UNIVERSITAS PERTAHANAN

SINERGITAS BSSN DAN KOMINFO DALAM MENINGKATKAN KESIAPAN *CYBER SECURITY* PADA SEKTOR *E-COMMERCE* DI INDONESIA

TESIS

PATHRESIA MARLINA SILALAHI
NIM: 120170102015

Tesis yang ditulis untuk Memenuhi Sebagian Persyaratan
dalam Mendapatkan Gelar Magister Pertahanan

FAKULTAS STRATEGI PERTAHANAN
PROGRAM STUDI PEPERANGAN ASIMETRIS

BOGOR
Maret 2019

LEMBAR PENGESAHAN

Tesis ini diajukan oleh:

Nama	:	Pathresia Marlina Silalahi
NIM	:	120170102015
Program Studi	:	Peperangan Asimetris
Judul Tesis	:	**Sinergitas BSSN dan Kominfo Dalam Meningkatkan Kesiapan *Cyber Security* Pada Sektor *E-Commerce* di Indonesia**

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Magister dalam Ilmu Pertahanan pada Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Universitas Pertahanan

DEWAN PENGUJI

Pembimbing I : Fetri Miftach, Ph.D., C.Eng., MBCS ( )

Pembimbing II : Kolonel Caj. Dr. Surryanto D. W., M.H, M.M ( )

Penguji I : Laksamana Pertama TNI DR. Suhirwan, M.MT( )

Penguji II : Brigjen TNI DR. Moch. Afifuddin, M.Si (Han) ( )

Penguji III : Letkol Inf. Dr. Triyoga Budi Prasetyo, M.Si ( )

Ditetapkan di : Bogor
Tanggal : Maret 2019

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya atau bagian karya yang pernah ditulis ataupun diajukan orang lain untuk memperoleh gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang pengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraf, subbab, atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis dirujuk dalam naskah ini dan disebutkan dalam daftar Referensi.

Apabila di kemudian hari terbukti bahwa terdapat plagiat dalam tesis ini saya bersedia menerima sanksi sesuai ketentuan peraturan dan undang-undang yang berlaku.

Bogor, Maret 2019

Pathresia Marlina Silalahi

120170102015

PERNYATAAN PERSETUJUAN PUBLIKASI

TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pertahanan, saya yang bertanda tangan di bawah ini:

Nama : Pathresia Marlina Silalahi
NPM : 120170102015
Program Studi : Peperangan Asimetris
Fakultas : Strategi Pertahanan
Jenis Karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pertahanan Hak Bebas Royalti Non-ekskulusif (Non-exclusive Royalti-Free Right) atas karya ilmiah saya yang berjudul:

Sinergitas BSSN dan Kominfo Dalam Meningkatkan Kesiapan *Cyber Security* Pada Sektor *E-Commerce* di Indonesia

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Pertahanan berhak menyimpan, mengalih media/ formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta/ Karya Intelektual dari Tesis ini.

Demikian pernyataan ini saya buat dengan kesadaran penuh tanpa paksaan dari pihak manapun.

Bogor, Maret 2019

Pathresia Marlina Silalahi

KATA PENGANTAR

Puji syukur peneliti ucapkan kehadirat Tuhan Yang Maha Esa, karena berkat rahmat dan karunia-Nya, penyusunan tesis dengan judul Sinergitas BSSN dan Kominfo Dalam Meningkatkan Kesiapan *Cyber Security* Pada Sektor *E-Commerce* di Indonesia dapat diselesaikan.

Penyusunan tesis ini ditujukan sebagai salah satu syarat dalam memperoleh gelar Magister pada Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Universitas Pertahanan.

Penyusunan tesis ini dapat diselesaikan berkat bantuan dan dukungan dari berbagai pihak baik secara langsung maupun tidak langsung. Untuk itu, pada kesempatan ini peneliti mengucapkan terimakasih kepada :

1. Letnan Jendral TNI Dr. Tri Legionosuko, SIP, MAP Rektor Universitas Pertahanan
2. Mayor Jendral TNI Dr. Hipdizah, S.ADM., M.Si, Dekan Fakultas Strategi Pertahanan
3. Kolonel Kav. Dr. Yusuf, S.Sos, M.M. selaku Sesprodi Peperangan Asimetris
4. Fetri Miftach, Ph.D.,C.Eng.,MBCS selaku Pembimbing I
5. Kolonel Caj. Dr. Surryanto D. W., MH selaku Pembimbing II
6. Suami, anak, orang tua, abang, kakak dan adik tercinta yang telah mendukung penyusunan tesis ini
7. Rekan-rekan teman sekelas Program Studi Peperangan Asimetris Cohort VI Universitas Pertahanan dan rekan-rekan Cohort IX Universitas Pertahanan.

Semoga Tuhan Yang Maha Esa membalas kebaikan-kebaikan berbagai pihak atas bantuannya.

Peneliti menyadari bahwa tesis ini masih kurang sempurna, oleh karena itu, dengan kerendahan hati mengharapkan kritik dan saran yang konstruktif demi menunjang penelitian ini.

Akhirnya, semoga tesis ini dapat memberikan manfaat terhadap pengembangan ilmu pertahanan dan bermanfaat bagi stakeholder terkait dalam upaya meningkatkan kesiapan keamanan siber *e-commerce* di Indonesia.

Bogor, Maret 2019

Pathresia Marlina Silalahi

ABSTRAK

Sinergitas BSSN dan Kominfo Dalam Meningkatkan Kesiapan *Cyber Security* Pada Sektor *E-Commerce* di Indonesia

PATHRESIA MARLINA SILALAHI

Latar belakang dari penelitian ini adalah fenomena pertumbuhan *e-commerce* yang mendorong diterbitkannya peraturan tentang *Road Map E-Commerce,* dimana Kominfo sebagai penanggungjawab atas bidang *cyber security* pada sektor *e-commerce.* Namun kemudian diterbitkan peraturan penunjukan BSSN sebagai badan yang bertanggungjawab atas *cyber security*, sehingga membuat sinergitas kedua instansi tersebut penting dalam meningkatkan kesiapan *cybersecurity* pada sektor *e-commerce* terutama pada aspek hukum dan organisasi. Permasalahan penelitian, yaitu tentang belum adanya sinergitas antara BSSN dan Kominfo dalam penerapan *cyber security* pada sektor *e-commerce* dan aspek-apek yang perlu diperhatikan dalam sinergitas BSSN bersama Kominfo untuk meningkatkan kesiapan *e-commerce* guna mewujudkan ketahanan ekonomi nasional. Tujuan penelitian adalah menganalisis kesiapan dan faktor-faktor penting sinergitas yang dapat meningkatkan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia. Penelitian ini menggunakan metodologi kualitatif dengan pendekatan deskriptif. Data yang diperoleh dari para informan yang telah ditetapkan selanjutnya dianalisis dengan teknis analisis kualitatif. Hasil penelitian menemukan bahwa penerapan *cyber sercurity* pada sektor *e-commerce* Indonesia mengalami keterbatasan dalam hal monitoring dan penindakan serta masih bersifat sektoral. Sinergitas antara BSSN dan Kominfo dalam aspek hukum masih memerlukan regulasi untuk memperjelas pembagian tanggungjawab dan wewenang dalam penerapan *cyber security,* sedangkan dalam aspek organisasi belum memiliki standar koordinasi yang berlaku pada ISO 22301:2012 dan NIST SP 800-61. Kesimpulan yang diperoleh untuk meningkatkan sinergitas pada aspek hukum diperlukan fleksibilitas dalam penyusunan dan penyesuaian regulasi namun memiliki kekuatan penegakan hukum. Pada aspek organisasi diperlukan kesetaraan struktur organisasi diantara lembaga/kementerian terkait sehingga dapat terjalin komunikasi dan koordinasi yang efektif guna meningkatkan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia.

Kata Kunci: *Cyber Security*, *E-Commerce,* Sinergitas, BSSN dan Kominfo.

ABSTRACT

Synergy of BSSN and KOMINFO in Enhancing Cyber Security Readiness in the E-Commerce Sector in Indonesia

PATHRESIA MARLINA SILALAHI

The background of this study is the phenomenon of e-commerce that has growth and has led to the issuance of regulations on the Road Map of E-Commerce, in which Kominfo is responsible for the cyber security sector in the e-commerce sector. Afterwards, there is a regulation that issued BSSN as a institution who responsible for cyber security, thus making the synergy of the two agencies important in increasing cybersecurity readiness in the e-commerce sector, especially in legal and organizational aspects. The research problem is about the lack of synergy between BSSN and Kominfo in the application of cyber security at the e-commerce sector and the aspects that need to consider in the synergy of BSSN and Kominfo in order to improve e-commerce readiness for enhancing national economic resilience. The purpose of the study was to analyze preparedness and important factors of synergy that could improve cyber security readiness in the e-commerce sector in Indonesia. This study uses a qualitative methodology with a descriptive approach. Data obtained from the informants that have been determined has analyzed by technical qualitative analysis. The results of the study found that the application of cyber security in the e-commerce sector in Indonesia experienced limitations in terms of monitoring and enforcement and was still sectoral. The synergy between BSSN and Kominfo in the legal aspects still requires regulations to clarify the division of responsibilities and authorities in the application of cyber security, while in the organizational aspect there is no coordination standard that applies to ISO 22301: 2012 and NIST SP 800-61. Conclusions obtained to improve synergy in legal aspects require flexibility in the preparation and adjustment of regulations but have the power of law enforcement. In the organizational aspect, an organizational structure needed between relevant institutions / ministries so that effective communication and coordination will establish and increase cyber security readiness in the e-commerce sector in Indonesia.

Keywords: Cyber Security, E-Commerce, Synergy, BSSN and Kominfo.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era globalisasi dan menuju revolusi industri 4.0, perkembangan teknologi berdampak signifikan terhadap kemajuan ekonomi. Salah satu perubahan yang paling signifikan adalah semakin meningkatnya peralihan dari transaksi ekonomi konvensional menuju ke transaksi non konvensional. Hal ini dibuktikan dengan peningkatan nilai penjualan bisnis online setiap tahunnya meningkat 40 persen pada penjualan retail melalui transaksi komersial berbasis elektronik (*e-commerce*) bahkan pada tahun 2014 nilai bisnis industri perdagangan elektronik di Indonesia mencapai USD 12 miliar dan diprediksi dapat menjadi salah satu negara digital ekonomi terbesar di Asia Tenggara[1]. Prediksi yang serupa juga dinyatakan oleh Jaz Frederick dalam buku *Global E-Commerce Book*:

> *With a growing middle class and an advancing economy, Indonesia's smartphone population and internet connectivity are expanding. Retail eCommerce sales grew over 65% last year, and the country will likely remain one of the fastest growing eCommerce markets in the Asia-Pacific region in the coming years[2].*

Indonesia juga diprediksi akan mengalami peningkatan pertumbuhan tahunan sampai dengan 50 persen pada tahun 2020 dengan nilai penjualan mencapai 130 miliar dolar Amerika Serikat[3]. Prediksi tersebut tampak realistis mengingat Indonesia merupakan pasar terbesar ketiga di Asia Pasifik untuk penggunaan *smartphone*, dimana pemilik telepon seluler bahkan lebih besar daripada jumlah penduduk Indonesia itu sendiri, yaitu sebanyak 338.948.340 juta pengguna *smartphone* dengan

---

[1] Berita Kementerian, "*Indonesia Akan Jadi Pemain Ekonomi Digital Terbesar di Asia Tenggara*" dalam https://bit.ly/2uQRqZR, diakses pada 17 Juli 2018.
[2] Jaz Frederick., *Global E-Commerce Book,* (Texas: PFSweb, Inc., 2016), hlm. 22.
[3] Berita Kementerian, *loc.cit*.

jumlah penduduk 255.461.000 juta[4]. Tingginya angka pengguna *smartphone* tersebut telah mempengaruhi tren transaksi online di Indonesia, dimana hampir setiap orang melakukan transaksi *e-commerce* melalui selular pintar. Frekuensi transaksi yang dilakukan dapat dilihat pada gambar berikut:

Gambar 1.1 Frekuensi Transaksi Online di Indonesia Tahun 2016
Sumber: Kominfo, *Keamanan Siber untuk E-Commerce.* (Indonesia: Seri Literasi Digital, 2018), hlm. 12

Pertumbuhan ekonomi digital yang begitu pesat tentu disertai dengan semakin meningkatnya kejahatan di dunia maya dan membuat jumlah *cybercrime* di Indonesia berada di peringkat pertama dan peringkat kedua di dunia untuk aksi *hacking*[5]. Sehingga sebagian besar alasan orang yang tidak memilih belanja online adalah karena transaksi perdagangan melalui elektronik masih dianggap tidak aman dan sebagian besar lainnya mengaku tidak mengetahui cara melakukannya[6]. Kesenjangan teknologi yang ada di masyarakat salah satunya menyebabkan ketidakpahaman

[4] Persada, RM, *"Indonesia Pasar Terbesar Smartphone"* dalam https://bit.ly/2JBB10U, diakses pada 17 Juli 2018.
[5] Rahardjo, Budi, "*Fintech: Layanan Baru, Ancaman Baru"* dalam https://bit.ly/2MdwdUE, diakses pada 9 Agustus 2018.
[6] Kominfo, *Keamanan Siber untuk E-Commerce* (Indonesia: Seri Literasi Digital, 2018), hlm. 13.

masyarakat tentang aspek keamanan dalam transaksi digital. Informasi dan edukasi yang diberikan oleh pihak ketiga terkait resiko yang ada dalam perdagangan melalui sistem elektronik bahkan cenderung diabaikan karena bentuk serangan siber tidak terlihat dan sebagian besar hanya diketahui oleh institusi yang mengalami serangan. Kurangnya informasi masyarakat terkait serangan siber tersebut juga disebabkan oleh faktor bisnis, dimana untuk menjaga kredibilitas merk dagangnya, seringkali pelaku bisnis yang mengalami serangan siber tidak mempublikasikannya.

Hal ini tidak luput dari perhatian pemerhati *Information and Communication Technology* (ICT) *Institute*, yang meminta Pemerintah segera menyusun langkah untuk melindungi *e-commerce,* mengingat semakin berkembangnya ekonomi digital di Indonesia dan sejarah perang siber pada tahun 2013 yang telah membuat sejumlah situs perdagangan di Indonesia *down*[7]*.* Sejalan dengan pendapat ICT *Institute*, Kamar Dagang dan Industri (KADIN) Indonesia juga menyatakan bahwa sebanyak 60 persen serangan siber adalah pada platform *e-commerce*[8]. Lebih lanjut *Kaspersky* telah menyatakan bahwa kawasan Asia Pasifik adalah area sasaran para penjahat siber dan pelaku *ransomware*[9]. *Microsoft* juga mencatat bahwa serangan siber di tahun 2015 telah menyebabkan 71% perusahaan menjadi korban dan menyebabkan kerugian bagi ekonomi global sebesar US$ 3 Triliun atau sama dengan 300 Triliun Rupiah[10].

Kasus *RupiahPlus* adalah permasalahan yang terbaru dalam transaksi online di Indonesia dari berbagai permasalahan lain terkait *financial technology (fintech)* yang semakin menunjukkan perlunya segera dilakukan pengamanan standar di dunia siber oleh Pemerintah untuk

---

[7] Erdianto, Kristian, "*Pemerintah Diminta Lindungi E-Commerce Dari Serangan Siber"* dalam https://bit.ly/2LzFL98, diakses pada 19 Juli 2018.
[8] Anonim, "*E-Commerce Jadi Sasaran Siber Rusia Bisa Tolong RI",*dalam https://bit.ly/2JDhwop, diakses pada 19 Juli 2018.
[9] Ngazis, Amal Nur, "*Ini Tiga Ancaman Utama Bagi E-Commerce",* dalam melalui: https://bit.ly/2uWLHC3, diakses pada 19 Juli 2018.
[10] Pinandita, Satrya, "*Keamanan Digital di Tahun 2017: Bagaimana Organisasi di Asia Pasifik Dapat Berlindung dari Serangan Siber",* dalam https://bit.ly/2LqFRTE, diakses pada tanggal 18 Juli 2018.

jaminan transaksi ekonomi digital[11]. Kerentanan terhadap ancaman di dunia maya ini membuat kepentingan membangun keamanan sistem informasi dan elektronik menjadi bukan hanya milik Pemerintah, namun sudah menjadi kebutuhan bagi pihak swasta maupun individu[12]. Ketika ekonomi digital suatu negara semakin berkembang, maka peran negara akan semakin memudar apabila tidak dapat mengikuti perkembangan pada era digital. Kehadiran negara antara lain adalah melalui kebijakan yang memenuhi kebutuhan yang berkembang di masyarakat serta keberadaan instansi yang bertanggungjawab untuk menjamin keamanan dan kesejahteraan nasional.

Pemerintah telah menetapkan visi untuk menjadikan Indonesia sebagai negara dengan ekonomi digital terbesar di Asia Tenggara pada tahun 2020. Hal ini menjadi dasar diterbitkannya Peraturan Presiden Nomor 74 Tahun 2017 yang mengatur tentang *Road Map E-Commerce* untuk Tahun 2017-2019 yang salah satunya mencakup program *cyber security*[13]. Peta jalan ini disusun untuk memberikan arah dan panduan strategis dalam percepatan pelaksanaan Sistem Perdagangan Nasional Berbasis Elektronik pada tahun 2017-2019 dan salah satu prinsip yang perlu menjadi perhatian adalah prinsip kepastian dan perlindungan hukum demi tercapainya ekonomi berbasis elektronik yang berkesinambungan. Kesiapan keamanan informasi tentu akan berdampak positif terhadap terlaksananya prinsip tersebut dalam *e-commerce* yang diharapkan dapat menjadi tulang punggung perekonomian nasional Indonesia[14].

Dalam rangka menjaga keamanan informasi pada sektor *e-commerce* maka perlu dibangun suatu sistem *cyber security* dalam transaksi elektronik yang mampu meminimalisir segala resiko yang

---

[11] Raharjo, *op.cit.*
[12] Anonim, "*Kebijakan Keamanan dan Pertahanan Siber",* dalam https://bit.ly/2O3g0zx, diakses pada 20 Juli 2018.
[13] Peraturan Presiden Nomor 74 Tahun 2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik, Pasal 2, ayat (2), huruf g.
[14] Berita Kementerian, "*Indonesia Akan Jadi Pemain Ekonomi Digital Terbesar di Asia Tenggara*" dalam https://bit.ly/2uQRqZR, diakses pada 17 Juli 2018.

mungkin muncul baik yang bersumber dari manusia, alam ataupun sistem itu sendiri[15]. Penerapan keamanan siber tersebut juga dapat membantu memastikan pertumbuhan *e-commerce* berjalan sesuai yang diharapkan. Penyusunan *road map e-commerce* yang didorong oleh Pemerintah saat ini adalah merupakan salah satu jalan untuk dapat meningkatkan *cyber security* Indonesia guna mewujudkan ketahanan ekonomi nasional yang mampu menghadapi ancaman nontradisional, yaitu ancaman siber pada ekonomi digital. Adanya visi yang ditetapkan Pemerintah menuntut strategi *cyber security* yang disusun harus memenuhi standar yang digunakan di kawasan Asia Tenggara.

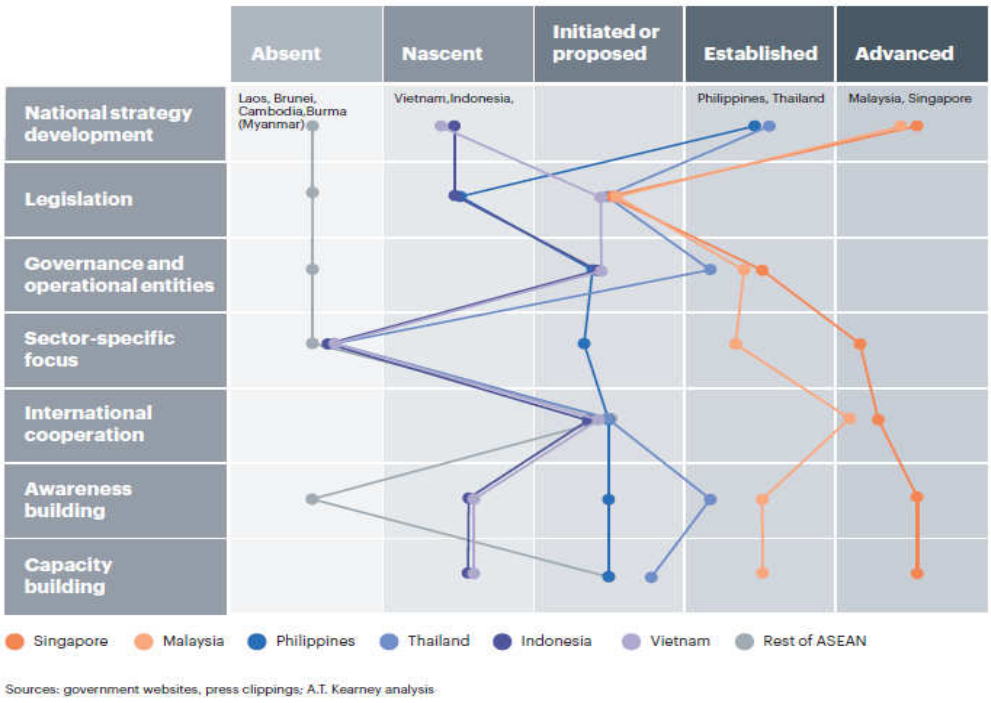
Program *cyber security* untuk *e-commerce* yang ditargetkan selesai Januari 2018 ini merupakan tanggung jawab Menteri Komunikasi dan Informatika bekerjasama dengan instansi terkait lainnya dibawah Kementerian Koordinator Bidang Perekonomian, dengan berkoordinasi dengan Kementerian Keuangan, Kementerian Perdagangan dan Bank Indonesia[16], namun hingga saat ini belum dapat diselesaikan. Disamping itu, dengan diterbitkannya Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara pada 19 Mei 2017 yang telah disempurnakan dengan Peraturan Presiden Nomor 133 Tahun 2017, tugas dan fungsi di bidang keamanan informasi telah beralih menjadi tanggungjawab dari BSSN. BSSN sebenarnya bukan lembaga yang baru dibentuk karena BSSN merupakan lembaga penguatan dari Lemsaneg dengan memimdahkan Direktorat Keamanan Informasi yang sebelumnya berada pada Direktorat Jenderal Aplikasi Informatika di Kementerian Komunikasi dan Informatika[17]. Perubahan struktur organisasi yang ada tentu mempengaruhi tugas dan fungsi yang dijalankan dari masing-masing instansi/lembaga tersebut dalam mendukung kesiapan *cyber security* pada sektor-sektor strategis. Sehingga dalam menjamin terwujudnya aspek

[15] *Ibid*.
[16] *Ibid*.
[17] Badan Siber dan Sandi Negara, *Sejarah Pembentukan BSSN* dalam https://bssn.go.id/sejarah-pembentukan-bssn/ diakses pada 10 Desember 2018.

keamanan siber dibutuhkan sinergitas dari kedua lembaga/kementerian tersebut.

Apabila melihat penelitian terhadap kemampuan siber pada negara-negara di Asia Tenggara, Indonesia merupakan salah satu yang terindikasi akan terus mendapatkan serangan siber sampai dengan 2025 dikarenakan masih rendahnya tingkat pengawasan kebijakan, minimnya tenaga ahli yang terampil di bidang digital, tingkat kerentanan yang tinggi serta masih rendahnya nilai investasi di bidang *cyber security*[18]. Gambaran umum terkait perbedaan *cyber security* yang dimiliki oleh negara-negara di Asia Tenggara dapat dilihat dibawah ini:

Tabel 1.1 Kebijakan *Cyber security* di negara-negara ASEAN



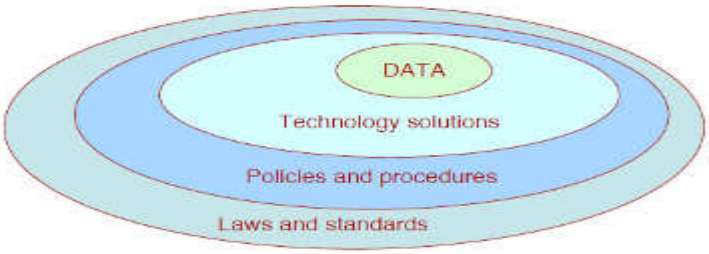
Sumber: A. T. Kearney, *Cybersecurity in ASEAN: An Urgent Call to Action.* (India: A.T.Kearney Limited. 2018), hlm. 7

Hal yang menarik dari tabel 1.1 tersebut adalah indikator yang menunjukkan bahwa negara Singapura dan Malaysia telah berada pada level kesiapan

[18] Alfarizi, Moh. Khory, "*Indonesia Akan Sering Terkena Serangan Siber Sepanjang 2018-2025"* dalam https://bit.ly/2mwzIXG, diakses pada 18 Juli 2018.

yang lebih tinggi (*advanced*) sekalipun pada tahapan peraturan perundang-undangan (*legislation*) masih berupa usulan (*initiated or proposed*), yang tidak berbeda dengan Indonesia yang baru berupa wacana (*nascent*). Namun pada tata kelola operasional Singapura dan Malaysia sudah berada pada level berjalan (*established*).

Adapun ruang lingkup pengaturan keamanan yang dibutuhkan dalam *e-commerce* sendiri secara global dapat digambarkan terdiri dari 4 (empat) bagian yaitu sebagai berikut:



Gambar 1.2
The E-Commerce Security Environment
Sumber: An Introductury Course on E-Commerce Systems,
alt. http://www.it.uu.se/edu/course/homepage/ehandel/vt08/
diakses pada tanggal 2 Agustus 2018

Gambar tersebut menjelaskan bahwa dalam membangun sebuah lingkungan yang aman bagi *e-commerce,* dimana keamanan data adalah yang menjadi fokus pengamanan, maka faktor hukum yang mengatur standar keamanan informasi serta kebijakan terkait prosedur pengamanan yang diterapkan menjadi faktor-faktor penentu terbentuknya lingkungan keamanan sebuah sistem *e-commerce*.

Pengamanan *e-commerce* menjadi bersifat strategis karena berbagai macam informasi rahasia yang ada pada penyimpanan data berpindah melalui jaringan ketika dilakukannya transaksi perdagangan secara online[19]. Sehingga pengaturan keamanan siber yang dilakukan tidak dapat lepas dari sistem elektronik atau jaringan disediakan. Hal ini semakin

[19] Hussain, Mohammed Ali, "A Study of Information Security in *E-Commerce* Application", *International Journal of Computer Engineering Science (IJCES),* Vol 3, issue 3, 2013, hlm. 1.

menekankan perlunya sinergitas antara BSSN sebagai pengampu keamanan siber dan Kominfo sebagai penanggungjawab sistem dan jaringan elektronik, dalam menyiapkan *cyber security* pada sektor *e-commerce* yang mampu menghadapi ancaman di dunia maya sekaligus tantangan atas persaingan global di era ekonomi digital. Dalam strategi pertahanan negara juga dinyatakan bahwa ketahanan ekonomi yang kokoh akan mendukung kebijakan ekonomi bidang pertahanan dalam penyelenggaraan pertahanan militer, terutama ketahanan ekonomi nasional dalam menghadapi ancaman non militer di bidang ekonomi pada era perdagangan bebas saat ini[20].

Penjabaran diatas menunjukkan bahwa kesiapan strategi *cyber security* pada sektor *e-commerce* di Indonesia merupakan tantangan bagi Pemerintah sehingga bukan hanya sekedar dapat memberikan jaminan terhadap keamanan investasi di era transaksi digital, namun sekaligus menyiapkan pertahanan berlapis yang memiliki daya tangkal terhadap ancaman serangan siber. Melalui latar belakang yang telah disampaikan diatas, maka penulis tertarik untuk mengangkat penelitian dengan judul **"Sinergitas BSSN Dan Kominfo Dalam Meningkatkan Kesiapan *Cyber Security* Pada Sektor *E-Commerce* Di Indonesia"**

1.2 Fokus danSubfokus Penelitian

1.2.1 Fokus Penelitian

Agar pembahasan penelitian ini lebih fokus dan terarah secara sistematis pada pokok pembahasan yang menjadi topik penulisan tesis, maka penulisan ini perlu diuraikan menjadi pokok-pokok bahasan dengan memberikan perumusan dan fokus masalah pada kesiapan Pemerintah dalam menerapkan *cyber security* pada sektor perdagangan melalui sistem elektronik (*e-commerce*) di Indonesia.

