menjadi ancaman masyarakat Indonesia terkait kurangnya pemahaman saat ini tentang apa yang dimaksud dengan keamanan. Penerapan definisi baru keamanan ini tidak sepenuhnya tanpa kekurangan. Analisis terhadap kerjasama Indonesia dengan Interpol untuk mengambil langkah identifikasi masalah dan membagikan pandangan yang relevan terkait dengan metode penggunaan, keamanan, situs web layanan berbasis data yang berpotensi terancam infeksi virus terhadap tindak kriminal. Hal ini dapat menjadi kontribusi studi HI untuk semakin membangun pengetahuan tentang ancaman siber.

1.4 KAJIAN LITERATUR

Kajian dari sumber literatur utama yang digunakan oleh penulis dalam penelitian ini akan terbagi ke dalam topik yang mendukung argumen bahwa metode kerja sama lintas sektor pribadi, organisasi internasional, dan negara (sebagai aktor utama) merupakan metode yang perlu dikembangkan lebih daripada menunggu

sebuah konsensus internasional. Dengan menggunakan sekuritisasi sebagai pilar utama, dan komponen aktor, audiens, dan konsep sebagai tiga aspek penelitian, kajian literatur akan membagi argumen ke dalam dua sisi. Pertama menyediakan argumen bahwa negara adalah aktor yang harus bertanggung jawab penuh terhadap keamanan siber nasional, memberikan ruang untuk kerja sama namun tidak secara inklusif. Kedua, menyatakan bahwa kerja sama diluar pihak negara merupakan metode yang perlu dilaksanakan, dengan mengutamakan kawasan regional sebagai penyedia sumber daya optimum. Kajian yang akan mendukung kedua argumen diatas adalah sebagai berikut:

Bersamaan dengan mengadopsi pandangan bahwa karya tulis ini akan memfokuskan pembahasan isu utamanya sebagai isu keamanan atau *security*, maka karya tulis ini akan menelaah isu perkembangan kebijakan keamanan siber nasional melalui teori sekuritisasi/*securitization*. Teori ini merupakan produk yang hadir dari konsep keamanan dari paradigma ‘*Copenhagen School*’ oleh Barry Buzan, Ole Wæver and Jaap de Wilde. Maka karya tulis ini merujuk kepada konsep terkandung dalam buku ‘*SECURITY: A New Framework for Analysis*’ oleh Barry Buzan, Ole Wæver and Jaap de Wilde yang menjelaskan bahwa keamanan berdasarkan ‘*Copenhagen School*’ memiliki tiga pilar utama diantaranya: non-politis; memandang sebuah isu hanya sebagai *existential threat*, politis; dan *extraordinary measures* dan tersekuritisasi; disaat sudah melewati proses.¹⁹ Tiga pilar ini akan menjadi pembagian utama dalam membedah kasus keamanan non-tradisional dalam karya tulis ini.

¹⁹ Buzan, B., Wæver & de Wilde. SECURITY: A New Framework for Analysis. 1998.

Namun literatur ini memberikan pengertian mengenai sekuritisasi namun tidak memberikan nuansa pada peran organisasi internasional dengan sektor pribadi sebagai preferensi dalam menjalankan isu tersebut. Tulisan ini menekankan peran negara dan bagaimana interaksi politik berperan dalam sistem anarki negara tetap menjadi pemeran utama. Literatur ini mendukung peran negara namun tidak mendukung argumen bagaimana negara harus menggunakan perannya sebagai aktor internasional.

Sementara proses 'globalisasi' terus meningkat, respons global sepenuhnya terhadap masalah keamanan di era siber muncul dan upaya untuk mengamankan dunia siber dapat dianggap memiliki karakteristik reaktif daripada proaktif. Perkembangan dalam mengatur 'ruang siber' yang sangat penting dalam menangani kejahatan dunia siber adalah fokus dari makalah ini dan menguraikan yang telah dicapai masyarakat internasional sejauh ini. Mengontrol kejahatan yang melibatkan teknologi digital dan jaringan komputer juga memerlukan berbagai jaringan baru: jaringan antara polisi dan lembaga-lembaga lain dalam pemerintahan, jaringan antara polisi dan lembaga-lembaga swasta, dan jaringan penegak hukum lintas batas negara. Dalam menganalisa perkembangan implementasi sekuritas/keamanan lintas negara, tidak hanya dibutuhkan pemahaman mengenai sekuritisasi berdasarkan '*Copenhagen School*', namun perlu juga dipahami contoh implikasi dan impartasi teori tersebut dalam analisis yang secara lebih mendalam dan terstruktur. Maka dari itu karya tulis ini akan merujuk:

