KERJASAMA ASEANAPOL DAN EUROPOL DALAM MENGATASI CREDIT CARD FRAUD (CARDING)

Oleh:

Albet Nego

NPM: 14430018

Skripsi

Disusun dan Diajukan untuk Melengkapi Persyaratan Dalam Memperoleh Gelar Sarjana Ilmu Politik Program Studi Ilmu Hubungan Internasional

PROGRAM STUDI ILMU HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS SLAMET RIYADI

SURAKARTA

2019

PERSETUJUAN

Skripsi ini telah disetujui untuk dipertahankan di hadapan Tim Penguji Skripsi Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Slamet Riyadi Surakarta.

Persetujuan Pembimbing.

Surakarta, 13 Agustus 2019

Pembimbing I	Pembimbing II
Ganjar Widhiyoga, S.IP, M.Si, Ph.D.	Halifa Haqqi, S.IP, M.Si
NIPY. 0109.0251	NIPY. 0109.0252

PENGESAHAN

Skripsi ini telah diuji dan disahkan di hadapan Tim Penguji Skripsi Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Slamet Riyadi Surakarta dan diterima sebagai persyaratan mendapatkan Gelar Sarjana Ilmu Politik.

Hari : Selasa

Tanggal : 13 Agustus 2019

Tim Penguji

Ketua : Ganjar Widhiyoga, S.IP, M.Si, Ph.D. (.....)

Sekretaris : Halifa Haqqi, S.IP, M.Si (.....)

Penguji : Dra. Christy Damayanti, M.Si (.....)

Disahkan oleh

Fakultas Ilmu Sosial dan Ilmu Politik

Universitas Slamet Riyadi Surakarta

Dekan

Drs. Buddy Rivanto, M.Si.

NIPY. 0191.0139

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini, saya:

Nama	: Albet Nego
NPM	: 14430018
Prodi	: Ilmu Hubungan Internasional
Fakultas	: Ilmu Sosial dan Ilmu Politik

Menyatakan bahwa Skripsi yang berjudul:

"KERJASAMA ASEANAPOL DAN EUROPOL DALAM MENGATASI CREDIT CARD FRAUD (CARDING)"

Dengan ini saya menyatakan bahwa Skripsi ini benar-benar pekerjaan saya sendiri dan sepanjang pengetahuan saya tidak berisi materi yang dipublikasikan atau ditulis orang lain atau telah digunakan sebagai persyaratan penyelesaian studi di Perguruan Tinggi lain kecuali pada bagian tertentu yang saya ambil sebagai acuan.

Surakarta, 30 Agustus 2019

Yang Menyatakan

Albet Nego
NPM. 14430018

MOTTO

“ Segala perkara dapat kutanggung bersama DIA yang memberi kekuatan kepadaku“

Filipi 4 : 13

“Takut akan TUHAN adalah permulaan pengetahuan, tetapi orang bodoh menghina hikmat dan didikan”

Amsal 1 : 7

“Dum Spiro Spero

“Selagi aku bernafas, aku berharap”

PERSEMBAHAN

Skripsi ini peneliti persembahkan kepada:

1. Pertama kepada Tuhan YME di dalam nama Bapa, Putra, dan Roh Kudus yang selalu membimbing, menyertai, dan memberkati.
2. Kedua Orang tua tecinta Hioe Tik Liang dan Sumiati yang selalu mendoakan dan memotivasi selama penulis mengerjakan skripsi.
3. Teman-teman di Program Studi Ilmu Hubungan Internasional angkatan 2014 yang telah berjuang bersama dari awal perkuliahan sampai akhir.
4. Yang terakhir semua pihak – pihak terkait yang belum bisa saya sebutkan satu per satu, saya mengucapkan terima kasih yang sebesar – besarnya.

KATA PENGANTAR

Dengan mengucapkan puji syukur kepada Tuhan YME yang telah memberikan berkat dan rahmat-Nya, skripsi dengan judul "Kerjasama ASEANAPOL dan EUROPOL dalam mengatasi *Credit Card Fraud (Carding)*", dapat diselesaikan dengan baik dan lancar sesuai dengan harapan peneliti.

Skripsi ini disusun untuk memenuhi persyaratan guna menyelesaikan jenjang pendidikan sarjana pada Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Slamet Riyadi Surakarta. Pada skripsi ini dibahas mengenai bagaimana kerjasama internasional antara ASEANAPOL dan EUROPOL dalam mengatasi *credit card fraud (carding)*

Dengan penulisan dan penyusunan skripsi ini penulis mendapat dukungan, bantuan dan kerjasama dari berbagai pihak, oleh karena itu penulis ingin mengucapkan rasa terimakasih kepada yang terhormat:

1. Prof. DR. Ir. Sutardi, M. App. Sc, selaku Rektor Universitas Slamet Riyadi Surakarta.
2. Drs. Buddy Riyanto, M.Si., selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Slamet Riyadi Surakarta
3. Ganjar Widhiyoga, Ph.D., selaku Ketua Program Studi Ilmu Hubungan Internasional dan Pembimbing Utama.
4. Halifa Haqqi, S.IP., M.Si., selaku Pembimbing Pendamping yang telah memberikan saran, waktu serta bimbingan bagi penulis hingga sidang skripsi dan Dra. Christy Damayanti, M.Si sebagai dosen Penguji Skripsi.
5. Dosen pengajar Program Studi Ilmu Hubungan Internasional, Halifa Haqqi, S.IP., M.Si., Dra. Christy Damayanti, M.Si, Ganjar Widhiyoga, Ph.D, Dra. Herning Suryo Sardjono, M.Si, Setyasih Harini, S.IP, M.Si, Lukman Fahmi, S.IP, M.Si, Dra. Damayanti

Suhita, M.Si dan seluruh staff Fakultas Ilmu Sosial dan Ilmu Politik Universitas Slamet Riyadi Surakarta.

Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan dalam skripsi ini tidak lain karena kemampuan penulis yang terbatas. Namun demikian penulis mengharapkan agar skripsi ini memberikan manfaat bukan hanya kepada penulis tetapi juga almamater dan pembaca agar menambah wawasan terutama yang tertarik dengan hubungan internasional.

Surakarta, 30 Agustus 2019

Albet Nego
NPM. 14430018

DAFTAR ISI

HALAMAN JUDUL …… i

PERSETUJUAN……... ii

PENGESAHAN iii

KEASLIAN iv

MOTTO v

PERSEMBAHAN vi

KATA PENGANTAR vii

DAFTAR ISI ix

DAFTAR GAMBAR …… xii

ABSTRAK …… xiii

BAB I PENDAHULUAN

A. Latar Belakang ……. 1

B. Rumusan Masalah …… 5

C. Tujuan Penelitian ……. 5

D. Manfaat Penelitian ……... 6

BAB II KAJIAN TEORI DAN KERANGKA BERPIKIR

A. Kajian Teori …….. 7

1. Keamanan Internasional …… 7

1.1 *Cyber Security* …….. 9

1.2 *Cyberspace, Cyberlaw* dan *Cybercrime* .. 10

1.2.1 *Cyberspace* ……. 10

1.2.2 *Cyberlaw* …… 11

1.2.3 *Cybercrime* …… 15

2. Rezim Internasional …….. 18

B. Penelitian Terdahulu ……. 22

1. Kerjasama Kepolisian Negara Republik Indonesia (POLRI) Dalam *ASEAN*

National Police (ASEANAPOL) Untuk Menangani Terorisme Di Indonesia Periode 2002-2006 ……. 23

2. Dampak *Transnational Crime Hacktivism – Carding* Terhadap *Human Security* ……... 23

C. Kerangka Berpikir ……. 24

BAB III METODE PENELITIAN

A. Metode Penelitian ……. 26

B. Jenis Penelitian ……. 26

C. Sumber Data ……. 27

D. Obyek Penelitian …….. 27

E. Teknik Pengumpulan Data ……... 27

F. Teknik Analisa Data ……. 27

1. Reduksi Data …… 28

2. Penyajian Data ……. 28

3. Kesimpulan atau Verifikasi Data ……. 28

BAB IV PEMBAHASAN

A. Aktor Pelaksana Kerjasama dalam *Payment Card Fraud* ...…….. 30

1. EUROPOL (*European Union Agency for Law Enforcement Cooperation)* …….. 31

2. ASEANAPOL (*ASEAN National Police)* … 33

B. *Strategic Meeting on Payment Card Fraud* … 36

1. *The 1st PCF* di Singapura, 11 – 12 November 2015 …….. 37

2. *The 2nd PCF* di Malaysia, 22 – 23 Maret 2016 …… 39

3. *The 3rd PCF* di Thailand, 13 – 14 Desember 2016 …… 40

4. *The 4th PCF* di Jakarta, 19 – 20 Juli 2017 ... 42

C. Perubahan Rezim dalam *Strategic Meeting on Payment Card Fraud* ……... 42

1. Kekuatan …….. 42

2. Bentuk Organisasi……...…….. 44

3. Ruang Lingkup …...…….. 46

4. Modus Alokasional …….. 47

BAB V PENUTUP

A. Kesimpulan …….. 50

B. Saran …… 51

DAFTAR PUSTAKA …… 52

DAFTAR GAMBAR

1. Ruang Lingkup *Cybercrime* ……..... 9
2. Struktur Organisasi EUROPOL ……. 32
3. Struktur Organisasi ASEANAPOL …… 34

ABSTRAK

Penelitian ini membahas mengenai Kerjasama Kepolisian Lintas Negara Dalam Mengatasi Kejahatan *Credit Card Fraud (Carding)*. Pentingnya kerjasama internasional, dimana banyak kasus kejahatan *cybercrime* yang tidak kenal batas wilayah, terlebih *carding* dengan kejahatan minim resiko dan kerugian yang banyak akan mengganggu keamanan internasional suatu negara. Tujuan dari penelitian ini adalah untuk mendeskripsikan bagaimana kerjasama lintas negara yang dilakukan antara EUROPOL, ASEANAPOL dan INTERPOL. Jenis penelitian ini kualitatif dengan wawancara sebagai data primer dan studi pustaka sebagai data sekunder. Selanjutnya, dalam penelitian ini penulis menggunakan teori Keamanan Internasional dan Rezim Internasional. Hasil dari penelitian ini yaitu adanya pertemuan *Strategic Meeting on Payment Card Fraud* selama empat kali sebagai bentuk kerjasama untuk mengatasi kejahatan *carding,* yang mengalami perubahan rezim, baik melalui kekuatan, bentuk organisasi, ruang lingkup dan modus alokasional.

Kata Kunci: Keamanan Internasional, Rezim Internasional, Kartu Kredit, PCF

ABSTRACT

This research deals with the cross-border police cooperation in overcoming Credit Card Fraud (Carding) crimes. The importance of international cooperation, where many cases of cybercrime crimes knows no borders of the region, especially carding with low risk and much loss that will interfere with the international security of a country. The purpose of this study is to describe how cross-border cooperation is conducted between EUROPOL, ASEANAPOL and INTERPOL. This type of research is qualitative with interviews as primary data and library studies as secondary data. Furthermore, in this research the authors use the theory of international security and the international regime. The result of this research is the meeting of Strategic Meeting on Payment Card Fraud for four times as a form of cooperation to overcome the crimes of carding, which underwent regime change, both through strength, organizational form, scope and allocational mode.

Keywords*: International Security, Regime International, Carding, PCF*

BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi masa kini telah banyak mengalami perkembangan yang begitu pesat. Berawal dengan munculnya internet atau *interconnected network* sebagai bentuk inovasi teknologi yang terbarukan. Sibero (2013:10) menjelaskan internet adalah hubungan teknologi digital dengan teknologi telekomunikasi yang saling terkait dalam satu jaringan secara global, seperti media maupun informasi. Internet saat ini telah banyak dimanfaatkan oleh masyarakat kalangan dunia dalam semua aspek kehidupan, baik mencari informasi maupun mengirim informasi.