[20] *Strategi Pertahanan Negara 2015,* (Kementerian Pertahanan, 2015), Hlm. 70-71.

1.2.2 Subfokus Penelitian

Pengerucutan penelitian ini dibatasi pada penyusunan subfokus antara lain:

1. Kesiapan *cyber security* pada sektor *e-commerce* di Indonesia
2. Faktor-faktor penting dalam sinergitas BSSN dan Kominfo yang dapat meningkatkan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia.

1.3 Rumusan Masalah

Rumusan masalah dari fokus dan subfokus yang telah ditetapkan tersebut adalah bagaimanakah sinergitas BSSN dan Kominfo dalam meningkatkan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia? Adapun dari permasalahan tersebut maka dapat dikembangkan menjadi beberapa permasalahan yang lebih spesifik, yaitu sebagai berikut:

1. Bagaimana kesiapan *cyber security* pada sektor *e-commerce* di Indonesia?
2. Bagaimana sinergitas BSSN dan Kominfo dalam meningkatkan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia?

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah tersebut, maka tujuan penelitian yang ingin dicapai sebagai berikut:

1. Menganalisis kesiapan *cyber security* pada sektor *e-commerce* di Indonesia.
2. Menganalisis faktor-faktor penting dalam sinergitas BSSN dan Kominfo yang dapat meningkatkan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia.

1.5 Manfaat Penelitian

1.5.1 Teoritis

Penelitian ini diharapkan dapat memberikan manfaat dan kontribusi positif dalam pengembangan ilmu pertahanan nirmiliter, dimana melihat dinamika lingkungan strategis yang berkembang saat ini, ancaman yang dihadapi Indonesia pada khususnya dan secara global juga dihadapi dunia internasional, adalah semakin berkembangnya ancaman non-militer atau non-tradisional yang salah satunya sasarannya adalah sektor perekonomian.

Penelitian tentang keamanan informasi ini dilakukan untuk mengukur kesiapan lembaga/kementerian terkait *cyber security* pada sektor *e-commerce* dalam rangka mewujudkan visi Indonesia sebagai negara dengan ekonomi digital terbesar di Asia Tenggara pada tahun 2020. Selain itu juga diharapkan dapat menambah referensi bagi mahasiswa-mahasiswi yang mendalami ilmu terkait keamanan informasi dalam kaitannya dengan ketahanan ekonomi nasional di era globalisasi dan *cyber security* melalui perspektif pertahanan siber di Indonesia.

1.5.2 Praktis

Hasil penelitian ini secara praktis diharapkan dapat menjadi masukan bagi pemangku kepentingan, khususnya Kementerian Komunikasi dan Informatika dan Badan Siber dan Sandi Negara dalam mencapai *cyber security* serta Kementerian Perdagangan sebagai penanggungjawab sektor *e-commerce,* sehingga dapat selaras dengan kemajuan ekonomi digital yang dicita-citakan. Penelitian ini juga diharapkan sebagai masukan penelitian selanjutnya serta menjadi evaluasi untuk pengembangan keamanan dan pertahanan siber di Indonesia pada sektor perekonomian.

BAB II
KAJIAN TEORITIK

2.1 Deskripsi Konseptual

2.1.1 Teori Ilmu Pertahanan

Pasal 30 Undang-Undang Dasar 1945 yang mengatur tentang Pertahanan Negara dan Keamanan Negara merupakan dasar pelaksanaan segala upaya yang dilakukan bangsa Indonesia untuk mewujudkan sistem pertahanan dan keamanan semesta. Pengaturan tentang Pertahanan Negara lebih lanjut diatur dalam UU Nomor 3 Tahun 2002, yang menjelaskan bahwa pertahanan negara adalah[1]:

> *Segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara*

Segala usaha tersebut diwujudkan dalam Buku Putih Pertahanan yang berisi kebijakan pertahanan secara menyeluruh dalam menghadapi dinamika perkembangan lingkungan strategis dan dituangkan dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 23 Tahun 2015. Dalam rangka mewujudkan pengembangan pertahanan secara berkelanjutan, maka pertahanan negara perlu dikaji dalam suatu keilmuan. Makmur Supriyatno (2014) mendefinisikan ilmu pertahanan sebagai[2]:

ilmu mengenai bagaimana mengelola sumber daya dan kekuatan nasional pada saat damai, perang dan sesudah perang guna menghadapi ancaman dari luar dan dari dalam negeri, baik berupa ancaman militer maupun non militer terhadap keutuhan wilayah, kedaulatan negara dan keselamatan bangsa dalam rangka mewujudkan keamanan nasional

Melalui definisi tersebut dapat disimpulkan bahwa ilmu pertahanan harus mengkaji seluruh aspek yang diperlukan untuk mempersiapkan negara dalam menghadapi berbagai ancaman dalam segala kondisi guna

---

[1] Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara Pasal 1 ayat (1)
[2] Suriyatno, Makmur, *Tentang Ilmu Pertahanan,* (Jakarta: Yayasan Pustaka Obor Indonesia, 2014), Hlm. 29.

terwujudnya keamanan nasional. Sehingga dalam rangka mempersiapkan pertahanan Indonesia. Dalam perspektif filsafat ilmu, ilmu pertahanan berada pada posisi multidisiplin, interdisiplin dan transdisiplin[3].

Jika mengacu pada prinsip pertahanan negara yang bersifat semesta, maka kewajiban untuk menyelenggarakan keamanan dan pertahanan pada dunia maya menjadi tanggungjawab bersama sesuai dengan kapasitas dan kapabilitasnya. Bagi negara, selain memiliki *cyber security* yang dapat menjamin investasi dan sekaligus memiliki daya tangkal yang dapat menjamin ketahanan ekonomi nasional, strategi *cyber security e-commerce* Indonesia juga harus dapat sejalan dengan visi sebagai negara dengan ekonomi digital terbesar di Asia Tenggara. Bagi swasta dan individu, kemanan siber diperlukan untuk menjamin kerahasiaan informasi dan sistem elektronik yang dimiliki berdasarkan kepentingan masing-masing dan secara tidak langsung turut berkontribusi membangun pertahanan siber.

2.1.2 Teori Strategi

Dalam Buku Strategi Pertahanan Negara Kementerian Pertahanan Indonesia Tahun 2015, strategi pertahanan disusun untuk merumuskan tujuan, sasaran strategis, cara serta sarana yang digunakan guna terwujudnya kekuatan dan kemampuan pertahanan negara yang tangguh, efektif dan berdaya tangkal tinggi. Adapun dalam penyusunannya dirumuskan dalam 3 elemen dan 3 substansi dasar sebagai pedomannya. 3 elemen yang harus dimuat dalam menyusun sebuah strategi adalah elemen membentuk, merespon dan menyiapkan. Sedangkan 3 substansi dasarnya adalah tujuan yang ingin dicapai, sumber daya yang digunakan serta cara menggunakan sumber daya tersebut guna mewujudkan tujuan

[3] Tippe, Syarifudin, *Ilmu Pertahanan: Sejarah, Konsep, Teori dan Implementasi*, (Jakarta: Salemba Humanika,2016), hlm.72.

atau sasaran strategis yang telah ditetapkan[4]. Doktrin manual Amerika Serikat, strategi adalah seni dan ilmu dalam membangun dengan menggunakan politik, ekonomi, psikologi dan kekuatan militer sesuai kebutuhan selama masa damai dan perang untuk memperoleh dukungan maksimal dalam kebijakan dalam rangka meningkatkan kemungkinan dan hasil yang diharapkan, yaitu kemenangan dan memperkecil kemungkinan dikalahkan[5]. Carl Von Clausewitz melihat strategi adalah penggunaan pertempuran dalam mencapai tujuan tertentu yang diharapkan[6].

Strategi menurut Manhken dapat didefinisikan sebegai pendekatan menyeluruh yang berkaitan dengan pelaksanaan gagasan, perencanaan dan eksekusi sebuah kegiatan dalam jangka waktu tertentu[7]. Namun pemahaman strategi yang sesuai dengan penelitian ini adalah definisi dari Anthony, Parrewe dan Kachmar yang melihat strategi sebagai sebuah formula atas misi dan tujuan yang ada pada organisasi,termasuk rencana aksi untuk mencapai tujuan tersebut dengan mempertimbangkan kondisi persaingan dan pengaruh langsung maupun tidak langsung terhadap keberlangsungan organisasi[8].

2.1.3 Teori Keamanan Informasi

Cyber security merupakan bagian dari keamanan informasi, sehingga kerangka dasar dalam membahas keamanan informasi menjadi dasar dalam pebahasan terkait *cyber security*. Kerangka dasar pembangunan keamanan informasi terdiri dari 3 (*tiga*) unsur yang disingkat

---

[4] Kementerian Pertahanan Republik Indonesia. *Strategi Pertahanan Indonesia",* (Jakarta: Kementerian Pertahanan Republik Indonesia, 2015), hlm 51-53.
[5] O'Neill, Robert, *War, Strategy & History,* (Canberra: Australian National University Press, 2016), hlm 182.
[6] Clausewitz, Carl Von, *On War,* (New York: Oxforld World's Classics, 2007), hlm 163.
[7] Mahnken, Thomas & Maiolo, Joseph A. 2008. *Strategic Studies: A Reader*. New York: Taylor and Francis e-Library. Hlm 22 dalam Saputera, Moehammad Yuliansyah, *Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare,* (Indonesia: Jom FISIP Vol 2, No.2,2015), hlm 1.
[8] Nainggolan dalam Freddy Rangkuti, *Analisa SWOT Teknis Membedah Kasus Bisnis,* (Jakarta: Gramedia Pustaka Utama, 1998), hlm 3-4.

sebagai C.I.A, yaitu *Confidentiality, Integrity* dan *Availability*[9]*.* Dalam literature United State Law, keamanan informasi didefinisikan sebagai berikut[10]:

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

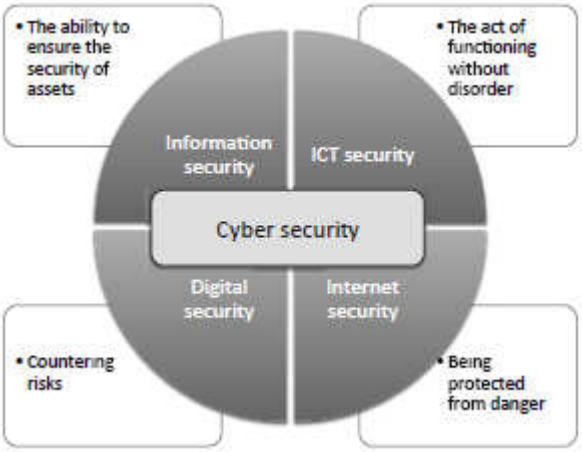
Pengertian tentang *cyber security* menurut Prof. Eko Indrajit adalah berbagai usaha pengamanan yang dilakukan pihak berkepentingan guna menangkal dan menghindari serangan siber yang cenderung bersifat destruktif agar tidak merugikan banyak pihak[11]. Pengertian keamanan informasi difokuskan pada penjagaan informasi terhadap seluruh jenis ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalisasi resiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis[12]. Lebih lanjut dijelaskan bahwa pengamanan tersebut dapat dilakukan melalui 3 (*tiga*) cara, yaitu termasuk di dalamnya perlindungan atas infrastruktur, pengamanan data, informasi atau konten yang ada dan Pengamanan terhadap komponen-komponen yang terkait dalam proses interaksi[13].

Ghernaouti melalui bukunya *Cyber Power,* menekankan bahwa *cyber security* menjadi fokus terkait kedaulatan negara, keamanan nasional dan keamanan warganegara, sehingga dibutuhkan institusi resmi dan hukum agar solusi keamanan yang diberikan bukan hanya melindungi lingkungannya melainkan juga sekaligus mencegah tindakan kriminal[14].

---

[9] Andress, Jason, *The Basic of Information Security: Understanding the Fundamental of InfoSec in Theory and Practice,* (USA: Elsevier Inc, 2011), hlm. 4.
[10] *Ibid,* hlm. 2.
[11] Indrajit, Eko Richardus, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber,* (Yogyakarta: Graha Ilmu. 2014) Hlm 8.
[12] Sarno, Riyanarto dan Irsyat Iffano, *Sistem Manajemen Keamanan Informasi,* (Surabaya: ITS Press) Hlm 26.
[13] *Ibid.*
[14] Ghernaouti, Solange, *Cyber Power* (Switzerland: EPFL Press, 2013), Hlm 332.

Hubungan antara *cyber security* dan *information security* lebih lanjut diterangkan dalam gambar berikut:

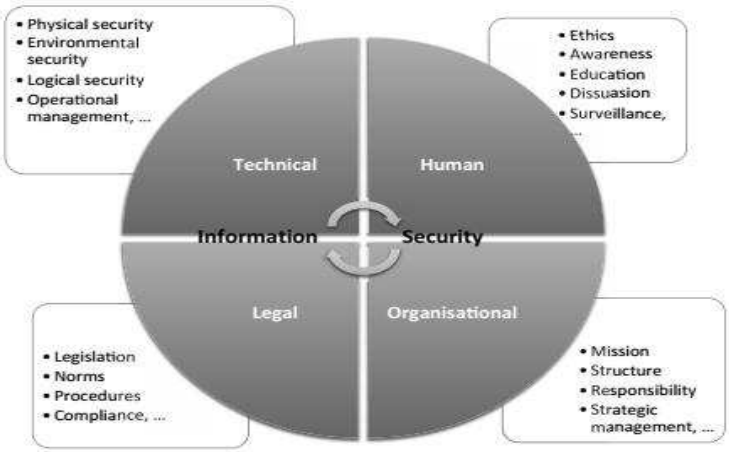


Gambar 2.1 Dimensi dari *Cyber Security*

Sumber: Ghernaouti, Solange, *Cyber Power* (Switzerland: EPFL Press, 2013), hlm. 330

Apabila melihat hubungan diatas, maka diperlukan sebuah arsitektur yang kuat dalam berbagai dimensi yang mempengaruhi keberlangsungan keamanan siber. Dalam penjelasannya, Ghernouti menjabarkan berbagai isu terkait *information security* yaitu antara lain kedaulatan negara, keamanan nasional, perlindungan terhadap infrastruktur kritis, keamanan atas aset *tangible* dan *intangible* dan proteksi terhadap data personal. Disamping itu keamanan informasi juga membahas masalah kejahatan siber dan potensi penyalahgunaan IT dan keamanan. Sehingga dalam buku *Cyber Power* Ghernouti lebih lanjut membagi dimensi *information security* menjadi 4 (empat) dimensi, dimana pada peletakan dimensi hukum dan organisasi menjadi pondasi yang mendukung 2 (*dua*) dimensi lainnya. Secara lebih lengkap dapat dilihat sesuai gambar berikut[15]:

[15] *Ibid.*, Hlm 330.



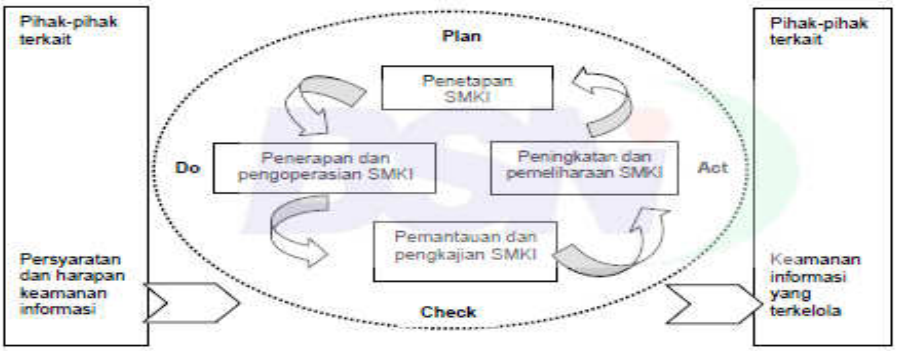
Gambar 2.2 Dimensi dari Keamanan Informasi

Sumber: Ghernaouti, Solange, *Cyber Power* (Switzerland: EPFL Press, 2013), hlm. 330

Dimensi keamanan informasi yang terdiri dari teknis, manusia, hukum dan organisasi juga merupakan kerangka kerja penyelenggaraan pertahanan siber yang diatur dalam Permenhan Nomor 82 Tahun 2014 tentang Pertahanan Siber[16]. Pada aspek hukum, pedoman ini menjelaskan bahwa kebijakan atau regulasi merupakan landasan pelaksanaan tugas organisasi terkait serta sebagai penjaga arah atas pengembangan program dan penerapan penyelenggaraan siber[17]. Sedangkan pada aspek kelembagaan/organisasi yang dibangun dalam penyelenggaraan pertahanan siber perlu disesuaikan dengan kebutuhan, untuk memastikan tercapainya tujuan yang dicita-citakan secara optimal, dengan memperhatikan persyaratan kejelasan perumusan tugas dan fungsi, kewenangan untuk melakukan koordinasi, struktur organisasi dan bentuk kelembagaan yang disesuaikan dengan kesiapan dan kebutuhan[18].

[16] Kementerian Pertahanan, *Peraturan Menteri Nomor 82 Tahun 2014 tentang Pertahanan Siber*, hlm 22.
[17] *Ibid,* hlm 23.
[18] *Ibid,* hlm 33.

Dalam menjamin keamanan informasi terdapat berbagai macam model keamanan informasi, namun yang saat ini digunakan secara global adalah ISO/IEC 27001, dimana konsep ini telah diadopsi oleh SNI dan digunakan sebagai standar bagi Sistem Manajemen Keamanan Informasi (SMKI) di Indonesia sejak tahun 2009. Standar ini menggunakan pendekatan lingkaran *Plan-Do-Check-Act* (PDCA) yang dapat dilihat pada gambar berikut[19]:



Gambar 2.3 Model PDCA

Sumber: Badan Standardisasi Nasional, *Model PDCA yang diterapkan untuk proses SMKI SNI ISO/IEC 27001:2009*, hlm 7.

Plan adalah penetapan kebijakan, sasaran, tahapan dan prosedur dari SMKI yang disesuaikan dengan manajemen resiko dan perbaikan keamanan informasi untuk dapat memperoleh hasil sesuai dengan tujuan organisasi secara keseluruhan. Sedagkan *Do* adalah penerapan dan pengoperasian dari kebijakan serta pengendalian dan tahapan serta prosedur dari SMKI. Lebih lanjut *Check* adalah mengakses dan mengukur hasil pelaksanaan dengan tujuan yang telah ditetapkan dan pengalaman praktis serta melaporkan kepada manajemen untuk dapat dilakukan pengkajian. Terakhir adalah *Act* dimana SMKI diharapkan dapat mengambil tindakan korektif dan pencegahan apabila hasil audit internal dan hasil tinjauan manajemen menunjukkan hal tesebut diperlukan untuk mencapai

[19] Badan Standardisasi Naisonal, *Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Infromasi-Persyaratan SNI ISO/IEC 27001:2009,* (Jakarta: BSN, 2009), hlm v

perbaikan yang berkelanjutan pada SMKI. Dalam setiap detail bagian dari cycle tersebut memilki standar lain pelaksanaan yang lebih detail, yaitu contohnya terkait manajemen resiko didetailkan melalui ISO 27005.

Model keamanan informasi lainnya terdapat dari National of Institute Standards and Technology (NIST) yang diterbitkan oleh Departemen Perdagangan Amerika Serikat dengan berbagai versi dalam kerangka keamanan yang antara lain terdiri dari SP 800-12 yang merupakan *Handbook* dari NIST, SP 800-26 sebagai panduan untuk *self-assessment,* SP 800-30 yang adalah panduan terkait manajemen resiko dan NIST 800-61 yang merupakan panduan untuk penanganan insiden terhadap keamanan informasi[20].

Salah satu bagian terpenting dari keamanan informasi adalah *contingency plan* karena serangan siber pasti terjadi, walaupun tidak diketahui waktu dan bentuknya, namun *contingency plan* menjadi sebuah rencana strategi untuk memastikan keberlanjutan ketersediaan dari sistem informasi yang dijalankan[21]. Komponen dari *contingency plan* dapat dilihat pada bagan berikut:

Gambar 2.4 *Components of Contingency Planning*
Sumber: Whitman, Michael E dan Herbert J. Mattord, *Principles of Information Security Third Edition,* (USA: Course Technology, 2009), hlm 210.

[20] Whitman, Michael E dan Herbert J. Mattord, *Principles of Information Security Third Edition,* (USA: Course Technology, 2009), hlm 192.
[21] *Ibid,* hlm 209.

Ketiga bagian dari sebuah *contingency plan* dalam keamanan informasi memiliki fokus berbeda dalam melihat sebuah serangan siber. *Incident Response* (IR) bertanggungjawab untuk mengidentifikasi, melakukan klasifikasi, merespon dan memulihkan sistem dari sebuah serangan. Sedangkan *Disaster Recovery* (DR) memiliki tugas untuk persiapan untuk dan pemulihan dari sebuah bencana baik itu natural atau buatan. *Business Continuity* di sisi lain memiliki tugas untuk memastika bahwa fungsi kritis dari bisnis tetap berjalan sekalipun terjadi bencana atau musibah[22].

2.1.4 Konsep *Cyber security E-Commerce*

Dalam melaksanakan perdagangan elektronik, perlu dipastikan terlaksananya prinsip-prinsip dasar privasi atas informasi, dimana terdapat 6 (*enam*) aspek keamanan *e-commerce* yang perlu diterapkan dalam aplikasi elektroniknya, yaitu antara lain[23]:

a. *Access Control,* akses kontrol adalah untuk memastikan bahwa hanya orang yang memiliki otorisasi yang dapat mengangkses.
b. *Confidentiality,* keamanan informasi adalah ketika data yang ada tidak diakses oleh orang yang tidak memiliki otorisasi atau data tereskpose pada jaringan yang tidak aman. Ketika informasi terbukti telah dimodifikasi maka hasilnya adalah hilangnya integritas.
c. *Authentication,* dalam bisnis melalui jaringan, keamanan computer dan informasi sangan penting untuk menjamin originalitas dari data, transaksi atau komunikasi. Otentikasi juga diperlukan untuk melakukan validasi atas kebenaran identitas para pihak yang bertransaksi.
d. *Non Repudiation,* dalam istilah hukum hal ini berarti keinginan para pihak untuk memenuhi tanggungjawab mereka atas kontrak yang

[22] *Loc cit.*
[23] Down, P.W & J.T. McHenry. Network Security: it's time to take it seriously. *Computer*,Vol 31, No.9. September 1998. Hlm 24-28, dalam jurnal Mohammed Ali Hussain, A Study of Information Security in E-Commerce Applications*, International Journal of Computer Engineering Science (IJCES)* Vol 3, Issue 3. Maret 2013. Hlm 5-8

ada. Hal ini juga berarti bahwa pihak tersebut tidak dapat menolak telah menerima/mengirim transaksi dan umumnya menggunakan teknologi seperti *digital signature* dan *encryption* untuk *authentication* dan non-repudiation.

e. *Integrity,* integritas sangat penting dalam transaksi elektronik yang memerlukan pengamanan khusus seperti transfer dana, *air traffic control* dan akutansi keuangan. Informasi dapat dihapus atau tidak dapat diakses sehingga orang yang memiliki otorisasi sudah tidak dapat memiliki akses.

f. *Availability,* dalam sistem informasi dibutuhkan ketersediaan informasi kapanpun informasi tersebut dibutuhkan untuk tujuannya. Hal ini membuat sistem computer harus terbiasa untuk menyimpan dan memproses informasi, *security control* harus dapat melindungi informasi dan saluran komunikasi harus dapat berfungsi secara benar sehingga akses kepada informasi tersebut tidak terganggu. Suatu sistem ketersediaan harus tetap tersedia setiap saat, mencegah gangguan servis yang disebabkan oleh pemadaman listrik, kegagalan perangkat maupun peningkatan sistem.

Dalam menjamin standar keamanan sesuai dengan 6 (*enam*) hal diatas, maka diperlukan metode keamanan yang dapat dijadikan sandaran. Beberapa metode yang digunakan secara umum dalam perlindungan bisnis *e-commerce,* antara lain adalah *encryption, Secure Socket Layer* (SSL), *digital signature, digital certificates, smart cards* dan *electronic money* [24]. Melalui berbagai penjelasan terkait aspek dan metode *cyber security* dalam *e-commerce*, maka dapat dipastikan bahwa lingkungan *cyber security e-commerce* perlu dibentuk untuk melindungi kepastian akan keamanan data yang dapat disalahgunakan dalam transaksi. Perlindungan data tesebut dilakukan melalui solusi teknologi yang memadai untuk menjamin

[24] Hussain, Mohammed Ali, "A Study of Information Security in E-Commerce Applications", *International Journal of Computer Engineering Science (IJCES)* Vol 3, Issue 3. Maret 2013, hlm 5-8.

keamanan dan dilengkapi dengan kebijakan dan prosedur berdasarkan peraturan perundang-undangan yang berlaku dan diawasi oleh lembaga yang memiliki kompetensi.

2.1.5 Teori Analisis Kebijakan

Teori analisis kebijakan yang digunakan untuk menganalisa kebijakan *cyber security* yang ada di Indonesia dan negara-negara lainnya adalah teori analisis Versi *Dunn* yang menyatakan analisis kebijakan adalah kegiatan intelektual dan praktis yang bertujuan untuk menciptakan, menilai dan mentransfer pengetahuan yang relevan dengan kebijakan[25]. Selanjutnya Dunn membagi tahapan kebijakan menjadi delapan tahap, yaitu *agenda setting, policy formation, policy adoption, policy implementation, policy assessment, policy adaptation, policy succession* dan *policy termination*[26]. Dalam melakukan analisis terhadap kebijakan juga dibutuhkan pemahaman terhadap perbedaan kebijakan publik dan hukum, dimana dalam penelitian ini menggunakan pendekatan akademis yang menggolongkan hukum sebagai bagian dari kebijakan formal dan kebijakan formal merupakan bagian dari kebijakan publik[27].

Melalui analisis kebijakan dari tiap negara maka akan ditemukan kelemahan dan kekuatan yang dimiliki sehingga dapat dibandingkan, terutama untuk digunakan sebagai acuan dalam menilai level kesiapan ekonomi digital Indonesia. Dalam studi perbandingan kebijakan, hal yang harus selalu diingat adalah bahwa setiap proses kebijakan publik dapat mencerminkan karakter politik dari masing-masing negara[28]. Dari proses kebijakan tersebut maka dapat dilihat model negara tersebut, dimana menurut McLennan model negara dapat dikategorikan menjadi 3 (*tiga*),

[25] Nugroho, Riant, *Public Policy,* Edisi Keenam, (Jakarta: PT. Elex Media Komputindo, 2009), hlm. 307.
[26] *Ibid.*, hlm. 315-323.
[27] *Ibid.,* hlm 156.
[28] *Ibid.*, hlm. 627.

yaitu *competitive state, fragmented state dan non-competitive states.* Model negara ini dapat mempengaruhi dalam perkembangan penyusunan kebijakan publiknya, dimana negara dengan model *competitive state* akan cenderung mengglobal dan fokus pada pertumbuhan ekonomi sehingga kebijakan yang dibuat mampu mengatasi ancaman globalisasi, sedangkan pada *fragmented state* menjelaskan bahwa proses perumusan kebijakan dalam institusi formal tidak selalu mencerminkan proses yang sesungguhnya dan distribusi kekuasaan masih bersifat tradisional karena negara bersifat transisi dan pada *non competitive states* ditunjukkan dengan elit yang memonopoli kekuasaan secara absolut, mendikte kebijakan dan cenderung otokratik [29].