'Security in Translation Securitization Theory and the Localization of Threat', Holger Stritzel School of International Relations, University of St Andrews.²⁰ Buku ini membahas kerja sama internasional dalam sekuritisasi sebagai salah satu metode yang dapat digunakan untuk memulai proses sekuritisasi itu sendiri. Namun tidak menekankan poin bahwa harus ada pembagian regime dari aktor-aktor yang terlibat. Buku ini membahas tentang bagaimana interdependensi kompleks dalam upaya penanganan isu keamanan dan dampak terhadap proses sekuritisasi. Penelitian ini akan membahas isu kejahatan transnasional akibat adanya perkembangan TIK yang semakin dominan dalam aspek politik, sosial dan ekonomi masyarakat Indonesia.

Maka penelitian ini akan menggunakan literatur yang mengangkat topik yang menyangkut dengan penyediaan keamanan masyarakat transnasional dalam penggunaannya untuk menentukan resiko dan dampak yang sesuai dalam penggunaan dunia siber dalam aspek Teknologi Informasi dan Komunikasi adalah *'The Role of Cyber Security in World Politics. V.T. Tsakanyan Peoples' Friendship University of Russia, dari Moscow, Russia'*. Artikel dalam jurnal ini menjelaskan bahwa dampak kemajuan internet dan media telah meningkatkan kemajuan dari aktivitas kejahatan transnasional.²¹ Literatur ini meletakkan keamanan siber sebagai isu utama dan implikasinya dalam dunia politik internasional. Pembahasan ini membukakan ruang bagi pihak-pihak yang mampu untuk mengambil peran dalam sekuritisasi isu keamanan siber. Dengan memberikan fokus kepada peran negara dalam politik dunia,

²⁰ Putnam, Tonya L & David D. Elliott. *International Responses to Cyber Crime*, 2019.

²¹ Vladimir Tsakanyan, *THE ROLE OF CYBERSECURITY IN WORLD POLITICS*. V.T. Tsakanyan Peoples' Friendship University of Russia (RUDN University), Moscow, 2017.

jurnal ini menekankan argumen bahwa pendekatan global/internasional merupakan metode yang dianggap paling optimum.

Selain dari itu terdapat juga jurnal dari *International Responses to Cyber Crime* karya Tonya L. Putnam, David D. Elliott. Jurnal ini menjelaskan bahwa ada korelasi antara kemajuan dan perkembangan literasi internet dengan kemampuan untuk menjaga dan menyelesaikan isu keamanan negara.²² Kelompok negara-negara yang memiliki, atau akan segera memiliki, undang-undang yang secara khusus ditujukan untuk kejahatan cyber termasuk negara-negara yang paling maju, yang, sebagai suatu peraturan, juga merupakan negara yang paling tergantung pada komputer dan jaringan interkoneksi.²³ Literatur yang sesuai untuk membahas pandangan tersebut adalah Artikel Jurnal Ilmu Hukum Brawijaya terkait Persetujuan Kerjasama Transnasional *Vol. 3 Issue Number 2, Contemporary Indigenous and Constitutional Issues Transnational Organised Crime in Indonesia – The Need for International Cooperation*. Seiring dengan perkembangan teknologi dan fenomena tak terbatas di era globalisasi, kejahatan transnasional terorganisir telah muncul. Peningkatan pesat kejahatan terorganisir transnasional di kawasan Asia Tenggara selama beberapa tahun terakhir telah mendorong tindakan oleh negara-negara yang bertindak secara domestik melalui undang-undang dan kebijakan, serta internasional melalui kerjasama bilateral dan multilateral. Kejahatan yang telah secara khusus dibahas dalam esai ini adalah perdagangan manusia, terorisme, dan pembajakan. Setiap

²² Ibid.

