UPAYA ASEAN DALAM MENGATASI KASUS CYBERCRIME DI INDONESIA (2019-2021)

Oleh : Muhammad Rafizi Ismail
Pembimbing: Saiman Pakpahan, S.IP., M.Si
Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Riau
Kampus Bina Widya, Jl. H.R. Soebrantas Km 12,5 Simp. Baru, Pekanbaru 28293
Telp/Fax. 0761-63277

Abstract

This study discusses ASEAN's efforts to overcome cybercrime cases in Indonesia. The issue of this crime resulted in losses for various parties including the state. Low security, low education, and low law enforcement are among the factors that encourage the issue of this crime to move freely. Efforts are being made to cooperate with ASEAN through ASEAN documents on transnational crime, as well as implementing cyber security, cyber resilience, and cyber diplomacy.

This research uses qualitative methods, using case study research techniques through indirect sources such as notes, reports, articles or journals. This research uses the perspective of Neorealism, Cyber Security theory.

The result of this paper is that ASEAN's efforts are still ongoing but Indonesia's support is also needed so that the implementation of security, resilience and diplomacy can be carried out properly.

Keywords: *ASEAN, Cybercrime, Cyber Diplomacy, Cyber Security, Cyber Resilience*

Pendahuluan

Penelitian ini membahas masalah dalam kajian isu-isu kejahatan transnasional, yang disebut dengan kejahatan siber atau *cybercrime. Cybercrime* merupakan istilah umum yang digunakan dalam mengelompokkan tindakan kejahatan berbasis dunia maya atau siber atau sering disebut kriminal di dunia elektronik dan komputer. Kejahatan yang satu ini merupakan salah satu kejahatan transnasional yang bisa dikatakan serius karena dapat menjadi ancaman besar khususnya bagi

pemerintah karena bila tidak ditanggulangi ataupun diatasi maka ini akan terus berlanjut dan bertambah luas, karena kejahatan yang dilakukan dengan teknologi komputer, terkhusus untuk jaringan internet dan intranet itu

cukup sulit untuk diimbangi.[1] Oleh karena itu, dengan adanya kasus *cybercrime* ini, maka permasalahan akan menjadi cukup merepotkan dan harus bisa dituntaskan secara perlahan. Karena banyak sekali bentuk-bentuk *cybercrime* baik di Indonesia ataupun di beberapa negara ASEAN, tiga contoh kasus terbanyak yaitu Phising, merupakan kejahatan lewat internet yang paling banyak memanfaatkan metode pencurian identitas, kemudian Ddos atau Distributed Denial of Service Attack, merupakan bentuk serangan yang dilakukan dengan mengirim paket secara terus menerus kepada mesin bahkan jaringan komputer dan berakibat pada sumber daya mesin ataupun jaringan yang tidak dapat diakses oleh pengguna, dan Pembajakan situs website, merupakan pencurian atau pengambilan secara paksa akses atau *gaining access* dalam mengelola situs tersebut, sehingga pembajak atau pencuri tadi dapat menulis, menghapus, ataupun merubah seluruh isi website tersebut sesuai dengan keinginannya.

Kemudian, menurut bapak Bhakti Eko Nugroho, M.A., yang merupakan salah satu dosen Departemen Kriminologi, FISIP, Universitas Indonesia dalam seminarnya mengatakan bahwa *cybercrime* ini menjadi salah satu kejahatan transnasional yang mengalami peningkatan yang cukup signfikan, juga memiliki trik yang beragam apakah pencurian data ataupun pembobolan rekening. Pengguna internet di dunia ataupun di Indonesia setiap tahunnya semakin meningkat, dan dengan adanya Covid-19 pada tahun 2020 kemarin membuat dampak yang cukup besar pada pola hidup masyarakat Indonesia, karena lebih banyak mengandalkan internet. Sebenarnya sisi positifnya tinggi, namun masih ada orang yang menyalahgunakan perkembangan teknologi yang ada. Berdasarkan data dari Patroli Siber, pada tahun 2019 hingga 22 Mei 2020, ada sekitar 6.388 kasus cybercrime dan jenis terbanyak yaitu penyebaran konten provokatif sekitar 2.584 laporan, disusul dengan penipuan online sekitar 2.147 kasus, dan terakhir kasus pornografi dengan 536 kasus. [2]

Kemudian dilanjutkan pada data 2020 hingga 2021 yang berasal dari POLRI, ada sekitar 937 kasus yang dilaporkan dan tiga teratas yaitu sama dengan yang terjadi pada tahun 2019-2020 yaitu kasus provokatif, dilanjutkan dengan *hate content* dan *hate speech* dengan laporan sekitar 473 kasus, kemudian 259 kasus untuk penipuan online, dan terakhir yaitu konten porno dengan 82 kasus. [3] Jadi, berdasarkan data diatas, dapat dilihat

[1] Dr. H. Obsatar Sinaga, M.Si, *Penangguulangan Kejahatan Internasional Cyber Crime di Indonesia*, Microsoft Word - CYBER CRIME ICMI (unpad.ac.id)

[2] Patroli Siber, *Jenis Kejahatan Siber di Indonesia, 2019-2020,* diakses dari Lokadata pada 21 November 2022, Jenis kejahatan siber di Indonesia, 2019-2020 - Lokadata (beritagar.id)