2.1.6 Teori Manajemen Strategik

Manajemen stratejik adalah sebuah proses yang dinamis dan berlangsung secara terus menerus pada suatu organisasi, dimana strategi membutuhkan peninjauan ulang atau bahkan perubahan di masa yang akan datang[30]. Adapun tahapan dalam proses manajemen stratejik terdiri dari 12 tahapan, yaitu perumusan misi organisasi (perusahaan), penentuan profil organisasi, analisis dan piihan strategik, penetapan sasaran jangka panjang, penentuan strategi induk, penentuan strategi operasional, penentuan sasaran jangka pendek, perumusan kebijaksaan, pelembagaan strategi dan penciptaan sistem pengawasan. Namun yang menjadi fokus pada penelitian ini adalah tahap perumusan kebijaksanaan dan pelembagaan strategi[31]. Perumusan kebijaksanaan dapat diartikan sebagai penentuan segala petunjuk untuk menjadi panduan bagi cara berpikir, cara pengambilan keputusan dan cara bertindak yang semuanya diarahkan

[29] *Ibid.*, hlm 637.
[30] Siagian, Prof. Dr. Sondang P, *Manajemen Strategik*, (Indonesia: Bumi Aksara, Edisi 10, 2012), hlm 27.
[31] *Ibid,* hlm 30.

pada implementasi dan operasionalisasi dari strategi organisasi[32]. Salah satu bentuk baku dari kebijaksanaan adalah *standard operating procedures* (SOP) atau prosedur operasional yang baku.

Sedangkan pelembagaan strategi adalah menciptakan satu persepsi tentang seluruh gerak langkah dari semua komponen yang ada pada orgaisasi dalam mengimplementasikan strategi induk maupun strategi operasional, tujuan, sasaran dan misi yang telah dirumuskan dan ditetapkan[33]. Pelembagaan strategi dapat lebih menjamin tingkat efektivitas dan efisiensi yang tinggi dari operasionalisasi strategi, dengan memperhatikan 3 (*tiga*) elemen organisasi yaitu struktur organisasi, kepemimpinan dan kultur yang ada pada organisasi tersebut[34]. Dimensi organisasional pada *cyber security e-commerce* di Indonesia tidak hanya menjadi tanggungjawab satu instansi, melainkan beberapa instansi secara bersama-sama yaitu Kementerian Komunikasi dan Informatika dan Badan Siber dan Sandi Negara. Disamping itu, mengingat *cyber security e-commerce* adalah untuk transaksi perdagangan maka dalam pelaksanaannya juga akan melibatkan Kementerian Perdagangan. Dalam menganalisis strategi *cyber security e-commerce* dan kesiapannya akan melihat perangkat organisasi dan hukum yang telah berlaku maupun yang belum terakomodir.

2.1.7 Konsep Perdagangan Melalui Sistem Elektronik (*e-commerce*)

Amir Hartman, *Professor UCLA Berkeley*, mendefinisikan ekonomi digital sebagai sebuah tempat virtual dimana bisnis dijalankan, nilai dibuat dan dipertukarkan, transaksi berjalan dan matangnya hubungan satu-ke-satu dengan menggunakan Internet dan TIK sebagai media. Pemahaman tersebut selaras dengan konsep *Interlinked Economy,* dimana Kenichi Ohmae menggambarkan bahwa keterkaitan ekonomi global akan

[32] *Ibid*, hlm 38.
[33] *Ibid,* hlm 39.
[34] Ibid hlm 229.

bervariasi, namun memiliki pola yang jelas yaitu mengikuti logika ekonomi dan berkembang bagaikan jaringan kepentingan yang tidak dapat dibatasi oleh batas-batas negara atau dalam konsep yang saat ini umum dikenal dengan *borderless world*[35]. Konsep inilah yang berkembang dalam ekonomi digital.

Ekonomi digital meliputi sektor kesehatan, pariwisata, industri, pendidikan, pertanian, perdagangan, bank, transportasi dan lain sebagainya. *UNICITRAL*, salah satu komisi dibawah PBB yang khusus membahas perdagangan internasional, membuat *model law* yang berisi *guidelines* dalam melaksanakan perdagangan elektronik pada tahun 1996 dan mendefinisikan perdagangan elektronik (*e-commerce*) sebagai perdagangan melalui elektronik dengan menggunakan semua jenis informasi dalam bentuk data untuk kepentingan komersial[36]. Sedangkan *WTO* mendefinisikan ekonomi digital sebagai proses produksi, distribusi, marketing, penjualan, pengiriman barang dan jasa dengan menggunakan alat elektronik[37].

Undang-Undang Nomor 7 Tahun 2014 yang mengatur tentang Perdagangan mendeskripsikan perdagangan melalui sistem elektronik adalah[38]:

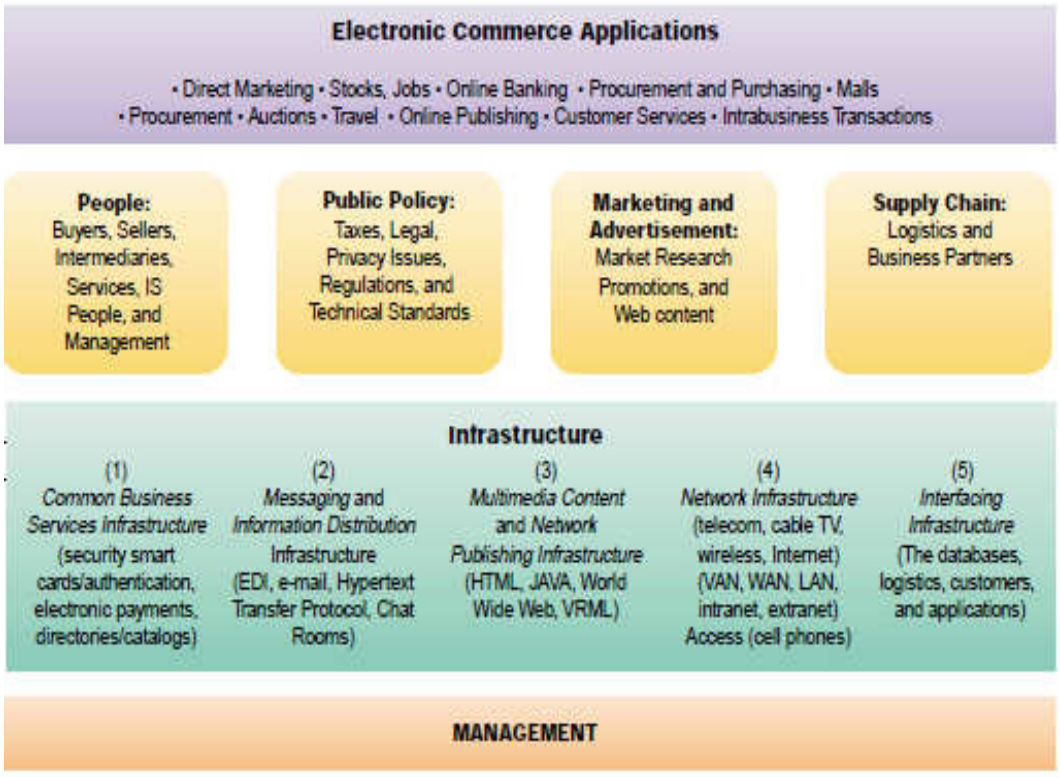
Perdagangan yang transaksinya dilakukan melalui serangkaian perangkat dan prosedur elektronik

Pemahaman tersebut menggarisbawahi pengertian *e-commerce* pada hubungan transaksional yang menggunakan media digital tanpa memerlukan proses temu muka dan tanpa batas. Dalam pelaksanaan perdagangan elektronik memiliki faktor pendorong dan penghambat yang mempengaruhi kemajuan perekonomian digital. Pemetaan terhadap faktor

---

[35] Ohmae, Kenichi, *Borderless World: Power and Strategy in The Interlinked Economy,* (New York: HarperCollins Publishers Inc, Rev.ed,1999), Hlm. 190.
[36] Dewi, Shinta, *Cyber Law: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional,* (Bandung: Widya Padjajaran,2009), Hlm. 57.
[37] *Ibid.*
[38] Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan, Pasal 1, angka 23.

pendorong dan penghambat yang dihadapi dalam sistem perdagangan elektronik dapat menjadi pemetaan terhadap kelemahan dan kekuatan yang dimiliki Indonesia dalam mewujudkan visi menjadi negara dengan ekonomi digital terbesar di Indonesia. *E-Commerce* sendiri memiliki 5 (*lima*) pilar utama di dalamnya yang dapat digambarkan dalam kerangka berikut:



Gambar 2.5 A Framework for E-Commerce

Sumber: "Electronic Commerce" dalam
https://www.wiley.com/college/turban/0471073806/sc/ch09.pdf,
diakses pada 25 Juli 2018

Dari kerangka aplikasi *e-commerce* diatas dapat dilihat pilar yang saling berhubungan tersebut, adalah *people, public policy, marketing and advertising, supply chain* dan *infrastructure.* Manajemen dalam perdagangan melalui elektronik harus mengatur kelima pilar tersebut agar dapat mencapai tujuan dari perdagangan itu sendiri namun tetap memenuhi aspek keamanan yang dibutuhkan. Dalam penelitian ini hanya terbatas

pada 2 (*dua*) aspek dalam konsep *e-commerce* diatas, yaitu terkait *stakeholder*s dalam *e-commerce* (*people*) dan aspek kebijakan dalam setiap aspek *e-commerce* (*public policy*) dengan melihat aspek manajemen *e-commerce* yang terkait dengan sinergitas dan penilaian resiko keamanan.

2.1.8 Konsep Sinergitas

James A. F. Stoner mendeskripsikan sinergi sebagai hubungan antar beberapa pihak yang menghasilkan jenjang komunikasi dalam membangun kerjasama dan kepercayaan[39]. Najiyati dan Rahmat mengartikan sinergi sebagai kombinasi atau perpaduan antara unsur atau bagian yang dapat menghasilkan keluaran (*output*) yang lebih baik dan lebih besar. Adapun sinergitas tersebut dapat tercapai melalui 2 (*dua*) cara yaitu komunikasi dan koordinasi[40]. Mulyana (2008) menjelaskan bahwa koordinasi adalah hubungan antara *stakeholders* dalam berbagai bentuk antara lain vertikal, horizontal, komando, baik dalam bentuk koordinasi dan kemitraan sedangkan komunikasi menekankan pada pertukaran informasi antar pihak[41]. Sedangkan pola sinergitas yang digunakan dalam model keamanan informasi NIST terdapat pada SP 800-61 adalah koordinasi dan pembagian informasi, yang diyakini data menguntungkan dan memperkuat stakeholder terkait dalam menghadapi ancaman, serangan dan juga kerentanan[42]. Namun dalam koordinasi dan pembagian informasi ini memerlukan pengaturan yang jelas dan dilengkapi dengan regulasi yang jelas baik itu dari Pemerintah maupun industri yang menaungi, sehingga menjamin penggunaan sinergitas ini untuk kepentingan yang saling menguntungkan dan tidak digunakan sebaliknya. Dalam koordinasi, NIST

---

[39] Stoner, J. A. F dan Charles Wankel, *Mangement,* 3rd edition, (London: Prentice Hall International Inc, 1986), hlm. 216.
[40] Rahmawati, Triana, Irwan Noor dan Ike Wanusmawatie, "Sinergitas *Stakeholders* Dalam Inovasi Daerah", *Jurnal Administrasi Publik (JAP),* Vol. 2, No. 4, hlm. 643.
[41] Mulyana, Deddy, *Ilmu Komunikasi: Suatu Pengantar,* (Bandung: Remaja Rosdakarya, 2008), hlm. 58.
[42] Cichonski, Paul dan Tom Milar dkk, *NIST SP 800-61 Computer Security Handling Guide Second Revision,* (US: Department of Commerce, 2012), hlm 45.

membagi hubungan koordinasi menjadi 3 (tiga) kategori yaitu sebagai berikut[43]:

Tabel 2.1 Hubungan Koordinasi

Category	Definition	Information Shared
Team-to-team	Team-to-team relationships exist whenever technical incident responders in different organizations collaborate with their peers during any phase of the incident handling life cycle. The organizations participating in this type of relationship are usually peers without any authority over each other and choose to share information, pool resources, and reuse knowledge to solve problems common to both teams.	The information most frequently shared in team-to-team relationships is tactical and technical (e.g., technical indicators of compromise, suggested remediation actions) but may also include other types of information (plans, procedures, lessons learned) if conducted as part of the Preparation phase.
Team-to-coordinating team	Team-to-coordinating team relationships exist between an organizational incident response team and a separate organization that acts as a central point for coordinated incident response and management such as US-CERT or an ISAC. This type of relationship may include some degree of required reporting from the member organizations by the coordinating body, as well as the expectation that the coordinating team will disseminate timely and useful information to participating member organizations.	Teams and coordinating teams frequently share tactical, technical information as well as information regarding threats, vulnerabilities, and risks to the community served by the coordinating team. The coordinating team may also need specific impact information about incidents in order to help make decisions on where to focus its resources and attention.
Coordinating team-to-coordinating team	Relationships between multiple coordinating teams such as US-CERT and the ISACs exist to share information relating to cross-cutting incidents which may affect multiple communities. The coordinating teams act on behalf of their respective community member organizations to share information on the nature and scope of cross-cutting incidents and reusable mitigation strategies to assist in inter-community response.	The type of information shared by coordinating teams with their counterparts often consists of periodical summaries during "steady state" operations, punctuated by the exchange of tactical, technical details, response plans, and impact or risk assessment information during coordinated incident response activities.

Sumber: NIST SP 800-61, hlm 47.

Sedangkan terkait pola yang digunakan untuk pembagian informasi, panduan ini mengatur perlunya dibuat dalam sebuah perjanjian terkait pembagian informasi atau umumnya disebut *nondisclosure agreement* (NDA) dan pelaporan insiden yang diwajibkan oleh Pemerintah dilengkapi dengan persyaratan pelaporan untuk melindungi kerahasiaan dari informasi sensitif milik perusahaan[44]. Seluruh pihak telah meyadari pentingnya pembagian informasi sebagai elemen utama dalam mempermudah koordinasi lintas organisasi yang membantu menghadapi insiden dengan lebih efektif dengan membagi *sharing information* menjadi 2 (dua) yaitu *Ad*

[43] *Ibid*, hlm 47.
[44] *Ibid,* hlm 47.

Hoc dan *Partially Automated*[45]*.* ISO 22301:2012 juga mengatur standar komunikasi lintas organisasi yang perlu termuat dengan jelas dalam BCP sebuah organisasi yang berisi yaitu apa yang akan dikomunikasikan, kapan dilakukan dan dengan siapa komunikasi tersebut dilaksanakan[46].

2.2 Penelitian Terdahulu

Sebagai bahan perbandingan, penelitian ini juga menjadikan penelitian-penelitian terdahulu sebagai salah satu dasar pemikiran. Peneliti berharap dapat memberikan analisa lanjutan dari penelitian-penelitian sebelumnya mengingat terdapat beberapa persamaan dan perbedaan dalam penelitian yang akan dilakukan dengan penelitian yang terdahulu, yaitu antara lain:

1. Velmurugan (2009) dalam *Secuirty and Trust in E-Business: Problem and Prospects* memfokuskan penelitian kualitatif deskriptif terhadap isu kepercayaan yang timbul dalam bisnis yang menggunakan sistem elektronik. Isu kepercayaan dalam keamanan sistem elektronik ini dapat mempegaruhi berbagai aspek dalam bisnis.
2. Hussain (2013) melalui penelitian dengan judul *A Study of Information Security in E-Commerce Application* meneliti tentang ancaman keamanan terhadap perdagangan melalui elektronik dan cara mengatasi ancaman tersebut. Persamaan dengan penelitian ini terdapat pada faktor-faktor *cyber security e-commerce* yang menjadi obyek penelitian. Perbedaan dengan penelitian ini adalah aspek yang diangkat hanya berdasarkan teknologi pengamanannya.
3. Kaur dkk (2015) dalam *E-Commerce Privacy and Security System* membahas mengenai pentingnya sistem keamanan yang menjamin privasi dalam pelaksanaan *e-commerce* pada penelitian kualitatif

[45] *Ibid,* hlm 48.
[46] ISO, *Society Security-Business Continuity Management Systems-Requirements,* (Switzerland: ISO copyright office, 2012) hlm. 13

dengan pendekatan studi kasus di bidang perbankan. Penelitian ini menjabarkan tentang aspek keamanan melalui implementasi sistem perbankan, sistem keamanan resiko keamanan dan kebijakan tentang privasi serta pembagian tanggungjawab dan pengaruhnya terhadap loyalitas nasabah.

4. Patil (2017) melalui *The Most Principle Security Issues in E-Commerce* melakukan penelitian yang memfokuskan tentang pentingnya peran keamanan dan privasi bukan hanya dari penyedia jasa, namun juga pentingnya pengetahuan konsumen terkait pentingnya *security* sebagai pengguna *e-commerce.*

Persamaan penelitian ini dengan penelitian-penelitian terdahulu adalah penelitian adalah tentang *cyber security e-commerce.* Namun perbedaan penelitian yang akan dilakukan peneliti dengan penelitian-penelitian terdahulu adalah menganalisis kesiapan *cyber security* pada sektor *e-commerce* khusus pada aspek legal dan organisasional, dimana penelitian sebelumnya lebih fokus kepada aspek teknis dan sumber daya manusia maupun aspek bisnis dari transaksi perdagangan melalui sistem elektronik.

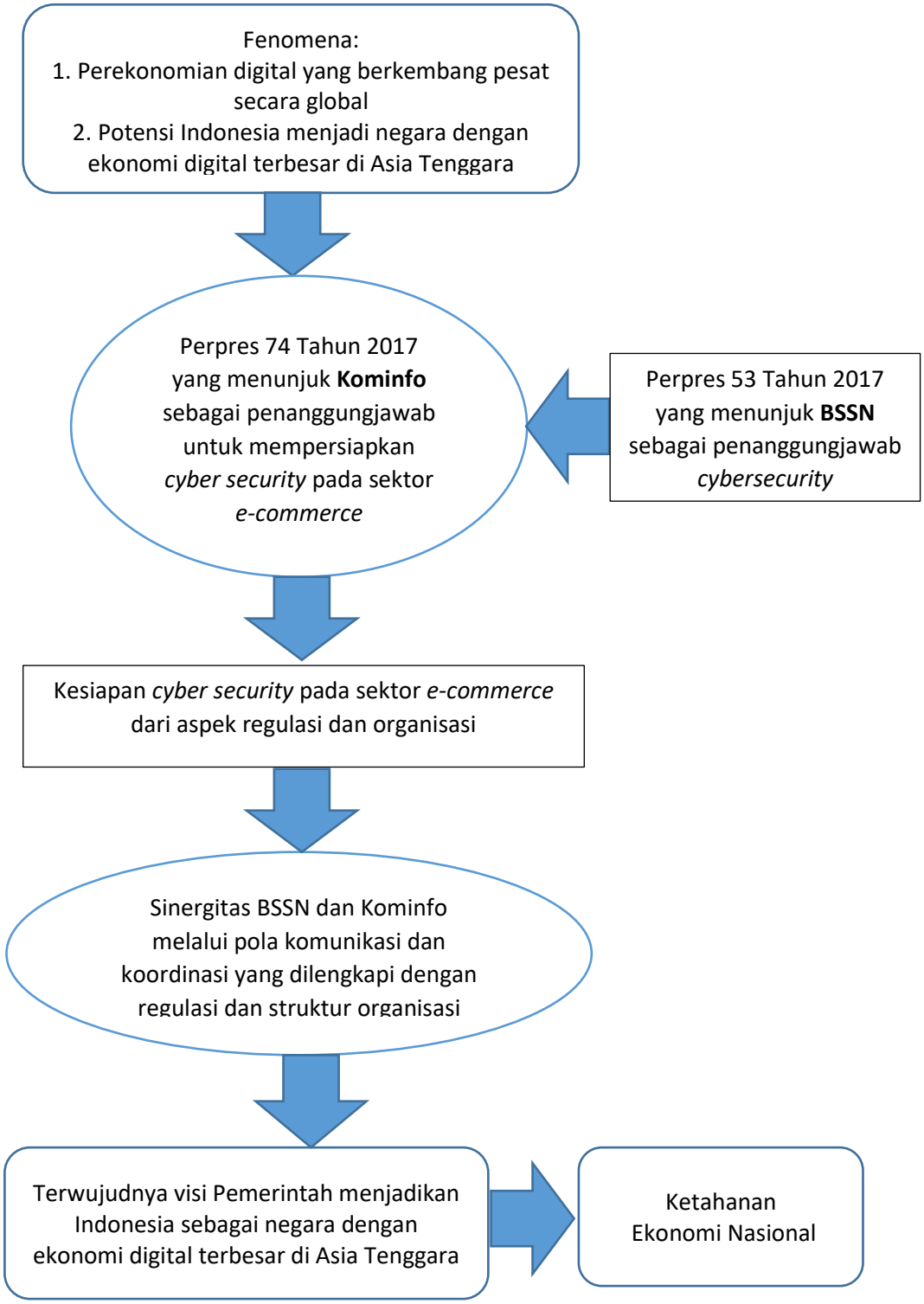
Tabel 2.2 Penelitian Terdahulu

No	Nama/Tahun/Judul	Metodologi/Teori	Permasalahan	Hasil
1	Manivannan Senthil Velmurugan, 2009, *Secuirty and Trust in E-Business: Problem and Prospects*	Kualitatif, Deskriptif/ Teori keamanan, Kepercayaan	Mempelajari tentang permasalahan implementasi *e-business* sehingga dapat meningkatkan pemahaman terkait aspek keamanan pada *e-business* demi meningkatkan kepercayaan terhadap transaksi online	Teori dan konsep terkait *e-business trust and security* dapat menuntun perusahaan untuk membangun strategi dalam menghadapi konsumen sehingga dapat meningkatkan kualitas kepercayaan yang dapat berpengaruh terhadap bisnis.
2	Dr. Mohammed Ali Hussain, 2013, *A Study of Information Security in E-Commerce Application*	Kualitatif, Deskriptif / Teori *Cybersecurity E-Commerce, Cybersecurity Technology*	*E-Commerce* memegang peran penting dalam perkembangan industri sehingga jumlah dan jenis serangan terhadap keamanannya akan semakin meningkat. Untuk itu penting untuk membuat internet menjadi tempat yang aman	Perubahan dari transaksi tradisional menuju tradisional online yang semakin pesat, membuat 3 (*tiga*) konsep keamanan informasi menjadi penting untuk diimplementasikan. Dalam penelitian juga menjabarkan tentang jenis-jenis ancaman terhadap *e-commerce*, yaitu antara

			dalam melaksanakan transaksi	lain *viruses, worms, Trojan horse, Denial of service, password thefting.* Adapun beberapa cara untk melindungi dari ancaman siber tersebut adalah *encryption, SSL, digital signature, digital sertificates, smart card* dan *e-cash*
3	Kuldeep Kaur, Dr. Ashutosh Pathak, Parminder Kaur dan Karamjeet Kaur, 2015, *E-Commerce Privacy and Security System*	Kualitatif, Studi Kasus/ Teori *Cybersecurity, E-Commerce Cybersecurity,*	Keamanan informasi merupakan isu penting dalam seluruh proses *e-commerce,* sehingga perlu diketahui jenis ancaman yang dihadapi dan perlindungan yang diperlukan	Penelitian ini menjelaskan tentang 4 (empat) komponen sistem *e-commerce*, 5 (lima) prinsip keamanan dan 2 (dua) ancaman keamanan *e-commerce* dan solusi dasar dalam keamanan *e-commerce* yaitu edukasi dan pelatihan *web security* serta menggunakan SSL
4	Mohamed, Abdikadir Yusuf dan Akram M Zeki, 2015, *The Most*	Kualitatif, Deskriptif/	Aspek keamanan transaksi yang belum terimplementasi dalam transaksi melalui	Tulisan ini merangkum solusi profesional terhadap serangan keamanan dan pertahanan pada

	Principle Security Issues in E-Commerce	*E-Commerce*, *Security issues*	elektronik menyebabkan munculnya berbagai isu terkait privasi dan keamanan	sistem *e-commerce,* yang menitikberatkan melalui teknologi terbaru pada desain website yang aman.

2.3 Kerangka Pemikiran



Gambar 2.6 Kerangka Pemikiran
Sumber: Dioleh oleh peneliti, 2018

BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Penelitian ini menggunakan metode kualitatif yang menurut Moleong, dari hasil mensintesiskan berbagai pendapat pakar, adalah penelitian holistik yang ditujukan untuk memahami fenomena yang dialami oleh subyek penelitian dan dituangkan secara deskriptif dalam kata-kata, pada suatu konteks khusus dan dengan memanfaatkan berbagai metode yang alamiah[1]. Lebih lanjut, pendekatan yang digunakan adalah pendekatan deskriptif, yaitu melalui pendeskripsian korelasi antara variabel dengan berdasarkan hubungan model, namun makna dibalik korelasi/fenomena tersebut hanya perlu dijelaskan apabila dibutuhkan pemahaman yang lebih dalam[2].

Pendekatan deskriptif dilakukan melalui pengumpulan data-data dan gambar yang kemudian ditelaah satu persatu dengan menggunakan pertanyaan mengapa, alasan apa dan bagaimana, sehingga suatu peristiwa tidak dipandang sebagai sesuatu yang sudah demikian adanya[3]. Melalui metode kualitatif deskriptif ini penulis akan mendeskripsikan hasil analisis mengenai kesiapan *cyber security* pada sektor *e-commerce* di Indonesia pada aspek hukum dan aspek organisasional serta hasil analisis tentang sinergitas BSSN dan Kominfo dalam meningkatkan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia dengan melihat pada standar regulasi serta tata kelola yang telah berjalan pada negara di Asia Tenggara lainnya.

---

[1] Moleong, Lexy. J, *Metodologi Penelitian Kualitatif,* Edisi Revisi, (Bandung: PT. Remaja Rosdakarya, 2014), hlm. 6
[2] Leksono, Sonny, *Penelitian Kualitatif Ilmu Ekonomi: Dari Metoologi ke Metode,* (Jakarta: PT. RajaGrafindo Persada, 2013), hlm.183.
[3] *Ibid,* hlm. 11

3.2 Tempat dan Waktu Penelitian

3.2.1 Tempat Penelitian

Dalam melakukan penelitian tesis ini, tempat penelitian dilaksanakan pada Kementerian Komunikasi dan Informatika, yang beralamat di Jl. Medan Merdeka Barat No. 9 Jakarta Pusat, sebagai penanggungjawab sistem *cyber security* serta Badan Siber dan Sandi Negara, yang beralamatkan di Jl. Harsono RM. 70 Ragunan Pasar Minggu, Jakarta Selatan, yang saat ini bertugas sebagai badan pemerintah yang bertanggungjawab dalam menangani isu di bidang siber.

3.2.2 Waktu Penelitian

Penelitian telah dilakukan dalam jangka waktu 6 (enam) bulan sejak Agustus 2018 sampai dengan Januari 2019 dengan jadwal pelaksanaan sebagai berikut:

Tabel 3.1
Pelaksanaan Penelitian

No	Kegiatan	Agst	Sept	Okt	Nov	Des	Jan
1	Pembuatan Proposal	√					
2	Bimbingan Penelitian	√	√	√	√	√	√
3	Seminar Proposal		√				
4	Perbaikan Proposal		√				
5	Penelitian Lapangan		√	√	√		
6	Penyusunan Tesis		√	√	√	√	
7	Ujian Tesis					√	
8	Perbaikan Tesis						√

3.3 Subyek dan Sampel Penelitian

3.3.1 Subyek Penelitian

Penelitian adalah sesuatu hal yang memiliki kedudukan yang penting di dalam penelitian yang harus ditata sebelum peneliti siap untuk mengumpulkan data. Subjek penelitian ini dapat berupa benda, hal, ataupun orang. Dengan demikian, secara umum subjek penelitian merupakan manusia atau hal-hal yang menjadi urusan manusia itu sendiri[4]. Oleh karena itu, dalam penelitian ini yang menjadi subjek penelitian ini adalah lembaga/institusi pemerintah yang terkait dalam pembuatan strategi *cyber security* pada sistem perdagangan elektronik di Indonesia serta ahli/akademisi serta praktisi di bidang *cyber security* dan pelaku pengguna sistem perdagangan elektronik. Dalam hal ini, instansi yang bertanggungjawab adalah Badan Siber dan Sandi Negara (BSSN) dan Kementerian Komunikasi dan Informatika (Kominfo).

3.3.2 Sampel Penelitian

Teknik penentuan sampel yang digunakan dalam penelitian kualitatif umumnya adalah *purposive sampling* karena tujuan dari penelitian kualitatif adalah untuk mendapatkan atau menggali informasi sebanyak-banyaknya dari sumber informasi yang disebut informan, narasumber atau konsultan ahli. Mengingat lingkup penelitian yang cukup spesifik maka peneliti memilih untuk menggunakan *non-probability sampling,* dimana penentuan sampel sudah dipilih berdasarkan pertimbangan yang sesuai dengan fokus dan tujuan penelitian.