²³ Wanja Eric Naef. "A Proposal for an International Convention on Cyber Crime and Terrorism." Iwar.org.uk, 2021. <http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm>.

masalah dalam artikel ini telah diperiksa secara individual, dengan garis besar awal sifat kejahatan, diikuti dengan analisis pendekatan domestik dan internasional khusus untuk memeranginya.²⁴ Literatur ini menyatakan bahwa kerja sama internasional merupakan metode yang terbaik, namun mendukung argumen bahwa pendekatan regional di area aktor dapat menjadikan sistem kerja sama internasional menjadi semakin efisien.

Dikatakan bahwa kontrol efektif kejahatan transnasional terorganisir membutuhkan lebih dari masing-masing Negara yang bekerja secara individu untuk melindungi kepentingan mereka sendiri. Kerjasama internasional antara negara-negara yang melibatkan strategi yang koheren dan konsisten yang disesuaikan dengan sifat kejahatan sangat penting jika kejahatan transnasional terorganisir harus ditangani secara efektif di Asia Tenggara. Buku yang menjadi bahasan yang sesuai dalam konteks ini adalah *Developments in the Global (international) Law Enforcement of Cyber-Crime*, Roderic Broadhurst, Queensland University of Technology, 2006. Perluasan konektivitas komputer yang cepat telah memberikan peluang bagi para pelaku kejahatan siber atau *cyber crime* untuk mengeksploitasi kerentanan keamanan di lingkungan online. Fenomena ini menjadi fokus utama yang dibahas dalam artikel di jurnal ini. Mayoritas aksi kejahatan ini adalah kode berbahaya yang mampu mengeksploitasi dan mengganggu operasi komputer pada skala global dan bersama dengan kejahatan siber lainnya mengancam *e-commerce* – *e-commerce* yang

²⁴ Policing: An International Journal of Police Strategies and Management 29(2): pp. 408-433. Law Enforcement of Cyber-Crime, Roderic Broadhurst, Queensland University of Technology, 2006.

menggunakan TIK.²⁵ Sementara proses integrasi internet terus meningkat, respons global sepenuhnya terhadap masalah keamanan di era digital belum muncul dan upaya untuk mengamankan dunia siber telah reaktif daripada proaktif. Perkembangan dalam pemolisian transnasional 'ruang siber' yang sangat penting dalam menangani kejahatan dunia siber adalah fokus dari makalah ini dan menguraikan prestasi yang telah dicapai masyarakat internasional sejauh ini.²⁶

Salah satu pandangan yang akan berperan secara esensial dalam pembahasan *Big Data* dan dampaknya dalam konflik antar negara adalah pandangan yang dituangkan oleh Charles J. Dunlap Jr dalam artikel jurnal: “*The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict,*” *Georgetown Journal of International Affairs* 15, *International Engagement on Cyber IV* (2014).²⁷ Merupakan pedoman dari karya tulis ini yang menjadi acuan utama dari karya tulis ini dalam menjabarkan bahaya *Big Data* apabila disalahgunakan dan dampak-dampak yang berdekatan dengan perang. Bahaya dari bagaimana kontribusi Perkembangan TIK merupakan salah satu pilar yang dibedah dalam pembahasan spektrum dampak positif dan negatif. Dampak ini menjalar kepada berbagai aspek dalam argumen karya tulis ini. Dunlap akan menjadi salah satu kiblat yang akan digunakan dalam argumen mengenai dampak *Big Data* yang mendatangkan ancaman baru. Dunlap adalah seorang penulis buku, artikel, dan mayor jenderal di kemiliteran

²⁵ Ibid.

²⁶ *Developments in the Global (International) Law Enforcement of Cyber-Crime*, Roderic Broadhurst, Queensland University of Technology, 2006. Open Paper, pp 1-5.

²⁷ “*The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict,*” *Georgetown Journal of International Affairs* 15, *International Engagement on Cyber IV*, 2014.