[3] Hafidz, *Kejahatan Siber Meningkat di Masa Pandemi*, dipublish pada 2 Agustus 2021, diakses pada 21 November 2022, Universitas Indoneisa, Kejahatan Siber Meningkat di Masa Pandemi - Universitas Indonesia (ui.ac.id)

bahwa sudah adanya penurunan yang terjadi pada kasus *cybercrime* di Indonesia, namun angka tersebut masih terbilang besar dan masih meresahkan masyarakat sekitar. Oleh karena itu, pemerintah Indonesia telah mencoba untuk bekerja sama dengan ASEAN atau *Association of Southeast Asian Nations* karena ancaman *cybercrime* ini sendiri bukan hanya menyerang Indonesia saja, melainkan sudah menyerang beberapa negara lain yang juga bagian dari ASEAN. Negara yang berada di lingkup ASEAN sebenarnya memiliki pertahanan siber yang terbilang rendah atau mungkin kurang baik karena kasus yang terjadi sebenarnya tidak menggunakan trik baru atau yang jarang dikenal, namun trik yang sama yang sudah ada sejak beberapa tahun sebelumnya yaitu *phising*, Ddos, *ransomware*. Dua diantaranya merupakan cara ataupun trik yang sering terjadi di Indonesia dan itu disebabkan karena adanya kelengahan atau celah yang dilakukan oleh manusia tersebut.[4] Begitu juga dengan jenis kasus yang terjadi dalam lingkup ASEAN, dimana jenis kasus yang ada merupakan jenis yang sama dengan Indonesia yaitu phising, data breach, ransomware.[5]

Secara singkat, perlu diketahui bahwa ASEAN merupakan organisasi yang mewadahi kerja sama regional di Asia Tenggara. Salah satu kejahatan transnasional ini membuat ASEAN melakukan beberapa pertemuan sekaligus mempersiapkan hal apa saja yang dapat dilakukan untuk menanggulangi kasus cybercrime ini, karena salah satu tujuan dari ASEAN itu sendiri yaitu meningkatkan kerjasama dan saling membantu dalam mengatasi segala bentuk permasalahan di berbagai bidang untuk kepentingan bersama.[6] Selain itu, ASEAN juga memiliki komunitas yang terdiri dari tiga pilar, dan dari ketiga komunitas ASEAN diatas, APSC atau *ASEAN Political Security Community*, yang bertujuan untuk memastikan perdamaian regional dan lingkungan yang adil, demokratis, dan harmonis. menjadi komunitas yang paling berkaitan dengan penelitian ini, namun bukan berarti hanya komunitas ini saja yang berupaya di ASEAN untuk menanggulangi kasus *cybercrime*.

Adapun beberapa upaya yang dilakukan ASEAN untuk menanggulangi serta memberantas kasus *cybercrime* ini di Indonesia yaitu dengan adanya Deklarasi ASEAN untuk Mencegah dan Memerangi Kejahatan Dunia Maya atau ASEAN Declaration to Prevent and Combat

[4] Pramudita, B.A. (2021). *Rangkaian Kejahatan Siber tahun 2020 di Asia Tenggara Versi Kaspersky*, diakses pada 21 November 2022, Warta Ekonomi.co.id, Rangkaian Kejahatan Siber Tahun 2020 di Asia Tenggara Versi Kaspersky (wartaekonomi.co.id)

[5] Lisna Threestayanti, *Lima Kasus Cybersecurity Paling Menggemparkan di Dunia dan ASEAN*, diakses pada 22 November 2022, InfoKomputer, Lima Kasus Cybersecurity Paling Menggemparkan di Dunia dan ASEAN - Semua Halaman - Info Komputer (grid.id)

[6] M. Prawiro, *Pengertian ASEAN: Arti, Negara Anggota, dan Tujuan ASEAN*, diakses pada 22 November 2022, Maxmanroe, Pengertian ASEAN adalah: Arti, Negara Anggota, dan Tujuan ASEAN (maxmanroe.com)

Cybercrime pada 13 November 2017 di Manila, Filiphina. Berikutnya, akan ada beberapa tindakan juga rencana yang akan dilakukan oleh negara-negara ASEAN untuk mengatasi kejahatan transnasional termasuk *cybercrime* atau kejahatan siber, yaitu dengan menerapkan beberapa hal seperti *cyber security, cyber resilience,* dan *cyber diplomacy* seperti yang sudah disebutkan sedikit pada beberapa poin diatas. Walaupun diluar dari tiga poin diatas, Indonesia juga sudah sedikit mendapatkan bantuan dari permasalahan ini yaitu dengan melahirkan *cyber law,* yang mana pemikiran ini berasal dari *Convention on Cyber Crime* tahun 2001 yang digagas oleh negara-negara Uni Eropa.

Adapun salah satu faktor yang bisa dikatakan cukup mempersulit Indonesia dalam mengatasi kasus *cybercrime* ini ialah karena Indonesia tidak memiliki Undang-Undang keamanan siber secara khusus, tetapi hanya mengandalkan UU ITE. Namun, dengan adanya kekurangan ini maka membuat Indonesia semakin aktif dalam melaksanakan kerja sama dengan ASEAN.

Metode Penelitian

Penulis menggunakan riset studi kasus karena pendekatan ini memberikan penjelasan yang mendalam tentang sebuah kasus, sehingga pendekatan ini tepat untuk digunakan dalam penelitian kali ini. Penelitian studi kasus merupakan pendekatan kualitatif yang penelitinya mengeksplorasi kehidupan nyata yang dibatasi waktu dan tempat, dengan pengumpulan data yang mendalam yang melibatkan berbagai macam sumber informasi (dokumen, laporan, dan lainnya).

Data ini diperoleh secara tidak langsung melalui perantara (yang dicatat ataupun didapatkan oleh pihak lain). Data sekunder itu seperti catatan, laporan-laporan, artikel, yang sudah tersusun dalam sebuah file ataupun arsip. Data yang diperoleh juga berasal dari internet ataupun jurnal dan laporan yang sudah ditulis. Penulis tidak mendapatkan data primer karena rata-rata berdasarkan dari jurnal dan buku yang sudah dibuat oleh orang lain.

Kerangka Teori

Perspektif Neo-Liberal Institusionalisme

Berdasarkan beberapa perspektif yang dibaca, maka penulis menyimpulkan untuk menggunakan Neo-liberal institusionalme sebagai perspektif pada tulisan ini. Perspektif ini merupakan perspektif yang menggunakan pandangan liberal. Dikembangkan oleh Robert Keohane, ia menegaskan bahwa institusi internasional dapat menciptakan kerja sama yang nyata dan lebih baik antar negara-negara. Neo-liberal institusional sangat mendukung antar kerjasama antar negara dengan memakai pendekatan ilmiah dan *behavioralistik,* yang artinya dalam membangun kerjasama sangat menekankan pada perilaku aktor.