Dalam penelitian ini sampel yang terkait dalam kesiapan *cyber security* pada transaksi perdagangan melalui sistem elektronik (*e-commerce*) di Indonesia adalah:

[4] Arikunto, *Prosedur Penelitian Suatu Pendekatan Praktik,* (Jakarta: Penerbit PT Rineka Cipta, 2006), hlm. 152.

Tabel 3.2
Sampel Penelitian atau Informan

No	Nama	Jabatan	Instansi
1	Herry Abdul Aziz M	Staff Ahli Menteri Kominfo Bidang Teknologi	Kominfo
2	Sulistyo	Direktur Deteksi Ancaman	BSSN
3	Inu Baskara	Direktur Penanggulangan dan Pemulihan Ekonomi Digital	BSSN
4	Riki Arief Gunawan	Direktur Pengendalian Aplikasi Informatika	Kominfo
5	Baderi	Kasubdit Proteksi E-Commerce	BSSN
6	Intan Rahayu	Kasubdit Identifikasi Kerentanan & Penilaian Resiko	BSSN
7	I Nyoman Adhiarna	Kasubdit Tata Kelola Sistem Elektronik	Kominfo
8	Rosihan	Ketua Tim Tenaga Ahli Road Map E-Commerce	Kemenkokuin/ idEA
9	Salahuedin	Tenaga Ahli Keamanan Siber Road Map E-Commerce	Kemenkokuin
10	Septo	Kasubdit E-Commerce	Kemendag
11	Luat Sihombing	Kasie Bidang Ekonom Digital	Kominfo
12	Budi Rahardjo	Pakar Cyber Security	ITB
13	Yuliardi Sutedja	Komunitas Cyber Security	ICSF
14	M. Tesar Sandigapura	Pelaku E-Commerce	LiteBig

3.4 Teknik Pengumpulan Data

Pengumpulan Data merupakan tahapan yang paling penting yang yang dilakukan peneliti untuk menemukan penjelasan yang dapat membantu peneliti memahami masalah yang diteliti melalui berbagai teknik pengumpulan data yang telah memiliki standar data yang ditetapkan[5]. Adapun dari 4 (*empat*) macam teknik pengumpulan data, yaitu observasi, wawancara, dokumentasi dan triangulasi/gabungan yang dijabarkan oleh

[5] Sugiyono, *Metode Penelitian Kombinasi (Mixed Methods),* (Bandung: Alfabeta, 2016), hlm. 308.

Sugiono, peneliti memilih 2 (dua) teknik pengumpulan data, yaitu wawancara dan studi dokumentasi.

3.4.1 Wawancara

Creswell menyatakan bahwa peneliti dapat melakukan wawancara dengan berbagai metode yaitu antara lain wawancara berhadap-hadapan langsung dengan partisipan, wawancara melalui media telekomunikasi atau melalui *focus group interview*[6]. Esterberg membagi jenis wawancara menjadi 3 (tiga) yaitu, wawancara terstruktur, semiterstruktur dan tidak terstruktur[7]. Peneliti memilih jenis wawancara semi terstruktur yang juga masuk dalam kategori *in-dept interview,* dengan tujuan untuk menemukan permasalahan secara lebih terbuka melalui pendapat dan ide dari informan.

3.4.2 Studi Dokumentasi

Dokumentasi menurut Sugiono adalah catatan kejadian yang sudah lampau yang dinyatakan bisa dalam bentuk lisan, tulisan dan karya monumental dari seseorang[8]. Dalam penelitian ini yang dimaksud dokumentasi adalah semua catatan, gambar dan peraturan terkait dengan strategi *cyber security* pada perdagangan elektronik di Indonesia dan peraturan serta strategi yang ada di negara-negara lain di Asia Tenggara.

3.5 Pemeriksaan Keabsahan Data

Pemeriksaan keabsahan data dalam penelitian kualitatif sangat diperlukan untuk menguji ataupun memeriksa akurasi data yang telah dikumpulkan dari proses penelitian berlangsung. Nasution mengemukakan bahwa pengujian keabsahan dan keterandalan data diperlukan untuk membuktikan kesesuaian hasil yang sudah diamati dengan fakta dan

---

[6] Creswell, John. W, *Research Design: Pendekatan Metode Kualitatif, Kuantitatif dan Campuran,* (Yogyakarta: Pustaka Pelajar, 2016), hlm.254.
[7] Sugiono, *op. cit.,* hlm. 317.
[8] *Ibid*, hlm. 326.

peristiwa yang sebenarnya terjadi[9]. Terdapat beberapa cara untuk melakukan pemeriksaan keabsahan data, yaitu antara lain perpanjangan keikutsertaan, ketekunan pengamatan, pengecekan sejawat, kecukupan referensial, kajian kasus negatif, pengecekan anggota dan triangulasi[10].

Dalam penelitian ini, peneliti menggunakan triangulasi, yang menurut Sugiono, terdiri dari 3 bagian, yaitu, triangulasi sumber, triangulasi teknik/metode, triangulasi waktu[11]. Triangulasi sumber adalah meguji kredibilitas data melalui beberapa sumber, sedangkan triangulasi teknik atau metode adalah menguji kredibilitas data melalui teknik yang berbeda, sedangkan triangulasi waktu adalah melakukan pengecekan kredibilitas data pada waktu dan situasi yang berbeda.

3.6 Teknis Analisis Data

Miles dan Huberman menyatakan bahwa teknik analisis data dilakukan pada saat pengumpulan data di lapangan dan setelah semua data terkumpul dengan teknik model yang terdiri dari 3 (*tiga*) yaitu[12]:

a. *Data Condensation*

   Menjelaskan tentang proses pemilihan, memfokuskan, menyederhanakan dan merangkum dan/atau mentransformasikan data yang muncul dalam bentuk lengkap, untuk membuat data menjadi lebih kuat.

b. Data Display

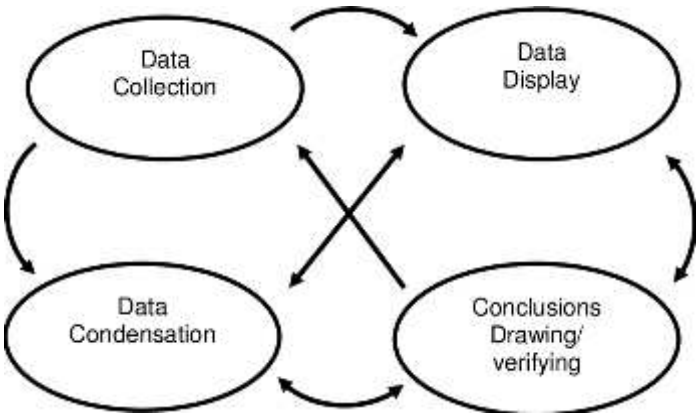
   Menjelaskan tentang pengaturan dan penekanan imformasi secara umum sehingga dapat disusun kesimpulan dan rencana aksi

c. Drawing and Verifying Conclusion

---

[9] Nasution, *Metode Penelitian Naturalistik-Kualitatif*, (Bandung: Tarsito, 2003), hlm. 105
[10] Moleong, Lexy. J, *Metodologi Penelitian Kualitatif,* Edisi Revisi, (Bandung: Remaja Rosdakara, 2014), hlm. 327.
[11] Sugiono, *op.cit,* hlm. 370-371.
[12] Miles, Matthew. B, A. Michael Huberman dan Johnny Saldana, *Qualitative Data Analysis: A Methods Source Book,*3rd edition, (US: SAGE Publciation, Inc, 2014), Hlm.33

Proses pengambilan kesimpulan berdasarkan seluruh data yang diperoleh dengan dasar keterbukaan namun dengan tetap mempertahankan skeptisme selama proses penelitian hingga nanti kesimpulan yang disusun semakin jelas dan kuat. Ketiga proses tersebut dapat dilihat pada gambar dibawah ini:



Gambar 3.1 Interaktif Model Analisis Data

Sumber: Miles, Matthew. B, A. Michael Huberman dan Johnny Saldana, *Qualitative Data Analysis: A Methods Source Book,* third edition
(US: SAGE Publication, Inc, 2014), hlm. 33

Proses analisis data dilakukan terhadap data primer maupun data sekunder yang diperoleh oleh peneliti melalui proses pengumpulan data yang dilakukan melalui wawancara dan studi dokumentasi terhadap subyek dan sampel penelitian yang sudah ditetapkan berdasarkan pedoman wawancara yang sudah dibuat berdasarkan kajian teoritik yang ada. Melalui pemilahan data berdasarkan variabel yang ditetapkan kemudian dilanjutkan dengan melakukan proses pengambilan kesimpulan dan dilanjutkan dengan proses verifikasi untuk mendapatkan kesimpulan akhir.

BAB IV
ANALISIS DATA DAN PEMBAHASAN

4.1 Hasil Penelitian

4.1.1 Gambaran Umum Subyek Penelitian

Dalam penelitian ini yang menjadi subyek penelitian adalah Kementerian Komunikasi dan Informatika (Kominfo) yang terletak di Jalan Medan Merdeka Barat nomor 9 Jakarta Pusat dan Badan Siber dan Sandi Negara (BSSN) yang berada di Jalan Harsono RM 70 Ragunan Jakarta Selatan, yang masing-masing memiliki tugas dan fungsinya dalam Strategi Keamanan Siber di Indonesia. Berdasarkan Peraturan Presiden Republik Indonesia Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika, tugas Kominfo adalah membantu Presiden dalam menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika[1]. Salah satu fungsi Kominfo yang terkait dalam penelitian ini adalah sebagai kementerian yang melakukan fungsinya sebagai lembaga yang merumuskan, menetapkan dan melaksanakan kebijakan di bidang pengelolaan sumber daya dan perangkat pos dan informatika, penyelenggaraan pos dan informatika, penatakelolaan aplikasi informatika, pengelolaan informasi dan komunikasi publik[2].

Fungsi Kominfo dalam penatakelolaan aplikasi informatika tersebut salah satunya adalah sebagai penanggungjawab keamanan informasi (*information security*) yang ada di Indonesia. Hal ini dibuktikan dengan adanya Direktorat Keamanan Informasi sejak tahun 2010 yang bertugas merumuskan, melaksanakan, menyusun kebijakan, norma, standar, prosedur, kriteria dan pemberian bimbingan teknis dan evaluasi pada bidang keamanan informasi[3]. Namun pada tahun 2016 tugas Direktorat ini

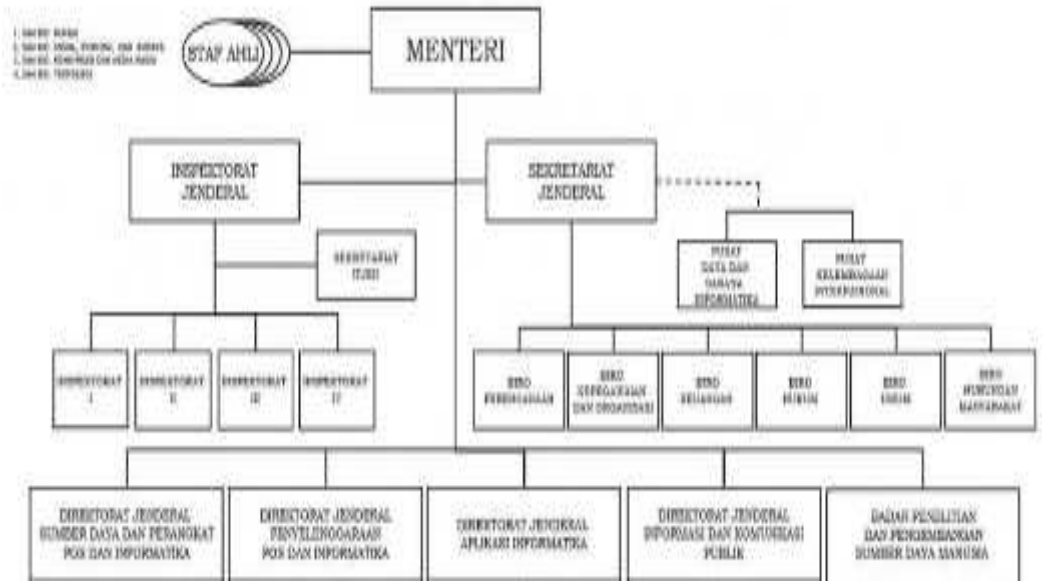
---

[1] Peraturan Presiden Republik Indonesia Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika, Pasal 2
[2] *Ibid*, Pasal 3 ayat (a) dan (b)
[3] Peraturan Menteri Komunikasi dan Informatika Nomor 17 Tahun 2010 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika, Pasal 465

berubah menjadi bidang penatakelolaan keamanan informasi[4] dan pada tahun 2018 Direktorat Keamanan Informasi yang berada di bawah Direktorat Jenderal Aplikasi Informatika Kominfo tersebut kemudian dilebur dengan Lembaga Sandi Negara (Lemsaneg) dan menjadi Badan Siber dan Sandi Negara (BSSN)[5]. Sehingga sejak diterbitkannya Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara pada 19 Mei 2017, tugas dan fungsi di bidang keamanan informasi beralih menjadi tanggungjawab dari BSSN.

4.1.1.1 Kementerian Komunikasi dan Informatika

Kementerian Komunikasi dan Informatika memiliki 7 (tujuh) unit kerja yaitu sesuai bagan berikut:

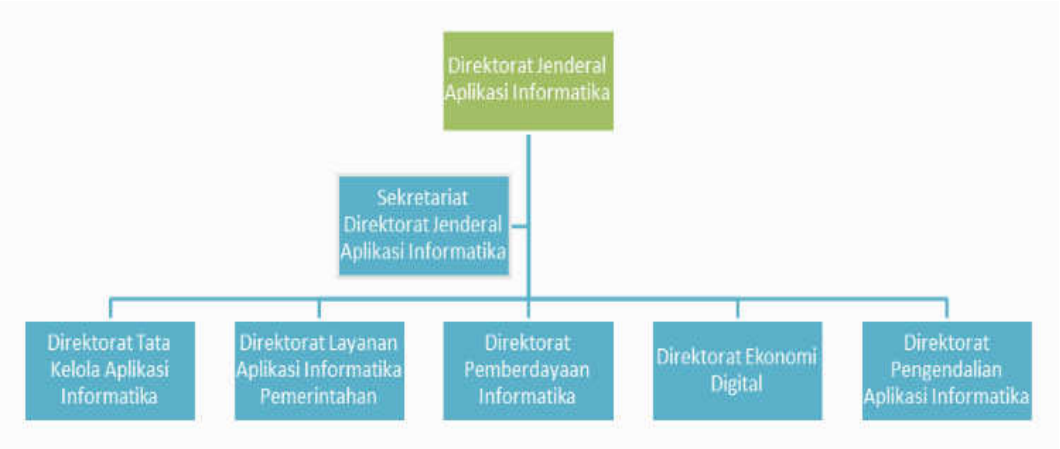


Gambar 4.1 Struktur Kementerian Komunikasi dan Informatika
Sumber: Unit Kerja dalam https://www.kominfo.go.id/unit-kerja, diakses pada 6 September 2018

[4] Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2016, tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika, Pasal 480
[5] Sejarah Pembentukan BSSN, https://bssn.go.id/sejarah-pembentukan-bssn/

a. Direktorat Jenderal Aplikasi Informatika

Direktorat Jenderal Aplikasi Informatika merupakan direktorat jenderal yang terkait langsung dengan keamanan siber dan memiliki tugas merumuskan serta melaksanakan kebijakan di bidang penatakelolaan aplikasi informatika. Sejak diterbitkannya Peraturan Menteri Komunikasi dan Informatika Nomor 6 Tahun 2018 tentang Organisasi dan Tata Kerja Komunikasi dan Informatika yang diterbitkan pada bulan Juli 2018, terdapat perubahan dalam struktur organisasi dibawah Direktorat Jenderal Aplikasi Informatika menjadi sebagai berikut:



Gambar 4.2 Struktur Direktorat Jenderal Aplikasi Informatika

Sumber: https://aptika.kominfo.go.id/profil/struktur-organisasi/,
diakses pada tanggal 6 September 2018

Berdasarkan Pasal 371 dijelaskan bahwa Direktorat Jenderal Aplikasi Informatika memiliki fungsi antara lain:

a. Perumus dan pelaksana kebijakan penatakelolaan *e-Government, e-Business* dan keamanan informasi, peningkatan teknologi dan infrastruktur aplikasi serta pemberdayaan informatika
b. Penyusun standar, prosedur, norma dan kriteria dalam pelaksanaan penatakelolaan *e-Government*
c. Pelaksanaan bimbingan teknis dan supervisi penatakelolaan *e-Government*
d. Melakukan evaluasi dan laporan di bidang penatakelolaan

e. Pelaksanaan administrasi Direktorat dan fungsi lain yang diberikan Menteri

1) Direktorat Tata Kelola Aplikasi Informatika

Direktorat Tata Kelola Aplikasi Informatika merupakan direktorat yang baru dibentuk pada tahun 2018 ini dengan tugas sebagai pelaksana perumus kebijakan, norma, standar, prosedur dan kriteria serta pelaksanaan bimbingan teknis, supervise, pemantauan serta evaluasi dan pelaporan terkait penatakelolaan aplikasi informatika. Subdirektorat tata kelola yang menangani langsung terkait sistem elektronik pada sektor perdagangan elektronik adalah Subdirektorat Tata Kelola Sistem Elektronik Ekonomi Digital, dengan fungsi menyiapkan dan merumuskan kebijakan, norma, standar, prosedur dan kriteria serta bimbingan teknis dan supervisi, pemantauan, evaluasi dan pelaporan di bidang perencanaan dan penerapan sistem elektronik dan ekonomi digital, pusat informasi jaringan internet, nama domain Indonesia dan penerimaan negara bukan pajak (PNBP) di bidang aplikasi informatika. Disamping itu subdirektorat ini bertanggungjawab dalam memberikan pelayanan terpadu.

2) Direktorat Ekonomi Digital

Direktorat ekonomi digital dalam melaksanakan fungsinya dibagi menjadi 4 (empat) subdirektorat yang salah satunya adalah subdirektorat pengembangan ekonomi digital pariwisata, transportasi dan perdangangan. Fungsi yang dijalankan oleh direktorat ini diatur pada pasal 437 yaitu adalah menyiapkan pelaksanaan kebijakan, melakukan pemantauan, evaluasi dan pelaporan di bidang pengembangan masing-masing subdirektorat, dimana salah satunya adalah *platform* perdagangan. Direktorat Ekonomi Digital adalah direktorat yang baru dibentuk pada tahun 2018 dengan tugas diatur dalam Pasal 436 yaitu melaksanakan kebijakan dan melakukan pemantauan serta evaluasi dan pelaporan di bidang ekonomi digital.

3) Direktorat Pengendalian Aplikasi Informatika

Direktorat Pengendalian Aplikasi Informatika sebelumnya dikenal dengan Direktorat Keamanan Informasi. Namun dalam nomenklatur baru yang disesuaikan dengan pembagian tugas dan tanggungjawab dengan BSSN, tugas utama direktorat ini berdasarkan Pasal 476 adalah melaksanakan kebijakan, memantau, mengevaluasi dan melaporkan segala sesuatu di bidang pengendalian aplikasi informatika. Tugas tersebut dilaksanakan melalui penyelenggaraan fungsinya sesuai Pasal 477 yaitu menyiapkan pelaksanaan kebijakan, pemantauan, evaluasi dan pelaporan di bidang pengendalian sistem elektronik termasuk ekonomi digital serta perlindungan data pribadi dan pengendalian konten, penyidikan dan pengendalian penyelenggaraan sertifikasi elektronik. Subdirektorat yang terkait langsung adalah subdirektorat pengendalian sistem elektronik, ekonomi digital dan perlindungan data pribadi serta subdirektorat pengendalian penyelenggara sertifikasi elektronik.

4.1.1.2 Badan Siber dan Sandi Negara

Obyek penelitian selanjutnya adalah BSSN yang memiliki tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengkonlosidasikan semua unsur yang terkait dengan keamanan siber[6]. Latar belakang pembentukan BSSN adalah karena Pemerintah mulai menyadari pentingnya untuk mendorong dan memperkuat keamanan siber sebagai salah satu upaya untuk meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional[7]. Untuk memenuhi tujuan tersebut maka BSSN memiliki fungsi menyusun, melaksanakan, memantau dan melakukan evaluasi terhadap kebijakan teknis di bidang identifikasi dan deteksi, proteksi dan

[6] Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, Pasal 2
[7] *Ibid,* pembukaan

penanggulangan serta pemulihan keamanan siber di berbagai sektor strategis[8].

Kepala BSSN dalam melaksanakan fungsi tersebut dibantu oleh 4 (empat) deputi yaitu Deputi Bidang Identifikasi dan Deteksi, Deputi Bidang Proteksi, Deputi Bidang Penanggulangan dan Pemulihan serta Deputi Bidang Pemantauan dan Pengendalian. Pada setiap deputi tersebut terdapat 3 (tiga) sektor utama yaitu sektor Pemerintahan, sektor IIKN (Infrastruktur Informasi Kritis Nasional) dan sektor Ekonomi Digital. Melihat adanya sektor khusus yang menangani ekonomi digital pada setiap deputi menunjukkan keseriusan Pemerintah dalam menangani pertumbuhan ekonomi digital dan isu keamanan siber yang berkembang seiring dengan kemajuan teknologi yang digunakan dalam transaksi elektronik.

a. Deputi Bidang Identifikasi & Deteksi

Deputi Bidang Identifikasi dan Deteksi bertugas sebagai penyusun dan pelaksana kebijakan teknis di bidang identifikasi dan deteksi keamanan siber dan terdiri dari 4 (empat) direktorat yaitu Direktorat Identifikasi Kerentanan dan Penilaian Resiko pada sektor Pemerintah, sektor Infrastruktur Informasi Kritikal Nasional dan sektor Ekonomi Digital serta Direktorat Deteksi Ancaman[9]. Direktorat yang menjadi obyek penelitian pada Deputi ini adalah Direktorat Identifikasi Kerentanan dan Penilaian Risiko Ekonomi Digital serta Direktorat Deteksi Ancaman.

1) Direktorat Identifikasi Kerentanan dan Penilaian Risiko Ekonomi Digital

Direktorat ini terdiri atas 3 (tiga) subdirektorat, yaitu Subdirektorat Identifikasi Kerentanan dan Penilaian Risiko Informasi Perdagangan Berbasis Elektronik, Subdirektorat Identifikasi Kerentanan dan Penilaian

[8] *Ibid*, Pasal 3 ayat (a), (b) dan (c)
[9] *Ibid,* Pasal 73

Risiko Informasi *e-Business* dan Kelompok Jabatan Fungsional[10]. Subdirektorat yang menjadi obyek penelitian ini adalah Subdirektorat Identifikasi Kerentanan dan Penilaian Risiko Informasi Perdagangan Berbasis Elektronik (*e-commerce*) mempunyai tugas melaksanakan penyiapan, penyusunan, koordinasi, pelaksanaan, pengendalian, evaluasi dan pelaporan kebijakan teknis di bidang identifikasi aset, celah keamanan, dampak dan kontrol serta analisis risiko keamanan sistem informasi *e-commerce*[11].

2) Direktorat Deteksi Ancaman

Direktorat Deteksi Ancaman memiliki tugas melaksanakan penyusunan, koordinasi, pelaksanaan, pengendalian, evaluasi dan pelaporan kebijakan teknis di bidang identifikasi potensi dan deteksi ancaman[12]. Adapun subdirektorat dibawahnya terdiri dari 4 (empat) yaitu Subdirektorat Deteksi Serangan Siber, Deteksi Sosiokultural, Deteksi Potensi Ancaman dan Kelompok Jabatan Fungsional. Pemilihan direktorat deteksi ancaman sebagai salah satu obyek penelitian adalah untuk mengidentifikasi dan menganalisa serangan siber yang terjadi dan potensi ancaman siber yang ada pada transaksi perdangangan melalui elektronik.

b. Direktorat Proteksi Ekonomi Digital

Deputi Bidang Proteksi mempunyai tugas melaksanakan penyusunan, pelaksanaan dan pengendalian kebijakan teknis di bidang proteksi keamanan siber[13]. Dalam melaksanakan tugas dan fungsinya deputi proteksi terdiri atas Direktorat Proteksi Pemerintah, Direktorat Proteksi Infrastruktur Informasi Kritikal Nasional dan Direktorat Proteksi Ekonomi Digital[14]. Direktorat Proteksi Ekonomi Digital dipilih menjadi salah

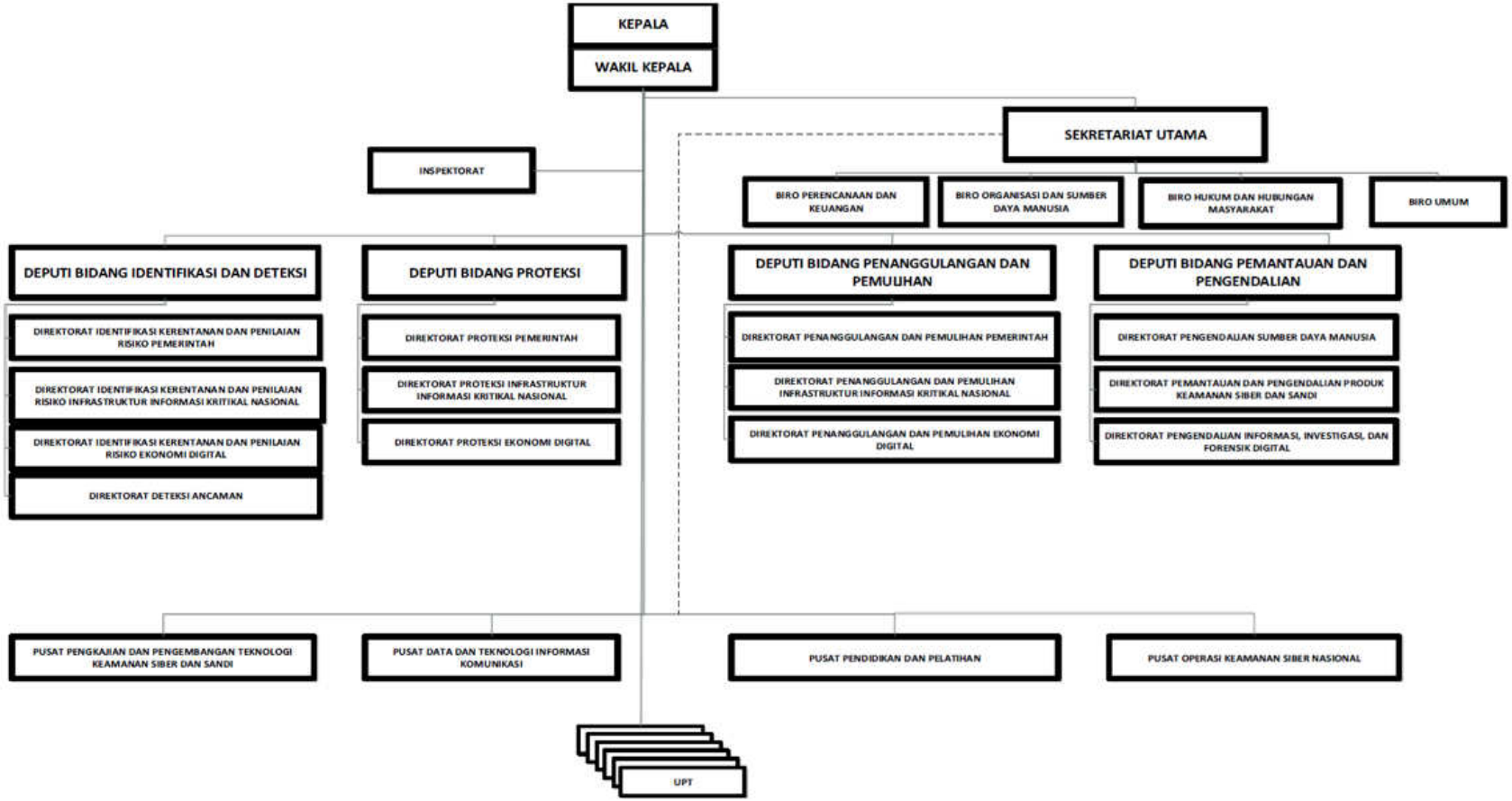
[10] Peraturan Kepala BSSN Nomor 2 Tahun 2018 tentang Organisasi dan Tata Kerja Badan SIber dan Sandi Negara, Pasal 90
[11] *Ibid*, Pasal 91
[12] *Ibid,* Pasal 93
[13] *Ibid,* Pasal 100
[14] *Ibid,* Pasal 102

satu obyek penelitian mengingat direktorat ini yang bertugas melaksanakan penyusunan, koordinasi, pelaksanaan, pengendalian, evaluasi dan pelaporan kebijakan teknis di bidang jaminan keamanan informasi ekonomi digital yang salah satunya dilaksanakan oleh Subdirektorat Proteksi Informasi Perdagangan Berbasis Elektronik[15].