Kemajuan teknologi informasi saat ini membuat aktivitas masyarakat menjadi serba cepat dengan akses yang lebih luas atau tanpa batas, yaitu melalui dunia internet atau yang biasa disebut *cyber space* sehingga menjadikan perubahan aktivitas manusia menjadi lebih bersifat internasional. Dengan perkembangan teknologi internet sekarang ini, mengakibatkan munculnya berbagai kasus kejahatan baru di dunia maya atau *cybercrime* yaitu kejahatan yang dilakukan di dalam system jaringan internet (Hius, Saputra dan Nasution, 2014). Wakil Kepala Kepolisian RI Komisaris Jenderal Syafruddin mengungkapkan bahwa Indonesia menjadi negara ke 2 dengan kasus serangan *cybercrime* tertinggi setelah Jepang, total serangan mencapai 90 juta kali (CNN Indonesia. 17 Juli 2018). Kasus *cybercrime* sendiri merupakan kasus yang paling banyak ditangani oleh

Ditreskrimsus Polda Metro Jaya sepanjang tahun 2016 (CNN Indonesia, 30 Desember 2016). Indonesia menyadari bahwa *cybercrime* bukanlah kejahatan yang bisa dianggap sepele. Menurut *2Chekout*, yaitu lembaga survey *online payment* yang mengawasi setiap 780 ribu kegiatan transaksi *online* secara global Indonesia bahkan disebutkan masih mempunyai peran yang besar terhadap berbagai kasus kejahatan di dunia maya, sehingga dianggap menjadi negara tertinggi di dunia dalam kasus kejahatan di dunia maya khususnya dalam hal pembayaran *online*. Pada puncaknya, kasus *cybercrime* juga telah menjadikan ekonomi dunia mengalami banyak kerugian sekitar USD 445 miliar setiap tahunnya. Sedangkan kerugian mencapai USD 160 miliar dari sisi bisnis akibat pencurian hak intelektual (*2Checkout*, 28 Mei 2014). Hal inilah yang menjadikan *cybercrime* sebagai kejahatan internasional berdasarkan pada *United Nation Convention Against Transnational Organized Crime (Palermo Convention)* November 2000 dan dalam deklarasi ASEAN tanggal 20 Desember 1997 di Manila, Filipina.

Pemanfaatan teknologi informasi bukan hanya dilakukan melalui pendekatan sistem hukum yang konvensional saja, melainkan karena sifatnya yang tidak kenal batas teritorial suatu negara, dengan aksesnya yang begitu mudah dilakukan kapanpun dan dimanapun, sehingga menyebabkan kerugian baik kepada para pelaku internet dan pengguna yang tidak pernah terhubung sekalipun. Contohnya, tindakan yang disebut *credit card fraudulent* atau yang lebih popular disebut *carding*, merupakan penipuan melalui kartu kredit hanya dengan mengetahui nomor kartu yang masih *valid* saja, selanjutnya para pelaku dapat memesan barang apa saja

secara *on-line* dan kemudian biaya tagihan ditujukan kepada pemilik asli kartu kredit, pelaku disebut sebagai *carder,* kejahatan jenis ini biasa disebut sebagai *cyberfraud* atau penipuan di dunia maya (Detik, 20 Maret 2018).

Berdasarkan pada laporan The Global Cybersecurity 2017 oleh The UN International Telecommunication Union (ITU), Indonesia termasuk negara yang keamanan *cyber*nya paling lemah (GCI, 2017). Kasus kejahatan terbaru adalah pembobolan kartu kredit senilai lebih dari 500 Juta rupiah dengan melakukan pola kejahatan *spamming* dan *carding* (Liputan6, 21 Maret 2018). Komplotan pelaku yang mempunyai jaringan komunitas besar di *facebook* bernama Kolam Tuyul ini menggunakan akun palsu di Apple dan Paypal kemudian mencuri data dari korban yang ada di luar negeri berupa nomor kartu kredit dan tanggal habis masa berlaku. Setelah mendapatkan data akun pengguna kartu kredit, para pelaku membelanjakan sejumlah barang di luar negeri secara *online*.

Kejahatan *carding* bisa terjadi pada siapa saja, dan berkarakteristik global. Pelaku dan korban terjadi dilintas negara yang tak kenal batas-batas geografis dan waktu. Pelaku biasanya melakukan transaksi menggunakan kartu kredit palsu untuk membelanjakan kebutuhan pribadinya. Kejahatan *carding* terbagi menjadi dua ruang lingkup, yaitu nasional dengan pelaku *carding* yang melakukan tindak kejahatannya di dalam negara, sedangkan transnasional yaitu pelaku *carding* yang melakukan tindak kejahatannya secara global dan tidak kenal batas negara.

Carding dalam bahasa formal, adalah *credit card fraud* yaitu penipuan dengan menggunakan kartu kredit. Sedangkan menurut IFCC (*Internet Fraud Complaint Center*), yaitu salah unit FBI yang secara khusus menangani berbagai komplain dari masyarakat terkait kasus *cybercrime*, adalah: "*The unauthorized use of a credit/debit card number can be stolen from unsecured web sites, or can be obtained in an identity theft scheme*". *Cybercrime* dalam dunia maya itu sendiri menimbulkan berbagai kesulitan dalam penegakan hukumnya seperti menentukan tempat kejadian perkara. Sebagai contoh pada kasus pencurian yang konvensional biasanya menentukan lokasi terakhir barang yang dicuri dapat diketahui. Namun, tidak dengan di dunia maya jika para pelaku yang mencuri data warga asing adalah dari negara lain. Selain itu penyidik juga akan mengalami kesulitan mencari saksi yang mengetahui kejadian perkara serta dalam pengumpulan alat bukti. Pengumpulan alat bukti akan memerlukan biaya yang banyak disamping penggunaan teknologi yang canggih maka pengoperasiannya haruslah dengan sumber daya manusia yang ahli (Josua Sitompul, 2012).

Kejahatan lintas negara jenis ini menjadi salah satu ancaman yang serius dalam keamanan dunia. Maka dari itu perlunya penanganan kejahatan transnasional mengharuskan melalui kerjasama antar negara (Malikkul Shaleh, 9 Juli 2009). Adapun organisasi internasional yang memerhatikan masalah tentang hukum *e*-commerce adalah beberapa negara Uni Eropa *(Council of Europe)*. 23 November 2001 tempatnya di Budapest, Hungaria telah dibuat dan disepakati bersama dalam *Convention on Cybercrime* yang selanjutnya disahkan dalam *European Treaty Series* nomor 185. Hasil

konvensi mengandung beberapa kebijakan kriminal *(criminal policy)* dengan tujuan untuk melindungi masyarakat dari tindak *cybercrime,* baik kebijakan domestik maupun lewat kerjasama internasional.

Pengguna internet yang semakin bertambah di Indonesia sekarang ini serta banyaknya modus operandi terbaru menjadikan salah satu alasan bahwa Indonesia mengalami gawat darurat *cybercrime* (Kompas. 11 Januari 2017). Indonesia telah memiliki Undang-undang khusus dalam menangani kasus kejahatan dunia maya seperti UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam hal menangani kasus kejahatan dunia maya Indonesia mengalami berbagai kesulitan baik dalam melakukan usaha pencegahan ataupun cara mengatasinya. Untuk itu Indonesia perlu melakukan kerjasama dengan aktor lain yang lebih berpengalaman dalam mengatasi *cybercrime*.

B. Rumusan Masalah

Berdasarkan pada latar belakang yang telah dijelaskan, maka masalah yang penulis angkat dalam penelitian ini yaitu "Bagaimana upaya kerjasama ASEANAPOL dan EUROPOL dalam mengatasi *credit card fraud?*"

C. Tujuan penelitian

Dalam penelitian ini bertujuan untuk menjelaskan dan mengetahui mengenai kerjasama kepolisian lintas negara dalam menangani penipuan kartu kredit.

D. Manfaat penelitian

Adapun beberapa manfaat yang bisa didapatkan dalam penelitian ini adalah sebagai berikut:

1. Pembaca

Penelitian ini sangat bermanfaat bagi pembaca guna memperluas ilmu tentang dinamika kejahatan transnasional terutama mengenai strategi penanggulangan dalam memberantas kasus *carding*.

2. Program Studi Ilmu Hubungan Internasional

Melalui penelitian ini, Penulis berharap isu mengenai Kerjasama Internasional dapat menjadi suatu hal yang menarik untuk dipelajari dan dipahami dalam studi Ilmu Hubungan Internasional, serta bermanfaat bagi Program Studi Ilmu Hubungan Internasional.

3. Bagi Masyarakat

Melalui penelitian ini, Penulis dapat memberikan informasi agar masyarakat pada umumnya dapat mengetahui modus operandi yang dilakukan oleh para pelaku pembobolan kartu kredit melalui internet *(carder)* dalam menjalankan aksinya disamping itu masyarakat juga dapat mengetahui upaya dan kendala yang dilakukan/dihadapi kepolisian dalam memberantas tindak pidana pembobolan kartu kredit melalui internet *(carding).*

BAB II

KAJIAN TEORI DAN KERANGKA BERPIKIR

A. Kajian Teori

1. Keamanan International

Keamanan internasional pada umumnya sering diartikan sebagai proses membangun keamanan dunia. Tidak lepas dari pemahaman penganut realis yang memandang bahwa dunia internasional sifatnya anarki sehingga pada dasarnya setiap negara memiliki keinginan untuk meningkatkan kekuatannya sebagai respon dari anarkisme itu sendiri. Buzan (1984) menilai bahwa konsep keamanan lebih komprehensif dalam memahami permasalahan yang ada di dalam hubungan internasional.

Kemanan internasional secara tradisional dilekatkan dengan penggunaan kekerasan serta adanya perang dan sekaligus dengan munculnya perdamaian. Rothschild (1995) dalam buku Broto Wardoyo (2015) menganggap bahwa kajian teori keamanan internasional terlalu sempit maka Rothschild mengusulkan empat perluasan dalam memahami konsep keamanan. Pertama, pemahaman mengenai konsep keamanan harus diperluas dari keamanan negara-bangsa menjadi keamanan kelompok dan individu. Kedua, pemahaman mengenai konsep keamanan tidak saja harus diperluas ke bawah (individu atau kelompok), namun juga ke atas dengan memasukan keamanan sistem internasional ataupun lingkungan fisik supranasional. Ketiga, konsep keamanan juga harus dipahami dalam berbagai dimensi, termasuk militer, politik, ekonomi, sosial, lingkungan,

dan insani. Terakhir, konsep keamanan juga harus diperluas dengan meletakkan tanggung jawab atas penyedia keamanan tidak hanya di tangan negara-bangsa, namun ke berbagai aktor dengan melibatkan organisasi internasional atatupun regional, pemerintah daerah (lokal), organisasi swadaya masyarakat, public, dan pasar.

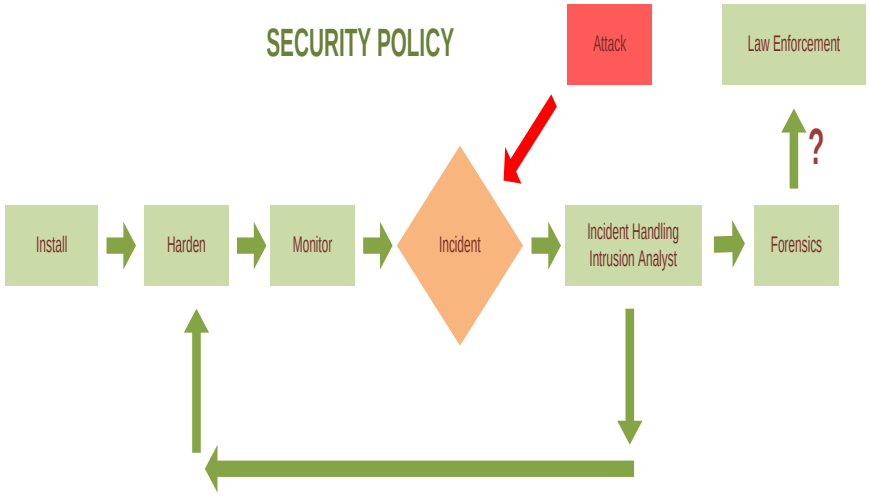
Kajian mengenai kemanan dari semula hanya dipahami dalam konteks militer dan terfokus pada aktor negara hingga saat ini mulai merambah dimensi-dimensi non-militer dan melibatkan pula aktor-aktor non-negara, termasuk individu. Pasca perang dingin mengakibatkan dunia internasional mengalami pergeseran, yaitu dalam membangun dunia yang lebih aman adalah dengan melakukan kerjasama dan globalisasi menjadi faktor penggerak interkonektifitas masyarakat internasional. Transformasi keamanan internasional sangat dirasakan dalam perluasan actor dan isu setelah berakhirnya perang dingin menurut Walt (1991).

Salah satu bentuknya adalah ancaman *cybercrime* disebut juga sebagai *cyber security* yang menjadi perhatian dunia saat ini. Perkembangan teknologi informasi ini menjadikan ruang interaksi tidak terbatas sehingga memberikan perubahan yang signifikan dalam konsep keamanan sendiri. Perkembangan teknologi digital yang pesat selalu diikuti kemunculan ancaman baru di dunia siber.

1.1. *Cybersecurity*

Cybersecurity adalah sekumpulan alat, kebijakan, dan jaminan teknologi yang digunakan dalam melindungi lingkungan *cyberspace*, baik organisasi maupun *user* atau pengguna (Handrini Ardiyanti 2015). Tujuan

dalam *cybersecurity* yaitu memastikan tercapainya keamanan dalam lingkungan *cyber*.