Angkatan Udara Amerika Serikat (*United States' Air Force*). Dunlap memberikan argumen bahwa akan ada perubahan dalam pencitraan konflik antar-negara dalam ruang dunia siber dan ambiguitas batasan.²⁸ Hal ini disebabkan oleh Perkembangan TIK sebagai variabel yang berkontribusi terhadap perubahan skala penanganan konflik. Artikel jurnal ini menjelaskan bahwa dengan adanya sebuah sistem yang mengakumulasi data secara otomatis dan meletakkannya dalam satu tempat yang dapat diakses dengan protokol yang benar, maka *Cybersecurity* dapat memetakan pihak yang berperan pada konflik secara implisit tanpa diwajibkan adanya naungan negara dan aparat pemerintahan sebagai batasan pelindung yang bertanggung jawab atas rakyatnya secara absolut.²⁹ Oleh sebab itu, *Securitization Theory: How Security Problems Emerge and Dissolve* akan digunakan sebagai salah satu contoh pihak yang aktif berperan dalam aktivitas dan isu ancaman tradisional negara, namun ikut mengedepankan isu keamanan siber sebagai prioritas yang perlu diperhatikan negara. Kedua jurnal diatas menekankan bahwa peran negara adalah peran yang utama dan dengan menyerahkan otoritas penuh kepada negara, pengembangan keamanan siber sudah dapat diakomodasi.

Namun, selain dari memahami bahwa integrasi masyarakat ke dalam dunia digital, salah satu aktor yang ikut berperan aktif dalam perkembangan isu keamanan non-tradisional adalah Organisasi Internasional. Organisasi Internasional merupakan

²⁸ Dunlap, C. Jr, *Technology and the 21st Century Battlefield: Recomplicating Moral Life for the Statesman and Soldier*, 1999. Pp 24-25.

²⁹ Balzacq, Thierry. *Securitization Theory: How Security Problems Emerge and Dissolve*. Augustus 2010.

aktor yang ikut berperan dalam mengatasi permasalahan dan ancaman yang merupakan implikasi ancaman siber. Organisasi Internasional memiliki fungsi-fungsi yang dapat membantu negara sebagai aktor tradisional untuk mengatasi ancaman-ancaman non-tradisional tersebut. Untuk menghadapi ancaman yang bersifat transnasional, maka dibutuhkan fasilitas/lembaga yang mempunyai kapasitas dan mobilitas yang dianggap mampu untuk menghadapi masalah tersebut. Organisasi internasional terbagi menjadi tiga fungsi utama, diantaranya: aktor, instrument dan arena. Maka buku yang akan digunakan untuk membantu argumen terkait dengan peran Interpol adalah *Clive Archer - International Organizations 3rd Edition, London 1983*. Buku ini menjelaskan peran yang dapat diambil oleh organisasi internasional antar pemerintah dalam pelaksanaan fungsi dan tugas-tugas negara. Buku ini digunakan sebagai acuan untuk memandang peran organisasi internasional dalam upaya pemeliharaan keamanan nasional dan keamanan siber secara spesifik.³⁰ Nuansa yang perlu ditambahkan dalam pembahasan ini adalah ‘*Cyber Security in East Asia: Governing Anarchy*’ karya Nicholas Thomas.³¹ Literatur ini menambahkan pandangan mengenai isu keamanan siber dan bagaimana isu tersebut mengalami sekuritisasi di Asia secara khusus. Dengan mempertimbangkan bagaimana negara-negara dan aktor-aktor non-negara di Asia (seperti ASEANAPOL dan APEC) beroperasi, literatur ini mempertimbangkan mengenai bagaimana Indonesia dianggap

³⁰ Archer, Clive, *International Organizations* Third edition, 2001 by Routledge 11 New Fetter Lane, London EC4P 4EE.