c. Direktorat Penanggulangan & Pemulihan Ekonomi Digital

Deputi Bidang Penanggulangan dan Pemulihan mempunyai tugas melaksanakan penyusunan dan pelaksanaan kebijakan teknis di bidang penanggulangan dan pemulihan keamanan siber pada jaringan komunikasi pemerintah, infrastruktur vital nasional, dan ekonomi digital[16]. Direktorat Penanggulangan dan Pemulihan Ekonomi Digital melaksanakan penyusunan, koordinasi, pelaksanaan, pengendalian, evaluasi, dan pelaporan kebijakan teknis di bidang investigasi, analisis dampak insiden, mitigasi pasca insiden, penanggulangan insiden, dan pemulihan pasca insiden keamanan siber dan/atau sandi ekonomi digital[17]. Berkoordinasi langsung dengan Pusat Operasi Keamanan Siber Nasional (Pusopkamsibnas) yang merupakan bagian yang menaungi ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infractructure*) setelah dipindahkan dari Kominfo ke BSSN. Adapun struktur organisasi secara lengkap dapat dilihat pada gambar berikut:

[15] *Ibid,* Pasal 117
[16] *Ibid,* Pasal 122
[17] *Ibid,* Pasal 137



Gambar 4.3 Struktur BSSN

Sumber: Tentang BSSN dalam https://bssn.go.id/tentang/, diakses pada 5 November 2018

4.1.2 Deskripsi Umum Hasil Penelitian

Fokus penelitian ini adalah kesiapan Pemerintah dalam menghadapi ancaman siber pada sektor perdagangan melalui sistem elektronik di Indonesia dan obyek penelitian yang dipilih adalah *cyber security* dengan Kominfo dan BSSN sebagai penanggungjawab dalam mempersiapkan program keamanan siber di Indonesia terutama dalam rangka mendukung percepatan pada sektor perdagangan melalui sistem elektronik (*e-commerce*). Peraturan Presiden Nomor 74 Tahun 2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik (*Road Map E-commerce*), yang bertujuan untuk memberikan panduan strategis dalam percepatan pelaksanaan *Road Map E-commerce,* dimana Menteri Koordinator Bidang Perekonomian sebagai Ketua Komite Pengarah dengan 19 (sembilan belas) kementerian dan lembaga terkait sebagai anggotanya. Hal ini menjadi langkah awal penyusunan strategi *e-commerce* yang memiliki 7 (tujuh) fokus bidang yang dapat dilihat sesuai gambar berikut:

Gambar 4.4 *Road Map E-Commerce 2017-2019*

Sumber: Paparan Kasubdit E-Commerce Kemendag, 19 September 2018

Salah satu bagian dari peta jalan tersebut adalah bidang keamanan siber (*cyber security*) yang ditargetkan selesai pada awal tahun 2018 dengan Menteri Koordinator Politik Hukum dan Keamanan (Menkopolhukam) dan Menteri Komunikasi dan Informatika sebagai penanggungjawab. Penelitian ini menganalisis sejauh mana pencapaian program-program tersebut dan bagaimana harmonisasinya dengan program keamanan siber pada sektor ekonomi digital saat ini telah menjadi tanggungjawab BSSN. Selanjutnya penelitian ini juga menganalisis faktor-faktor penting dalam membangun sinergitas yang dibutuhkan antar lembaga/kementerian terkait, keduanya dengan memfokuskan pada 2 (dua) aspek keamanan siber yaitu aspek hukum yang menjadi landasan terlaksananya *cyber security* pada sektor *e-commerce* serta aspek organisasional terkait tugas, tanggungjawab dan kewenangan setiap lembaga/kementerian terkait dan sinergitas antar lembaga/instansi terkait lainnya untuk mencapai tujuan yang diharapkan.

Adapun data yang digunakan dalam bab ini adalah merupakan data primer melalui wawancara dengan narasumber yang sudah ditentukan sebelumnya yaitu dari Kominfo yang terdiri dari Staff Ahli Menteri Bidang Teknologi, Direktur Pengendalian Aplikasi Informatika, Kepala Subdirektorat Tata Kelola Sistem Elektronik serta Kepala Seksi Direktorat Ekonomi Digital. Sedangkan narasumber dari BSSN terdiri dari Direktur Deteksi Ancaman, Direktur Penanggulangan dan Pemulihan Ekonomi Digital, Kepala Subdirektorat Proteksi Ekonomi Digital dan Kepala Subdirektorat Identifikasi Kerentanan dan Penilaian Resiko. Disamping itu terdapat narasumber dari Kementerian Perdagangan yaitu Kepala Subdirektorat *E-Commerce*, serta tim tenaga ahli dari Kemenkokuin, pakar *cyber security* dari Institut Teknologi Bandung (ITB) dan perwakilan komunitas *cyber security* (ICSF) serta pelaku *e-commerce* (LiteBig).

Disamping itu penelitian ini juga menggunakan data sekunder yang diperoleh dari instansi terkait dan/atau yang dirujuk oleh narasumber

sehingga dapat digunakan untuk menganalisis kesiapan *cyber security* pada sektor *e-commerce* di Indonesia serta faktor-faktor penting yan dalam meningkatkan sinergitas antar lembaga/kementerian terkait *cyber security* pada sektor tersebut, sebagai salah satu tulang punggung perekonomian di Indonesia, guna mendukung visi Pemerintah menuju negara dengan ekonomi digital terbesar di Asia Tenggara.

4.1.3 *Cyber Security* pada sektor *E-Commerce* di Indonesia

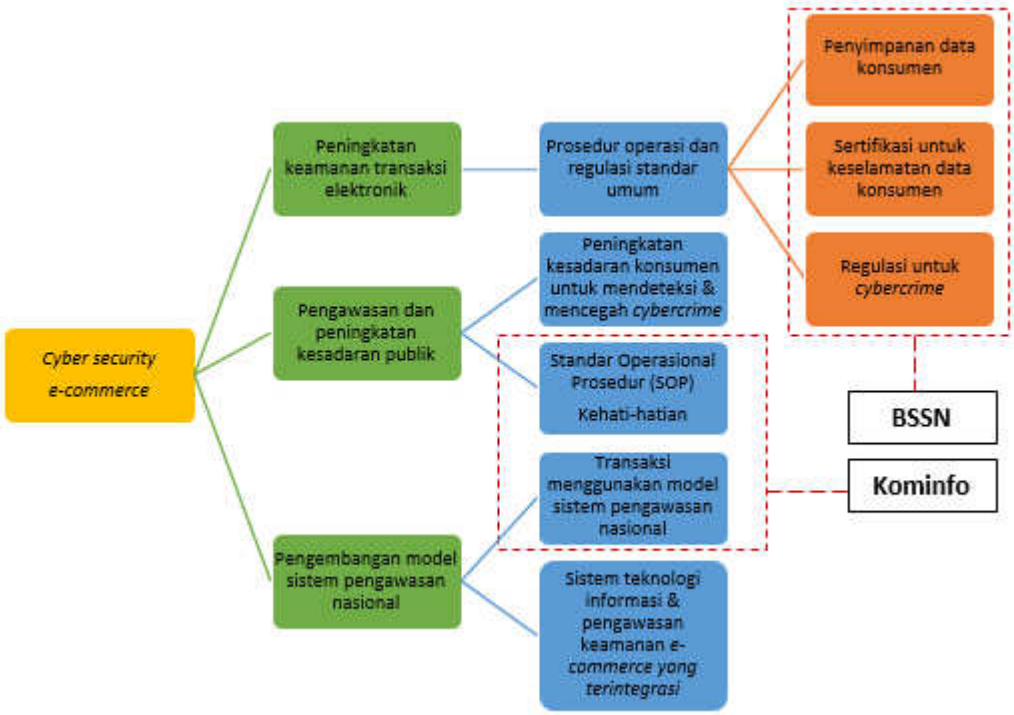
Potensi *e-commerce* Indonesia yang tinggi menurut kasubdit *e-commerce* Kementerian Perdagangan (wawancara, 2018) sebagai narasumber dari pengampu sektor, dikarenakan oleh potensi pasar Indonesia yang merupakan terbesar ke-4 (keempat) di dunia, yaitu 262 juta orang dengan 143,26 juta atau 54,68% pengguna internet per tahun 2017. Jumlah transaksi retail *e-commerce* tercatat hingga USD 7,056 juta di tahun 2017 dan diperkirakan mencapai USD 8, 591 juta di tahun 2018. Lebih lanjut kasubdit *e-commerce* Kemendag menjelaskan dari aspek penerapan teknologi pada Usaha Kecil Menengah (UKM) di Indonesia, Kementerian Perdagangan membagi menjadi 4 (empat) kategori yaitu memiliki akses internet (bisnis online dasar), menggunakan jejaring sosial (bisnis online menengah), memiliki kemampuan bisnis *e-commerce* (bisnis online lanjutan) dan yang belum memanfaatkan jaringan online (UKM offline), yang presentasenya dapat dilihat sesuai gambar berikut:

Gambar 4.5 Data penerapan teknologi pada UKM Indonesia

Sumber: Paparan Kasubdit E-Commerce Kemendag, 2018

Melihat masih belum optimalnya pemanfaatan ekonomi digital diharapkan dapat diatasi dengan adanya *road map* yang sudah disusun. Salah satu yang menjadi tanggungjawab Kemendag berdasarkan peta jalan tersebut adalah menyusun kebijakan untuk transaksi perdagangan sistem elektronik yang sebenarnya sudah diamanatkan pada Pasal 66 Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan. Tugas Kemendag antara lain terdiri dari 4 (empat) yaitu menyusun Peraturan Pemerintah mengenai *e-commerce,* menyusun Permendag tentang pendaftaran pelaku usaha *e-commerce,* edukasi *e-commerce* kepada stakeholder dan pengembangan fasilitator edukasi *e-commerce.* Namun terkait program di bidang keamanan siber, Kemendag sebagai *leading sector* mempercayakan sepenuhnya kepada BSSN dan Kominfo dan mendukung program yang dibutuhkan namun dengan harapan tidak mempersulit perkembangan *e-commerce*.

Khusus aspek keamanan siber yang diatur dalam peta jalan, terdapat 3 (tiga) program, 3 (tiga) kegiatan dan 5 (lima) keluaran dengan penanggungjawab adalah Kominfo dan Menkopolhukam. Namun dengan adanya BSSN sebagai penanggungjawab keamanan siber nasional, berdasarkan informasi dari Kasubdit Direktorat Proteksi Ekonomi Digital BSSN (wawancara, 2018), akan dilakukan pengalihan tugas dari Menkopolhukam kepada BSSN. Pada wawancara tersebut juga disampaikan bahwa BSSN sendiri sedang menyusun Pedoman Pengamanan Transaksi Perdagangan melalui Sistem Elektronik sebagai tindak lanjut Perpres tersebut. Sedangkan menurut keterangan dari Direktur Pengendalian Aptika Kominfo (wawancara, 2018), yang menjadi tugas Kominfo dalam Perpres 74 Tahun 2017 adalah menyusun pedoman kehati-hatian dan menganalisa model sistem pengawasan transaksi *e-commerce* nasional. Namun selain 2 (dua) hal tesebut, program lainnya bukan merupakan tugas dan tanggungjawab Kominfo. Sehingga secara detail program dan pembagian tugasnya dapat dilihat pada gambar berikut:



Gambar 4.6 Program *Cyber Security Road Map E-Commerce*

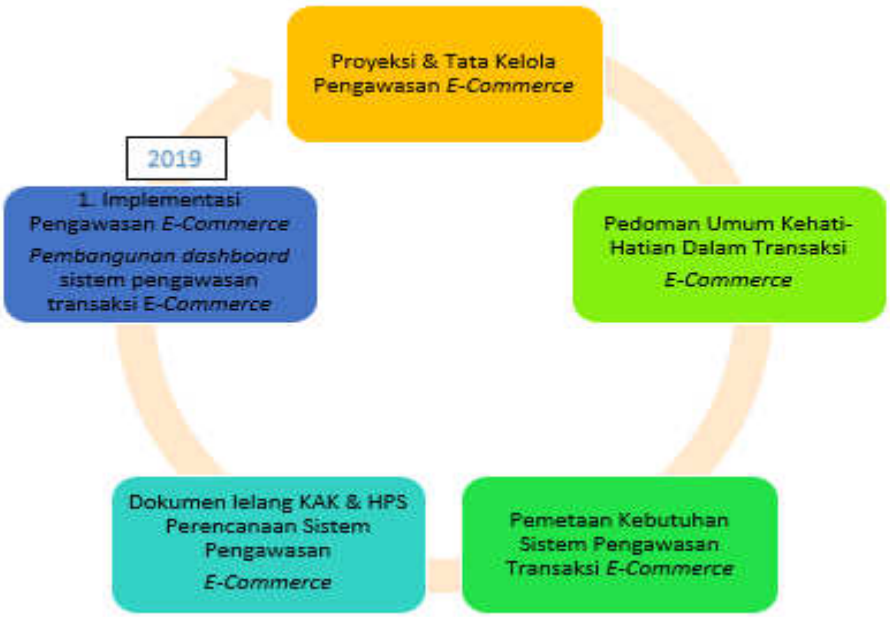
Sumber: diolah oleh peneliti, 2018.

Tim Tenaga Ahli *Road Map E-commerce* Kemenkokuin (wawancara, 2018) membenarkan bahwa dalam kegiatan evaluasi 1 (satu) tahun pelaksanaan peta jalan *e-commerce* yang dilaksanakan pada tanggal 3 Oktober 2018 di Hotel Borobudur Jakarta, disampaikan bahwa belum terdapat keluaran sesuai yang diharapkan pada aspek keamanan siber. Saat ini kegiatan pada aspek *cyber security* yang sedang berjalan adalah penyusunan prosedur operasi dan regulasi standar umum yang terkait dengan penyimpanan data konsumen, sertifikasi untuk keselamatan data konsumen serta perumusan regulasi untuk *cybercrime*[18]. Lebih lanjut ketua tim tenaga ahli yang juga merupakan wakil ketua bagian hubungan pemerintahan Asosiasi E-Commerce Indonesia (idEA) menjelaskan bahwa

[18] Salahuddin Rudy Deputi Bidang Koordinasi Ekonomi Kreatif, Kewirausahaan dan Daya Saing KUKM, Capaian dan Kendala Pelaksanaan Perpres 74 Tahun 2017, 3 Oktober 2018, Jakarta

ketiga keluaran tersebut merupakan hasil yang diharapkan dari program peningkatan keamanan atas prinsip aktivitas transaksi elektronik, dimana bentuk kegiatannya diharapkan dapat meningkatkan penerapan prinsip-prinsip keamanan siber oleh pedagang online dan/atau operator[19].

Sedangkan terkait 2 (dua) program keamanan siber lainnya yang menjadi bagian dari Kominfo belum termasuk dalam program yang selesai atau sedang berjalan, namun pada kesempatan wawancara tersebut informan tersebut tidak mengetahui kelanjutan atas program yang belum terselesaikan, meskipun target waktu yang ditetapkan sudah berlalu namun hasil yang diharapkan belum tercapai. Perkembangan penyusunan program keamanan siber untuk *road map e-commerce* yang telah dilakukan oleh Kominfo menurut keterangan dari kasubdit tata kelola sistem elektronik Kominfo (wawancara, 2018) dapat dilihat secara lebih detail dalam gambar dibawah ini:



Gambar 4.7 Laporan Progress Road Map Kebijakan & Pedoman Kehati-hatian dan Pengawasan Nasional *E-commerce*
Sumber: Paparan Kasubdit Tata Kelola Sistem Elektronik Kominfo, 2018

[19] Lampiran Peraturan Presiden Nomor 74 Tahun 2017 tentang *Road Map E-Commerce 2017-2019,* huruf G Nomor 23.

Berdasarkan wawawancara dengan kasubdit tata kelola sistem elektronik yang bertanggungjawab terhadap penyusunan ini (wawancara, 2018), membenarkan bahwa saat ini Kominfo masih menyelesaikan kotak 2-3 pada gambar 4.7 diatas, yaitu penyusunan pedoman umum dan pemetaan kebutuhan sistem pengawasan, dimana diperlukan pemetaan resiko pada masing-masing bagian dalam transaksi perdagangan elektronik untuk dapat mengetahui aspek yang perlu diwaspadai dan bagaimana model pengawasan yang tepat. Contoh pengawasan yang dilakukan apakah terkait perpajakan, konten lokal dari barang yang diproduksi atau logistik dari transaksi elektronik, karena masing-masing aspek tersebut termasuk dalam rantai *e-commerce* namun tidak semua aspek memerlukan pengawasan. Hingga saat ini Kominfo masih belum mendapatkan arahan yang jelas dari Kementerian Perdagangan sebagai pengampu sektor, mengenai model pengawasan yang dibutuhkan pada transaksi *e-commece.*

Kasubdit *e-commerce* Kementerian Perdagangan (wawancara, 2018) juga membenarkan tentang belum jelasnya model pengawasan yang dimaksud, namun mereka berharap Kemenkokuin sebagai pengarah *road map e-commerce* yang dapat memutuskan pengawasan yang diharapkan. Menurut keterangan narasumber tenaga ahli dari sekretariat *road map e-commerce* Kemenkokuin (wawancara, 2018) menyatakan bahwa hal ini memerlukan penentuan tujuan akhir dari *e-commerce* yang harus diperjelas sehingga dengan berkembangnya nilai transaksi *e-commerce* harus benar-benar menguntungkan masyarakat Indonesia dan bukan hanya menjadi pasar. Informan menambahkan bahwa kondisi *e-commerce* Indonesia saat ini perlu kebijakan seperti China yang menetapkan batasan bahwa hanya 40% yang merupakan barang yang berasal dari global, sehingga produk lokal dapat berkembang. Hal ini tentu membutuhkan kerjasama dan kesadaran dari seluruh sektor, sehingga potensi ekonomi digital yang ada dapat benar-benar dimanfaatkan untuk pertumbuhan ekonomi nasional.

Narasumber dari BSSN, Kasubdit Identifikasi Kerentanan dan Penilaian Resiko Informasi *E-commerce* (wawancara, 2018) juga membenarkan bahwa saat ini Pemerintah memang sedang mengupayakan penyusunan profil resiko *e-commerce* nasional melalui *information gathering* yang dilakukan dengan pelaku usaha. Melalui SOP transaksi *e-commerce* yang disusun oleh BSSN juga diharapkan dapat menjadi panduan bagi para pelaku perdagangan elektronik. SOP kehati-hatian bertransaksi tersebut merupakan keluaran program pertama dalam aspek *cyber security e-commerce.* Kemendag menyatakan bahwa dalam RPP Transaksi Perdagangan Melalui Sistem Eletronik (RPP TPMSE) yang sedang disusun nantinya hanya mencantumkan kewajiban untuk mengikuti standar keamanan sesuai peraturan perundang-undangn yang berlaku yaitu baik yang disusun oleh BSSN maupun Kominfo. Sedangkan terkait pengawasan transaksi *e-commerce*, narasumber dari Direktorat Identifikasi Kerentanan dan Penilaian Resiko Ekonomi Digital BSSN (wawancara, 2018) menyatakan berusaha mendorong setiap pelaku usaha untuk dapat melakukan *self assessment* terutama terhadap kerentanan dan resiko yang dimiliki sesuai dengan yang sudah diatur pada Indeks KAMI.

Hal ini diperlukan mengingat, kasubdit *e-commerce* Kemendag (wawancara, 2018) juga menyatakan terdapat kesulitan pengumpulan data *e-commerce*, dimana Kominfo dalam pendaftaran sistem dan transaksi elektronik belum memiliki pengkategorian untuk khusus pelaku perdagangan elektronik dan belum adanya klasifikasi data yang dianggap penting pada sektor perdagangan melalui elektronik. Isu lainnya disampaikan oleh narasumber wakil ketua idEA (wawancara, 2018) yang menyatakan bahwa belum adanya regulasi perlindungan data yang sebenarnya justru merupakan isu keamanan siber yang berpengaruh pada perkembangan transaksi *e-commerce* secara global atau yang saat ini lebih dikenal dengan istilah *cross border e-commerce.* Sehingga untuk menjadi

negara dengan ekonomi digital terbesar di Asia Tenggara pada tahun 2020, kebijakan terkait perlindungan data menjadi salah satu syarat utama.

4.1.4 Kesiapan *Cyber security e-commerce* di Indonesia

Analisa terhadap kesiapan *cyber security e-commerce* Indonesia diperlukan mengingat visi Pemerintah untuk menjadikan Indonesia sebagai negara dengan ekonomi digital terbesar di Asia Tenggara. Visi tersebut tentu menjadi tujuan bagi setiap kebijakan dan rencana kerja yang disusun untuk pertumbuhan ekonomi digital yang dicita-citakan. Namun seiring dengan semakin besarnya perekonomian suatu negara maka semakin besar pula celah serangan yang dapat dilakukan oleh pihak lawan, terutama ketika salah satu andalan dari perekonomian tersebut adalah perdagangan melalui elektronik. Sehingga untuk mempersiapkan diri diperlukan kesiapan pada aspek kebijakan sebagai landasan untuk setiap perencanaan dan aspek organisasional sebagai pelaksana disamping aspek teknis dan aspek Sumber Daya Manusia (SDM) yang juga menjadi standar kesiapan dalam dimensi *cyber security*.

Untuk menilai kesiapan *cyber security e-commerce* yang dimiliki Indonesia maka dapat melihat aspek hukum dan aspek organisasi pada keamanan siber perdagangan melalui sistem elektronik yang telah dimiliki oleh Indonesia dan standar yang ada di negara lain di Asia Tenggara yang dinilai sudah lebih siap pada aspek keamanan siber, yaitu Malaysia dan Singapura. Berdasarkan keterangan narasumber dari deputi identifikasi kerentanan dan penilaian resiko BSSN (wawancara, 2018), Malaysia sudah setahun lebih awal membuat inisiatif *National E-commerce Strategic Roadmap* pada tahun 2016, Malaysia menargetkan perkembangan *e-commerce* 2 (dua) kali lipat pada tahun 2020, dengan fokus pada 6 (enam) area yang dirumuskan ke dalam 11 (sebelas) program. Sedangkan Singapura, sudah sejak lama memulai pengaturan pada sektor *e-commerce* yaitu sejak diperkenalkannya *E-Commerce Hotbed Program*

pada tahun 1996 dan dilanjutkan dengan pengaturan yang lebih spesifik pada *Electronic Commerce Master Plan* pada tahun 1998. Visi Singapura adalah menjadi pusat *e-commerce* internasional sudah mulai dicanangkan melalui *master plan* tersebut dengan mendorong pembangunan kekuatan dalam perdagangan internasional, jasa keuangan internasional serta infrastruktur telekomunikasi dan transportasi.

4.1.4.1 Aspek Hukum

Peraturan perundang-undangan merupakan salah satu sarana prasarana yang dapat digunakan untuk mencapai tujuan yang dicita-citakan. Berdasarkan informasi yang dihimpun dari seluruh narasumber, saat ini keamanan siber *e-commerce* masih sepenuhnya tergantung pada regulasi terkait sistem elektronik yang ada di Kominfo, yaitu UU ITE dan Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Apabila dilihat dari aspek strategi yang dibutuhkan untuk dapat menghadapi serangan siber, regulasi yang disusun dapat dilihat menjadi 3 (tiga) aspek yaitu pembentukan, merespon dan menyiapkan diri, yang berdasarkan wawancara dengan narasumber dari BSSN dapat dilihat pada tabel berikut:

Tabel 4.1
Elemen Strategi dalam Regulasi *E-Commerce*

Level	Regulasi
Pembentukan	**Pasal 16 Undang-Undang ITE:** 1. Dapat menampilkan kembali informasi eletronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan 2. Dapat melindungi ketersediaan, keutuhan, keontetikan, kerahasiaan dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik 3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik

	4. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi atau simbol yang dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik 5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaharuan, kejelasan dan kebertanggungjawaban prosedur atau petunjuk
Merespon	**Pasal 20 PP PSTE:** 1. Wajib memiliki dan menjalankan prosedur dan sarana untuk menghindari gangguan, kegagalan dan kerugian 2. Wajib memiliki sistem pengamanan yang melingkupi prosedur dan sistem pencegahan & penanggulangan terhadap ancaman dan serangan 3. Apabila terjadi gangguan atau kegagalan pada sistem yang berdampak, maka wajib mengamankan data dan segera melaporkan dalam kesempatan pertama kepada pihak yang berwajib dan Instansi Pengawas dan Pengatur Sektor (IPPS) terkait
Menyiapkan diri	**Pasal 22 PP PSTE:** Wajib menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan dan dapat ditelusurinya suatu informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan

Sumber: Wawancara dengan Direktur Deteksi Ancaman BSSN, 2018

Narasumber juga menjelaskan bahwa ketiga aspek regulasi tersebut dituangkan dalam berbagai peraturan dan kebijakan yang bersifat operasional diharapkan dapat mengimplementasikan manajemen keamanan yang ditetapkan oleh Pemerintah. Penyelenggaraan keamanan siber menurut Strategi Keamanan SIber Nasional mencakup antara lain Pencegahan, Penanggulangan, Pemulihan, Evaluasi dan Penyempurnaan[20]. Berbagai regulasi operasional yang sudah

[20] Kementerian Koordinator Bidang Politik, Hukum dan Keamanan, *Strategi Keamanan Siber Nasional Indonesia,* (Kemenkopolhukam, 2017), hlm 25.

diimplementasikan apabila dibagi dalam cakupan penyelenggaraan keamanan siber maka dapat dilihat sesuai tabel berikut:

Tabel 4.2
Aspek *Cyber Security* dalam Regulasi *E-Commerce*

Pencegahan	1. Peraturan Menteri Nomor Komunikasi dan Informatika Nomor 36 Tahun 2014 tentang Tata Cara Pendaftaran Penyelenggaraan Sistem Elektronik 2. Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2018 tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik Bidang Komunikasi dan Informatika serta Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik 3. Peraturan Menteri Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik 4. Surat Edaran Menteri Komunikasi dan Informatika Nomor 5 Tahun 2016 tentang Batasan dan Tanggungjawab Penyedia Platform dan Pedagang (*Merchant*) Perdagangan Melalui Sistem Elektronik yang berbentuk *User Generated Content*
Penanggulangan & Pemulihan	1. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manejemen Pengamanan Informasi 2. Pedoman Indeks KAMI
Evaluasi & Penyempurnaan	1. Revisi Peraturan Pemerintah nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik 2. Rancangan Peraturan Pemerintah tentang Transaksi Perdagangan Melalui Sistem Elektronik 3. Rancangan Undang-Undang Perlindungan Data 4. Rancangan Undang-Undang Keamanan SIber

Sumber: diolah oleh peneliti, 2018

Namun apabila dibandingkan dengan regulasi yang ada di negara lain di Asia, melalui laporan UNCTAD tahun 2013 dibawah ini dapat dilihat bahwa 6 (enam) regulasi utama yang dibutuhkan dalam *e-commerce* yaitu

transaksi elektronik, privasi, *cybercrime*, perlindungan konsumen, regulasi terkait konten serta nama domain telah tersedia. Ketiadaan 2 (dua) bidang regulasi yaitu *privacy* dan *consumer protection* di Indonesia hingga saat ini juga masih belum berubah. Secara lebih jelas perbedaan kesiapan aspek regulasi diantara Indonesia, Malaysia dan Singapura dapat dilihat pada gambar berikut[21]:

Member Country	Electronic Transactions	Privacy	Cybercrime	Consumer Protection	Content Regulation	Domain Names
Brunei Darussalam	Enacted	None	Enacted	Partial	Enacted	Enacted
Cambodia	Draft	None	Draft	None	Draft	Enacted
Indonesia	Enacted	Partial	Enacted	Partial	Enacted	Enacted
Lao People's Democratic Republic	Enacted	None	None	Draft	Enacted	Partial
Malaysia	Enacted	Enacted	Enacted	Enacted	Enacted	Enacted
Myanmar	Enacted	None	Enacted	Enacted	Enacted	Enacted
Philippines	Enacted	Enacted	Enacted	Enacted	None	Enacted
Singapore	Enacted	Enacted	Enacted	Enacted	Enacted	Enacted
Thailand	Enacted	Partial	Enacted	Enacted	Partial	Partial
Viet Nam	Enacted	Partial	Enacted	Enacted	Enacted	Enacted

Gambar 4.8
Status Harmonisasi Regulasi *E-Commerce* di ASEAN per Maret 2013
Sumber: UNCTAD, 2013

Menurut informan dari *founder* ICSF (wawancara, 2018) ketertinggalan Indonesia pada aspek kebijakan merupakan hambatan dalam mempersiapkan diri menghadapi tantangan pada era ekonomi digital. Menurut informan yang merupakan kasubdit terkait *e-commerce* dari Kementerian Perdagangan (wawancara, 2018) sejauh ini proses penyusunan regulasi lebih lanjut yang mengatur detail teknis *e-commerce* masih menunggu penerbitan rancangan peraturan pemerintah (RPP) transaksi perdagangan melalui sistem elektronik yang sedang dalam proses persetujuan di lembaga legislatif. Narasumber tersebut

[21] United Nations, *Review of e-commerce legislation harmonization in the ASEAN,* (US: United Nations Publication, 2013), Hlm 5.

menambahkan bahwa RPP TPMSE tersebut dirancang untuk menjadi payung hukum bagi regulasi terkait *e-commerce* lainnya, yaitu antara lain peraturan menteri perdagangan terkait pendaftaran dan peraturan kepala BSSN terkait SOP Kehati-hatian serta peraturan bidang komunikasi dan informatika terkait SOP penyimpanan data dan perlindungan data. melihat Apabila dibandingkan denganperkembangan negara Malaysia yang memiliki kebijakan yang disebut Malaysia Super Koridor, berdasarkan keterangan dari tenaga ahli *cyber security e-commerce* Kemenkokuin (wawancara, 2018) kebijakan di Malaysia dibangun dengan konsensus instansi/lembaga terkait untuk merevisi peraturan siber setiap 2 (dua) tahun sekali. Revisi tersebut juga dapat digunakan oleh setiap instansi terkait tanpa harus membuat regulasi baru.