Gambar 1. Ruang Lingkup *Cybersecurity*

Sumber: **Technology Perscpetive: National Cyber Security, Universitas Pertahanan Indonesia**

Dari gambar tersebut dapat dijelaskan bahwa ruang lingkup *cybersecurity* dimulai dari install, harden atau keamanan terkait dengan perangkat keras yang digunakan dalam mengoperasikan internet, kemudian monitor, yang menyebabkan terjadinya insiden atau kejadian dan insiden itu dapat pula berasal dari serangan atau *cyber attact* yang membutuhkan penangganan terhadap insiden tersebut dengan melakukan uji forensik sebagai pembuktian dalam penegakan hukum terhadap terjadinya *cybercrime*.

Beberapa elemen pokok *cyber security* menurut Ardiyanti (2015) adalah sebagai berikut:

1. Dokumen *security policy* adalah dokumen yang menjalankan segala proses yang berkaitan dengan keamanan informasi.

2. *Information infrastructure* berperan sebagai pendukung dalam kelangsungan operasi informasi yaitu *hardware* dan *software*.

3. *Perimeter Defense* berperan sebagai komponen pertahanan pada infrastruktur informasi seperti *firewall*.

4. *Network Monitoring System* adalah untuk memonitor kelangsungan dalam infrastruktur informasi.

5. *System Information and Event Management* berperan sebagai media dalam menampilkan berbagai insiden yang terjadi.

6. *Network Security Assessment* berperan sebagai elemen-elemen dalam *cybersecurity* yang memberikan *measurement level* keamanan informasi.

7. *Human resource* dan *security awareness* yang berkaitan dengan adanya sumber daya manusia dan kesadarannya terhadap system keamanan informasi.

1.2. *Cyberspace, Cyberlaw dan Cybercrime*

1.2.1 *Cyberspace*

Seperti kebanyakan peristilahan computer lainnya, *cyberspace* tidak memiliki definisi yang standar pada umumnya. *Cyberspace* biasanya hanya digunakan untuk mendeskripsikan dunia virtual computer saja. *Cyberspace* lebih menunjukan sekumpulan data yang ada pada suatu jaringan komputer (*network)*. *Cyberspace* yang sekarang ini lebih mengalami perkembangan menjadi sebuah global *network* dari suatu komputer.

Istilah *cyberspace* menurut William Gibson dalam bukunya Neuromancer (1984) "*Cyberspace. A consensual hallucination experienced daily by millions of legitimate operators. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding"* (William Gibson). Intinya adalah *cyberspace* merupakan sebuah halusinasi konsensual yang terjadi setiap hari yang berasal dari milyaran operator-operator di seluruh dunia. Seperti sebuah grafis yang direpresentasikan dari suatu data yang kemudian diabstraksikan dari setiap komputer-komputer yang ada dalam suatu sistem.

Cyberspace menyebabkan perbedaan antara hubungan koordinasi dan komunikasi dalam kehidupan nyata. Dalam *cyberspace* seseorang dapat melakukan hubungan interaksi dengan orang lain secara langsung tanpa harus bertemu pada satu tempat dan bahkan dalam *cyberspace* seseorang bisa berinteraksi dengan orang baru yang tak dikenal sekalipun, dan yang paling buruk adalah merencanakan suatu hal untuk melakukan kejahatan internasional.

1.2.2 *Cyberlaw*

Perkembangan internet seringkali ini menyebabkan pengguna internet atau *user* dalam melakukan banyak hal apapun. Sebagai contoh dari memanfaatkan kemajuan internet yaitu dengan melakukan berbagai interaksi sosial tanpa bertatap muka sekalipun. Bahkan dapat melakukan

suatu transaksi-transaksi jual-beli barang atau mengirim dan menerima barang dari satu negara ke negara lain tanpa harus bertemu langsung antara penjual dan pembeli dalam melakukan transaksi. Perkembangan ini dapat menimbulkan tindakan penyalahgunaan terhadap internet yang biasa disebut sebagai *cybercrime* sehingga diperlukan adanya suatu tindakan dalam pencegahan dan perlindungan bagi para pengguna internet.

Di mana ada kejahatan maka disanalah hukum berpijak, setiap kejahatan harus ada hukuman yang diberikan. Sedangkan hukum yang berlaku dalam mengatur keamanan dan etika dalam memanfaatkan kemajuan *cyberspace* atau internet adalah *cyberlaw.* Menurut *Information Security Awareness (ISEA), Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet.*

Kongres PBB mengenai *The Prevention Of Crime and The Treatment Of Offenders* telah membahas mengenai masalah *cybercrime* yang diagendakan pada Kongres PBB VIII/1990 di Havana dan Kongres X/2000 di Wina mengenai *computer related crimes* yang mengajukan beberapa kebijakan:

1. Menghimbau negara anggota untuk mengupayakan penanggulangan penyalahgunaan computer secara intesif dengan mempertimbangkan langkah-langkah sebagai berikut:

    a. Memodernisasikan hukum pidana material dan hukum acara pidana.

b. Melakukan peningkatan dalam tindak pencegahan dan pengamanan komputer.

c. Sosialisasi kepada masyarakat, aparat pengadilan dan penegak hukum untuk membuat peka terhadap pentingnya tindak pencegahan *cybercrime*.

d. *Training* atau pelatihan bagi para hakim, pejabat, dan aparat penegak hukum dalam kejahatan ekonomi dan *cybercrime.*

e. Mengajarkan *rules of ethics* melalui kurikulum informatika.

f. Mendorong korban dari tindak kejahatan *cybercrime* untuk mengambil langkah dalam melaporkan pada pihak berwajib.

2. Menghimbau negara anggota untuk meningkatkan berbagai kerjasama internasional dalam fokus menanggulangi *cybercrime.*

3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*Committee on Crime Prevention and Control)* PBB untuk:

a. Menyebarluaskan dan mensosialisasikan pedoman standar dalam membantu anggota negara untuk mengatasi *cybercrime* di tingkat nasional, regional maupun internasional.

b. Mengembangkan penelitian serta analisis terbarukan untuk mengatasi *cybercrime* di masa mendatang.

c. Meninjau pengimplementasian perjanjian ektradisi dalam bidang penanggulangan *cybercrime.*

Dalam resolusi PBB tersebut tindakan dengan kebijakan pencegahan merupakan suatu hal yang perlu dilakukan, hal ini terkait dengan pendekatan *techno-prevention,* yaitu upaya mencegah dan menanggulangi kejahatan yang semakin berkembang menggunakan teknologi. Dengan adanya kemajuan teknologi ini maka tidak dapat ditanggulangi dengan pendekatan yuridis saja, melainkan perlu dengan pendekatan teknologi. Seperti membangun *self-awarness* dari warga masyarakat dan apart penegak hukumnya, serta mensosialisasikan etika penggunaan computer secara benar dan tepat melalui media pendidikan.

1.2.3 *Cybercrime* (Kejahatan Siber)

European Commission menyatakan bahwa *Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems*. Sedangkan menurut Lita Sari (2015) *Cybercrime* merupakan suatu tindak kejahatan yang dilakukan dengan memafaatkan teknologi komputer seperti internet sebagai alat kejahatan utama. *The Australian Cybercrime Online Reporting Network* (ACORN) berpendapat bahwa

> *Cybercrimes are crimes which are: directed at computers or other devices (for example, hacking), and where computers or other devices are integral to the offence (for example, online fraud, identity theft and the distribution of child exploitation material).*

Cybercrime merupakan kejahatan transnasional, bertempat di dunia virtual (maya), menggunakan alat berteknologi tinggi (berbasis komputer)

dengan cara yang bervariasi dalam jangka waktu yang singkat, dan akibatnya sangat banyak dan menjangkau wilayah yang sangat luas.

Karakteristik dalam *cybercrime* adalah sebagai berikut:

1. *Unauthorized access*

2. *Unauthorized alteration* atau *destruction of data*

3. Mengganggu ataupun merusak sistem operasi komputer

4. Mencegah maupun menghambat akses komputer.

Encyclopedia of Cybercrime membagi tindakan *cybercrime* yang berkaitan pada penyalahgunaan dari system informasi menjadi:

1. Kelalaian dalam menggunakan system informasi dan melanggar kebijakan keamanan dengan cara menyebarluaskan system dan data untuk tindak kejahatan/

2. Menggunakan komputer atau alat elektronik lainnya untuk berkomunikasi atau menyimpan hasil rekaman yang dipakai untuk aktivitas illegal.

3. *Phising, spoofing, skimming* dilakukan untuk menipu, menyamarkan dan menduplikat data dari kartu pembayaran orang lain untuk mendapatkan keuntungan sendiri secara online dalam penipuan kartu pembayaran atau mencuri identitas.

4. *Hacking, computer trespassing,* dan *password cracking* dilakukan untuk menembus kata sandi dalam akun computer secara ilegal atau melanggar hukum dalam system informasi secara *online* maupun *offline.*

5. *Malicious writing* dan membagikan kode computer untuk membuat, mengkopi dan menyebarkan *malware*

6. Pembajakan digital terhadap music, film, dan *software.*

7. *Cyber harassment* atau bentuk ancaman dan pemaksaan secara sengaja sehingga membuat rasa malu pada korban seperti *cyber bullying.*

8. *Online Stalking* dan *Cyber-sex* yaitu mengirimkan pesan yang tidak diinginkan atau mengandung unsur seksual menggunakan internet serta untuk memfasilitasi tindakan penjualan manusia untuk kegiatan seksual atau lainnya.

9. Kecurangan akademik dan *scientific misconduct* dilakukan aik oleh pelajar maupun pengajar untuk menjiplak metode riset atau penemuan dan segala bentuk tugas maupun ujian.

10. Kejahatan terorganisir yang menggunakan basis internet untuk memfasilitasi kegiatan legal dan ilegal seperti penyelundupan manusia, senjata dan obat-obatan.

11. Tindakan mematai-matai yang dilakukan oleh pemerintah atau *intel* yang melibatkan penggunaan *spyware* dan *keylogger* untuk mencuri data dan informasi yang akan digunakan untuk aktivitas kejahatan.

12. *Cyberterrorism* dilakukan untuk memajukan kepentingan sosial, agama, dan politik dengan menyebar ketakutan atau mengganggu informasi infrastruktur yang penting.

Pada dasarnya *cybercrime* meliputi semua tindak pidana yang berkaitan dengan informasi, komunikasi yang sebagaimana merupakan sarana dalam menyampaian dan bertukar informasi. Oleh sebab itu penulis menggunakan konsep keamanan internasional dalam mengkaji kasus *cybercrime* dan mengupas bagaimana upaya membangun pertahanan dan keamanan melalui keamanan *cyber* khususnya *carding* dengan berbagai upaya kerjasama internasional untuk mengatasi tindak kejahatan tersebut.

2. Rezim Internasional

Kondisi masyarakat internasional terdiri dari berbagai macam pelaku hubungan internasional. Para pelaku hubungan internasional tersebut terdiri dari aktor non-negara dan aktor negara. Dalam rangka menciptakan keteraturan hubungan diantara para aktor tersebut, maka dibutuhkan sebuah wadah yang dapat digunakan untuk mengatur hubungan tersebut. Rezim internasional muncul sebagai wadah yang digunakan dalam mengatur hubungan tersebut.

Menurut Krasner (1983), rezim internasional adalah seperangkat norma, peraturan dan prosedur dalam pembuatan keputusan secara eksplisit maupun implisit dimana semua para actor berkumpul dalam hubungan internasional. Prinsip merupakan kepercayaan pada fakta, hubungan sebab-akibat, dan kebenaran. Norma adalah standar perilaku yang ada dalam hak dan kewajiban. Peraturan merupakan adanya ketentuan dan larangan dalam bertindak dan berperilaku. Sedangkan prosedur dalam pembuatan keputusan

adalah praktek dari pembuat dan pelaku dalam mengimplementasikan keputusan bersama.

Young (1982) berpendapat bahwa suatu rezim terbentuk mulai dari sifat alamiah manusia, sehingga rezim bekerja karena sifat sekelompok manusia. Rezim akan berubah tergantung sikap manusia ke depannya dan yang mendasari hal itu adalah sifat alamiah manusia itu sendiri.