³¹ Nicholas Thomas, “Cyber Security in East Asia: Governing Anarchy,” *Asian Security* 5, no. 1 (January 30, 2009): 3–23,

dalam indeks pengukuran literasi keamanan siber. Literatur ini menyatakan bahwa Indonesia dapat dianggap memiliki kemampuan keamanan siber yang maju secara kapasitas kawasan.³² Literatur ini juga menekankan bahwa adanya urgensi dalam kerja sama negara dengan organisasi internasional dan sektor pribadi yang memiliki kapasitas untuk berkontribusi dalam perwujudan keamanan siber. Namun dalam meneliti keamanan siber di Asia, harus dipertimbangkan juga bagaimana perkembangan yang sudah terjadi dalam dunia internasional melalui organisasi seperti Perserikatan Bangsa-Bangsa. Hal ini merupakan upaya penyesuaian keamanan siber yang perlu diperhatikan baik secara *regional* maupun *global*.

Berdasarkan rangkaian kajian literatur diatas, terdapat dua segmentasi mengenai bagaimana pendekatan keamanan siber harus dipraktikkan oleh negara. Pertama, argumen bahwa negara adalah aktor yang bertanggung jawab penuh dalam pelaksanaan dan pemeliharaan keamanan siber di dasari oleh kedaulatan. Kedua, adalah negara tetap menjadi aktor utama, namun harus disertai dengan bantuan sektor-sektor pribadi dan organisasi internasional karena keterbatasan kapasitas negara. Penulis mengambil perspektif yang kedua, akibat adanya kasus ini sudah menjadi bukti bahwa negara secara tunggal tidak mampu mengakomodasi keamanan siber nasional. Menunggu untuk adanya konsensus internasional akan mengakibatkan kerugian yang berlipat kali ganda, dan hal ini dapat dihindari apabila negara memutuskan untuk mengerahkan sumber daya baik dari pihak luar maupun dalam, untuk menangani kasus *skimming* yang sudah terjadi dalam kasus *Night Fury*.

³² Ibid, 15.

1.5 KERANGKA PEMIKIRAN

Penelitian ini dimulai dengan gagasan bahwa Indonesia sudah mulai mengarahkan fokusnya kepada keamanan siber nasional masyarakat Indonesia. Fokus ini tidak hanya dengan cara mengakomodasi aspirasi masyarakat secara domestik. Pemerintah Indonesia mulai membentuk hubungan kerja sama internasional dalam bentuk program dan hubungan multilateral dengan berbagai metode meliputi kerjasama bilateral dan menuju kepada organisasi internasional.³³ Indonesia sebagai aktor utama sudah menjalankan peran dalam menegakkan hukum demi melindungi keamanan rakyat. Masalah keamanan nasional merupakan isu yang menjadi prioritas bagi tiap negara. Banyak peran dari berbagai macam aktor sudah mulai berkontribusi terhadap hubungan kerja sama keamanan siber antar negara, baik secara bilateral maupun multilateral. Studi ini berbicara mengenai hubungan yang bersifat saling ketergantungan dalam lingkungan politik regional dan dunia internasional.³⁴ Iklim hubungan internasional berskala regional dapat dikaitkan kepada bentuk-bentuk kebijakan yang telah dibentuk dalam region tersebut. Kebijakan dirancang untuk menyesuaikan dengan kebutuhan dan agenda yang dimiliki oleh negara-negara anggota yang ada dalam region tersebut.³⁵ Telah dinyatakan bahwa ada hubungan sebab akibat antara tingkat saling ketergantungan dan penggunaan aspek tindakan politik dalam penelitian ini, tetapi pengembangan gagasan umum bahwa kebijakan

³³ Kshetri, N., 2016, *Cybersecurity in National Security and International Relations: The Quest to Cyber Superiority*, pp 6.

³⁴ Robert O. Keohane & Joseph S. Nye Jr., Maret 2008, *Power and Interdependence*, pp 158-165.

³⁵ Ibid

kerjasama multilateral yang berkembang dapat menawarkan solusi belum dapat dipercaya masyarakat maupun aktor internasional.³⁶ Solusi untuk situasi yang ditandai dengan persiapan perang bersama dan akhirnya mengarah pada lenyapnya konflik antar provinsi maupun antar negara di kawasan yang sama.