Neo-liberal Institusionalme berasumsi bahwa “negara merupakan aktor penting dalam studi hubungan

internasional, namun bukan satu-satunya aktor yang ada. Aktor-aktor *non-state* juga memiliki kontribusi dalam hubungan dan kerjasama antar negara". Pada buku Pengantar Studi Hubungan Internasional: Teori dan Pendekatan yang ditulis oleh Jackson dan Sorensen (2013), dikatakan bahwa ketika negara yang menjadi aktor utama dalam menjalani kerjasama dan hubungan internasional, maka negara akan selalu ada untuk kepentingan nasionalnya, oleh karena itu, ketika semua negara memiliki kepentingan nasional, akan ada negara yang dirugikan dan berkemungkinan terjadinya perang oleh karena ada rasa persaingan dan tidak adil.

Neo-liberal juga hadir untuk memberikan solusi yaitu dengan membangun kerjasama. Keohane dan Nye (1977) mengatakan kerjasama yang dimaksud yaitu situasi internasional yang saling bergantung antar satu dengan yang lainnya (*complex interpendence*), dimana tidak mengenal aktor baik negara maupun bukan negara semuanya memiliki sifat saling tergantung, dengan demikian kebijakan serta tindakan satu aktor dapat berdampak dengan aktor lainnya. Tujuan liberalisme institusional juga untuk mempromosikan keamanan manusia, kesejahteraan manusia, dan kebebasan manusia sehingga dapat menghasilkan dunia yang lebih damai, sejahtera, dan bebas.[7] Perspektif ini terbilang cukup berkaitan dengan penelitian ini, hal tersebut dikarenakan adanya peranan aktor *non-state* yaitu ASEAN.[8]

Teori Organisasi Internasional

Teori yang digunakan dalam tulisan ini yaitu teori Organisasi Internasional, dimana teori ini menurut Gutner merupakan suatu organisasi formal yang anggotanya terdiri dari tiga atau lebih negara untuk mencapai tujuan yang spesifik. Organisasi internasional memiliki dua bentuk, yaitu *inter govermental organization* atau IGO dan *International Non-Governmental Organization* atau INGO.

Organisasi internasional merupakan aktor non negara yang memliki peran yang sangat penting dalam dinamika hubungan internasional. Organisasi internasional mulai dibicarakan pada abad ke 20 di wilayah barat sebagai lembaga formal untuk kerjasama internasional. Organisasi internasional bersifat global, oleh karena itu diperlukan wadah yang beranggotakan banyak negara yang memiliki visi yang sama. Kemudian, dikatakan sebagai organisasi internasional karena adanya kerjasama yang dilakukan untuk mencakup banyak aspek, seperti perdagangan, hukum, pendidikan,

[7] Neoliberalisme Institusional Kerangka Teori dan Konseptual, https://text-id.123dok.com/document/oy83vpn2q-neoliberalisme-institusional-kerangka-teori-dan-konseptual.html, diakses pada 15 Juni 2023.

[8] Bab II, Tinjauan Pustaka, Teori Neo-Liberal Institusional, https://repository.uksw.edu/bitstream/123456789/24188/20/T1_372017077_Bab%20II.pdf, diakses pada 15 Juni 2023.

pangan, hak asasi manusia, hingga pencegahan aksi terorisme.

Dalam buku *International Organization*, Clive Archer menyatakan bahwa organisasi internasional merupakan suatu struktur formal dan berkelanjutan yang dibentuk berdasarkan suatu kesepakatan antara anggota-anggotanya baik itu pemerintah atau non-pemerintah dari dua atau lebih negara yang berdaulat dengan tujuan mengejar kepentingan bersama dengan anggotanya. Archer juga mengungkapkan beberapa syarat sebagai organisasi internasional, antara lain:

1. Tujuannya harus merupakan tujuan internasional.
2. Harus memiliki anggota yang setiap anggotanya memiliki hak suara mereka masing-masing.
3. Dibentuk berdasarkan pada anggaran dasar dan harus memiliki markas besar (*headquarter*) demi kelangsungan organisasi.
4. Pejabat atau pegawai mempunyai tugas yang menjalankan pekerjaan organisasi harus terdiri dari berbagai bangsa atau negara.
5. Organisasi harus dibiayai oleh anggota yang berasal dari berbagai negara/bangsa. Organisasi harus berdiri sendiri (*independent*) dan hars masih aktif. Jika sudah tidak aktif lebih dari lima tahun, maka tidak akan diakui lagi. [9]

Clive Archer menjelaskan mengenai peran yang harus dimiliki oleh organisasi internasioal yaitu sebagai berikut:

1. Sebagai instrumen. Digunakan oleh negara anggotanya untuk mencapai tujuan tertentu berdasarkan tujuan politik luar negerinya.
2. Sebagai arena. Merupakan tempat bertemu bagi anggota-anggotanya untk membicarakan masalah-masalah yang sedang dihadapi, terkadang organisasi internasional juga digunakan oleh bebereapa negara untuk mengangkat masalah dalam negerinya ataupun dari negeri lain dengan tujuan untuk mendapatkan perhatian internasional dan memecahkan masalah yang dihadapi bersama-sama.
3. Sebagai aktor independen. Dapat membuat keputusan mereka sendiri tanpa dipengaruhi oleh kekuasaan dari luar organisasi. Sebuah organisasi internasional dapat menjalankan

[9] Bab II, Tinjauan Pustaka, https://repository.uksw.edu/bitstream/123456789/22107/3/T1_372017015_BAB%20II.pdf, diakses pada 18 Juni 2023.

kebijakannya tanpa adanya intervensi dari luar.[10]

Secara singkat, ASEAN merupakan organisasi yang mewadahi kerjasama regional di Asia Tenggara. Pada hakikatnya peran organisasi internasional memang dibutuhkan dalam hubungan internasional. Hal itu dikarenakan kurangnya peran pemerintah sehingga diperlukannya kerjasama melalui organisasi internasional agar tercapainya kepentingan suatu negara dan dapat mengikuti laju dari perkembangan globalisasi. [11]