Awal terbentuknya rezim terbagi menjadi tiga, menurut Young (1982):

1. *Spontaneous order*

Yaitu terbentuknya rezim secara spontan karena adanya kesadaran akan kesamaan tujuan dan kepentingan oleh para actor. Adanya tujuan dan kepentingan tersebutlah yang akan membuat sistem atau tatanan baru

2. *Negotiated order*

Yaitu terbentuknya rezim karena adanya negosiasi antara para aktor. Kesepakatan yang terjalin antara kedua aktor akan dimuat dalam syarat dan aturan yang telah disetujui untuk mencapai kepentingan bersama. Dalam kesepakatan tersebut terdapat *legislative bargains* yaitu kesepakatan para aktor dalam memenuhi syarat-syarat yang berlaku supaya kesepakatan bisa berjalan dengan baik. *Negotiated order* dianggap dinamis karena mampu mengatasi perubahan dengan cara merevisi kesepakatan yang sudah ada. Sedangkan kelemahannya adalah ketika mayoritas para aktor tidak sepaham dengan ide yang diusulkan maka kesepakatan tidak akan terjadi.

3. *Imposed order*

Adanya suatu rezim yang terbentuk secara tidak sengaja karena perbedaan kekuatan yang lebih dominan dari aktor yang lain. Biasanya hal tersebut dilakukan oleh aktor hegemon secara tidak formal, yaitu dengan memaksa bertindak secara eksplisit supaya mengikuti rezim yang diinginkan oleh aktor hegemon tersebut. *Imposed order* terdapat dua jenis, yang pertama adalah *overt hegemony* yaitu aktor dominan secara terbuka dan eksplisit mengartikulasikan pengaturan suatu institusi yang memaksa aktor yang lebih lemah untuk menaatinya. Lalu yang kedua adalah *de facto imposition* yang lebih mengarah pada cara-cara implisit sehingga aktor yang lebih dominan membuat aturan dan melakukan tindakan untuk menguntungkan diri sendiri dengan berbagai cara.

Perubahan rezim menurut Owen (2010) adalah istilah politik dan satu polarisasi, perubahan rezim terjadi karena adanya pemaksaan kekuatan yang lebih dominan atau *rezim changer*

Perubahan rezim terjadi dalam 4 cara menurut Haggard (1987), yaitu:

a. Kekuatan

Yaitu kekuatan suatu rezim diukur dari tingkat kepatuhan masyarakat terhadap perintah rezim, yaitu dalam suatu kasus dimana melemahnya atau runtuhnya suatu rezim dalam masyarakat karena tidak sejalan dengan aturan rezim yang ada.

b. Bentuk Organisasi

Seperti rezim *fixed-exchange-rate* yang menuntut negara memberikan intervensi yang positif, namun dengan tidak terpusatnya pengaturan kebijakan dan bentuk rezim *one nation one vote* dan *weighted*

voting (IMF dan World Bank). Sebagian besar rezim cenderung memiliki beberapa perangkat administrasi yang baik dalam menjalankan tugasnya karena dalam kerjasama yang komplek membutuhkan struktur organisasi yang baik dan independen. Perubahan bentuk organisasi seiring waktu menuntut perubahan rezim yang lebih dinamis sesuai dengan kebutuhan seperti masalah *cybercrime*.

c. Ruang Lingkup

Yaitu mengacu pada berbagai perubahan isu-isu yang mencakup suatu rezim dapat menimbulkan *misleading characterizations* (seperti GATT). Kegagalan untuk mematuhi ketentuan-ketentuan dalam GATT (*General Agreement on Tariffs and Trade*) menandakan melemahnya rezim perdagangan pada tahun 1970. Ruang lingkup suatu rezim yang terlalu luas dapat meningkatkan biaya administrative dan kompleksitasnya, sedangkan ruang lingkup yang sempit akan mempersulit proses tawar menawar dalam suatu hubungan antar isu.

d. Modus Alokasional

Suatu rezim yang mendukung mekanisme sosial yang berbeda dalam pengalokasian sumber dayanya. Rezim yang berorientasi pada pasar mendukung alokasi sumber daya pribadi, menghambat kontrol nasional serta menjamin hak kepemilikan. Di sisi lain, alokasi otoritatif melibatkan kontrol langsung sumber daya oleh otoritas rezim, dan akan menuntut struktur organisasi yang lebih luas.

Situasi dalam hubungan internasional yang cenderung bersifat dinamis dengan munculnya isu-isu baru menjadi permasalahan dalam

keamanan internasional salah satunya *payment card fraud.* Untuk menghadapi isu tersebut, salah satu opsi yang perlu dipakai penulis adalah dengan membentuk rezim internasional dari berbagai kerjasama yang dilakukan EUROPOL *(European Police Office)* dengan POLRI yaitu penyelenggaraan *Strategic Meeting on Payment Credit Card Fraud* yang dilaksanakan bersama-sama dengan negara anggota ASEANAPOL (*ASEAN National Police*) secara bergiliran. Dari berbagai pertemuan yang dilaksankan di Singapura, Malaysia, Thailand dan Jakarta menghasilkan beberapa solusi dalam menangani *payment card fraud* seiring dengan adanya perubahan dalam setiap pertemuan dari tahun ke tahun.

Owen (2010), melihat bagaimana suatu perubahan rezim terjadi adalah dengan melakukan analisis terhadap perkembangan (*evolution*) dari variabel-variabel: Perubahan kepentingan dari adanya pertemuan yang dilakukan EUROPOL sebagai *observer* dalam *Strategic Meeting on Payment Credit Card Fraud* bersama ASENAPOL, maupun adanya perubahan persamaan kepentingan dari anggota negara ASEANAPOL, kerugian-kerugian dalam kerjasama yang dilakukan serta keuntungan dari adanya beberapa pertemuan tersebut, dan perubahan kebutuhan publik yang semakin berkembang dari waktu ke waktu dalam pertemuan tersebut.

B. Penelitian Terdahulu

Penelitian terdahulu yang dipakai penulis digunakan sebagai bahan perbandingan dan kajian. Adapun hasil-hasil penelitian yang dijadikan perbandingan oleh penulis adalah sebagai berikut:

1. Kerjasama Kepolisian Negara Republik Indonesia (POLRI) Dalam *ASEAN National Police* (ASEANAPOL) Untuk Menangani Terorisme Di Indonesia Periode 2002-2006

Penulis : Bima Andrianto P, Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Diponegoro, Semarang.

Tahun : 2016

Dalam penelitian Andrianto, membahas mengenai upaya kerjasama POLRI dalam ASEANAPOL untuk menangani terorisme di Indonesia. Yang dilakukan melalui kesepakatan bersama tahun 2002 sampai 2006 dalam bentuk pengembangan kapasitas yaitu dengan berbagi keahlian dan tukar menukar informasi. Dan diperlukannya kerjasama dalam bidang pendidikan berupa latihan dan pertukaran personil seorang ahli dari negara ASEAN yang memiliki keahlian khusus. Serta bertukar pengalaman dan praktek latihan, seminar, workshop dan konsultasi pada operasi penanganan terorisme. Dalam penelitian ini membantu penulis dalam memahami bentuk-bentuk kerjasama apa saja yang dilakukan oleh POLRI dan ASEANPOL dalam mengatasi kejahatan lintas negara sehingga selanjutnya dapat digunakan untuk dijadikan acuan dalam penelitian penulis.

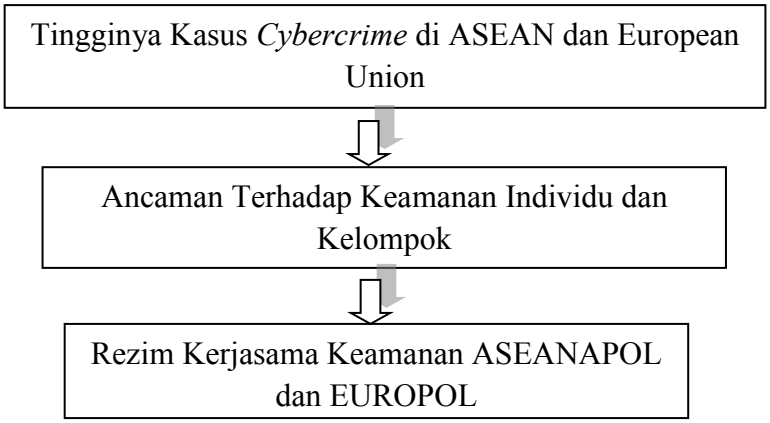
2. Dampak Transnational *Crime Hacktivism – Carding* Terhadap *Human Security*

Penulis : Kurniawan Chandra Febrianto, Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Muhammadiyah, Malang.

Tahun : 2013

Dalam penelitian Chandra membahas bagaimana dampak *Carding* terhadap *Human Security*, dan bagaimana kejahatan kartu kredit dilakukan oleh *carder* baik motif kegiatan *Cybercrime* dan modus operandinya. Dijelaskan dalam penelitian tersebut bagaimana cara *Carder* mendapatkan kartu kredit, alur proses transaksi *Carder* melalui kartu kredit dan bagaimana cara membobol kartu kredit. Membahas mengenai regulasi (*Cyber Law)* mengenai aktivitas kejahatan *Cyber Crime* di dunia internasional, cara pencegahan yang dapat dilakukan terhadap pembobolan kartu kredit serta berbagai kerjasama peraturan dan kebijakan hukum di negara Singapore, Malaysia, Thailand, Vietnam. Penelitian Chandra tersebut membantu penulis dalam memahami bentuk regulasi, kerjasama dan peraturan hukum tentang *carding* khususnya di Singapore, Malaysia, Thailand, Vietnam sebagai strategi Indonesia dalam menangani kasus *carding* serta bagaimana kejahatan *Carding* itu dilakukan.

C. Kerangka Berpikir



BAGAN KERANGKA BERPIKIR

Melalui skema kerangka berpikir penulis menggambarkan pola atau alur pemikiran dalam penelitian tersebut, yaitu:

1. Dalam penelitian ini, penulis mengangkat permasalahan mengenai tingginya kasus *cybercrime* yang terjadi di Indonesia. Pada tahun 2016 tercatat ada 4.931 kasus yang ditangani Polri. Sedangkan pada tahun 2017, aparat menangani kasus *cybercrime* sebanyak 5.061 kasus-kasus yang dengan demikian *cybercrime* terus meningkat di Indonesia (OKE zone. 29 Desember 2017). Sedangkan di Eropa kerugian finansial dalam kejahatan menggunakan kartu kredit mengalami peningkatan sebesar 13% (Europol. 2019).

2. Lemahnya keamanan siber di Indonesia, yang berdampak pada meningkatnya serangan siber (Kompas. 20 November 2017). Dimana modus operandi *cybercrime* di Indonesia semakin canggih dan berubah seiring perkembangan jaman. Luasnya kejahatan dunia maya terjadi karena tidak dibatasi oleh ruang dan waktu yaitu secara lokal atau nasional tetapi

juga transnasional dan internasional, sehingga dapat mengancam keamanan individu maupun kelompok.

3. Dalam pencegahan kejahatan transnasional khususnya kejahatan *carding* diperlukan kerjasama internasional dalam mencapai keamanan internasional yang dapat diterapkan dalam pencegahan kejahatan *carding*. Munculnya rezim kerjasama keamanan ASEANAPOL dan EUROPOL merupakan upaya kerjasama keamanan untuk meningkatkan keamanan kawasan.

BAB III

METODE PENELITIAN

A. Metode Penelitian

Manusia melakukan penelitian untuk mencari kebenaran dari suatu fenomena yang diteliti dengan menggunakan metodologi. Metode penelitian merupakan langkah-langkah dalam mendapatkan kebenaran dari pengetahuan ilmiah yang tersusun secara sistematis (Suryana, 2010). Metode penelitian merupakan gambaran dari rancangan penelitian yang terdiri dari prosedur dan langkah-langkah yang harus dijalankan dalam memperoleh atau menganalisis suatu data.

B. Jenis Penelitian

Jenis penelitian yang dipakai penulis sebagai pisau analisis untuk memahami persoalan yang diteliti menggunakan penelitian kualitatif deskriptif analitis. Deskriptif analitis adalah suatu cara membuat gambaran dalam penelitian menjadi bagian dari permasalahan yang akan diteliti (John Creswell, 1994). Menurut Sandu Sunyoto (2015: 27) metode penelitian kualitatif adalah metode penelitian yang hanya menekankan pada pemahaman secara mendalam (*indepth analysis*) terhadap suatu masalah, yaitu dengan mengkaji masalah secara terperinci karena sifat suatu masalah dengan masalah lainnya pasti akan berbeda. Jadi tujuan dari metodologi itu sendiri adalah pemahaman secara mendalam terhadap suatu permasalahan saja bukan secara generalisasi.

C. Sumber Data

Sumber data yang di sajikan dalam penelitian ini adalah data primer dan data sekunder. Data primer yang dipakai diambil langsung dari Atase POLRI di KBRI Den Haag dalam bentuk dokumen yang kemudian diolah/dianalisis. Data sekunder diperoleh melalui studi kepustakaan seperti jurnal, skripsi atau tesis, buku, majalah, artikel, instituti dan lembaga terkait. Data yang digunakan adalah data yang berkaitan langsung dengan penelitian penulis tentang upaya dalam mengatasi *carding* dan kerjasama ASEANAPOL dan EUROPOL dalam menangani kasus *carding*.