Negara-negara di dunia memiliki berbagai macam karakteristik dan permasalahan rumah tangganya sendiri. Tidak mungkin bagi suatu negara untuk memenuhi kebutuhan rumah tangganya secara utuh tanpa ada bantuan dari negara lain.³⁷ Hal ini disebabkan oleh keterbatasan negara dari berbagai macam faktor seperti sosial, politik dan ekonomi, aset yang berbeda-beda, literasi internet/teknologi, dan kekuatan militer.³⁸ Tujuan dari kerjasama yang akan dipaparkan disini adalah upaya untuk mencapai kedamaian melalui upaya yang beroperasi dalam berbagai macam level untuk menangani permasalahan negara yang bersifat multidimensional untuk mencapai kedamaian. Dengan mempraktekkan kegiatan fungsional hubungan internasional dalam berbagai level, organisasi dapat membantu pemerintah negara untuk mengakomodasi kebutuhan negara yang tidak dapat disampaikan apabila hanya mengandalkan institusi resmi negara. Perdamaian dan kemajuan internasional seringkali menjadi dua tumpuan dari pelaksanaan kerjasama dengan aktor non-negara diutamakan dalam penerapannya. Apabila suatu negara ingin menjaga perdamaian dalam rumah tangga dan dengan negara-negara lainnya, maka yang terbaik adalah

³⁶ Nicholas Thomas, (2009) *Cyber Security in East Asia: Governing Anarchy*, Asian Security, pp 5.

³⁷ Firth, Stewart., *Sovereignty and Independence in the Contemporary Pacific*, The Contemporary Pacific Spring/Fall Edition, pp 2.

³⁸ Ibid

memberikan sebagian dari aset yang dimiliki untuk ditukarkan dengan aset yang tidak dimiliki oleh negara sendiri. Indonesia sebagai sebuah negara yang menyadari keberadaan ancaman yang datang dengan adanya inovasi TIK.

Berangkat dari pemahaman diatas, sekuritisasi akan menjadi pembahasan analisis utama yang akan digunakan dalam makalah ini. Dengan menyadari bahwa komponen utama sekuritisasi adalah *existential threat*, *emergency actions*, dan *effects on interunit relations*, maka harus terlebih dahulu dilihat awal aktor memandang isu ini sebagai ancaman. Berdasarkan teori sekuritisasi buzan, ancaman baru dari makalah ini akan bertumpu pada keberadaan virus sebagai *existential threat* yang akan bersifat semakin relevan dengan keberadaan inovasi yang sudah dijelaskan diatas. Dalam makalah ini, penjelasan ancaman tersebut akan membahas mengenai virus JS-Sniffer yang menjadi senjata yang digunakan para pelaku untuk meretas dan mencuri data kartu kredit para pengguna layanan maupun para penyedia layanan belanja *online*. Selain dari itu, ancaman ini telah direspon oleh beberapa lembaga negara dan aktor dari sektor pribadi yang ikut memandang ancaman siber sebagai isu keamanan terutama pada kasus *Night Fury* ini. Penanganan kasus ini merupakan upaya penanganan melalui kerja sama dengan sektor pribadi dan aktor negara yang bersifat tumpang tindih dan bersifat baru. Dimana Indonesia sudah memiliki badan nasional yang menangani kasus keamanan siber (Badan Siber dan Sandi Nasional), namun kasus ini diberikan kepada Dittipidsiber. Dittipidsiber merupakan Direktorat

Tindak Pidana Siber yang dibentuk atas dasar kerja sama POLRI Divisi Hubungan Internasional dan Interpol.³⁹

Interpol merupakan organisasi internasional bersifat antar pemerintah yang memfasilitasi bantuan dalam menjaga pemeliharaan keamanan nasional dari ancaman-ancaman lintas batas dan internasional.⁴⁰ Hal ini menunjukkan bahwa negara-negara secara global menyadari bahwa adanya keperluan terkait keamanan nasional. Keamanan nasional yang dimaksud merujuk kepada isu keamanan tradisional dan non-tradisional. Penelitian ini akan membahas mengenai bagaimana kasus *Night Fury* Interpol menjadi faktor yang mempengaruhi bagaimana negara Indonesia menentukan prioritas isu keamanan-keamanan sebagaimana adanya faktor waktu, tingkat ancaman, penilaian risiko dan lain-lain. Hal ini diimplementasikan melalui adanya upaya kerja sama. Kerja sama sebagai konsep yang akan dibahas dalam penelitian ini adalah kerja sama Indonesia-Interpol dalam menjaga keamanan nasional. Kerja sama ini diadakan berdasarkan meningkatnya ancaman yang diidentifikasi oleh Indonesia dan Interpol. Penelitian ini akan membahas bagaimana identifikasi tersebut berasal dari perkembangan TIK yang semakin dominan dalam kehidupan masyarakat Indonesia.