Hasil dan Pembahasan

Dokumen ASEAN tentang Kejahatan Transnasional

ASEAN berupaya untuk menanggulangi kasus cybercrime. Hal ini dilakukan karena salah satu tujuan ASEAN yaitu untuk meningkatkan kerjasama dan saling membantu dalam mengatasi segala bentuk permasalahan di berbagai bidang untuk kepentingan bersama.[12] Kemudian, meningkatkan keamanan siber baik di Indonesia maupun di kawasan Asia Tenggara juga menjadi salah satu upaya dari ASEAN untuk mengurangi kasus kejahatan siber, dan hal tersebut sudah berlangsung sejak tahun 2001 hingga saat ini. Namun pengimplementasi keamanan siber sulit dilakukan karena adanya perbedaan dalam kemampuan siber dari negara anggota ASEAN, baik dalam hal teknologi, operasional, kebijakan, maupun kapasitas hukum. Adapun upaya yang dilakukan ASEAN untuk menangani kasus kejahatan dunia maya atau *cybercrime* telah tertulis dalam Dokumen ASEAN tentang Kejahatan Transnasional : Terorisme dan Ekstremisme Kekerasan; Narkoba; Kejahatan Dunia Maya; dan Perdagangan Manusia. [13] Penjabaran dua poin dokumen dibawah dapat dilihat melalui ASEAN Document Series on Transnational Crime.

1. **ASEAN Declaration to Prevent and Combat Cybercrime** atau **Deklarasi ASEAN untuk Mencegah dan Memerangi Kejahatan Dunia Maya**, Manila, Filipina, 13 November 2017.

2. **ASEAN Regional Forum Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security**

[10] Rudy T. May,(2009), "Administrasi dan Organisasi Internasional", PT.Refika Aditama, Bandung, Hal.2

[11] M. Prawiro, *Pengertian ASEAN: Arti, Negara Anggota, dan Tujuan ASEAN*, diakses pada 22 November 2022, Maxmanroe, Pengertian ASEAN adalah: Arti, Negara Anggota, dan Tujuan ASEAN (maxmanroe.com)

[12] M. Prawiro, *Pengertian ASEAN: Arti, Negara Anggota, dan Tujuan ASEAN*, diakses pada 08 Maret 2023, Maxmanroe, Pengertian ASEAN adalah: Arti, Negara Anggota, dan Tujuan ASEAN (maxmanroe.com)

[13] Association of Southeast Asian Nations, ASEAN Main Portal, Our Communities, diakses pada 08 Maret 2023, Our Communities - ASEAN Main Portal

atau **Pernyataan Forum Regional ASEAN oleh Menteri Luar Negeri tentang Kerjasama dalam Memastikan Keamanan Cyber,** Phnom Penh, Kamboja, 12 Juli 2012.

Cyber Security, Cyber Resilience, dan Cyber Diplomacy

Cyber security merupakan keamanan informasi yang diterapkan ke kompuiter atau jaringan dengan tujuan untuk membantu pengguna mencegah penipuan atau mendeteksi segala upaya penipuan dalam sistem berbasis informasi. Keamanan siber atau *cyber security* juga sebagai bentuk upaya untuk melindungi informasi dari serangan siber. Serangan siber pada operasi informasi ialah semua tindakan yang disengaja untuk mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Tindakannya dapat berupa gangguan fisik atau gangguan aliran logis sistem informasi.

Kemudian, *cyber resilience* atau ketahanan nasional merupakan sebuah istilah yang digunakan untuk keamanan siber yang berhubungan dengan aset atau sumber daya suatu negara.[14] Ketahanan nasional ialah konsepsi pengembangan kekuatan siber melalui pengaturan dan penyelenggaraan kesejahteraan dan keamanan yang seimbang, serasi, dan selaras dalam seluruh aspek kehidupan secara utuh dan terpadu berlandaskan UUD NKRI 1945 dan wawasan nusantara. Dalam hal lain, konsepsi ketahanan siber nasional merupakan pedoman untuk meningkatkan keuletan dan ketangguhan bangsa yang mengandung kemampuan mengembangkan kekuatan siber dengan pendekatan kesejahteraan dan keamanan.

Adapun tujuan *cyber resilience* dan *cyber security* adalah untuk perlindungan, dominasi, dan kontrol data dan informasi. Keamanan dan ketahanan nasional berkaitan erat dengan operasi informasi yang melibatkan berbagai pihak seperti militer, pemerintah, badan usaha milik negara, perusahaan, akademisi, sektor swasta, individu, dan dunia internasional. Kebijakan keamanan dan ketahanan siber telah dikoordinasikan oleh Kementerian Komunikasi dan Informatika (Kominfo). Dalam sistem dan strategi tersebut terdapat tiga organisasi pemerintah Indonesia, yaitu Keamanan Informasi Tim Koordinasi, Direktorat Keamanan Informasi, dan *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII)[15]

Sebagian besar negara di ASEAN membuat beberapa bentuk undang-undang dan kebijakan untuk menangani masalah siber, dan salah

[14] M. Boisot, *Knowledge Assets: Securing Competitive Advantage in the Information Economy*, OUP Oxford, Oxfortd, 1998, p.18.