D. Obyek Penelitian

Adanya obyek penelitian dalam penelitian ini untuk memfokuskan kasus permasalahan yang diangkat oleh penulis. Antara lain mengenai Penanggulangan *carding* sebagai kejahatan transnasional di ASEANAPOL dan EUROPOL.

E. Teknik Pengumpulan Data

Kegiatan penelitian yang terpenting adalah dengan pengumpulan data. Dalam pengumpulan data penulis menggunakan metode wawancara dengan Atase Kepolisian Indonesia untuk Belanda Kombes Pol. Ricky Purnama, S.i.K, MH. Dan data yang diperoleh haruslah dapat terjaga tingkat validitas dan reliabilitasnya (Sandu Sunyoto, 2015: 27).

F. Teknik Analisa Data

Teknik analisa data yang penulis gunakan adalah menggunakan tehnik analisa kualitatif. Penulis menggunakan tiga analisis data yaitu:

1. Reduksi Data

   Dalam reduksi data, penulis merangkum, menyederhanakan dan memilih data pada hal-hal pokok saja. Dilakukan dengan membuat rangkuman, pengabstrakan dan menajamkan dari pernyataan-pernyataan yang berkaitan dengan penelitian serta menyederhanakan data dengan memilah dan membuang hal-hal yang tidak berkaitan dengan penelitian yang diperoleh selama pencarian data, sehingga data yang diperoleh merupakan data yang tercakup dalam scope penelitian saja.

2. Penyajian Data

   Penyajian data yang dilakukan penulis dalam analisis data adalah untuk dapat melihat informasi keseluruhan dan bagian-bagian pentingnya. Pada tahap ini peneliti berupaya mendeskripsikan dan menyajikan data sesuai dengan pokok permasalahan dalam penelitian. Penulis menyajikan sekumpulan informasi yang tersusun dan melakukan penyederhanaan tanpa mengurangi isinya sehingga dapat memberikan informasi yang bermakna.

3. Kesimpulan atau Verifikasi Data

Peneliti membuat kesimpulan dari data-data yang sudah diperoleh dan diverifikasi. Untuk mencari makna-makna dari data yang sudah dikumpulkan adalah dengan mencari hubungan persamaan atau perbedaan yang sudah diuji kebenaran dan kecocokannya. Hal ini dilakukan agar penarikan kesimpulan bisa dilakukan dengan membandingkan setiap pernyataan yang sesuai dari subyek penelitian dengan makna dari data yang terkandung dengan konsep-konsep dasar dalam penelitian penulis.

BAB IV
PEMBAHASAN

A. Aktor Pelaksana Kerjasama dalam *Payment Card Fraud*

Kejahatan dengan menggunakan kartu pembayaran atau *carding* merupakan kejahatan dengan tingkat resiko paling rendah dan menyebabkan kerugian finansial paling banyak (Europol. 2019). Jenis kejahatan ini semakin bertumbuh seiring perkembangan teknologi masa kini dengan meningkatnya pengetahuan terhadap penggunaan teknologi informasi termasuk jaringan computer dan internet begitu juga dengan mudahnya mendapatkan alat-alat *Phising* dan *Skimming* yang dijual lewat *Darknet* (jalur gelap internet). Kejahatan yang dilakukan adalah dengan melakukan transaksi illegal dalam membeli produk dan jasa melalui situs *e-commerce* atau lewat media sosial menggunakan kartu pembayaran orang lain secara global. Tidak terbatasnya tempat dan waktu dalam aktivitas *carding* ini tidak hanya mengancam keamanan nasional negara tetapi mengancam keamanan internasional serta mengharuskan penanganannya melalui kerjasama antar negara.

Di Eropa, tingkat kasus kejahatan menggunakan kartu pembayaran menurun sebesar 26% namun mengalami peningkatan 13% dalam total kerugian secara finansial sekitar 1,5 miliar euro per tahun, hal tersebut terjadi karena penggunaan EMV (chip dan pin) yang belum maksimal di negara Asia Tenggara khususnya Indonesia dan Filipina (Europol. 2019). Begitu juga halnya dengan Indonesia dengan tingkat kejahatan *cybercrime*

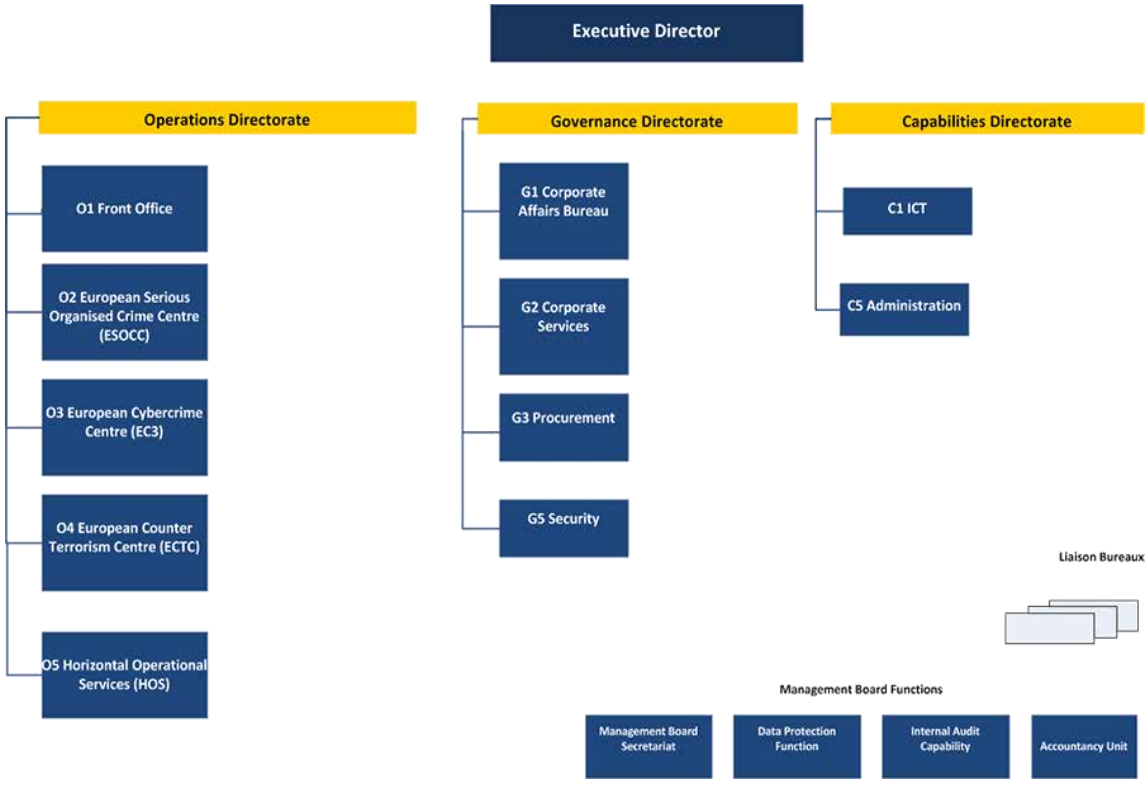
yang paling banyak ditangani oleh Ditreskrimsus Polda Metro Jaya sepanjang tahun 2016 (CNN Indonesia, 17 Juli 2018), sehingga menjadikan Indonesia gawat darurat *cybercrime*. Atas dasar kepentingan EUROPOL sebagai lembaga penegak hukum Uni Eropa yang memprioritaskan untuk memerangi kejahatan menggunakan kartu pembayaran, maka EUROPOL menginginkan kerjasama dengan ASEANAPOL sebagai wadah kerjasama dengan Asia Tenggara dalam menciptakan keamanan internasional.

1. EUROPOL (*European Union Agency for Law Enforcement Cooperation*)

Adalah lembaga penegak hukum Uni Eropa yang berfungsi sebagai pusat informasi mengenai kegiatan kriminal dan wadah bagi para ahli penegak hukum yang bertujuan untuk mencapai kawasan Eropa yang lebih aman. Selain sebagai wadah bagi negara-negara Uni Eropa, EUROPOL juga bekerjasama dengan banyak negara non Uni Eropa dan berbagai Organisasi Internasional lainnya. Markas besar berada di Den Haag, Belanda. Beranggotakan 28 negara-negara anggota Uni Eropa dan memiliki lebih dari 1000 staff termasuk 220 *Europol Liaison Officer* (ELOS) yaitu petugas perwakilan dari negara anggota EUROPOL yang ditempatkan di kantor pusat EUROPOL dan juga negara-negara mitra non-Uni Eropa lainnya seperti Australia, Kanada, Amerika Serikat dan Norwegia (Europol. 2019).

Tugas ELOS adalah menjamin kerjasama yang cepat dan efektif berdasarkan kontak pribadi dan rasa saling percaya terhadap negara asalnya. Petugas EUROPOL tidak memiliki kewenangan

dalam penangkapan atau penyidikan, namun memiliki tugas tersendiri dalam mengumpulkan data kejahatan, menganalisa, membagikan informasi dan mengkoordinasikan operasi. Negara anggota EUROPOL menggunakan informasi yang diberikan EUROPOL untuk mencegah, mendeteksi dan menyelidiki pelanggaran, kemudian melakukan penyidikan dan mengadili mereka yang melakukan kejahatan. EUROPOL merupakan pusat operasi *high security* yang berurusan lebih dari 40.000 kasus per tahun dengan analisis berkualitas tinggi sehingga menjamin keberhasilan operasionalnya.



Gambar 2. Struktur Organisasi EUROPOL

Sumber: Europol. 2019

EUROPOL dipimpin oleh Direktur Eksekutif yang dijabat oleh Catherine De Bolle sejak Mei 2018 lalu, dan dibantu Wil van Gemert sebagai *Operations Directorate*, Oldrich Martinu sebagai *Governance Directorate,* Luis de Eusebio Ramos sebagai *Capabilities Directorate.* Sebagai lembaga penegak hukum Uni Eropa, EUROPOL memiliki misi untuk mendukung negara-negara anggota dalam mencegah dan memerangi segala bentuk kejahatan internasional yang terorganisir, *cybercrime* dan terorisme dalam rangka menciptakan keamanan kawasan.

2. ASEANAPOL *(ASEAN National Police)*

Asia Tenggara juga memiliki organisasi kepolisian regional yang serupa seperti EUROPOL yaitu ASEANAPOL. ASEANAPOL adalah sebuah organisasi kepolisian yang berada di wilayah regional Asia Tenggara dan beranggotakan para Kepala Kepolisian dari organisasi ASEAN *(Association of Southeast Asian Nations).* ASEANAPOL saat ini memiliki 10 anggota yaitu Brunei, Kamboja, Indonesia, Laos, Malaysia, Myanmar, Filipina, Singapura, Thailand, Vietnam (Aseanapol.org, 20 Februari 2019). Tujuan dibentuknya ASEANAPOL adalah meningkatkan kerjasama di bidang kepolisian untuk memastikan keamanan wilayah serta sebagai wadah untuk saling berkontribusi dan bersinergi di kebijakan sumber daya dan keahlian dalam mengatasi kejahatan transnasional untuk mewujudkan ASEAN yang aman.

Gambar 3. Struktur Organisasi ASEANAPOL

Sumber: ASEANAPOL. 2019

ASEANAPOL dipimpin oleh *Executive Director* dengan masa jabatan 2 tahun, dan dibantu dengan *Directors* dengan masa jabatan 2 – 3 tahun. Tugas *Executive Director* adalah membuat laporan dari adanya setiap kegiatan, laporan isu-isu kinerja keuangan, pengadaan karya. Pergantian ketua ASEANAPOL akan berlangsung pada setiap pertemuan secara bergiliran. Markas besar Sekretariat ASEANAPOL berada di Kuala Lumpur dengan menempatkannya di Markas besar Polis Diraja Malaysia (PDRM).

Keberadaan ASEANAPOL diharapkan dapat membantu menjaga stabilitas serta memerangi tindak kejahatan transnasional yang ada di kawasan dan meningkatkan kerjasama serta menguatkan komitmen antar-penegak hukum se-ASEAN dalam mengantisipasi kejahatan transnasional. Hasil kerjasama yang dilakukan ASEANAPOL sebagai wadah kerjasama di Asia Tenggara adalah penyelenggaraan *ASEANAPOL Conference*, konferensi tersebut merupakan acara tahunan yang diselenggarakan sebagai wadah pertemuan kepala-kepala kepolisian negara ASEAN dan dilaksanakan secara bergilir di negara-negara ASEAN. Dalam konferensi tersebut membahas isu-isu terkini terkait dengan pencegahan dan penanggulangan kejahatan lintas negara serta peningkatan kemampuan anggota kepolisian di kawasan ASEAN.