Sedangkan di Indonesia, rancangan undang-undang perlindungan data privasi yang menurut keterangan dari komunitas *cybersecurity* (wawancara, 2018) telah diusulkan sejak tahun 2000, masih belum juga menjadi prioritas sekalipun berbagai isu terkait data privasi sudah berkembang pesat baik secara global maupun nasional. Perlindungan data sebenarnya sudah diatur dalam Peraturan Menteri, namun karena bentuknya hanya sebatas peraturan menteri dan hanya bersifat administratif sehingga tidak terlihat dalam penegakan hukumnya. Direktur deteksi Ancaman BSSN (wawancara, 2018) menjelaskan bahwa ada negara yang sudah memiliki regulasi terkait perlindungan data, penegakan hukum bukan hanya bersifat administratif melainkan juga masuk pada ranah pidana dan perdata.

Informan dari pakar *cyber* (wawancara, 2018) melihat hal ini berpendapat bahwa hal ini dikarenakan *culture* masyarakat Indonesia yang pada dasarnya tidak mempermasalahkan privasi. Informan pakar tersebut juga menambahkan perlunya pendalaman terkait bisnis jual-beli data yang berkembang di Indonesia apakah justru terdorong dengan tidak adanya peraturan tersebut. Kendala lain pada aspek hukum menurut pendapat

tenaga ahli *cyber security* Kemenkokuin (wawancara, 2018) adalah lambatnya proses untuk memperoleh pengesahan terhadap sebuah regulasi yang telah disusun sehingga tertinggal dengan kecepatan teknologi. Lebih lanjut menurut narasumber beberapa regulasi masih menemui kendala, yaitu antara lain terkait pendaftaran yang masih memerlukan harmonisasi dengan yang terdapat pada Badan Koordinasi Penanaman Modal (BKPM) dimana setiap bidang usaha telah memiliki perijinan dan *e-commerce* merupakan aspek online dari berbagai bidang usaha tersebut.

Mengenai regulasi pada level operasional yang spesifik mengatur tentang mekanisme respon terhadap serangan siber di bidang *e-commerce* menurut BSSN (wawancara, 2018) saat ini sedang dalam proses penyusunan, yaitu Penyelenggaraan dan Pelaksanaan Penganggulangan dan Pemulihan Insiden Keamanan Siber dan Sandi Sektor Ekonomi Digital dan SOP keamanan bertransaksi untuk pelaku *e-commerce,* serta SOP kehati-hatian untuk konsumen, yang sedang disusun oleh Kominfo. Sektor *e-commerce* menurut keterangan dari Direktur Deteksi Ancaman BSSN (wawancara, 2018), belum memiliki prosedur formal yang khusus mengatur penggunaan sumber daya yang spesifik pada level operasional.Namun menurut Tim Ahli dari Kemenkokuin (wawancara, 2018) dalam proses penyusunan regulasi, seluruh lembaga Pemerintahan telah memiliki perspektif yang seragam mengenai tujuan regulasi yang diharapkan tidak menghambat pertumbuhan *e-commerce* melainkan dapat mendukung pengembangannya.

Dari pengalaman informan pelaku *e-commerce* (wawancara, 2018), Indonesia terbilang sangat minim dalam pengaturan penyelenggaraan sistem elektronik dan dengan sistem pendaftaran membuat pelaku usaha tidak merasa memiliki kewajiban untuk harus melakukannya selama tidak ada kendala pada sistem elektronik yang dijalankan. Dalam menerapkan kebijakan yang dapat mendorong *cyber security* pada sektor *e-commerce,*

Pemerintah menyusun sebuah panduan yang disebut Indeks KAMI. Indeks KAMI merupakan alat bantu dalam menganalisa dan mengevaluasi kesiapan penerapan keamanan informasi pada sebuah organisasi berdasarkan kriteria yang ada pada SNI ISO/IEC 27007 yang terdiri dari 5 (lima) aspek yaitu aspek tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset dan aspek teknologi. yang wilayah pengaturannya dapat dilihat sesuai gambar berikut:

Gambar 4.9 INDEKS KAMI

Sumber: https://bssn.go.id/indeks-kami/, diakses pada 25 November 2018

Selain melakukan pemeringkatan indeks KAMI, BSSN juga mendorong para pelaku *e-commerce* untuk dapat memiliki kemampuan dalam manajemen risiko berdasarkan standar Indeks KAMI. Pelaksanaan self assessment dengan melakukan penilaian resiko yang bertujuan agar pelaku *e-commerce* mengetahui dan memahami resiko yang dihadapi dalam penyelenggaraan bisnisnya. Salah satu cara untuk meminimalisir resiko yang harus diikuti oleh pelaku usaha adalah memenuhi 6 (enam) aspek keamanan informasi penggunaan sistem dan transaksi elektronik yang dilakukan, yaitu kerahasiaan, integritas, ketersediaan, keauntentikan, otorisasi dan kenirsangkalan sesuai ketentuan perundangan yang berlaku[22].

[22] Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pasal 38 ayat (3).

Aspek-aspek keamanan informasi tersebut dapat dipenuhi dengan penggunaan beberapa metode keamanan informasi yang ada, namun menurut informan Kominfo (wawancara, 2018), Pemerintah saat ini mendorong penggunaan *digital signature* dan *digital certificate.* Dengan diterbitkannya Permen Kominfo nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik maka diharapkan dapat mendorong penggunaan tanda tangan elektronik. Informan dari BSSN yang merupakan Kasubdit Proteksi (wawancara, 2018) juga sepakat bahwa penggunaan CA yang dapat membantu memenuhi aspek keamanan informasi yang dibutuhkan dalam transaksi elektronik.

Salah satu isu lain terkait keamanan siber pada revisi PP PSTE tersebut adalah terkait pengaturan kewajiban membangun data center di Indonesia, dimana masih terdapat perbedaan pendapat baik di kalangan internal Pemerintahan maupun di antara para pakar dan pelaku *e-commerce* tentang penghapusan kewajiban tersebut. Disamping itu salah satu hasil evaluasi kebijakan yang tidak terimplementasi dengan maksimal adalah Peraturan Menteri tentang Perlindungan Data yang disadari tidak memiliki kekuatan hukum yang cukup untuk dapat memaksa penyelenggara sistem dan transaksi elektronik untuk menjaga kerahasiaan informasi selayaknya perlindungan terhadap konsumen sehingga harus ditingkatkan menjadi setidaknya Undang-Undang, menurut Direktur Pengendalian Aptika Kominfo (wawancara, 2018).

Kesimpulan yang dapat diambil terkait berdasarkan wawancara dengan informan dari luar Pemerintahan sepakat aspek hukum pada *cyber security* di *e-commerce* sudah dapat dikategorikan berjalan dengan baik sekalipun belum dapat dinilai berhasil karena masih terbatasnya regulasi yang dibutuhkan akibat lambatnya proses penyusunan. Narasumber juga menambahkan bahwa bahwa pada implementasi tidak ada standar yang baku sehingga pelaksanaannya hanya berdasarkan *best practice* di kalangan pelaku usaha. Kelonggaran dalam penetapan standar ini diakui

narasumber yang merupakan Direktur Pengendalian Aptika Kominfo sebagai bagian dari upaya Pemerintah untuk tidak menghambat pertumbuhan ekonomi digital (wawancara, 2018). Disamping itu, pada evaluasi dan penyempurnaan masih dikategorikan minim karena keterbatasan pelaksanaan monitoring dan audit terhadap pelaku *e-commerce*. Ditambahkan oleh informan yang merupakan Direktur dari BSSN (wawancara, 2018), bahwa terdapat keterbatasan aspek penegakan hukum karena sanksi masih bersifat administratif sehingga baik BSSN maupun Kominfo memiliki keterbatasan dalam melakukan penindakan yang dibutuhkan untuk menjamin terlaksananya *cyber security* pada sektor *e-commerce.*

4.1.4.2 Aspek Organisasi

Dari sudut pandang pertahanan siber, penunjukan Kementerian Komunikasi dan Informatika sebagai penanggungjawab sudah sejalan dengan pedoman Pertahanan Siber yang dirumuskan dalam Peraturan Menteri Pertahanan Nomor 82 Tahun 2014, dimana Kementerian Komunikasi dan Informatika adalah sebagai unsur utama kekuatan pertahanan nirmiliter di ranah siber. Namun dengan adanya Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang bertugas melaksanakan *cyber security*, maka peran BSSN dalam strategi *cyber security e-commerce* tidak dapat diabaikan. Apabila merujuk kepada pedoman pertahanan siber yang diterbitkan oleh Kementerian Pertahanan, dalam penyelenggaraan pertahanan siber harus memenuhi persyaratan antara lain perumusan tugas, fungsi dan kewenangan yang jelas termasuk untuk melakukan koordinasi.

Namun berdasarkan keterangan yang diberikan narasumber salah satu Direktur di Kominfo dan BSSN yang terkait (wawancara, 2018), sepakat menyatakan bahwa belum ada payung hukum terpadu yang

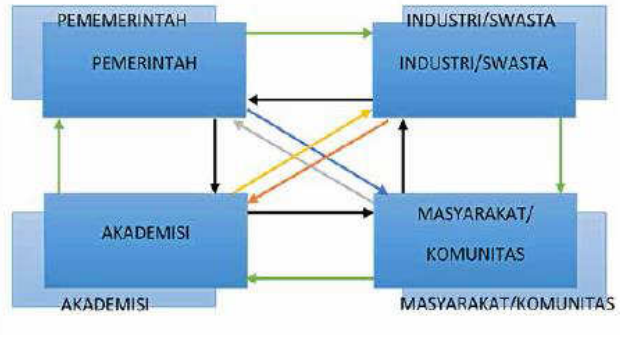
mengatur pembagian tugas dan tanggungjawab antar lembaga dalam mewujudkan *cyber security e-commerce*. Hingga saat ini regulasi yang ada masih bersifat parsial dan tersebar dalam berbagai level peraturan. Kominfo masih berpegang pada tugas dan tanggungjawab yang diamanahkan oleh Undang-Undang ITE dan Peraturan Pemerintah tentang PSTE. Namun dengan diterbitkannya Perpres tentang BSSN, maka Kominfo segera melakukan penyesuaian yang diperlukan yaitu antara lain dengan dialihkannya tugas dan fungsi Direktorat Keamanan Informasi dan ID-SIRTII ke BSSN.

BSSN sendiri telah melakukan pembentukan struktur organisasi melalui diterbitkannya Peraturan Kepala BSSN Nomor 2 Tahun 2018 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara pada 30 Januari 2018. Kominfo juga melakukan pengesahan perubahan struktur organisasi yang dimuat dalam Peraturan Kominfo Nomor 6 Tahun 2018 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika pada 19 Juli 2018. Hubungan fungsional diantara Kominfo sebagai kementerian dan BSSN sebagai lembaga non kementerian telah diatur dalam Undang-Undang Kementerian Negara, yaitu dilaksanakan secara sinergis sebagai satu sistem pemerintahan dan diatur lebih lanjut melalui Peraturan Presiden[23]. Berbeda dengan Kominfo yang sudah memiliki dasar hukum yang kuat mengenai tugas dan tanggungjawabnya dengan adanya UU ITE, pelaksanaan tugas dan tanggungjawab yang BSSN menurut Direktur Penanggulangan dan Pemulihan (wawancara, 2018) dirasa belum efektif karena belum adanya regulasi setingkat undang-undang yang menjadi landasannya.

Narasumber menambahkan bahwa sejak dibentuk BSSN secara aktif mengupayakan sinergitas dengan kementerian dan lembaga non kementerian lainnya dalam bentuk kolaborasi dan koordinasi. Dalam

[23] Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara, pasal 25.

strategi keamanan siber nasional, faktor organisasi juga merupakan alat (*means*) yang dapat digunakan untuk mencapai tujuan yang diharapkan. Strategi keamanan siber nasional mengidentifikasi 4 (empat) pihak yang merupakan komponen utama keamanan siber nasional yang disebut *quad helix*, yang memiliki hubungan interdependensi antara satu dengan yang lain yang saling menguatkan. Hubungan antar keempat komponen ini merupakan arsitektur kekuatan siber nasional yang dapat digambarkan sebagai berikut:



Gambar 4.10 Quad Helix Keamanan Siber

Sumber: Strategi Keamanan Siber Nasional, Menko Polhukam, 2017

Peran Pemerintah sebagai regulator, yang untuk *cyber security e-commerce* diamanahkan kepada BSSN bersinergi dengan Kominfo namun menurut keterangan seluruh informan di BSSN dan Kominfo, Kemendag adalah *leading sector* yang bertanggungjawab untuk menetapkan strategi *e-commerce* yang dibutuhkan untuk mencapai sasaran yang diinginkan. Hal ini tentu memerlukan dukungan dan kerjasama dari pihak industri/swasta, masyarakat/komunitas dan akademisi dalam penyusunan, implementasi dan evaluasi strategi keamanan siber nasional. Hal ini karena Pemerintah menyadari bahwa keamanan siber merupakan permasalahan bersama atau kolegial yang mencakup seluruh aspek kehidupan berbangsa dan bernegara dan sewajarnya memiliki konsekuensi yang setara antara

kedaulatan yang berlaku di dunia nyata dan kedaulatan di dunia siber[24]. Lingkup kedaulatan siber yang menjadi kewenangan Pemerintah sebagai regulator salah satunya adalah menjaga kewajaran penguasaan ekonomi global melalui penentuan kebijakan dan pengaturan perdagangan online global[25].

Tugas ini dapat terlaksana dengan efektif apabila mendapatkan dukungan dari sektor industri ekonomi digital, sebagaimana dijelaskan oleh Kasie Direktorat Ekonomi Digital Kominfo (wawancara, 2018), bahwa Komfinfo sebagai regulator diharapkan mampu mewadahi kebutuhan industri agar dapat berkembang dan mewujudkan visi Pemerintah. Lebih lanjut dijelaskan oleh Direktur Deteksi Ancaman BSSN (wawancara, 2018) apabila melihat dalam Strategi Keamanan Siber Nasional, dijelaskan bahwa dalam rangka menghadapi serangan siber, diperlukan pusat pengendalian siber di masing-masing sektor melalui *Security Operational Center* (SOC) yang dikoordinasikan secara terpusat oleh National SOC. Artinya, diperlukan SOC dan CSIRT yang dimiliki penyelenggara sistem elektronik masing-masing sebagai unit yang merespon serangan siber. Berdasarkan keterangan dari narasumber yang merupakan salah satu pemilik *e-commerce* (wawancara, 2018), industri lokal saat ini menunggu kebijakan yang dikeluarkan Pemerintah yang dapat mendukung pertumbuhan industri *e-commerce* dalam negeri.

Sedangkan impelementasi pelibatan akademisi dalam penyusunan kebijakan pada aspek keamanan siber telah dioptimalkan antara lain menurut Kasubdit Tata Kelola Sistem Elektronik (wawancara, 2018) keterlibatan dalam penyusunan model pengawasan yang dilakukan Kominfo yang dibantu oleh akademisi. Disamping itu menurut tenaga ahli keamanan siber sekretariat *road map e-commerce* Kemenkokuin (wawancara, 2018), dalam melaksanakan Perpres 74 Tahun 2017 yang melibatkan tenaga ahli akademisi dari berbagai bidang dan juga mempersiapkan sumber daya manusia yang mampu mengikuti

[24] *Ibid,* hlm 16.
[25] *Ibid.*

perkembangan ekonomi digital. Disamping itu, dalam Pasal 10 PP Nomor 82 tahun 2012, juga mewajibkan penggunaan tenaga ahli yang memiliki kompetensi di bidang Sistem Elektronik atau Teknologi Informasi. Tenaga ahli sebagaimana dimaksud wajib memiliki sertifikat keahlian. Peran komponen komunitas khusus siber baik itu otodidak, hacker atau cracker, youtuber, forum informal maupun forum dan komunitas formal atau asosiasi industri siber dibutuhkan dalam menganalisa perkembangan-perkembangan yang terjadi di dunia siber.

Beberapa komunitas yang terlibat aktif berkoordinasi dengan Pemerintah antara lain adalah Asosiasi *e-commerce* Indonesia (idEA) dan ICSF (Indonesia *Cyber Security* Forum). Berdasarkan keterangan Kasubdit Proteksi BSSN (wawancara, 2018), komunitas membantu Pemerintah melaukan audit penerapan keamanan informasi yang dikelola melalui kerjasama dengan komunitas dan juga hacker/peretas, sehingga dapat turut menjaga keamanan e-commerce. Disamping itu informan juga menambahkan bahwa Pemerintah berusaha mendorong peretas untuk bisa menjadi perusahaan keamanan informasi bahkan menjadi lembaga sertifikasi profesi yang ke depan bisa merekrut banyak SDM yang bisa diberdayakan dalam keamanan informasi. Informan dari komunitas *cyber security* (wawancara, 2018) menyatakan keterbatasan jumlah dan kualitas pada SDM di lembaga pemerintahan adalah salah satu faktor penghambat dalam melakukan implementasi kewajiban-kewajiban penyelenggara sistem elektronik. Dari berbagai sumber diatas dapat disimpulkan bahwa diperlukan struktur organisasi yang efektif dengan SDM yang sesuai serta bentuk kelembagaan yang dapat berkembang sesuai dengan kebutuhan dan kesiapan yang seluruhnya didasarkan dengan kebijakan formal yang jelas[26].

[26] Kementerian Pertahanan, *Permenhan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber*, hlm 33-34.

4.1.5 Sinergitas BSSN dan Kominfo Dalam Meningkatkan Kesiapan *Cyber Security* Pada Sektor *E-Commerce* di Indonesia

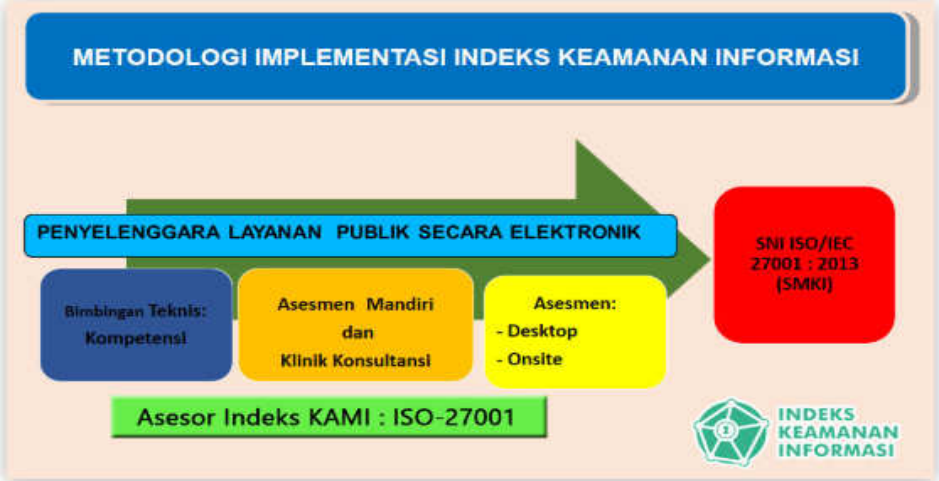
Sinergitas yang sudah ada di Kominfo dan BSSN pada aspek hukum dan organisasi, dari hasil wawancara dengan berbagai direktorat di kedua lembaga tersebut, dipandang telah berjalan cukup baik dalam sektor *cyber security e-commerce*. Walapun dari segi hukum masih menggunakan peraturan perundang-undangan yang ada di Kominfo dan masih fokus dibawah Undang-Undang Informasi dan Transaksi Elektronik. Sedangkan pada aspek organisasi, Kominfo juga telah melakukan penyesuaian struktur setelah dibentuknya BSSN. Hal ini juga dirasakan oleh informan dari Kementerian Perdagangan yaitu Kasubdit *e-commerce* (wawancara, 2018) sebagai mitra dari kedua lembaga tersebut. Namun, menurut informan dari komunitas dan pelaku *e-commerce* (wawancara, 2018), sinergitas masih dapat dilaksanakan dengan lebih baik apabila didukung dengan regulasi yang jelas sehingga lebih efektif dalam melakukan komunikasi dan koordinasi lintas lembaga.

4.1.5.1 Aspek Hukum

Sinergitas pada aspek hukum dilaksanakan mulai dari bagian pencegahan, dimana Direktur Deteksi Ancaman (wawancara, 2018) menjabarkan beberapa bentuk persiapan diri diantara lain adalah pemberdayaan kesadaran, penguatan literasi keamanan siber masyarakat, budaya perilaku etika siber (*cyber ethic*). Disamping itu dilakukan pula melalui deteksi serangan siber, indentifikasi dan database serangan siber, menata konfigurasi jaringan publik nasional dan gerbang NKRI, menata infrastruktur secure-transaction (*public-key-infrastructure*), menata konfigurasi setiap jaringan tertutup berstandar keamanan, menata konfigurasi setiap Pusat Data dengan standar keamanan membangun sistem monitoring dan deteksi yang memadai dan membangun tim dan sistem koordinasi yang tangguh. Sejak Direktorat Keamanan Informasi dan ID-SIRTII dipindahkan ke BSSN, Direktur Pengendalian Aptika menjelaskan (wawancara, 2018) bahwa sinergitas antara BSSN dan Kominfo

dalam melakukan pencegahan yaitu mendukung BSSN dalam menerapkan Peraturan terkait Sistem Manajemen Pengamanan Informasi (SMPI), penerapan indeks KAMI serta pelaksanaan tanda tangan elektronik.

Tugas BSSN berdasarkan penjelasan informan (wawancara, 2018) adalah memastikan pelaksanaan kebijakan indeks KAMI yang dilakukan melalui metode bimbingan teknis, asesmen dan konsultasi sesuai gambar berikut:



Gambar 4.11 Metodologi Implementasi Indeks KAMI
Sumber: https://bssn.go.id/indeks-kami/, diakses pada 25 November 2018

Direktur Penanggulangan & Pemulihan BSSN (wawancara, 2018) merupakan direktorat khusus yang berkonsentrasi dalam penanganan insiden siber yang dihadapi oleh pelaku *e-commerce* dan bertanggungjawab menyediakan rekomendasi penanggulangan serta memonitor prosesnya hingga mengevaluasi hasil rekomendasi yang diberikan, sehingga dapat menjadi saran atau masukan bagi BSSN dalam menghadapi insiden siber lainnya di kemudian hari. Disamping hasil pengawasan langsung BSSN, insiden siber yang terjadi juga dapat disampaikan melalui meja pengaduan insiden siber yang dikelola oleh Pusat Operasi Keamanan Siber nasional (Pusopkamsibnas) BSSN yang prosedur pengaduannya dapat dilihat dalam gambar berikut:

Gambar 4.12 Alur Pengaduan Insiden Siber

Sumber: https://bssn.go.id/indeks-kami/, diakses pada 25 November 2018

Adapun proses bisnis dalam penanggulangan dan pemulihan menurut keterangan Direktur terkait (wawancara, 2018) menggunakan standar ISO 22301:2012 tentang *Society Security-Business Continuity Management Systems-Requirements* dan NIST SP 800-81 tentang *Computer Security Incident Handling Guide*. Dari informasi diatas dapat disimpulkan bahwa sinergitas yang dilakukan BSSN dan Kominfo belum dilengkapi dengan regulasi yang mengatur pola komunikasi dan koordinasi yang dibutuhkan sehingga untuk meningkatkan kesiapan *cyber security* pada sektor *e-commerce* maka perlu ditetapkan standar komunikasi dan koordinasi yang diterapkan secara global baik untuk melakukan peran Pemerintah dalam melakukan pencegahan maupun dalam penanggulangan dan pemulihan.

4.1.5.2 Aspek Organisasi

Informan dari BSSN dan Kominfo (wawancara, 2018) menyadari bahwa dalam pelaksanaan program kerja yang ada di BSSN maupun di Kominfo masih dilaksanakan masing-masing dan belum dilaksanakan secara sinergi dengan program dari *e-commerce* yang dijalankan oleh Perdagangan. Narasumber dari Kemendag membenarkan bahwa kehadiran atau keikutsertaan instansi/lembaga tersebut pada program

instansi/lembaga lainnya masih bersifat partisipatif (wawancara, 2018). Tenaga ahli keamanan siber sekretariat *road map e-commerce* (wawancara, 2018) menyampaikan perlu adanya sebuah terobosan dari Pemerintah untuk merangkul seluruh stakeholder dalam rangka bersinergi menyelesaikan isu-isu yang ada pada *e-commerce* melalui sebuah konsensus.

Lebih khusus untuk mengimplementasikan sinergitas yang lebih baik, Direktur Penanggulangan dan Pemulihan BSSN (wawancara, 2018) menganggap perlu ada Join Operation sebagai wadah koordinasi dari seluruh kementerian dan lembaga terkait demi tercapainya sinergitas lintas sektor yang diharapkan. Disamping itu informan dari BSSN juga menekankan perlukan adanya CERT pada setiap sektor yang saling berkoordinasi dibawah Gov-CERT dan pelaksanaan *Sharing Information* sebagai bagian dari upaya sinergitas. Saat ini pelaksanaan sinergitas antara Kominfo dan BSSN terkait keamanan siber pada sektor *e-commerce* yang sudah berjalan melingkupi 2 (dua) bagian yaitu pencegahan dan penanggulangan serta pemulihan.

Terkait membangun tim dan sistem koordinasi yang tangguh, menurut keterangan dari Kasubdit Identifikasi Kerentanan dan Penilaian Resiko Informasi *E-commerce* (wawancara, 2018) saat ini sedang mengupayakan dengan metode *information gathering* yang dilakukan salah satunya dengan mendorong pelaku *e-commerce* agar melakukan asesmen diri (*self assessment)* berdasarkan panduan indeks Keamanan Informasi yang telah disusun oleh Kominfo.