[15] Muhammad R. dan Yanyan M., *Cybersecurity Policy and Its Implementation in Indonesia*, Journal of ASEAN Studied, Vol.4, No.1 (2016), p.67.

satu upaya Indonesia yaitu dengan menerbitkan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 11 Tahun 2008 Informasi dan Transaksi sebagai perumusan regulasi dan kebijakan terkait keamanan informasi. Pemerintah Indonesia juga membentuk Badan Siber dan Sandi Nasional (BSSN) yang bertanggung jawab untuk mencegah serangan dunia maya, juga bekerja untuk memperkuat pertahanan negara terhadap ancaman dunia siber dan meningkatkan kesadaran publik tentang keamanan siber.[16]

Setelah peran nasional, peran kerja sama internasional untuk mendukung implementasi *cyber security* dan *cyber resilience* juga diperlukan. Indonesia dan ASEAN melakukan kerja sama untuk menangani kejahatan siber dengan meningkatkan keamanan siber di Indonesia. Salah satu alasan mengapa Indonesia perlu meningkatkan keamanan dan ketahanan infrastruktur informasi nasional yaitu karena adanya Ekonomi Digital yang berkaitan dengan teknologi untuk transaksi bisnis dan hal tersebut menjadi peluang baru untuk kejahatan siber.[17]

Indonesia dan ASEAN juga bersama-sama menangani kejahatan siber dengan meningkatkan keamanan siber di negara anggota dengan berpartisipasi dalam kegiatan ASEAN Forum Regional (ARF) yang berfokus pada ancaman kejahatan siber. Hal tersebut terbukti pada pertemuan "*Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space*" di Vietnam pada tahun 2012.[18]

Selain ASEAN, Indonesia juga bekerja sama dengan Malaysia dan Singapura yang termasuk dari anggota ASEAN karena kedua tersebut memiliki keunggulan dalam keamanan siber. Siberoc merupakan institusi yang menjalankan fungsi keamanan siber di Malaysia. Institusi ini mendukung kebijakan keamanan siber dan penerapannya di Indonesia, juga berkoordinasi dengan institusi lainnya seperti *Malaysian Computer Emergency Response Team (*MyCERT). Kemudian, Indonesia juga bekerja sama dengan Singapura yang memiliki sumber daya manusia yang unggul dalam jumlah pakar keamanan informasi di ASEAN. Dalam penerepannya, *cyber security* dan *cyber resilience* dapat bekerja terhadap beberapa kejahatan siber, antara lain *hacking* (peretasan), *skimming* (penyalinan informasi), *hijacking* (pembajakan software), *phising* (pengelabuan), serta pembajakan situs

[16] Jirapon Sunkhpo, dkk., *Cybersecurity Policy in ASEAN Countries,* Information Institute Conferences, Las Vegas, NV, 2018,p.4., diakses pada 27 Maret 2023.

[17] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing New Generation of National Cybersecurity Strategies for the Internet Economy,* OECD Digital Economy Papers, No.211 (2012). EOCD Publishing, Paris, 2012, *p.*

[18] ASEAN Secretaria, *Cooperation on Cybersecurity and against Cybercrime, Octopus Conference: Cooperation Against Cybercrime,* Council of Europe, Strasbourg, France, 2013, p.20.

web atau *defacing*. Penambahan keamanan serta pengedukasian terhadap masyarakat masih menjadi salah satu cara agar kejahatan siber dapat berkurang. [19]

Berikutnya, *cyber diplomacy* merupakan praktik internasional yang muncul atas upaya untuk membangun masyarakat siber internasional, dengan menjembatani antara kepentingan nasional negara dan dinamika masyarakat dunia dengan tujuan memenuhi fungsi-fungsi tradisional diplomasi, seperti menjaga perdamaian serta membangun rasa saling percaya di antara para pemangku kepentingan, di ruang siber. *Cyber diplomacy* memiliki banyak definisi, pertama yaitu sebagai upaya untuk memfasilitasi komunikasi, menegosiasikan perjanjian, mengumpulkan informasi dan intellijen dari negara lain untuk menghindari gesekan di ruang siber, dengan mengacu pada agenda kebijakan luar negeri. Kedua, sebagai upaya untuk menggunakan sumber daya dan fungsi diplomatik untuk mengamankan kepentingan nasional terkait ruang siber. Dan ketiga, *cyber diplomacy* juga dapat diartikan sebagai diplomasi di dalam ruang lingkup siber dan kinerja fungsi diplomatik untuk mengamankan kepentingan negara terkait ruang siber. Kepentingan *cyber diplomacy* pada umumnya diidentifikasi dalam strategi ruang siber (*cyberspace*) suatu negara atau keamanan siber (*cyber security*) yang disertakan dalam agenda diplomatik. *Cyber diplomacy* melibatkan diplomasi, resolusi konflik, perjanjian dan kebijakan yang mengelilingi dunia siber.

Indonesia merupakan salah satu negara yang memprakarsai *Treaty of Amity and Cooperation* atau Perjanjian Persahabatan dan Kerja Sama, dimana sesama negara anggota melaksanakan perjanjian tersebut dengan tidak saling menyerang dan menyelesaikan konflik dengan cara yang damai. Hal ini serupa dengan upaya yang dilakukan dengan *cyber diplomacy* yaitu melibatkan diplomasi, resolusi konflik, perjanjian dan kebijakan yang mengelilingi dunia siber. *Cybercrime* merupakan salah satu isu yang dibahas dalam *cyber diplomacy*. *Cyber diplomacy* dilakukan oleh diplomat dengan melakukan diplomasi dengan berbagai aktor dan melibatkan pemberdayaan suara-suara yang tertindas di negara-negara lain melalui teknologi.[20]

Cyber diplomacy dapat dilihat dari beberapa perspektif, yaitu diplomat, negara, dan aktor non negara. Sotiriu mengatakan, penggunaan *cyber diplomacy* seperti diplomat dapat meningkatkan audiensi dari pesan mereka, langsung terhubung dengan masyarakat tanpa adanya

[19] CNBC Indonesia, *Ada 5000 Kasus Perbulan, Indonesia Emergency Kejahatan Siber, 1*1 Oktober 2021, https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber

[20] Barrinha & Renard, *Cyber Diplomacy : the making of an international society in the digital age*,diakses pada 4 April 2023.

perantara oleh media yang dikendalikan oleh pemerintah dan negara yang berpotensi mengubah pesan awal.[21] Namun menurut Bjola dan Jiang, menggabungkan media sosial dengan bentuk interaksi diplomatik tradisional cenderung memberikan hasil yang lebih baik. Mereka mengatakan, media sosial dapat membantu menyampaikan pesan yang kuat dan efektif, namun tidak dapat bertindak sebagai pengganti dari perencanaan strategi yang baik, pengelola hubungan dan kriris yang merupakan ciri dan perilaku dari diplomatik profesional.[22]