Dalam pertemuan *34th ASEANAPOL Conference* yang dilaksanakan pada tanggal 12 – 16 Mei 2014 di Manila, Philippines. EUROPOL telah ditetapkan sebagai *Observer* dengan ASEANAPOL. Lalu pada tanggal 3 September 2015, *Deputy Director Operations at EUROPOL*, Mr Wil van Gemert menyampaikan keinginannya untuk menjadi *Dialogue Partner* dengan menyampaikan *Letter of Intents* antara kedua organisasi kepolisian untuk saling bekerja sama. *Letter of Intents* tersebut kemudian disetujui dan ditandatangani bersama oleh Brigadir Jenderal Yohanes Agus Mulyono selaku *Executive Director of ASEANAPOL Secretariat* di sela-sela pertemuan *85th Interpol General Assembly* pada 8 November 2016 di Bali, Indonesia.

Letter of Intents tersebut bertujuan untuk memperkuat kerjasama antara dua organisasi dan saling mendukung serta memfasilitasi pertukaran praktek yang terbaik dalam keahlian di bidang masing-masing anggota. Penandatanganan tersebut dihadiri oleh Khalid Abu Bakar selaku Kepala Kepolisian Malaysia dan sebagai presiden ASEANAPOL 2016, Lim Kok Thai selaku Wakil Komisaris Kepolisian Singapura dan Wakil Ketua ASEANAPOL 2016. Sebagai kejahatan kelompok yang terorganisir tidak hanya terbatas untuk kawasan di Eropa saja namun melakukan penyelidikan transnasional telah menjadi bahkan lebih penting untuk aparat penegak hukum di Uni Eropa.

Inilah sebabnya mengapa EUROPOL dan ASEANAPOL percaya bahwa kerjasama dengan pihak ketiga adalah elemen kunci dalam memerangi kejahatan transnasional dan memastikan keamanan internal di wilayah masing-masing mereka. Berdasarkan data di atas, Menurut Young (1982) maka terbentuknya rezim ini adalah dengan *negotiated order* yaitu adanya negosiasi antara para aktor EUROPOL dan ASEANAPOL kemudian terjalinnya sebuah kesepakatan bersama antara kedua belah pihak yang dimuat dalam satu syarat dan aturan yang telah disetujui untuk mencapai kepentingan bersama.

B. *Strategic Meeting on Payment Card Fraud*

Penyelenggaraan *Strategic Meeting on Payment Card Fraud* (PCF) merupakan hasil inisiatif EUROPOL untuk bekerjasama dengan ASEANAPOL dalam memberantas kejahatan menggunakan kartu

pembayaran yang dilaksanakan secara bergiliran di empat negara: Singapura, Malaysia, Thailand dan Indonesia. *Strategic Meeting on Payment Card Fraud* yang telah dilakukan oleh EUROPOL dan ASEANAPOL adalah sebuah rezim keamanan digital dalam kerjasama untuk memerangi kejahatan dengan penggunaan kartu pembayaran. EUROPOL dan ASEANAPOL menyadari bahwa kejahatan dengan menggunakan kartu pembayaran merupakan kejahatan yang mengalami kerugian terbanyak dengan tingkat resiko yang rendah serta mengancam keamanan internasional suatu negara. Sehingga menjadikan kerjasama multipihak merupakan prioritas utama dalam memerangi tindak *cybercrime.*

1. *The 1st PCF* di Singapura, 11 – 12 November 2015

Pada tanggal 11 – 12 November 2015, dalam *Interpol Global Complex for Innovation* (IGCI) di Singapura menghadirkan 18 orang ahli dari anggota Uni Eropa (Bulgaria, Perancis, Jerman, Romania) dan ASEANAPOL selama dua hari untuk mendiskusikan penipuan dengan menggunakan kartu pembayaran yang semakin meluas serta penarikan uang secara illegal di Asia Tenggara.

Dalam pertemuan tersebut diselenggarakan oleh EUROPOL, INTERPOL dan bekerjasama dengan petugas penghubung EUROPOL yang baru diangkat sebagai pendamping untuk IGCI yaitu bantuan Delegasi Uni Eropa di Singapura serta dukungan lembaga keuangan dari pemerintah Romania. Penipuan dengan kartu pembayaran merupakan bagian dari *cybercrime* yang menjadi salah satu dari sembilan prioritas utama Uni Eropa untuk kejahatan

terorganisir dan kejahatan internasional yang sudah disahkan oleh Dewan Uni Eropa

Tujuan dalam kegiatan ini adalah meningkatkan kesadaran di kalangan para ahli mengenai *skimming card* dan penggelapan uang dengan penarikan uang dari kartu pembayaran berdasar pada modus operandi yang terbarukan. Serta menangani kelompok-kelompok kejahatan terorganisir untuk mempertahankan keamanan di Eropa dan seluruh dunia. Dalam hal ini pendekatan multi-pihak adalah kunci utama seperti yang disampaikan pada komitmen yang diambil oleh semua anggota termasuk INTERPOL, ASEANAPOL, dan sektor swasta yang diwakili oleh *European* ATM *Security Team* (EAST) yang menyediakan aparat penegak hukum dengan komprehensif dalam menanggapi situasi global saat ini.

Meskipun terkait kasus penipuan ATM dalam Uni Eropa menurun sebesar 26% pada tahun 2014, kerugian keseluruhan naik menjadi 13%. Hal ini disebabkan karena penarikan uang diluar yurisdiksi Uni Eropa dimana keamanan EMV (chip dan pin) belum diimplementasikan dengan sepenuhnya, terutama Amerika dan Asia Tenggara – Indonesia dan Filipina khususnya. Beberapa kelompok kejahatan terorganisir tersebut mendirikan pangkalan permanen di lokasi tersebut untuk memfasilitasi kegiatan mereka.

ASEANAPOL yang diwakili oleh direktur untuk layanan polisi, ACP Mohamad Anil Shah menghadiri dan memberikan presentasi pada pertemuan tersebut. Yaitu membahas kerjasama

kepolisian yang ditujukan untuk mengidentifikasi dan menangkap penjahat dari Eropa yang bertanggung jawab untuk penarikan tunai ilegal di Asia. Hal tersebut dilakukan dengan menyediakan platform untuk negara-negara perwakilan dari pasukan kepolisian dari negara-negara anggota Uni Eropa, yang didukung oleh EUROPOL dalam menyajikan masalah dan saling bertukar informasi dengan Polisi di Asia dalam bidang tersebut dan untuk bekerja sama serta untuk melawan jaringan kriminal yang terlibat dalam tipe kejahatan dengan kartu pembayaran.

2. *The 2nd PCF* di Malaysia, 22 – 23 Maret 2016

Pada tanggal 22 – 23 Maret 2016, Europol's European Cybercrime Centre (EC3) ikut serta menghadiri PCF bersama dengan ASEANAPOL dan INTERPOL dan dukungan penuh dari Kepolisian Rumania serta Kepolisian Malaysia dalam mengatur pertemuan yang kedua membahas kasus kejahatan dengan kartu pembayaran di Kuala Lumpur, Malaysia.

Pertemuan yang dilakukan dua hari bersama dengan 25 aparat penegak hukum dari negara-negara anggota Uni Eropa (Bulgaria, Jerman, Yunani, Rumania dan Inggris) dengan ASEANAPOL (Brunei, Kamboja, Indonesia, Malaysia, Myanmar, Filipina, Singapura, Thailand dan Vietnam) untuk membahas kerjasama dalam mencegah dan memerangi jenis kejahatan dengan kartu pembayaran, meningkatkan kesadaran antara para pakar ahli tentang semua jenis pembayaran non tunai, termasuk alat yang

digunakan untuk *skimming card,* ATM malware dan penipuan lewat internet. Modus operandi terbaru yang didapatkan unit investigasi dilaporkan dan dibagikan antar para ahli serta membahas kasus-kasus yang melibatkan para pelaku Eropa yang aktif di Asia.

Bergabungnya EC3 dan dihadirinya 25 aparat penegak hukum menjadikan perubahan rezim sangat kuat. Kepala EC3 Steven Wilson, mengatakan: "Europol's Eropa Cybercrime Centre memiliki sejarah yang panjang dalam mengambil langkah-langkah proaktif untuk membantu lembaga penegak hukum di Uni Eropa serta untuk memerangi penipuan kartu pembayaran. Pertemuan strategis pertama yang sukses diadakan di Singapura pada November tahun 2015, yaitu memulai penyelidikan bersama di Uni Eropa dan Asia dan mendorong sesi kedua ini dengan tujuan untuk membangun jaringan antar wilayah untuk membantu penyelidikan internasional. EUROPOL mengakui beratnya ancaman global dalam penipuan dengan kartu pembayaran dan akan terus membantu lembaga penegak hukum dalam memeranginya.

3. *The 3rd PCF* di Thailand, 13 – 14 Desember 2016

Pada tanggal 13 – 14 Desember 2016, kembali Europol's Cybercrime Eropa Centre (EC3), bersama dengan ASEANAPOL dan INTERPOL, dan dengan dukungan dari Kepolisian Rumania dan Kepolisian Thailand mengadakan pertemuan yang ketiga di Bangkok, Thailand. Pertemuan tersebut diselenggarakan oleh

Electronic Transaction Development Agency (ETDA) dan Kementrian Ekonomi Digital dan Sosial.

Tiga puluh aparat penegak hukum dari empat anggota Uni Eropa (Austria, Perancis, Yunani dan Rumania) dan mitra Asean (Brunei, Kamboja, Indonesia, Malaysia, Myanmar, Filipina, Singapura dan Thailand) berpartisipasi dalam pertemuan dua hari tersebut untuk membahas rangkuman hasil dalam memerangi kejahatan *cyber* yang sudah dilaksanakan bersama-sama.

Pertemuan ini difokuskan pada pertukaran keahlian di bidang pencegahan dan mengatasi penipuan lewat ATM, pencurian data, ATM malware, dan penipuan lewat situs *e-commerce.* Mayor Jenderal Polisi Chayout Rattanaubol dari pusat biro Investigasi Kepolisian Thailand membahas isu-isu ancaman dalam sistem pembayaran digital dan perlunya sebuah aliansi global yang kuat untuk menghadapi kasus PCF. Keamanan transaksi elektronik sangat penting untuk bisnis dan pelanggan dan ini tidak dapat dicapai tanpa kerjasama internasional yang kuat antara publik dan sektor swasta. Pertemuan tersebut telah memberikan dampak bagi aparat penegak hukum dan masyarakat dengan gambaran yang komprehensif tentang penipuan dengan kartu pembayaran dan bagaimana kejahatan itu berkembang secara global.

Pertemuan ketiga ini membangun setup jaringan antar wilayah untuk mempermudah penyelidikan internasional yang menargetkan PCF. Bergabungnya Organisasi Internasional seperti

ETDA, LiquidNexxus dan peran aktif *Computer Emergency Response Teams* (CERTs) mempersempit ruang gerak para pelaku PCF dengan melakukan koordinasi penanganan insiden yang melibatkan pihak bersama.

4. *The 4th PCF* di Jakarta, 19 – 20 Juli 2017

Pada tanggal 19 - 20 Juli 2017, Pertemuan ke empat diadakan di Jakarta, Indonesia. DSP Saralathan Duraisamy yang mewakili sekretaris ASEANAPOL dan partisipan dari Brunei, Indonesia, Malaysia, Thailand dan Vietnam telah menghadiri pertemuan tersebut termasuk EUROPOL, INTERPOL dan lembaga aparat penegak hukum.

Kerjasama yang dilakukan adalah dengan terbentuknya EuroAsean+ Network sebagai hasil kesepakatan selama empat kali pertemuan dan kerjasama antar jaringan untuk memudahkan investigasi antar negara dengan EUROPOL, INTERPOL, ASEANAPOL sebagai fasilitatornya dan didukung langsung oleh *European Association for Secure Transactions* (EAST).