Metode penyelesaian isu keamanan siber masih menjadi perdebatan dalam komunitas internasional kawasan Asia Tenggara (ASEAN/ASEAN+3). Karakteristik ancaman yang dihadapi dengan keberadaan ancaman siber adalah karakteristik lintas

³⁹

⁴⁰ "What Is INTERPOL?," Interpol.int, 2017, <https://www.interpol.int/en/Who-we-are/What-is-INTERPOL>. diakses pada 3 Januari 2021.

batas. Tanpa menghiraukan domain maupun wilayah fisik, ancaman siber dapat menyerang data pribadi maupun nasional; data-data yang memiliki sifat sensitif dan berbahaya apabila terkompromisasi dapat menjadi sebuah alat untuk meningkatkan kekuatan politik, sosial, dan ekonomi baik itu merepresentasikan negara maupun diluar negara.⁴¹ Dalam diskusi utama mengenai pendekatan keamanan siber, dikatakan bahwa pendekatan kawasan/*regional* antar negara adalah pendekatan yang paling optimum. Namun beberapa ahli masih mengedepankan urgensi untuk menunggu partisipasi dan keterlibatan organisasi seperti Perserikatan Bangsa Bangsa dalam isu topik keamanan siber. Penelitian ini akan berfokus kepada kasus *Night Fury* sebagai kasus keamanan siber dengan pendekatan regional dan dengan melibatkan sektor pribadi dalam penangannya, untuk menguji apakah pendekatan regional mampu untuk mengakomodasi kebutuhan keamanan siber di Indonesia. BSSN tidak mengambil tindakan melalui kasus ini sebagai sebuah lembaga negara, namun memberikan penanganan kasus ini karena adanya unsur kerja sama internasional. Dampak *interunit* antar lembaga negara pun akan menjadi pokok pembahasan dalam makalah ini.

1.6. TEKNIK PENGUMPULAN DATA

1.6.1. Metode Penelitian

Metode penelitian yang akan digunakan dalam penulisan ini adalah metode penelitian kualitatif. Penulis menggunakan metode penelitian kualitatif dengan

⁴¹ Nicholas Thomas (2009) *Cyber Security in East Asia: Governing Anarchy*, Asian Security, pp 4.

pertimbangan karakteristik yang ditawarkan dalam pemaparan metode penelitian kualitatif mampu menjelaskan data bersifat baik statistik numerik dan non-numerik sesuai dengan konteks dari penelitian yang akan dicapai. Keterlibatan dari data teori juga menjadi pertimbangan yang digunakan oleh penulis untuk menggunakan metode kualitatif sebagai metode pengumpulan data. Maka dapat dianggap bahwa metode kualitatif merupakan metode yang sesuai dalam menganalisis permasalahan yang dipaparkan dalam penulisan ini.⁴² Penelitian kualitatif dapat mencakup banyak hal namun pada esensinya berdasarkan Rabbie; seorang profesor sosiologi dan ahli metode penelitian lulusan *Harvard University*, Penelitian Kualitatif dapat dibagi dalam konteks penelitian lapangan dan penelitian di luar lapangan. Variasi yang ada dapat dikatakan sebagai perbedaan antara kedua sisi spektrum dalam tingkat keterlibatan di lapangan.⁴³ Namun makalah ini akan menggunakan metode penelitian yang bergantung kepada pembelajaran kasus dan analisis penelitian kasus secara ekstensif untuk dapat dijadikan model pembelajaran dalam perihal menangani permasalahan serupa di waktu mendatang sehingga tujuan dari penelitian dapat tercapai secara empiris.⁴⁴ Metode penelitian yang digunakan akan adalah analisis resume kasus, analisis dokumen dan analisis berita yang sudah meliputi mengenai kasus yang dipandang relevan oleh peneliti untuk ditambahkan kepada penulisan makalah ini.