Kemudian dari perspektif negara, *cyber diplomacy* menjadi sarana komunikasi untuk menciptakan perdamaian negara. Untuk saat ini salah satunya yaitu berupaya untuk membentuk citra negara di dunia internasional. Cara yang digunakan yaitu dengan menggunakan situs jejaring sosial seperti Twitter dan Facebook. Dengan demikian, akun media sosial akan digunakan sebagai alat untuk menyajikan dan membentuk citra negara (*nation-branding*) di seluruh dunia. Terakhir, yaitu *cyber diplomacy* juga dapat digunakan oleh aktor non-negara untuk mengkampanyekan perdamaian atau melawan musuh bersama seperti teroris. Salah satu contoh yaitu kampaye Facebook *Israel Loves Iran*, dimana kampanye ini berupaya untuk menyatukan rakyat Israel dengan Iran serta untuk mempromosikan perdamaian di antara kedua negara.[23] Metode ataupun upaya yang dilakukan ASEAN terhadap Indonesia dapat dikatakan berhasil karena semenjak adanya konsep diatas membuat adanya penurunan jumlah kasus yang berawal dari 6.388 kasus cybercrime menjadi 937 kasus cybercrime. Belum adanya Undang-Undang khusus untuk kejahatan siber masih menjadi kendala dalam kasus ini, karena konsep ataupun metode yang diusung oleh ASEAN dapat bekerja lebih efektif lagi apabila Indonesia memiliki Undang-Undang tersebut. Oleh karena itu, penulis berharap dengan adanya beberapa upaya yang dilakukan oleh ASEAN diatas, maka Indonesia dapat memberikan dukungan ataupun support yang seimbang agar upaya tersebut dapat berjalan lebih baik kedepannya.

Simpulan

Kejahatan siber atau cybercrime merupakan kejahatan berbasis dunia maya, termasuk kedalam kejahatan transnasional yang dilakukan dengan teknologi komputer dan jaringan internet. kejahatan ini dilakukan dengan mempengaruhi media internet sebagai alat bentuknya, dan seiring berkembangnya zaman, maka jenis kejahatannya akan bertambah banyak. Faktor penyebab terjadinya kejahatan siber atau cybercrime di Indonesia terdiri dari banyak hal, mulai dari

[21] Sotiriu, *Digital DIplonacy : between promises and reality*, dipublis 24 Maret 2015, diakses pada 4 April 2023.
[22] Bjola & Jiang, *Digitanl Diplomacy, Theory and Practice*, diakses pada 4 April 2023.
[23] Sotiriu, *Digital DIplonacy : between promises and reality*, dipublis 24 Maret 2015, diakses pada 4 April 2023.

kelalaian manusia atau human error, akses internet yang tidak terbatas, sistem keamanan yang lemah, tidak adanya kesadaran hukum, kurangnya edukasi, hingga adanya tujuan politik. Kemudian, dampak yang ditimbulkan dari kejahatan ini terbilang cukup merugikan, seperti adanya virus yang dapat memperlambat perangkat atau bahkan menghilangkan data, serta memblokir akses ke sebuah website tertentu.

Berkembangnya teknologi informasi dan komunikasi tidak selamanya baik, jika tidak di ikuti dengan keamanan siber. Adanya kesenjangan digital di kawasan Asia Tenggara membuat adanya hambatan tersendiri untuk memerangi kejahatan siber atau cybercrime tersebut. Penyebab adanya cybercrime di beberapa negara Asia Tenggara juga tidak jauh berbeda, namun penanganan akan kasus tersebut di setiap kawasan Asia Tenggara memiliki perbedaan. Mulai dari pemahaman dan pola pikir setiap negara, prioritas penanganan, serta tindakan hukum suatu negara dapat mempengaruhi kejahatan tersebut. Dengan adanya kasus kejahatan ini membuat Indonesia mengambil tindakan untuk bekerja sama dengan ASEAN agar kasus kejahatan ini dapat berkurang seiring berjalannya waktu. Adapun tindakan yang dilakukan oleh ASEAN sendiri yaitu telah tertulis dalam Dokumen ASEAN tentang Kejahatan Transnasional : Terorisme dan Ekstremisme Kekerasan; Narkoba; Kejahatan Dunia Maya; dan Perdagangan Manusia, kemudian adanya penerapan *cyber security*, *cyber resilience*, dan *cyber diplomacy.*

Artikel

Aghatise, J.(2006). *Cybercrime Definition*, Institute of Human Virology, Nigeria, (PDF) Cybercrime definition (researchgate.net)

Alcianno G. Gani, "Cybercrime (Kejahatan Berbasis Komputer)

Anto, Rusdi. *Kasus-kasus Cyber Crime sebagai Dampak Perkembangan Teknologi Komunikasi yang Meresahkan Masyarakat*, https://www.researchgate.net/publication/326225839_Kasus-Kasus_Cyber_Crime_sebagai_Dampak_Perkembangan_Teknologi_Komunikasi_yang_Meresahkan_Masyarakat

Ardiyanti, Handrini. (2014), *Cyber Security Dan Tantangan Pengembangannya di Indonesia*, (PDF) Cyber Security Dan Tantangan Pengembangannya Di Indonesia

ASEAN Secretaria, *Cooperation on Cybersecurity and against Cybercrime, Octopus Conference: Cooperation Against Cybercrime*, Council of Europe, Strasbourg, France, 2013, p.20.