C. Perubahan Rezim dalam *Strategic Meeting on Payment Card Fraud*

Dalam setiap pertemuan yang telah dijelaskan diatas terdapat tujuan dan fungsi yang berbeda serta mengalami perubahan hasil kerjasama yang berbeda dalam setiap pertemuan, maka perubahan rezim terjadi dalam 4 cara menurut Haggard (1987: 496-498) yaitu:

1. Kekuatan

Dalam teori Haggard (1987), kekuatan suatu rezim diukur dari tingkat kepatuhan masyarakat terhadap aturan dan perintah atas rezim tersebut. Semakin tidak sejalannya aturan rezim dalam masyarakat akan menyebabkan pergantian rezim atau runtuhnya rezim. Dilihat dari pertemuan pertama yang hanya dihadiri 18 ahli dari UE (Bulgaria, Perancis, Jerman, Rumania) dan anggota ASEAN (Indonesia, Filipina, Thailand, Vietnam), kemudian pada pertemuan kedua dihadiri oleh 25 para ahli penegak hukum (Bulgaria, Jerman, Yunani, Rumania, Inggris) termasuk anggota lengkap ASEANAPOL, juga dihadiri EAST sebagai penyedia para ahli penegak hukum.

Pada pertemuan ketiga, INTERPOL kembali bergabung bersama Kepolisian Rumania dan Thailand, dan menghadirkan 30 para ahli penegak hukum dari UE serta semakin banyak di ikuti organisasi internasional seperti EAST, ETDA, CERTs, LiquidNexxus, Bank Thailand dan komersial bank lainnya. Pada pertemuan keempat di Jakarta, berdasarkan dari pertemuan pertama sampai ke tiga terbentuklah EURASEAN yang beranggotakan para ahli penegak hukum di Uni Eropa dan 10 negara ASEAN (Brunei, Kamboja, Indonesia, Laos, Malaysia, Myanmar, Filipina, Singapura, Thailand dan Vietnam) dengan bantuan

dari *European Association for Secure Transactions (EAST)* yang mewakili sektor swasta serta dengan dukungan penuh dari EUROPOL, ASEANAPOL dan INTERPOL.

Dengan semakin banyak yang bergabung dalam setiap pertemuan baik menjadi tenaga ahli untuk bertukar pendapat maupun penyedia fasilitator untuk kelangsungan pertemuan PCF tersebut dan dukungan penuh dari lembaga penegak hukum yang semakin banyak jumlahnya, serta terbentuknya EURASEAN menjadikan rezim menjadi semakin kuat dengan patuhnya aktor-aktor dibalik rezim tersebut dalam menjalankan kerjasama demi mencapai kepentingan bersama. Peran serta EURASEAN sebagai organisasi internasional menjadikan aktor yang mendukung dalam mempersempit ruang gerak para penjahat di dunia maya yaitu dengan bentuk aksi *ATM malware*, *Barber, Cloning connection, fraud migration-ATM cash outs, ATM logical attacks, sharing CCTV catalogue.*

2. Bentuk Organisasi

Dijelaskan menurut teori Haggard (1987), bahwa dalam kerjasama yang komplek membutuhkan struktur organisasi yang baik dan independen. Kerjasama yang telah dilakukan oleh EUROPOL dilaksanakan bersama-sama dengan negara anggota ASEANAPOL secara bergiliran menuntut adanya perubahan rezim yang lebih dinamis sesuai

dengan masalah *cybercrime* yang semakin komplek. Dimulai dari awal pertemuan sampai pertemuan yang ketiga dengan struktur organisasi yang kecil dengan membahas modus operandi, meningkatkan kewaspadaan, pengenalan ATM *malware*, kemudian berkembang lebih luas dalam bentuk organisasi dengan munculnya aktor-aktor baru dalam pertemuan PCF seiring dengan meningkatnya kejahatan PCF yang ditangani oleh setiap aktor.

Dalam pertemuan yang terakhir, yang awalnya pertemuan hanya membahas tindak kejahatan PCF sekarang mulai melakukan giat operasi dalam pemberantasan secara spesifik, yang didukung langsung oleh EURASEAN sebagai hasil dari empat pertemuan yaitu *Join Investigation* dan *Join Actions*, adalah sebuah tim investigasi gabungan sebagai alat kerjasama internasional ASEANAPOL dan EUROPOL berdasarkan kesepakatan untuk melaksanakan penyidikan dalam satu atau lebih dari negara-negara yang terlibat.

Tantangan dalam pengembangan kebijakan *cybersecurity* ke depan adalah sifat dari ancaman *cyber* yang multidimensional sehingga penanganannya tidak hanya menjadi tanggung jawab Polri tetapi oleh semua pihak anggota rezim. Dengan perubahan struktur organisasi yang semakin meluas ini menjadikan ruang gerak para penegak hukum semakin luas, sehingga berbagai fasilitas, *capacity*

building dan pertukaran informasi lebih mudah dilaksanakan dalam mengatasi tindak kejahatan *cybercrime* bersama para aktor organisasi internasional lain didalamnya.

3. Ruang Lingkup

Haggard (1987), menjelaskan bahwa ruang lingkup suatu rezim akan perubahan isu-isu yang luas dapat meningkatkan biaya administrasi, namun akan mempermudah proses negosiasi dalam satu hubungan antar isu. Dalam pertemuan PCF yang pertama diselenggarakan di Singapura sebagai tuan rumah dengan bantuan penuh dari lembaga keuangan Singapura, Kepolisian Rumania serta Delegasi Uni Eropa untuk Singapura. Tujuan dalam pertemuan pertama ini adalah fokus meningkatkan kewaspadaan terhadap *card skimming,* penarikan uang di luar negeri dan *ATM Malware.*

Pertemuan kedua diselenggarakan di Malaysia dengan kerjasama antara Kepolisian Rumania dan Kepolisian Malaysia sebagai aktor utama dalam membahas kejahatan menggunakan kartu pembayaran di Malaysia, penipuan menggunakan internet, penipuan menggunakan perdagangan elektronik dan penipuan pembayaran tiket transportasi. Pada pertemuan ketiga, Thailand sebagai tuan rumah membahas pertukaran keahlian dalam bidang pencegahan dan cara mengatasi penipuan lewat ATM serta situs-situs *e-commerce,*

dan membangun setup jaringan antar wilayah untuk mempermudah penyelidikan internasional antar EUROPOL dan ASEANAPOL. Pada pertemuan terakhir dilaksanakan di Jakarta, dan memprakarsai terbentuknya EURASEAN sebagai hasil utama dalam empat kali pertemuan.

Perubahan yang terjadi dalam pertemuan PCF selama empat kali tersebut adalah dengan terbentuknya *EuroAsean+ Network* sehingga ruang lingkup pembahasan menjadi lebih luas dengan tindakan proaktif dalam mengatasi PCF seperti membangun setup jaringan bersama, bergabung dalam tim investigasi dan latihan bersama dengan para ahli di EU. Pembentukan EURASEAN ini mempermudah para aktor dalam suatu rezim untuk mengembangkan kapasitasnya dan perbedaan masalah isu-isu yang berkembang akan mudah diselesaikan bersama oleh anggota rezim. Perlunya ruang lingkup yang luas dalam perubahan rezim ini adalah adanya perbedaan kepentingan dan isu-isu dalam kejahatan *cybercrime* yang berkembang antar tiap negara anggota.

4. Modus Alokasional

Haggard (1987) berpendapat bahwa suatu rezim yang berorientasi pada otoritatif alokasi sumber daya pribadi dalam setiap anggota akan menghambat proses kontrol nasional dalam rezim tersebut, demikian juga apabila suatu rezim mengkontrol langsung sumber daya setiap anggota

> rezim akan menuntut struktur organisasi yang lebih luas. Dalam pertemuan PCF tersebut rezim mendukung pada pengalokasian sumber daya dengan kontrol penuh atas rezim tersebut, dan menuntut struktur organisasi yang luas dengan bergabungnya aktor-aktor baru dalam rezim ini sebagai bentuk tindakan nyata atas rezim dalam menciptakan kemanan kawasan. Modus alokasional ini bisa dilihat dari setiap pertemuan yang difasilitasi langsung oleh rezim dalam membangun kapasitas bersama, mendatangkan para ahli, tempat dalam bertukar informasi, membangun jaringan antar wilayah dalam membantu penyelidikan internasional seperti EC3, EAST, ETDA dan terciptanya EURASEAN. Dengan adanya alokasi sumber daya atas kontrol rezim ini, menjadikan rezim keamanan digital menjadi lebih kuat.

Untuk melihatnya suatu perubahan dalam rezim menurut Owen (2010: 35-41) adalah dengan menganalisis terhadap perkembangan dalam perubahan kepentingan dalam setiap pertemuan, kerugian dan keuntungan dalam kerjasama yang dilakukan serta perubahan kebutuhan publik yang semakin berkembang.

Berdasarkan data diatas, terkait dengan kerjasama internasional dalam bidang *cybersecurity*. Asia Tenggara mendapat keuntungan dalam perkembangan sistem kartu pembayaran menggunakan EMV yaitu proteksi akan data pemilik kartu dengan menggunakan chip dan pin, serta saling bertukar informasi terkait para pelaku yang tersebar di seluruh kawasan

Asia Tenggara maupun Uni Eropa, dan modus operandi yang terbaru dimana EUROPOL memiliki peralatan yang lebih canggih dengan teknologi yang super maju dan penggunaan *face recognition* dalam satu sistem yang saling terhubung dengan EUROPOL, INTERPOL dan ASEANAPOL yaitu *EuroAsean+ Network* (EURASEAN).

Hasil kerjasama lain yang telah dilakukan antara lain *capacity building* dengan program pelatihan dan sebagai pembanding materi dalam *cybersecurity* antar para ahli penegak hukum maupun organisasi internasional lainnya. Adanya *Joint Investigation* sesuai peraturan perundang-undangan yang berlaku termasuk pendanaan dari EUROPOL apabila terdapat tindak pidana yang terjadi dan melibatkan minimal dua negara yang tergabung dalam EUROPOL. Secara khusus EUROPOL juga mengadakan kegiatan penanganan PCF di Markas EUROPOL Belanda pada tanggal 20 – 21 November 2017, Dittipidsiber Bareskrim Polri menunjuk Kompol Hans Papahit dan Brig. Bambang H. Siregar namun tidak hadir dalam kegiatan tersebut karena permasalahan teknis korespondensi pada email resmi Dittipidsiber yang tidak bisa diakses oleh Kompol Hans Papahit sehingga menyebabkan kerugian tersendiri bagi pihak Indonesia.

Berdasarkan pada hasil rapat pertemuan *Strategic Meeting on PCF*, perubahan rezim ASEANAPOL yang sebelumnya hanya berfungsi sebagai pusat pengumpul data melalui database *ASEANAPOL Database System (e-Ads)* diharapkan dapat mendekati kapasitas EUROPOL sebagai rezim internasional yang kuat dalam menciptakan kawasan yang aman.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan pemaparan mengenai Kerjasama Kepolisian Lintas Negara Dalam Mengatasi Kejahatan *Credit Card Fraud (Carding),* diperoleh kesimpulan bahwa :

1. Berkembangknya teknologi informasi dan komunikasi masa kini tidak hanya memberikan dampak positif, namun juga memberikan dampak negatif dalam setiap aspek kehidupan manusia. Semakin mudahnya akses internet dan fitur-fitur yang disediakan menciptakan wadah untuk melakukan tindak *cybercrime* dengan segala bentuk dan modus yang baru.

2. *Carding* merupakan kejahatan lintas negara yang menjadi salah satu ancaman serius dalam keamanan dunia sehingga memerlukan kerjasama internasional dalam menangani kasus tersebut.

3. Rezim Internasional dalam pertemuan *Strategic Meeting on Payment Card Fraud* merupakan wadah bagi EUROPOL dan ASEANAPOL untuk mengatur hubungan dalam kerjasama untuk menciptakan keamanan kawasan masing-masing negara anggota.

4. Dalam pertemuan *Payment Card Fraud,* perubahan rezim yang terjadi dengan terbentuknya EURASEAN sebagai bentuk *Join*

Actions dan *Joint Investigation* dalam mengatasi kejahatan dengan menggunakan kartu pembayaran.

B. Saran

Dari kesimpulan di atas ternyata masih banyak kelemahan dalam penulisan skripsi Kerjasama Kepolisian Lintas Negara Dalam Mengatasi Kejahatan *Credit Card Fraud (Carding).* Maka dari itu peneliti memiliki beberapa saran :

1. Penelitian ini berfokus pada kerjasama kepolisian lintas negara dengan *Strategic Meeting on Payment Card Fraud* pada tahun 2015. Sehingga penelitian ini bisa digunakan untuk penelitian lanjutan dengan rentang waktu terbaru
2. Analisis kerjasama ini berfokus pada tahun 2015 sedangkan upaya terkait kerjasama yang dilakukan adalah jangka panjang untuk mengetahui perkembangan selanjutnya selama berjalannya kerjasama ini.

DAFTAR PUSTAKA

Sumber Pustaka:

Broto Wardoyo. 2015. *Perkembangan, Paradigma, dan Konsep Keamanan Internasional & Relevansinya untuk Indonesia.* PT Nugra Media

Haggard, Stephan, and B. A. S. (1987). *Theories of International Regimes. International Organization.* Harvard University's DASH repository

J.G. Starke. 2010. *Pengantar Hukum Internasional*. PT Sinar Grafika. Hal 3.