Pada aspek penanggulangan dan pemulihan, Kemendag sebagai pengampu mengalami keterbatasan apabila terdapat laporan dari masyarakat terkait gangguan atau kegagalan pada suatu sistem *e-commerce.* Sehingga menurut keterangan subdit *e-commerce* (C6), Kemendag bertindak sebagai perantara yang akan membantu

menghubungkan pelapor dengan Kominfo untuk kegagalan sistem elektronik dan pihak berwajib atau kepolisian apabila terdapat indikasi kejahatan. Sedangkan Kominfo, berdasarkan keterangan dari Direktur Pengendalian Aplikasi Informatika (wawancara, 2018), hanya melakukan penutupan sistem elektronik atau aplikasi apabila dibutuhkan berdasarkan permintaan dari pengampu sektor terkait atau pihak berwajib.

Di BSSN penanganan dilakukan melalui Pusopkamsibnas, dimana Pusopkamsibnas melakukan penilaian apakah merupakan kejadian biasa atau insiden siber dan apabila insiden siber apakah dapat ditangani langsung atau harus melibatkan direktorat terkait. Apabila insiden tersebut tidak dapat ditangani oleh Pusopkamsibnas, maka akan diberikan tiket kepada direktorat terkait untuk dapat menganalisa lebih lanjut dan menyusun langkah yang dibutuhkan terkait penanggulangan dan pemulihan terhadap insiden siber yang terjadi dengan membentuk tim manajemen yang terdiri dari berbagai unsur lain.

Proses penanggulangan dan pemulihan apabila dihimpun dari di ketiga instansi terkait maka dapat digambarkan sebagai berikut:

Gambar 4.13

Alur Penanggulangan & Pemulihan Insiden Siber *E-Commerce*

Sumber: Diolah oleh peneliti, 2018

Berdasarkan keterangan dari Direktur Penanggulangan dan Pemulihan Ekonomi Digital BSSN (wawancara, 2018), hingga terbentuknya ID-SIRTII ketika masih berada di Kominfo hingga saat ini, belum pernah ada

pelaku *e-commerce* yang meminta bantuan kepada Pemerintah untuk menyelesaikan permasalahan insiden siber yang dihadapi. Hal ini dikarenakan pelaku *e-commerce* pada umumnya telah memiliki tim insiden respon dan sistem penanganan insiden sendiri. Namun BSSN tetap berkewajiban untuk memberikan rekomendasi penyelesaian dan juga melakukan pendampingan hingga insiden terselesaikan.

4.2 Pembahasan

Tujuan pembahasan adalah untuk dapat memperoleh hasil analisa yang komprehensif terkait permasalahan yang menjadi fokus penelitian. Pembahasan ini dilakukan dengan menggunakan metode kualitatif dengan pendekatan deskriptif, dimana peneliti menjabarkan setiap informasi yang diperoleh dari narasumber serta data yang diperoleh baik primer maupun sekunder terkait subfokus penelitian dan ditampilkan secara sistematis serta disajikan dengan akurat dan faktual dilengkapi dengan fakta terbaru yang terkait dengan permasalahan yang dibahas. Berdasarkan hasil penelitian yang disajikan secara obyektif diharapkan peneliti mampu menganalisa berdasarkan teori dan konsep yang telah dijelaskan pada bab kajian teoritik sehingga dapat memberikan pemahaman yang mendalam terhadap hasil penelitian yang telah diperoleh.

Adapun teori yang digunakan dalam pembahasan subfokus penelitian pertama ini adalah teori strategi dari konsep Strategi Pertahanan Indonesia. Disamping itu, teori *cyber security* yang digunakan adalah dari Prof. Eko Indrajit dan Ghernouti dengan mengaplikasikan model *information security* yang merupakan standar internasional dengan fokus pada dimensi hukum dan organisasi yang diperlukan untuk mencapai standar *cyber security.* Disamping itu juga menggunakan model PDCA dari ISO dan komponen rencana kontijensi sebagai bagian dari BCP yang menggunakan model dari NIST. Sedangkan pada konsep subfokus penelitian berikutnya menggunakan teori analisis kebijakan Dunn dan McLennan dan terkait

organisasi peneliti menggunakan teori manajemen stratejik dari Siagian dengan fokus pada proses perumusan kebijaksanaan dan pelembagaan strategi sebagai bagian penting dalam mencapai tujuan organisasi. Disamping itu juga melakukan pembahasan tentang sinergitas antar lembaga peneliti juga menggunakan teori Stoner dan juga standar sinergitas menurut model keamanan informasi yang digunakan secara global.

4.2.1 Kesiapan C*yber Security E-Commerce* Indonesia Menuju Negara dengan Ekonomi Digital Terbesar di Asia Tenggara

Berdasarkan buku putih pertahanan, terdapat 3 (tiga) elemen dari strategi yaitu membentuk, merespon dan menyiapkan diri. Penerbitan *Road Map E-Commerce* merupakan elemen dari pembentukan strategi yang dibutuhkan untuk mewujudkan visi Pemerintah menjadikan Indonesia sebagai negara dengan ekonomi digital terbesar di Asia Tenggara. Dimasukkannya aspek keamanan siber dalam pembentukan peta jalan tersebut merupakan bentuk elemen menyiapkan diri terhadap kerentanan dan ancaman yang akan dihadapi dalam mewujudkan visi yang ada. Melalui masuknya aspek keamanan siber, Pemerintah berharap mampu memiliki strategi yang memiliki kemampuan keamanan siber untuk merespon serangan siber yang dihadapi dalam kemajuan ekonomi digital yang akan menjadi salah satu tulang punggung perekonomian Indonesia. Hal ini sejalan dengan pemahaman doktrin manual Amerika Serikat, penggunaan strategi adalah merupakan seni dan ilmu dalam membangun dan menggunakan berbagai sektor agar sesuai kebutuhan dan siap menghadapi segala kondisi yang mungkin terjadi dan memperkecil resiko kekalahan. Sehingga kesiapan terhadap aspek kemanan siber *e-commerce* dapat memperkecil resiko kegagalan mewujudkan visi yang ingin dicapai dan meningkatkan potensi keberhasilan ekonomi digital di Indonesia.

Apabila dianalisa lebih lanjut dari program *cybersecurity e-*

commerce yang disusun fokus pada pembuatan standar dan prosedur kehati-hatian, pembuatan standar dan prosedur penyimpanan dan perlindungan data serta pembuatan model pengawasan transaksi. Maka dapat disimpulkan bahwa strategi pengamanan yang disusun diharapkan dapat menjamin pengamanan dari segi konsumen (kehati-hatian), segi pelaku usaha (penyimpanan dan perlindungan data transaksi) serta segi Pemerintah (pengawasan transaksi). Hal ini sejalan dengan pemahaman dair Prof. Eko Indrajit yang menyatakan bahwa keamanan siber adalah berbagai usaha pengamanan yang dilakukan untuk menangkal dan menghindari serangan siber yang dapat merugikan berbagai pihak. Dari hasil penelitian ditemukan bahwa data transaksi dan data konsumen adalah bagian paling penting dimana data berputar pada seluruh pilar dalam transaksi *e-commerce.* Sehingga pada konsep ekonomi digital sebuah bisnis dijalankan secara virtual dimana terjadi pertukaran seluruh informasi dan data yang dibutuhkan seluruhnya melalui sebuah sistem perdagangan elektronik perlu menggunakan metode keamanan tertentu guna memenuhi aspek keamanan informasi yang dibutuhkan bagi perdagangan elektronik.

Pendekatan dari teori keamanan informasi dalam konsep *cyber security e-commerce* melihat memfokuskan pada aspek kebijakan dan organisasi yang merupakan bagian dari 4 (empat) dimensi keamanan siber menurut Ghernouti. Sifat perdagangan elektronik yang dipahami sebagai ranah bisnis atau *private*, mendorong kebijakan pada sektor ini harus dapat mengakomodir seluruh aspek yang saling berkaitan pada kerangka kerja *e-commerce* sebagai satu kesatuan yang terdiri dari 5 (lima) pilar yaitu orang, kebijakan, marketing dan periklanan, rantai suplai serta infrastruktur. Disamping itu pada dimensi organisasi, Pemerintah telah memahami ketergantungan antara lembaga sehingga diperlukan pola koordinasi dan komunikasi yang sesuai dengan kebutuhan di bidang keamanan siber.

4.2.1.1 Aspek Hukum

Kebijakan merupakan salah satu sarana penting untuk dapat mencapai tujuan *cyber security e-commerce* yang diharapkan. Perencanaan yang telah disusun untuk mencapai tujuan keamanan siber memerlukan landasan formal mulai dari level strategis sampai dengan operasional. Undang-undang ITE sampai dengan Peraturan Menteri Kominfo serta Peraturan Kepala BSSN walaupun berada pada sektor yang berbeda namun berkembang berdasarkan teori analisis kebijakan Dunn, kebijakan yang berkembang sesuai dengan tantangan pada sistem transaksi elektronik untuk menciptakan dan mentransfer pengetahuan yang relevan dengan kebutuhan kebijakan di sektor *e-commerce*. Pelaksanaan pengamanan dalam keamanan informasi menurut Prof. Eko Indrajit dapat dilakukan dengan 3 (tiga) cara pengamanan, dimana ketiganya sudah diakomodir dalam peraturan perundang-undangan. Ketiga pengaman yaitu pengamanan infrastruktur yang sudah diatur dalam UU ITE, pengamanan data yang telah diakomodir dalam PP PSTE dan Permen Kominfo terkait Perlindungan Data serta Pengamanan terhadap komponen yang terkait dalam proses interaksi yang sudah diatur dalam Permen Kominfo tentang pemanfaatan pembiayaan teknologi informasi dan komunikasi layanan pita lebar.

Apabila dilihat proses kebijakan yang ada saat ini dimana semua regulasi yang dibutuhkan dalam program keamanan siber sebagai hasil keluaran yang telah dirumuskan dalam Perpres Peta Jalan Perdagangan melalui Elektronik, hingga 1 (satu) tahun sejak Perpres diterbitkan masih dalam tahap penyusunan dan pengajuan regulasi. Apabila dianalisa dalam 8 (delapan) tahap analisis kebijakan yang ada menurut Dunn, maka tahapan ini masih pada tahapan *policy formation* dimana pembahasan yang dilakukan masih menganalisa berbagai pilihan dalam mengatasi permasalahan yang dihadapi berjalan sangat lama.

Proses perumusan kebijakan yang lama pada *cyber security e-commerce* tersebut berdasarkan teori model McLennan dapat menggambarkan sistem politik yang dianut oleh Indonesia yaitu masuk pada kategori *fragmented state*. Dimana proses penyusunan kebijakan yang ada pada institusi tidak dapat menggambarkan kebijakan nyata yang akan diberlakukan karena masih terdapat distribusi kekuasaan yang bersifat tradisional. Distribusi kekuasaan yang bersifat trandisional yang dimaksud oleh McLennan adalah disebabkan oleh fragmentasi dari kekuatan politik yang memiliki pengaruh yang kuat pada proses perumusan kebijakan yang dilakukan. Hal ini menyebabkan pengambilan keputusan atau kebijakan seringkali sudah tidak semata-mata berdasarkan permasalahan yang dihadapi namun terdapat unsur kepentingan dari berbagai lapisan pemerintahan.

Permasalahan dalam perumusan kebijakan yang masih menggunakan standar penyusunan regulasi umum mengalami kendala ketika diterapkan untuk mengatur permasalahan yang muncul dalam *e-commerce*. Perkembangan permasalahan di dunia maya tidak dapat diprediksi untuk jangka waktu panjang, sehingga kebijakan yang diterapkan sudah tidak relevan dalam menghadapi permasalahan yang semakin berkembang. Penetapan visi Pemerintah untuk menjadi negara dengan ekonomi digital terbesar di Asia Tenggara juga harus diikuti dengan pola perumusan kebijakan yang mengikuti model *competitive state.* Pemerintah harus dapat menyusun kebijakan yang bersifat global dan fokus pada peningkatan pertumbuhan ekonomi sehingga mampu menghadapi persaingan yang berkembang di Asia Tenggara sekaligus mampu mengatasi ancaman terhadap ekonomi digital.

4.2.1.2 Aspek Organisasi

Sarana Prasarana utama yang digunakan pada *cyber security e-commerce* di Indonesia adalah *quad helix,* yaitu para stakeholder yang

memiliki tugas dan tanggungjawab untuk menjalankan fungsi pada bidangnya masing-masing dalam mewujudkan tujuan *cyber security e-commerce. Quad helix* pada sisi pemerintahan terdiri dari Kementerian Komunikasi dan Informatika bersama-sama dengan BSSN dan Perdagangan dibawah koordinasi Kementerian Koordinator Bidang Perekonomian. Pembagian tugas dan tanggungjawab yang diharapkan dari Pemerintah sebagai regulator harus dapat menyusun, mengimpementasikan dan mengevaluasi seluruh kebijakan yang terkait *cyber security e-commerce* dengan melibatkan akademisi, industri dan masyarakat.

Metode yang digunakan dalam memanfaatkan penggunaan sarana prasarana yang ada pada *cyber security e-commerce* menurut Prof. Eko Indrajit haruslah difokuskan pada penjagaan informasi terhadap seluruh kemungkinan ancaman untuk memastikan kelangsungan bisnis, meminimalsiasi resiko dan memaksimalkan pengembalian investasi serta peluang bisnis itu sendiri melalui perlindungan atas infrastruktur, pengamanan data, informasi atau konten di dalamnya, serta pengamanan terhadap komponen. Panduan indeks KAMI merupakan yang diterbitkan oleh Kominfo yang melakukan penilaian pada 5 (lima) yaitu aspek tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset dan aspek teknologi dilakukan untuk memenuhi standar yang diperlukan terhadap 4 (empat) bagian pengamanan tersebut.

Berdasarkan proses manajemen stratejik, pelembagaan strategi adalah salah satu proses penting dalam organisasi yang memiliki pola kerja koordinasi lintas sektor. Pelembagaan strategi ini dibutuhkan untuk meyamakan persepsi strategi sehingga dapat diimplementasikan secara harmonis pada seluruh level strategi yang disusun mulai dari strategi dasar, induk maupun operasional. Disamping itu, pelembagaan strategi juga memperhatikan 3 (tiga) elemen perbedaan yang dihadapi dalam koordinasi lintas lembaga yaitu struktur organisasi, pola kepemimpinan dan *culture*

yang ada pada masing-masing organisasi. Saat ini struktur organisasi yang berperan dalam *cybersecurity e-commerce* adalah 3 (tiga) lembaga yang memiliki perbedaan. Di Kominfo, terdapat 1 (satu) direktorat jenderal yang terkait dalam pelaksanaan keamanan siber pada sektor ekonomi digital, sedangkan di BSSN terdapat 3 (tiga) deputi yang fokus pada keamanan siber di sektor ekonomi digital. Namun pada Kementerian Perdagangan sebagai pengampu sektor penanganan *e-commerce* hanya dipercayakan pada sebuah subdirektorat pada sebuah direktorat. Ketidaksesuaian struktur organisasi ini tentu dapat berpengaruh terhadap pola sinergitas yang berlangsung. Kesiapan pada aspek organisasi juga menunjukkan keseriusan Pemerintah dalam mewujudkan sasaran yang telah ditetapkan.

4.2.2 Sinergitas BSSN dan Kominfo Dalam Meningkatkan Kesiapan *Cyber Security* Pada Sektor *E-Commerce* di Indonesia

Konsep sinergitas yang disampaikan oleh James A. F. Stoner adalah sebagai hubungan antar dua atau lebih pihak yang memiliki pola komunikasi untuk membangun kerjasama dan kepercayaan. Sinergitas antara BSSN sebagai penanggungjawab keamanan siber serta Kominfo sebagai penanggungjawab telekomunikasi dan informatika diperlukan untuk dapat meningkatkan *cyber security* pada sektor *e-commerce* yang saat ini sedang disusun oleh Pemerintah. Sesuai teori manajemen stratejik menurut Siagian, organisasi harus dapat melakukan peninjauan ulang bahkan perubahan yang dibutuhkan. Sehingga Pemerintah harus mampu menerapkan konsep manajemen strategik pada aspek *cyber security* di sektor *e-commerce* yang memiliki fase perubahan yang cepat, yaitu melalui proses penyusunan, implementasi dan evaluasi strategi yang dinamis dan berlangsung secara terus menerus.

Namun apabila dilihat dari pelaksanaan yang masih bersifat sektoral sejak diterbitkannya peraturan terkait *road map e-commerce* maupun

peraturan penunjukkan BSSN, masih belum terlihat penyesuaian yang signifikan dalam penyusunan, implementasi maupun evaluasi terhadap strategi yang sedang dan/atau akan disusun. Dalam pembahasan ini menganalisis sinergitas BSSN dan Kominfo pada aspek hukum dan aspek organisasi pelaksanaan *cyber security* pada sektor *e-commerce.*

4.2.2.1 Aspek Hukum

Dalam peraturan terkait *road map e-commerce* ditekankan tentang perlunya koordinasi antar lembaga. Adapun kementerian-kementerian yang terkait dalam sinergitas *cyber security e-commerce* beserta tugas dan fungsinya adalah Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN). Namun dalam pelaksanaannya tetap diperlukan koordinasi dengan Kementerian Perdagangan (Kemendag) dibawah pengawasan Kementerian Koordinator Bidang Perekonomian. Hal ini membuat sinergitas antar lembaga menjadi penting dalam pelaksanaan *cyber security e-commerce* Indonesia.

Sinergitas pada aspek hukum melingkupi Pencegahan, Penanggulangan, Pemulihan, Evaluasi dan Penyempurnaan yang diterapkan untuk *cyber security* pada sektor *e-commerce* yang saat ini telah menjadi tanggungjawab BSSN ini masih menggunakan standar yang telah ditetapkan oleh Kominfo pada sistem dan transaksi elektronik. Sehingga dalam melaksanakan tugas dan fungsi pada penerapan aspek keamanan siber tersebut di sektor *e-commerce*, BSSN dan Kominfo perlu bekerjasama. Saat ini standar yang digunakan oleh BSSN dalam pencegahan adalah Indeks KAMI, dimana pelaku *e-commerce* memerlukan bimbingan teknis hingga evaluasi sesuai pedoman yang telah disusun Kominfo.

Pengaturan tugas dan tanggungjawab antara BSSN dan Kominfo serta Kemendag perlu dibagi bukan hanya pada level kebijakan yang bersifat strategis melainkan juga operasional, sehingga aspek-aspek yang

dibutuhkan untuk menilai keamanan siber pada pelaku *e-commerce* dapat dilaksanakan secara optimal. Pedoman penyelenggaraan pertahanan siber menjelaskan bahwa aspek hukum merupakan landasan pelaksanaan tugas yang oleh Ghernaouti dijabarkan dalam bentuk peraturan, norma, prosedur dan kepatuhan (*compliance*). Sehingga untuk dapat memastikan pelaksanaan keamanan informasi yang telah bersinergi, maka sinergitas pada aspek legalitas menjadi faktor penting penentuan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia.

Kendala yang dihadapi Pemerintah dalam koordinasi dengan pelaku *e-commerce* dalam penanganan insiden karena adanya keterbatasan akses yang diberikan kepada Pemerintah menunjukkan bahwa belum ada regulasi yang cukup dapat memaksa para pelaku *e-commerce* untuk mengikuti prosedur yang diterapkan baik oleh BSSN maupun Kominfo. Di sisi lain, BSSN dan Kominfo memiliki keterbatasan dalam memaksa kepatuhan pelaku *e-commerce* mengingat regulasi yang mengatur hanya menerapkan sanksi administrasi yang ditetapkan oleh Kominfo terhadap sistem elektronik. Namun, pelaksanaan perdagangan sendiri seharusnya memiliki sanksi pidana dan perdata yang ditetapkan oleh Kemendag, namun hingga saat ini regulasi perdagangan terkait *e-commerce* masih belum ada dan sepenuhnya masih bergantung pada undang-undang perlindungan konsumen pada perdagangan konvensional.

Penyusunan dan penyesuaian regulasi-regulasi yang dibutuhkan dalam sinergitas BSSN dan Kominfo pada sektor *e-commerce* juga dapat meningkatkan kesiapan *cyber security* Indonesia pada sektor *e-commerce dimana* beberapa regulasi yang harus dipenuhi untuk dapat meningkatkan kesiapan *cyber security* di Indonesia sesuai standar yang telah berlaku di Asia Tenggara antara lain adalah adanya regulasi perlindungan konsumen dan perlindungan data. Kedua regulasi tersebut juga dibutuhkan oleh Pemerintah dalam mengoptimalkan unsur penindakan pada aspek

penegakan hukum yang dibutuhkan dalam menerapkan *cyber security* pada sektor *e-commerce*.

4.2.2.2 Aspek Organisasi

Jika mengacu pada teori strategi dari Anthony, Parrewe dan Kachmar yang melihat strategi sebagai sebuah formula yang terdiri dari misi dan tujuan yang ada pada organisasi termasuk rencana aksi untuk mencapainya dengan mempertimbangkan kondisi persaingan dan pengaruh langsung maupun tidak langsung terhadap keberlangsungan organisasi. Pemerintah harus segera menyusun rencana aksi yang dibutuhkan untuk menindaklanjuti belum adanya keluaran yang dihasilkan dari aspek keamanan siber setelah 1 (satu) tahun berjalannya *road map e-commerce*, demi mewujudkan visi sebagai negara dengan ekonomi digital terbesar di Asia Tenggara.

Mulyana menjelaskan bahwa koordiansi adalah hubungan antara *stakeholders* dalam berbagai bentuk koordinasi dan kemitraan sedangkan komunikasi adalah penekanan pada pertukaran informasi antar pihak. Pada kenyataanya hasil penelitian menunjukkan bahwa pelaksanaan koordinasi dan komunikasi yang ada diantara instansi terkait *cybersecurity e-commerce* masih belum memiliki pola yang baku. Namun apabila berdasarkan pada standar yang digunakan oleh BSSN yaitu ISO dan NIST, maka salah satu bagian dari SP 800-61 pengaturan secara jelas terkait hubungan koordinasi yang dapat dilakukan dengan pihak lain sesuai yang dibagi menjadi 3 (kategori), yaitu *team-to-team, team-to-coordinating team-coordinating team-to-coordinating team.*

Sedangkan dalam melakukan *information sharing* sebagai bagian dari proses komunikasi juga diperlukan standar yang jelas mengenai bentuk pembagian informasi. Sekalipun pembagian informasi tersebut terkait dengan insiden yang sedang dihadapi oleh penyelenggara *e-commerce* dan terdapat regulasi yang mengharuskan penyelenggara untuk

melaporkan secara jelas insiden siber yang dihadapi, namun tanpa aturan yang baku akan sulit terlaksana. Prinsip pembagian informasi dalam *e-commerce* juga mengutamakan keamanan informasi yang diperlukan dalam rangka menjaga data sensitif perusahaan. Sehingga perlu terdapat regualasi yang memuat standar prosedur materi yang perlu dikomunikasikan, kapan hal tersebut perlu dilakukan dan kepada siapa harus diberikan.

Belum adanya standar dalam melakukan koordinasi dan komunikasi ini disebabkan oleh belum adanya regulasi yang mengatur pola sinergitas serta adanya perbedaan struktur organisasi yang terdapat pada BSSN dan Kominfo serta Kemendag sebagai pengampu sektor. Hambatan pada aspek regulasi tentu menyebabkan keterbatasan pelaksanaan tugas, fungsi dan kewenangan instansi dan lembaga terkait untuk mencapai sasaran atau tujuan yang telah ditetapkan. Sedangkan perbedaan struktur organisasi menurut Siagian mempengaruhi gaya kepemimpinan dan kultur organisasi dalam menghadapi perkembangan *cyber security* pada sektor *e-commerce,* termasuk pada pola koordinasi dan komunikasi yang dilakukan dalam rangka sinergitas. Sebaliknya, jika sinergitas dapat berjalan dengan baik maka dapat meningkatkan kesiapan *cyber security* pada sektor *e-commerce* dalam mewujudkan visi Pemerintah menuju negara ekonomi digital terbesar di Asia Tenggara.

Apabila mengacu pada penelitian-penelitian terdahulu dapat dilihat bahwa pada awal penerapan *cyber security* difokuskan pada aspek teknis dan sumber daya manusia, namun aspek hukum dan organisasi dari *cyber security* belum menjadi perhatian hingga dalam penerapannya menemui berbagai kendala yang terkait dengan tidak adanya dukungan regulasi. Disamping itu, fokus pelaksanaan *cyber security* pada sektor *e-commerce* pada penelitian terdahulu belum mengakomodir peran dan fungsi Pemerintah karena *e-commerce* bersifat bisnis/privat. Namun seiring dengan perkembangan ekonomi digital menjadi salah satu infrastruktur

kritis pada sektor perekonomian nasional, menyebabkan semakin berkembangnya ancaman siber termasuk salah satunya pada sektor *e-commerce* sudah menjadi bagian dari kewenangan Pemerintah. Isu terkait privasi pada sektor *e-commerce* yang ada pada penelitian terdahulu juga masih menjadi salah satu aspek yang harus diperhatikan dalam meningkatkan kesiapan *cyber security* dimana sinergitas yang dilakukan melibatkan transfer informasi dan/atau data. Sehingga dalam meningkatkan kesiapan aspek *cyber security* pada sektor *e-commerce* di Indonesia yang mampu bertahan terhadap ancaman yang berkembang di era ekonomi digital global saat ini sangat bergantung pada aspek hukum dan aspek organisasi dalam sinergitas BSSN dan Kominfo.

BAB V
KESIMPULAN DAN REKOMENDASI

5.1 Kesimpulan

5.1.1 Kesiapan *Cyber Security* Pada Sektor *E-Commerce* di Indonesia

Kesiapan keamanan siber pada sektor perdagangan melalui sistem elektronik berdasarkan hasil penelitian apabila dilihat dari aspek hukum dan organisasi maka dapat disimpulkan sebagai berikut:

5.1.1.1 Aspek Hukum

Peraturan perundang-undangan yang ada terkait *cyber security* pada sektor *e-commerce* pada level kebijakan dasar telah mengakomodir 3 (tiga) elemen yang dibutuhkan dalam perspektif strategi pertahanan, yaitu pembentukan, merespon dan menyiapkan diri melalui Undang-Undang ITE dan PP PSTE yang telah berjalan sejak masih menjadi tanggungjawab Kominfo. Pada level operasional, peraturan perundang-undangan yang disusun juga telah mengakomodir penyelenggaraan keamanan siber yang terdiri dari pencegahan, penanggulangan & pemulihan serta evaluasi & penyempurnaan. Namun apabila dibandingkan dengan regulasi yang ada pada negara lainnya di Asia Tenggara, Indonesia masih belum memiliki 2 (dua) regulasi yaitu *privacy* dan *consumer protection* yang juga merupakan regulasi yang dibutuhkan untuk terwujudnya *cyber security* pada sektor *e-commerce.* Kendala yang menghambat kesiapan aspek hukum yang menjamin tujuan yang ingin dicapai melalui penerapan *cyber security* pada sektor *e-commerce* disebabkan oleh lambatnya proses penyusunan regulasi sehingga tidak dapat mengimbangi perkembangan ekonomi digital yang pesat. Disamping itu, belum adanya standar baku dan sifat yang tidak memaksa dalam implementasi serta minimnya evaluasi terhadap implementasi regulasi serta sanksi yang bersifat administrasi pada aspek *cyber security* juga menjadi kendala dalam penegakan hukum dan menghambat kesiapan *cyber security* pada sektor *e-commerce*.

5.1.1.2 Aspek Organisasi

Kesiapan dalam menghadapi hambatan dan tantangan di era ekonomi digital juga perlu didukung dengan aspek organisasi yang memadai. Pengalihan tugas dan tanggungjawab keamanan siber kepada BSSN dari Kominfo telah ditindaklanjuti dengan penyusunan struktur organisasi pada BSSN dan penyesuaian struktur pada Kominfo. Namun dalam pelaksanaanya, BSSN masih sepenuhnya bergantung pada regulasi yang ada pada Kominfo. Peran Kominfo sebagai pendukung pelaksaan keamanan siber dari aspek infrastruktur telekomunikasi dan informatika, masih perlu diperjelas dalam sebuah regulasi yang bersifat operasional. Pada penerapan standar pengamanan informasi juga perlu dibuat suatu standar terpadu yang disepakati bersama baik oleh BSSN maupun Kominfo sehingga dapat diintegrasikan dan diterapkan pada sektor *e-commerce* tanpa memberatkan pelaku bisnis. Untuk tercapainya kesiapan organisasi juga diperlukan SDM yang sesuai dengan bentuk kelembagaan yang dapat berkembang menyesuaikan kebutuhan. Disamping itu, pengoptimalan peran industri, akademisi dan komunitas sesuai dengan *quad helix* pada strategi keamanan siber nasional sangat diperlukan dalam menyiapkan peran organisasi menghadapi tantangan pada sektor *e-commerce* di Indonesia.