Bjola & Jiang, *Digitanl Diplomacy, Theory and Practice, diakses pada 4/4/2023*, https://www.routledge.com/Digital- Diplomacy-Theory-and-

Practice/Bjola-Holmes/p/book/9781138843820

Budi Trisno, S.T.,M.Kom., *Phising Crime,* Dosen S1 Teknik Informatika Universitas Widya Kartika, Surabaya., 23_fishing-crime (um.ac.id)

Chang, Y.C. Lennon, *Cybercrime and Cyber Security in ASEAN*, diakses pada 16 November 2022, (PDF) Cybercrime and Cyber Security in ASEAN

D. Singer, 1961, *The Level-of-Analysis Problem in International Relations, Vol.14, No., Hal.77,* https://www.jstor.org/stable/2009557

Dian Ekawati Ismail, *Cybercrime di Indonesia,* Fakultas Ilmu Sosial Universitas Negeri Gorontalo

Franky P. Roring SIP., MSi, *Cybercrime Dalam Perspektif Hubungan Internasional*

Hafidz, *Kejahatan Siber Meningkat di Masa Pandemi,* dipublish pada 2 Agustus 2021, Universitas Indoneisa, Kejahatan Siber Meningkat di Masa Pandemi - Universitas Indonesia (ui.ac.id)

Hansen & Nissenbaum, Digital Disaster, *Cyber Security and the Copenhagen School,* International Studies Quarterly, 53, 2009:1155-1175, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567410

Irhamni Ali, *Kejahatan Terhadap Informasi (Cybercrime) Dalam Konteks Perpustakaan Digital, April 2012*, https://www.researchgate.net/publication/281202241_Kejahatan_Terhadap_Informasi_Cybercrime_Dalam_Konteks_Perpustakaan_Digital

Jackson, R., & Sorensen, G. (2014). *Pengantar Studi Hubungan Internasional.* Yogyakarta: Pustaka (https://opac.perpusnas.go.id/DetailOpac.aspx?id=23255)

Jirapon Sunkhpo, dkk., *Cybersecurity Policy in ASEAN Countries*, Information Institute Conferences, Las Vegas, NV, 2018,p.4.,

Peraturan & Regulasi Indonesia dan Beberapa Negara, https://repository.unikom.ac.id/68624/1/PeraturanDanRegulasi.pdf, diakses pada 07/03/2023.

Pratama, Demby., *Serangan Ddos Pada Software Defined Network*, diakses pada 20 November 2022, (PDF) SERANGAN DDOS PADA SOFTWARE-DEFINED NETWORK (researchgate.net)

Prayuda, Rendi. *Kejahatan Transnasional Terorganisir di Wilayah Perbatasan : Studi Modus Operandi Penyelundupan Narkotika Riau dan Malaysia*, https://www.researchgate.net/publication/343509094_Kejahatan_Transnasional_Terorganisir_di_Wilayah_Perbatasan_Studi_Modus_Operandi_Penyelundu

pan_Narkotika_Riau_dan_Malaysia

Regner Sabillon, Jordi Serra-Ruiz, Victor Cavaller, Jeimy J.Cano M, *Cybercrime and Cybercriminals: A Comprehensive Study*, June 2016, https://www.researchgate.net/publication/304822458_Cybercrime_and_Cybercriminals_A_Comprehensive_Study

Rizal Rahman, *Cybercrime Cases In a Decade: The Malaysian Experience*, September 2019, *ISBN : 9781692537708*, Universiti Kebangsaan Malaysia, https://www.researchgate.net/publication/335867251_CYBERCRIME_CASES_IN_A_DECADE_The_Malaysian_Experience

Roderic, G. Broadhurst & Lennon Y.C. Chang, *Cybercrime in Asia: Trends and Challanges*, February 2013, https://www.researchgate.net/publication/256028676_Cybercrime_in_Asia_Trends_and_Challenges

Saeri, M. *Teori Hubungan Internasional Sebuah Pendekatan Paradigmatik*, https://www.bing.com/search?q=file%3a%2f%2f%2fc%3a%2fusers%2frafiz%2fdownloads%2fdownacademia.com_teori-hubungan-internasional-sebuah-pendekatan-paradigmatik.pdf&form=annth1&refig=b88c04cea42040e0b85dc072b7f943fa

Sinaga, Obsatar. *Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia*, https://pustaka.unpad.ac.id/wp-content/uploads/2012/02/pustaka_unpad_penanggulangan_kejahatan_internasional_cyber_crime_di_indonesia.pdfb

Sotiriu, *Digital DIplonacy : between promises and reality*, dipublis 24 Maret 2015, https://www.semanticscholar.org/paper/Digital-diplomacy%3A-between-promises-and-reality-Sotiriu/bda272e7ed218f39c5c9b1ed6db75a85f4508171

Buku

A.T.Kearney. 2018. *Cybersecurity in ASEAN-An Urgent Call to Action.* (Korea: Penerbit A.T. Kearney Korea LLC).

ASEAN Secretaria. 2013. *Cooperation on Cybersecurity and against Cybercrime, Octopus Conference: Cooperation Against Cybercrime.* (Strasbourg, France: Council of Europe).

ASEANstats. 2018. *ASEAN Statistical Yearbook 2018.* (Jakarta: Penerbit ASEAN).

Ikbar, Yanuar, 2014. *Metodologi & Teori Hubungan Internasional*, (Bandung:Penerbit PT Refika Aditama).

Muhaimin Zulhair Achsin, Organisasi Internasional, PT Cita Intrans Selaras, ISBN: 978-623-6548-36-3, November 2020, diakses pada 17 Juni 2023.

Raharjo, Agus. 2002. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi,* Bandung: Citra Aditya Bakti.

Sunkhpo, Jirapon. Dkk.. 2018. *Cybersecurity Policy in ASEAN Countries.* (Las Vegas, NV: Information Institute Conferences).