John M. Owen IV. 2010. *The Clash of Ideas in World Politics Transnational Networks, States, and Regime Change, 1510–2010.* Princeton University Press, 41 William Street

John, W. Creswell. 1994. *Research Design: Qualitative and Quantitative Approaches*. Thousand Oaks, Sage Publications, Inc. Hal 148

Josua Sitompul. 2012. *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*. PT Tatanusa, Hal 103

K.J Holsti. 1988. *Politik Internasional, Kerangka Untuk Analisis,* Jilid II, Terjemahan M. Tahrir Azhari. Jakarta: Erlangga.

Kusumaatmadja, Mochtar dan Etty R. Agoes. 2003. *Pengantar Hukum Internasional*. Jakarta. Alumni.

Samuel C. McQuade, 2009. *"Cybercrime", Encyclopedia of Cybercrime*, Greenwood Press, United State of America.

Sandu, Sinyoto. 2015. *Dasar Metodologi Penelitian*. Cetakan ke 1. Yogyakarta.

Sefriani. 2010. *Hukum Internasional*. Rajawali Press. Hal 2.

Walt, Stephen M. 1991. *The Renaissance of Security Studies*.

Widodo. 2013. *Aspek Hukum Pidana Kejahatan Mayantara.* Aswaja Pressindo, Yogyakarta.

Young, Oran R. 1982. *Regime Dynamics: The Rise and Fall of International Regimes*. The MIT Press, Vol. 36, No. 2, pp. 277-297.

Sumber Jurnal Ilmiah:

Abdullah Tulip. *Kerjasama Indonesia dengan Negara-Negara Tetangga Dalam Pemberantasan Kejahatan Transnasional*, Universitas Sriwijaya, 2009.

Aloysius Wisnubroto. *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya, Yogyakarta, 1999.

Handrini Ardiyanti. *Cybersecurity dan Tantangan Pengembangannya di Indonesia*. (P3DI) Setjen DPR RI, 2014

Hius, Saputra dan Nasution. *Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku.* Prosiding SNIKOM Banda Aceh, 2014

Lita Sari Marita. *Penerapan Cyber Law Dalam Pemberantasan Cyber Crime di Indonesia,* AMIK Bina Sarana Informatika Jakarta, 2015

Obsatar Sinaga. *Penanggulangan Kejahatan International Cyber Crime Di Indonesia*. Universitas Padjadjaran Bandung, 2010

Starlet Rallysa Injaya. *Kerjasama Internasional Indonesia dan Jepang Terhadap Isu Deforestasi di Indonesia Dalam Skema Asia Foret Partnership (AFP) Periode 2008-2011,* Universitas Islam Negeri Syarif Hidayatullah Jakarta, 2013

Sumber Artikel Ilmiah:

Evi Lestari, S. 2014. Kajian Yuridis Pembuktian Kejahatan Mayantara (Cybercrime) Dalam Lingkup Transnasional. Diakses dari https://jurnal.usu.ac.id/index.php/jmpk/article/viewFile/8413/3651, pada tanggal 12 Juli 2018 pukul 12:44 WIB.

Indonesian Defense University, *Technology Perscpetive: National Cyber Security.* http://binkorpspelaut.tnial.mil.id/index.php?option=com_docman&task=doc_download&gid=6&Itemid=22. diakses 17 April 2018 pukul 15:40 WIB.

Surya Dharma. 2008. *Pendekatan, Jenis dan Metode Penelitian Pendidikan*. Diakses dari http://staff.uny.ac.id/sites/default/files/PENELITIAN%20PENDIDIKAN.pdf, pada tanggal 18 Juli 2018 pukul 13:43 WIB.

Suryana. 2010. *Metodologi Penelitian: Model Praktis Penelitian Kuantitatif dan Kualitatif.* Universitas Pendidikan Indonesia. Diakses dari https://simdos.unud.ac.id/uploads/file_penelitian_1_dir/23731890cdc8189968cf15105c651573.pdf, pada 19 Juli 2018 pukul 13:00 WIB.

Sumber Media Elektronik:

ACORN. *Learn about cybercrime* https://www.acorn.gov.au/learn-about-cybercrime, Pada tanggal 29 Agustus 2018 pukul 13:29 WIB.

ASEANAPOL. 2019. *Organisational structure of Aeanapol* http://www.aseanapol.org/about-aseanapol/governance, Pada tanggal 20 Februari 2019 pukul 10.20 WIB

CNN Indonesia. 17 Juli 2018. *Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia*. Diakses dari https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia, Pada 19 September 2018 pukul 11:03 WIB.

CNN Indonesia. 30 Desember 2016. *Cyber Crime kasus kejahatan terbanyak di 2016.* Diakses dari https://www.cnnindonesia.com/nasional/20161230232449-12-183255/cyber-crime-kasus-kejahatan-terbanyak-di-2016, pada 12 Juli 2018 pukul 12:08 WIB.

Detik inet. 10 Juni 2014. *Indonesia Gawat Darurat Cyber Crime.* Diakses dari http://inet.detik.com/security/d-2604562/indonesia-gawat-darurat-cyber-crime/2, pada 12 Juli 2018 pukul 14:17 WIB.

Detik news. 24 Mei 2016. *Kapolri: Kerja Sama Antarnegara Penting untuk Basmi Kejahatan Transnasional*. Diakses dari https://news.detik.com/berita/3216308/kapolri-kerja-sama-antarnegara-penting-untuk-basmi-kejahatan-transnasional, pada 17 Juli 2018 pukul 13:10 WIB.

Detik. 20 Maret 2018. *Pelaku Spamming dan Carding Dibekuk Bobol Kartu Kredit Rp 500 Juta*. Diakses dari https://news.detik.com/berita-jawa-timur/d-3927140/pelaku-spamming-dan-carding-dibekuk-bobol-kartu-kredit-rp-500-juta , pada 12 Juli 2018 pukul 13:53 WIB.

Direktorat KIPS. 20 Januari 2016. *Penanggulangan Kejahatan Lintas Negara Teroganisir*. Diakses dari https://www.kemlu.go.id/id/kebijakan/isu-khusus/Pages/Penanggulangan-Kejahatan-Lintas-Negara-Teroganisir.aspx, pada 17 Juli 2018 pukul 13:00 WIB.

European Commission. 2018. *Cybercrime.* Diakses dari https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en, pada 31 Juli 2018 pukul 14.00 WIB.

EUROPOL. 2019. *Helping make Europe safer*. Diakses dari https://www.europol.europa.eu/about-europol, Pada 20 Februari 2019

INFOSEC. 25 Februari 2016. *Cyber Laws of India*. Diakses dari https://infosecawareness.in/cyber-laws-india, Pada 29 Agustus 2018 pukul 13:19 WIB.

ITU. *The Global Security Index 2017.* Diakses dari https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx, Pada 29 Agustus 2018 pukul 13.00 WIB.

Kompas. 11 Januari 2017. *Apa Urgensinya Badan Siber Nasional untuk Indonesia*. Diakses dari https://nasional.kompas.com/read/2017/01/11/06591651/apa.urgensinya.badan.siber.nasional.untuk.indonesia. Pada 10 Oktober 2018 pukul 14.01 WIB.

Kompas. 21 November 2017. *Keamanan Siber Indonesia Tak Lebih Baik Dibandingkan Malaysia dan Singapura.* Diakses dari https://nasional.kompas.com/read/2017/11/21/20480051/keamanan-siber-indonesia-tak-lebih-baik-dibandingkan-malaysia-dan-singapura, pada 17 Juli 2018 pukul 14:20 WIB.

Kompasiana. 17 Juni 2015. *Teknologi Cyber, Cyberspace.* https://www.kompasiana.com/lamigos/557217f3307a614e38ad23ca/teknologi-cyber-cyberspace, pada 31 Juli 2018 pukul 14.13 WIB.

Lauren Moraski, 2011, *Cybercrime Knows No Borders*. Diakses dari http://www.infosecuritymagazine.com/view/18074/cybercrime-knows-no-borders-/, pada 14 Juli 2018 pukul 13:10 WIB.

Liputan6. 21 Maret 2018, *Dasar 'Tuyul', Begini Cara Jaringan Kolam Tuyul Bobol Kartu Kredit.* Diakses dari https://www.liputan6.com/regional/read/3393459/dasar-tuyul-begini-cara-jaringan-kolam-tuyul-bobol-kartu-kredit, Pada 20 September 2018 pukul 12:34 WIB.

Malikkul Shaleh. 9 Juli 2009. *Penanganan Kejahatan Transnasional Perlu Kolaborasi Kuat Antarnegara.* Diakses dari http://news.unpad.ac.id/?p=29203, pada 14 Juli 2018 pukul 14:40 WIB.

NCB-Interpol Indonesia. 2 Januari 2013. *Cybercrime: Sebuah Fenomena Di Dunia Maya*. Diakses dari http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-dunia-maya/89-cybercrime-sebuah-fenomena-di-dunia-maya, pada 12 Juli 2018 pukul 14:04 WIB.

OKE zone. 29 Desember 2017. *Kapolri Sebut Kejahatan Siber Meningkat di Tahun 2017.* Diakses dari https://news.okezone.com/read/2017/12/29/337/1837388/kapolri-sebut-kejahatan-siber-meningkat-di-tahun-2017, Pada 17 Juli 2018 pukul 14:35 WIB

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS SLAMET RIYADI
Jl. Sumpah Pemuda No. 18 Kadipiro Surakarta Telp. (0271) 853839

SURAT TUGAS MEMBIMBING SKRIPSI
Nomor : 262 / S4 / AK / 2017

Dekan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Slamet Riyadi Surakarta, dengan ini menugaskan :

1. Nama	: Dr. Ganjar Widhiyoga, Phd
Pangkat/golongan	: Penata Muda Tk. I / III - B
Jabatan Akademik	: Asisten Ahli
Status	: Pembimbing Utama
2. Nama	: Halifa Haqqi, S.IP. M.Si.
Pangkat/golongan	: Penata Muda Tk. I / III - B
Jabatan Akademik	: Asisten Ahli
Status	: Pembimbing Pendamping

Untuk MEMBIMBING SKRIPSI SARJANA bagi mahasiswa :

Nama	: Albet Nego
NIM / NPM	: 14430018
Jurusan	: Ilmu Hubungan Internasional

Demikian untuk dilaksanakan dengan sebaik-baiknya.

Surakarta, 21 Nopember 2017
Dekan,

Drs. Buddy Riyanto, M.Si.
NIPY. 0191.0139.

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS SLAMET RIYADI

Jl. Sumpah Pemuda No. 18 Kadipiro Surakarta Telp. (0271) 857879

Nomor : / I / FISIP/ 2007

Lampiran : -

Hal : Undangan Seminar Proposal

Kepada Yth. : 1. Gayar Wahyogo, S.IP, M.Si, Ph.D

2. Halifa Maggi, S.IP, M.Si

Fakultas Ilmu Sosial dan Ilmu Politik

Universitas Slamet Riyadi

Surakarta

Mohon dengan hormat kehadiran Bpk/Ibu besuk pada :

Hari / tanggal : Selasa 14 agustus 2007

Pukul : 10.00

Tempat : Fakultas Ilmu Sosial dan Ilmu Politik

Keperluan : Seminar Proposal

Atas nama mahasiswa :

Nama : Albert Nego

NIM/NPM : 14430018

Jurusan : Ilmu Hubungan Internasional

Atas perhatian dan kehadiran saudara kami ucapkan terima kasih.

Surakarta,

An. Dekan

Satgas,

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS SLAMET RIYADI

Jl. SumpahPemudaNo.18 Joglo KadipiroSurakartaTelp. (0271)857757

Nomor : 23/ S4 / AK / 2019
Lampiran
Perihal : Undangan Menguji Skripsi

Yth. : 1. Ganjar Widhiyoga, SIP. M.Si Ph.D
2. Halifa Haqqi. SIP. M.Si.
3. Dra. Christy Damayanti, M.Si.

Dengan hormat,

Mohon Kehadiran Saudara besok pada

2

Hari/Tgl. : Selasa, 20 Agustus 2019
Pukul : 10.00 WIB
Tempat : Ruang Sidang Fisip
Keperluan : **Menguji Skripsi**
Nama : Albet Nego
NPM : 14430018
Jurusan : Ilmu Hubungan Internasional.

Atas Perhatian dan kehadiran saudara kami ucapkan terima kasih

Surakarta 13 Agustus 2019
Dekan,

Drg. Raddy Riyanto, M.Si.
NIK. 0191 . 0139.