5.1.2 Sinergitas BSSN dan Kominfo Dalam Meningkatkan *Cyber Security* Pada Sektor *E-Commerce* di Indonesia

Secara keseluruhan strategi *cyber sercurity e-commerce* Indonesia dapat dikategorikan sudah berjalan secara sinergi sejak diterbitkannya peta jalan perdagangan melalui elektronik yang ditargetkan selesai tahun 2018 walaupun dalam keterbatasan regulasi dan standar operasi prosedur terkait tugas, tanggung jawab dan kewenangan. Sejauh ini sinergitas yang berjalan adalah pada 2 (dua) aspek penyelenggaraan keamanan siber yaitu aspek pencegahan dan penganggulangan serta pemulihan. Namun dalam

komunikasi dan koordinasi yang dilakukan masih terdapat keterbatasan yang disebabkan oleh tidak adanya regulasi yang jelas mengatur pola komunikasi dan koordinasi sehingga pembagian tugas, tanggungjawab dan wewenang hanya berdasarkan program yang ditetapkan oleh sektor masing-masing. Perbedaan struktur organisasi yang sangat signifikan diantara BSSN, Kominfo dan Kemendag yang saling terkait dalam pelaksanaan *cyber security* pada sektor *e-commerce* memiliki faktor penting dalam mencapai sasaran atau tujuan yang telah ditetapkan, dimana kegiatan yang disusun tentu akan menyesuaikan struktur organisasi yang ada. Disamping itu, belum adanya regulasi yang mengatur pola komunikasi dan koordinasi juga merupakan faktor penting dalam menentukan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia.

5.2. Rekomendasi

5.2.1 Rekomendasi Teoritis

Diperlukan penelitian lanjutan terkait pentingnya perlindungan data dan perlindungan konsumen dalam perspektif *cyber security* guna mendukung pertumbuhan ekonomi digital. Disamping itu diperlukan penelitian terkait pola komunikasi dan koordinasi sesuai dengan budaya organisasi di Indonesia serta kebutuhan perekonomian nasional sehingga dapat mengoptimalkan potensi *e-commerce* di Indonesia.

5.2.2 Rekomendasi Praktis

Rekomendasi diberikan kepada:

5.2.2.1 BSSN dan Kominfo

a. Diperlukan penyusunan dan penyesuaian regulasi yang memperjelas tugas dan tanggungjawab masing-masing instansi.
b. Diperlukan strategi dalam menyusun regulasi sehingga dapat menerapkan *cyber security* yang sesuai dengan standar di Asia Tenggara pada sektor *e-commerce.* Regulasi tersebut harus bersifat dinamis dan bersifat implementatif namun tetap memiliki

kekuatan hukum yang mampu menjamin terlaksananya keamanan dan kenyamanan pada transaksi perdagangan melalui sistem elektronik.

c. Pola komunikasi dan koordinasi lintas instansi dalam menerapkan *cyber security* memerlukan standar yang dilengkapi dengan landasan hukum. Hal ini dikarenakan tingkat sensitivitas informasi yang ada pada sektor bisnis dan kekhawatiran yang tinggi atas penyalahgunaan informasi yang dibagikan.
d. Kolaborasi lintas instansi juga diperlukan dalam melaksanakan monitoring dan penanganan terhadap pelanggaran yang tidak sesuai dengan prosedur *cyber security* yang diterapkan pada sektor *e-commerce.*

5.2.2.2 Presiden

a. Adanya regulasi yang sesuai dengan standar yang digunakan oleh negara-negara lain di Asia Tenggara akan mempermudah sistem koordinasi diantara *quad helix.* Regulasi tersebut dapat mendorong optimalisasi peran Pemerintah, Pelaku Bisnis, Masyarakat/Komunitas dan Akademisi dalam mendukung kesiapan *cyber security* pada sektor *e-commerce* di Indonesia.
b. Instansi Pemerintah yang terkait perlu melakukan penyesuaian struktur organisasi guna mengoptimalkan penerapan keamanan siber pada sektor *e-commerce.* Ketimpangan struktur organisasi pada instansi Pemerintah menyebabkan koordinasi dan komunikasi tidak dapat berjalan efektif. Sebaliknya, kelengkapan struktur organisasi yang didukung dengan SDM yang memenuhi kualifikasi, dapat mendukung sinergitas yang dibutuhkan untuk meningkatkan kesiapan *cyber security* pada sektor *e-commerce* di Indonesia.

DAFTAR PUSTAKA

Buku

Andress, Jason. 2011. *The Basic of Information Security:Understanding the Fundamental of InfoSec in Theory and Practice.* USA: Elsevier Inc.

Arikunto. 2006. *Prosedur Penelitian Suatu Pendekatan Praktik*akarta: Penerbit PT Rineka Cipta.

A. T. Kearney. 2018. *Cybersecurity in ASEAN: An Urgent Call to Action.* India: A. T. Kearney Limited.

Bakry, Umar. 2015. *Ekonomi Politik Internasional Suatu Pengantar..* Yogyakarta: Pustaka Pelakar.

Burns-Howell, Tony, Piere Cordier dan Therese Eriksson. 2003. *Security Risk Assessment and Control.* New York: Palgrave Macmillan

Canuto, Octaviano. 2010. *The Day After Tomorrow.* Washington DC: The World Bank.

Cate, Fred. H. 2018. *The Failure of Fair Information Practise Principles: forthcoming in Consumer Protection in the Age of the Information Economy.* US: Indiana University.

Clausewitz, Carl Von. 2007. *On War.* New York: Oxforld World's Classics.

Creswell, John. W. 2016. *Research Design: Pendekatan Metode Kualitatif, Kuantitatif dan Campuran.* Yogyakarta: Pustaka Pelajar.

Dewi, Shinta. 2009. *Cyber Law: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional.* Bandung: Widya Padjajaran.

Frederick, Jaz. 2016. *Global E-Commerce Book.* Texas: PFSweb, Inc.

Ghernaouti, Solange. 2013. *Cyber Power.* Switzerland: EPFL Press.

Indrajit, Eko Richardus. 2014. *Konsep dan Strategi Keamanan Informasi di Dunia Cyber.* Yogyakarta: Graha Ilmu.

Mankiw, N. Gregory. 2009. *Principles of Economics: Pengantar Ekonomi Mikro.* 3rd edition. Jakarta: Salemba Empat.

Miles, Matthew. B, A. Michael Huberman dan Johnny Saldana. 2014. *Qualitative Data Analysis: A Methods Source Book,*3rd edition. US: SAGE Publication, Inc.

Moekijat. 1994. *Koordinasi (Suatu Tinjauan Teoritis).* Bandung: Mandar Maju.

Moleong, Lexy. J. 2014. *Metodologi Penelitian Kualitatif.* Edisi Revisi, Bandung: PT. Remaja Rosdakarya.

Mulyana, Deddy. 2008. *Ilmu Komunikasi: Suatu Pengantar.* Bandung: Remaja Rosdakarya.

Leksono, Sonny. 2013. *Penelitian Kualitatif Ilmu Ekonomi: Dari Metoologi ke Metode.* Jakarta: PT. RajaGrafindo Persada.

Nasution. 2003. *Metode Penelitian Naturalistik-Kualitatif*. Bandung: Tarsito.

Nugroho, Riant, 2009. *Public Policy.* Edisi Revisi. Jakarta: PT. Elex Media Komputindo.

Nugroho, Riant. 2014. *National Security Policy.* Yogyakarta: Pustaka Pelajar.

Ohmae, Kenichi. 1999. *Borderless World: Power and Strategy in The Interlinked Economy.* Revision Edition. New York: HarperCollins Publishers Inc.

O'Neill, Robert. 2016. *War, Strategy & History.* Canberra: Australian National University Press.

Sarno, Riyanarto dan Irsyat Iffano. 2009. *Sistem Manajemen Keamanan Informasi.* Surabaya: ITS Press

Stoner, J. A. F dan Charles Wankel. 1986. *Mangement,* 3rd edition. London: Prentice Hall International Inc.

Strategi Pertahanan Negara. 2015. Jakarta: Kementerian Pertahanan.

Sugiyono. 2016. *Metode Penelitian Kombinasi (Mixed Methods).* Bandung: Alfabeta.

Supriyatno, Makmur. 2014. *Tentang Ilmu Pertahanan.* Jakarta: Yayasan Pustaka Obor Indonesia

Tippe, Syarifudin. 2016. *Ilmu Pertahanan: Sejarah, Konsep, Teori dan Implementasi.* Jakarta: Salemba Humanika.

Jurnal

Down, P.W & J.T. McHenry. 1998. "Network Security: it's time to take it seriously" *Computer*, Vol 31 (9).

Hussain, Mohammad Ali. 2013. "A Study of Information Security in E-Commerce Application"*. International Journal of Computer Engineering (JCES).* Volume 3 (3).

Rahmawati, Triana, Irwan Noor dan Ike Wanusmawatie. "Sinergitas *Stakeholders* Dalam Inovasi Daerah". *Jurnal Administrasi Publik (JAP),* Vol. 2 (4).

Zhou, Zhitian dan Congyang Hu. 2008. "Study on E-Government Security Risk Management*". IJCSNS International Journal of Computer Science and Network Security.* Volume 8 (5).

Undang-Undang

Undang-Undang Dasar Negara Kesatuan Republik Indonesia Tahun 1945.

Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan.

Peraturan

Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara

Peraturan Presiden Nomor 74 Tahun 2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik.

Peraturan Menteri Pertahanan Republik Indonesia Nomor 23 Tahun 2015 tentang Buku Putih Pertahanan Indonesia 2015.

Internet

Anonim. “E-Commerce Jadi Sasaran Siber Rusia Bisa Tolong RI”, dalam https://bit.ly/2JDhwop, diakses pada 19 Juli 2018.

Anonim. “Kebijakan Keamanan dan Pertahanan Siber”, dalam https://bit.ly/2O3g0zx , diakses pada 20 Juli 2018.

Alfarizi, Moh Khory. “Indonesia Akan Sering Terkena Serangan Siber Sepanjang 2018-2025”, dalam https://bit.ly/2mwzIXG, diakses pada 18 Juli 2018.

Berita Kementerian. “Indonesia Akan Jadi Pemain Ekonomi Digital Terbesar di Asia Tenggara”, dalam https://bit.ly/2uQRqZR, diakses pada 17 Juli 2018.

Erdianto, Kristian. “Pemerintah Diminta Lindungi E-Commerce dari Serangan Siber”, dalam https://bit.ly/2LzFL98, diakses pada 19 Juli 2018.

Kementerian Komunikasi dan Informatika. “Indonesia Akan Jadi Pemain Ekonomi Digital Terbesar di Asia Tenggara”, dalam https://bit.ly/2uQRqZR, diakses pada 17 Juli 2018.

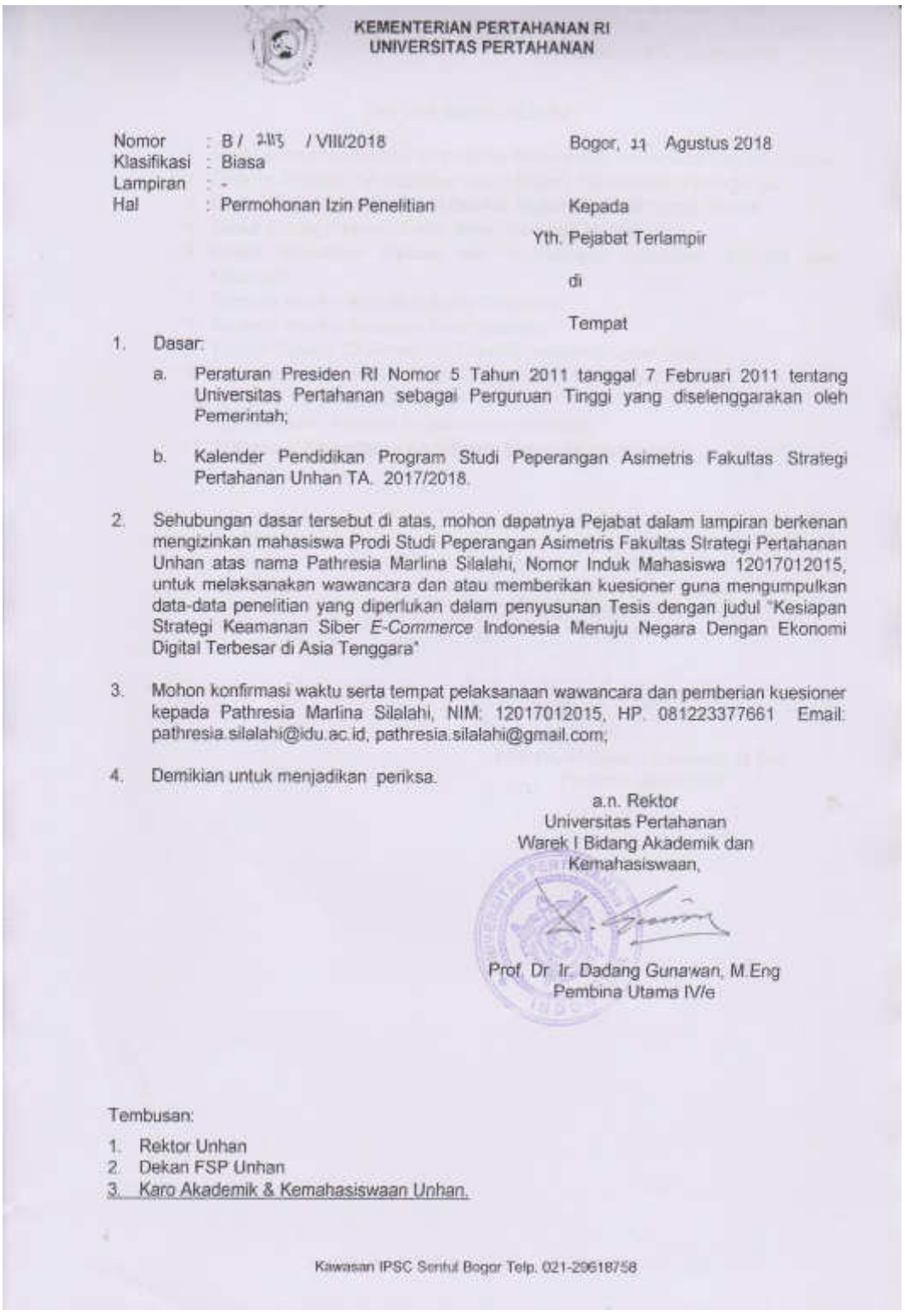
Persada, RM. “Indonesia Pasar Terbesar Smartphone”, dalam https://bit.ly/2JBB10U, diakses pada 17 Juli 2018.

Pinandita, Satrya. “Keamanan Digital di Tahun 2017: Bagaimana Organisasi di Asia Pasifik Dapat Berlindung dari Serangan Siber”, dalam https://bit.ly/2LqFRTE, diakses pada 18 Juli 2018.

Rahardjo, Budi, “Fintech: Layanan Baru, Ancaman Baru” dalam https://bit.ly/2MdwdUE, diakses pada 9 Agustus 2018.

LAMPIRAN 1

SURAT IJIN PENELITIAN



KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN

Nomor : B / 2113 / VIII/2018
Klasifikasi : Biasa
Lampiran : -
Hal : Permohonan Izin Penelitian

Bogor, 11 Agustus 2018

Kepada
Yth. Pejabat Terlampir
di
Tempat

1. Dasar:
   a. Peraturan Presiden RI Nomor 5 Tahun 2011 tanggal 7 Februari 2011 tentang Universitas Pertahanan sebagai Perguruan Tinggi yang diselenggarakan oleh Pemerintah;
   b. Kalender Pendidikan Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Unhan TA. 2017/2018.
2. Sehubungan dasar tersebut di atas, mohon dapatnya Pejabat dalam lampiran berkenan mengizinkan mahasiswa Prodi Studi Peperangan Asimetris Fakultas Strategi Pertahanan Unhan atas nama Pathresia Marlina Silalahi, Nomor Induk Mahasiswa 12017012015, untuk melaksanakan wawancara dan atau memberikan kuesioner guna mengumpulkan data-data penelitian yang diperlukan dalam penyusunan Tesis dengan judul "Kesiapan Strategi Keamanan Siber *E-Commerce* Indonesia Menuju Negara Dengan Ekonomi Digital Terbesar di Asia Tenggara"
3. Mohon konfirmasi waktu serta tempat pelaksanaan wawancara dan pemberian kuesioner kepada Pathresia Marlina Silalahi, NIM: 12017012015, HP. 081223377661 Email: pathresia.silalahi@idu.ac.id, pathresia.silalahi@gmail.com;
4. Demikian untuk menjadikan periksa.

a.n. Rektor
Universitas Pertahanan
Warek I Bidang Akademik dan
Kemahasiswaan,

Prof. Dr. Ir. Dadang Gunawan, M.Eng
Pembina Utama IV/e

Tembusan:
1. Rektor Unhan
2. Dekan FSP Unhan
3. Karo Akademik & Kemahasiswaan Unhan.

Kawasan IPSC Sentul Bogor Telp. 021-29618758

LAMPIRAN 2

PANDUAN WAWANCARA

KESIAPAN STRATEGI KEAMANAN SIBER *E-COMMERCE* INDONESIA MENUJU NEGARA DENGAN EKONOMI DIGITAL TERBESAR DI ASIA TENGGARA

INFORMASI UMUM

Peneliti mengharapkan kesediaan Bapak/Ibu/Saudara/I, berkenan untuk menjawab pertanyaan yang dibuat peneliti, dalam rangka menyelesaikan tesis di Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan. Mohon jawaban atas pertanyaan ini dengan benar dan sejujurnya. Terimakasih atas kesediaan Bapak/Ibu/Saudara/i dalam menjawab pertanyaan yang ada. Apabila terdapat keluhan, kritik dan saran, maka Bapak/Ibu/Saudara/i dapat menghubungi

Nama : Pathresia Marlina Silalahi
Program Studi : Peperangan Asimetris
Fakultas : Strategi Pertahanan
Perguruan Tinggi : Universitas Pertahanan
Alamat : Kawasan IPSC, Sentul, Sukahati, Citeureup
Bogor, Jawa Barat 16810
No. Telp/email : 081-2233-7766-1 / pathresia.silalahi@gmail.com

A. Identitas Informan

Nama : .....
Jabatan : .....
Institusi : .....

B. Deskripsi Penelitian

Penelitian mengenai keamanan siber dalam implementasinya di bidang ekonomi, yaitu pada perdagangan secara elektronik (*e-commerce*) ini, merupakan bagian dari kajian strategi pertahanan berlapis nirmiliter pada instrumen ekonomi yang diharapkan dapat mendukung kemampuan pertahanan negara yang tangguh, efektif dan berdaya tangkal tinggi dalam menghadapi ancaman non militer. Penekanan terhadap ketahanan ekonomi nasional sebagai bagian penting dalam mendukung pertahanan nasional membuat perkembangan ekonomi digital menjadi sebuah peluang sekaligus tantangan bagi Pemerintah mengingat perkembangan ancaman yang bersifat asimetris di era globalisasi ini, salah satunya adalah *cyber warfare*.

Melihat fenomena semakin meningkatnya ancaman siber pada ekonomi digital di Indonesia maka perlu dianalisis kesiapan strategi keamanan siber yang telah dimiliki Indonesia pada sektor *e-commerce*. Adapun aspek dalam pilar *e-commerce* yang diambil yaitu pada pilar *people* dan *public policy.* Hal ini menjadi penting mengingat visi yang telah ditetapkan oleh Pemerintah adalah Indonesia sebagai negara dengan ekonomi digital terbesar di Asia Tenggara pada tahun 2020. Hasil yang diharapkan adalah mengetahui strategi keamanan siber *e-commerce* dan mengetahui kesiapan keamanan siber pada sektor *e-commerce* di Indonesia, dalam rangka mewujudkan ketahanan ekonomi nasional yang mendukung pertahanan nirmiliter Indonesia.

Panduan wawancara / ***Interview Guide***

Penelitian ini menggunakan teori Cybersecurity Ghernaouti (2013) yang membagi dimensi *cybersecurity* yang memfokuskan diri pada 2 (*dua*) parameter saja, yaitu aspek ***legal*** dan ***organisasional*** dalam strategi keamanan siber *e-commerce* di Indonesia.

Adapun berdasarkan parameter tersebut maka pokok-pokok wawancara dalam penelitian ini adalah sebagai berikut:

I. **Aspek Legal**

1. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai legal framework keamanan siber untuk *e-commerce* dalam menghadapi serangan siber apakah telah memuat 3 aspek berikut dan jika sudah mohon jelaskan:
   a. Pembentukan
   b. Merespon
   c. Menyiapkan diri

2. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai *legal framework* keamanan siber *e-commerce* apakah telah melingkupi 3 tahap berikut:
   a. Tahap penyusunan
   b. Tahap implementasi
   c. Tahap evaluasi

3. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai *legal framework* keamanan siber *e-commerce* apakah telah memuat 3 substansi dasar strategi yaitu:
   a. Tujuan yang ingin dicapai
   b. Sumber daya yang digunakan
   c. Cara menggunakan sumber daya tersebut

4. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai aspek keamanan siber *e-commerce* di Indonesia apakah telah mengakomodir 6 aspek keamanan informasi, yaitu *access control, confidentiality, authentication, non-repudiation, integrity* dan *availability*?

5. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai metode standar yang digunakan dalam menjamin keamanan siber *e-commerce* di Indonesia, apakah *encryption, SSL, digital signature, digital certificates, smart cards atau e-money?*

6. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai peraturan perundang-undangan yang ada apakah sudah dapat mengakomodir aspek hukum yang dibutuhkan untuk menjamin terwujudnya keamanan siber *e-commerce* di Indonesia guna mendukung pertahahanan siber Indonesia:
   a. UU Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik
   b. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
   c. Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber

7. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai *legal framework* keamanan siber *e-commerce* Indonesia apabila dibandingkan dengan Singapore dan Malaysia?

8. Bagaimana menurut Bapak/Ibu/Saudara/I terkait hal-hal yang masih perlu diperhatikan pada aspek hukum yang dapat menjadi kerentanan dalam keamanan siber *e-commerce?* Apakah terdapat

peraturan yang masih perlu disesuaikan atau ditambahkan atau implementasi yang masih perlu ditingkatkan?

9. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai road map *e-commerce* yang dimuat dalam Peraturan Presiden Nomor 74 Tahun 2017, apakah strategi keamanan siber perlu disusun tersendiri atau perlu menjadi satu kesatuan dengan strategi lainnya? Dengan mempertimbangkan 5 pilar *e-commerce* yaitu *people, public policy, marketing and advertisement, supply chain* dan *infrastructure*

10. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai upaya pada aspek hukum yang dapat dilakukan untuk meningkatkan kesiapan keamanan siber *e-commerce* menuju negara dengan ekonomi digital terbesar di Asia Tenggara tahun 2020?

II. **Organisasional**

1. Bagaimana menurut Bapak/Ibu/Saudara/I terkait *legal framework* yang mengatur pembagian tugas dan tanggungjawab antar lembaga dalam mewujudkan keamanan siber *e-commerce* di Indonesia?

2. Bagaimana menurut Bapak/Ibu/Saudara/I terkait implementasi terhadap pembagian tugas dan tanggungjawab yang sudah diatur dalam peraturan perundang-undangan tersebut?

3. Bagaimana menurut Bapak/Ibu/Saudara/I terkait sinergitas antar lembaga dalam penyusunan, implementasi dan evaluasi terhadap keamanan siber *e-commerce* di Indonesia?

4. Bagaimana menurut Bapak/Ibu/Saudara/I terkait kelemahan-kelemahan pada aspek organisasional yang dapat menjadi

kerentanan dalam mewujudkan keamanan siber *e-commerce* di Indonesia, apakah terkait aspek hukum yang perlu dirubah atau ditambahkan atau terkait operasional/implementasi yang belum maksimal?

5. Bagaimana saran Bapak/Ibu/Saudara/I terkait upaya yang dapat dilakukan untuk sinergitas antar lembaga guna meningkatkan kesiapan keamanan siber *e-commerce?*

6. Bagaimana menurut Bapak/Ibu/Saudara/I terkait sinergitas antar lembaga untuk mewujudkan keamanan siber *e-commerce* di Indonesia jika dibandingkan dengan Singapore dan Malaysia?

7. Bagaimana menurut Bapak/Ibu/Saudara/I mengenai kesiapan keamanan siber *e-commerce* pada aspek organisasional menuju negara dengan ekonomi digital terbesar di Asia Tenggara tahun 2020?

LAMPIRAN 3

DATA NARASUMBER

Jabatan	Instansi	Kode
Staff Ahli Menteri Kominfo Bidang Teknologi	Kominfo	A
Direktur Deteksi Ancaman	BSSN	B1
Direktur Penanggulangan dan Pemulihan Ekonomi Digital	BSSN	B2
Direktur Pengendalian Aplikasi Informatika	Kominfo	B3
Kasubdit Proteksi E-Commerce	BSSN	C1
Kasubdit Identifikasi Kerentanan & Penilaian Resiko	BSSN	C2
Kasubdit Tata Kelola Sistem Elektronik	Kominfo	C3
Ketua Tim Tenaga Ahli Road Map E-Commerce	Kemenkokuin/ Wakil Ketua idEA	C4
Tenaga Ahli Keamanan Siber Road Map E-Commerce	Kemenkokuin	C5
Kasubdit E-Commerce	Kemendag	C6
Kasie Bidang Ekonomi Digital	Kominfo	D1
Pakar Cyber Security	ITB	E
Komunitas Cyber Security	ICSF	F
Pelaku E-Commerce	LiteBig	G

LAMPIRAN 4

DOKUMENTASI

KOMINFO

Wawancara Staff Ahli Menteri
Bid. Teknologi,
6 September 2018

Wawancara Direktur
Pengendalian Aptika,
10 September 2018

Wawancara Kasubdit Tata Kelola
Sistem Elektronik,
19 September 2018

Wawancara Kasie
Ekonomi Digital,
13 September 2018

BSSN

Wawancara Direktur Deteksi Ancaman,
26 Oktober 2018

Wawancara Kasubdit Proteksi Ekonomi Digital,
2 Oktober 2018

Wawancara Kasubdit Identifikasi Kerentanan & Penilaian Risiko,
29 Oktober 2018

Wawancara Direktur Penanggulangan & Pemulihan
Ekonomi Digital,
6 November 2018

KEMENDAG

Wawancara Kasubdit dan tim E-Commerce,
19 September 2018

KEMENKOKUIN

Wawancara Ketua Tenaga Ahli Sekretariat *Road Map E-Commerce* 5 Oktober 2018

Wawancara TA *Cyber Security* Sekretariat *Road Map E-Commerce* 16 Oktober 2018

KOMUNITAS *CYBER SECURITY*

Wawancara Founder ICSF, 28 September 2018

PELAKU *E-COMMERCE*

Wawancara Pelaku E-Commerce LiteBig, 15 September 2018

PAKAR *CYBER SECURITY*

Wawancara dengan pakar *cyber security*, 25 Oktober 2018

RIWAYAT HIDUP PENELITI

Pathresia Marlina Silalahi, lahir di Malang, pada tanggal 24 Maret 1986 Anak ke-2 dari pasangan Bapak Dr. M. H. Perwira Silalahi dan Lenni Saragih, M.Kes. Menyelesaikan pendidikan SDK. Santa Maria Malang II lulus tahun 1998, SMP Negeri 3 Malang lulus tahun 2001, SMA Negeri 04 Malang lulus tahun 2004, Sarjana (S-1) Universitas Brawijaya lulus tahun 2009 dan pada tahun 2017 melanjutkan program Magister (S-2) di Universitas Pertahanan.

Peneliti saat ini menjabat sebagai Legal Manager di PT. Tirta Wahana Bali Internasional, mengawali pekerjaan/karir di PT. Sinarmas Agribusiness and Food, PT. Smart, Tbk di tahun 2011.

Menikah dengan Semar Silengguri Ginting pada tahun 2014 di Jakarta Barat dan dikaruniai 1 (satu) orang anak bernama Cherish Trinity Pizarayona Ginting.