⁴² Earl R. Babbie, *The Practice of Social Research*. 12th ed. Belmont: Wadsworth Cengage, 2010 295-299.

⁴³ *Ibid*, 307-308.

⁴⁴ *Ibid*, 330.

1.6.2 Teknik Pengumpulan Data

Dalam penelitian ini, data akan dikumpulkan dari buku, penelitian yang sudah dapat diakses dan digunakan dalam artikel jurnal, arsip dan laporan resmi, dokumen publik, dan informasi yang dapat didapatkan dari karya tulis majalah dan redaksi daring. Teknik pengumpulan data tidak mengalienasi metode lain yang dapat menyatukan benang merah penelitian ini. Hal ini disebabkan oleh temuan peneliti yang juga turut dibantu dengan pembahasan topik secara impromptu dengan demografis pelajar Indonesia, namun menyertakan informasi tersebut

1.7 SISTEMATIKA PEMBAHASAN

BAB I berisi **Pendahuluan** yang terdiri dari Latar Belakang Masalah, Identifikasi Masalah (Deskripsi Masalah, Identifikasi Masalah, dan Pembatasan Masalah), Tujuan dan Kegunaan Penelitian, Kerangka Pemikiran, Kajian Pustaka, Metode Penelitian, Teknik Pengumpulan Data dan Sistematika Pembahasan. Bab I menjelaskan mengenai teori sekuritisasi dan pendekatan yang dilaksanakan terhadap analisis kasus *Night Fury*.

BAB II akan membahas **Kerja Sama Interpol dengan Indonesia dalam Keamanan Siber Nasional Masyarakat Indonesia**. Bagian ini akan memaparkan bagaimana Interpol berperan dalam upaya menegakkan hukum, UU, konstitusi dan perjanjian yang berlaku tentang Keamanan Siber dan Informatika melalui kerja sama dengan Interpol dan mengkritisi keberadaan Interpol sebagai organisasi internasional yang berada di dalam ruang lingkup domestik dan internasional. Bab ini juga menyampaikan kebijakan keamanan siber nasional untuk pengembangan keamanan siber Indonesia. Secara keseluruhan bab ini bertujuan untuk menentukan kesesuaian Indonesia Interpol sebagai *extraordinary measures* melalui penanganan kerja sama regional-nya.

BAB III akan membahas mengenai **Kasus Night Fury Interpol** yang melibatkan implementasi konsepsi organisasi internasional sebagai teori pendukung, Big Data sebagai konsep penyokong argumen dari hasil analisis, dan sekuritisasi sebagai teori utama dalam menganalisis pengaruh kasus *Night Fury* terhadap kebijakan keamanan nasional Indonesia. Tujuan ini dapat dilaksanakan dengan memaparkan upaya penanganan Indonesia-Interpol, kerugian yang disebabkan oleh kasus tersebut, dan bagaimana proses sekuritisasi sudah diimplementasikan dalam menjaga keamanan siber nasional dalam menangani kasus kejahatan siber serupa dengan *Night Fury*. Bagian ini akan membahas dikotomi baik dan buruknya pandangan mengenai kinerja

Indonesia dengan aktor Internasional, melalui *speech act* dan analisis *extraordinary measure* pemerintah Indonesia dengan Interpol dan IB Group. Bab ini juga berupaya untuk memberikan rekomendasi untuk perkembangan kebijakan keamanan siber Indonesia.

BAB IV akan menyimpulkan **Bagaimana Pengaruh Kasus *Night Fury* Interpol terhadap Keamanan Siber Masyarakat Indonesia** berdasarkan analisis Sekuritisasi. Bagian ini akan menyimpulkan pendekatan optimum melalui penanganan kasus ini sebagai pengaruh utama terhadap pengembangan keamanan siber di Indonesia.