Jurnal

Dahlia Br Ginting, *Modus Penyebab dan Strategi Penanggulangan Cybercrime, Jurnal Likmi, Media Informatika Vol. 10 No. 3 (2011),* Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI, https://jurnal.likmi.ac.id/Jurnal/11_2011/cybecrime_DAHLIA_.pdf

Dr. Darmawan Napitupulu, ST, M. Kom. *Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional, Deviance Jurnal Kriminologi, Vol 1, No. 1 (2017), ISSN 2580-3166*, Universitas Budi Luhur, https://journal.budiluhur.ac.id/index.php/deviance/article/view/595/508

Duryana binti Mohamed, *Combating the threats of cybercrime in Malaysia: The efforts, the cyberlaws and the traditional laws, Jurnal Computer Law & Security Review, Volume 29, Issue 1, February 2013, pages 66-76,* https://www.sciencedirect.com/science/article/abs/pii/S0267364912002014

Dwi Rezki Sri Astarini, Muhammad Syaroni Rofii, *Siber Intelijen Untuk Keamanan Nasional, Jurnal Renaissance, Volume 6 No.1, Mei 2021, ISSN (e): 2527-564X/ ISSN (p) 2621-0746*, "Cyber Intelligence in National Security" by Dwi Rezki Sri Astarini and Muhammad Syaroni Rofii (ui.ac.id)

Eko Budi, Dwi WIra, Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0, Prodi Ilmu Kepolisian Semarang, Volume 3, Tahun 2021, hlm. 223-234, diakses pada 18 Juni 2023

Eliasta Ketaren, *Cybercrime, Cyberspace, dan Cyber Law, Jurnal Times, Vol V, No. 2: 35-42, 2016, ISSN: 2337-3601*, STMIK TIME, https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/556/126

Febrian Kwarto, Madya Angsito, *Pengaruh Cybercrime*

Terhadap Cyber Security Compliance di Sektor Keuangan, Jurnal Akuntansi Bisnis, Vol.11 (No.2) : Hal. 99-110 Th. 2018, ISSN : 1979-360X, E-ISSN : 2598-6767, Universitas Mercu Buana, https://journal.ubm.ac.id/index.php/akuntansi-bisnis/article/view/1382/1198

Galuh Kartiko, *Pengaturan Terhadap Yurisdiksi Cybercrime Ditinjau dari Hukum Internasional, Jurnal Trunojoyo, e-ISSN: 2502-762X, p-ISSN: 1907-5790, Vol 8, No. 2 (2013),* Politeknik Negeri Malang, https://eco-entrepreneur.trunojoyo.ac.id/rechtidee/article/view/695

Iskandar H & Zainab A, *Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital, Padjajaran Journal of International Relations (PADJIR), e-ISSN: 2684-8082 Vol. 1 No. 4*, Februari 2020 (342-363) doi: 10.24198/padjir.v1i4.26246,

Kriatiani Virgi Kusuma Putri, *Kerjasama Indonesia Dengan ASEAN Mengenai Cyber Security Dan Cyber Resilience Dalam Mengatasi Cyber Crime*, Fakultas Hukum Universitas Brawijaya, *Jurnal Hukum Lex Generalis, Vol.2, No.7, Juli 2021*

Muhammad Prima Ersya, *Permasalahan Hukum dalam Menanggulangi Cybercrime di Indonesia, Journal of Moral And Civic Education, 1(1) 2017, ISSN: 2549-8851*, Prodi Pendidikan Kewarganegaraan Universitas Negeri Padang, https://www.researchgate.net/profile/Jmce-Unp-2/publication/328886042_Permasalahan_Hukum_dalam_Menanggulangi_Cyber_Crime_di_Indonesia/links/5be971284585150b2bb09cc7/Permasalahan-Hukum-dalam-Menanggulangi-Cyber-Crime-di-Indonesia.pdf

Muhammad R. dan Yanyan M., *Cybersecurity Policy and Its Implementation in Indonesia, Journal of ASEAN Studied, Vol.4, No.1 (2016), p.67.*

Mustika Indah Jelta Sinaga, *Penetapan Tersangka Dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum di Indonesia, Syntax Literate: Jurnal Ilmiah Indonesia, ISSN: 2541-0849, e-ISSN: 2548-1398, Vol.7, No. 3*, Maret 2022, Universitas Kristen Indonesia, https://www.jurnal.syntaxliterate.co.id/index.php/syntax-literate/article/view/6430/3725

Olivia, Yessi. 2013, *Level Analisis Sistem dan Teori Hubungan Internasional. Jurnal Transnasionnal, Vol 5, No. 1, Hal. 898*, https://transnasional.ejournal.unri.ac.id/index.php/JTS/article/view/1796/1767

Ramadhan, Iqbal. (2020). *STRATEGI KEAMANAN CYBER SECURITY DI KAWASAN ASIA TENGGARA: SELF-HELP ATAU MULTILATERALISM?. Jurnal Asia Pacific Studies, 3(2), 181-192.*

Vinsensio Dugis, *Teori Hubungan Internasional; Perspektif-Perspektif Klasik,* Cakra Studi Global Strategis (CSGS), 2016, [PDF] Teori Hubungan Inernasional; Perspektif-Perspektif Klasik (researchgate.net)

Website

Andrean Kristianto, *Cerita Lengkap Bocornya 91 Juta Data Akun Tokopedia*, diakses dari CNBC Indonesia pada 20 November 2022, Cerita Lengkap Bocornya 91 Juta Data Akun Tokopedia (cnbcindonesia.com)

Association Of Southeast Asian Nations, ASEAN Main Portal, Our Communities, Our Communities - ASEAN Main Portal, Our Communities - ASEAN Main Portal

Bab II, Tinjauan Pustaka, Teori Neo-Liberal Institusional, https://repository.uksw.edu/bitstream/123456789/24188/20/T1_372017077_Bab%20II.pdf

Barrinha & Renard, *Cyber Diplomacy : the making of an international society in the digital age,* https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924, diakses pada 4/4/2023.

Bernardino, Raul. *Cybercrime*, https://www.researchgate.net/publication/321124293_CYBERCRIME

CNBC Indonesia, 11 Oktober 2021, *Ada 5000 Kasus Perbulan, Indonesia Emergency Kejahatan Siber,* https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber

FBI, Business Email Compromise, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise

Freelancer, *Cyber Security in Thailand: Everything You Need to Know*, https://www.chiangraitimes.com/learning/cyber-security-in-thailand-everything-you-need-to-know/

IBM, *What is Ransomware?*, https://www.ibm.com/topics/ransomware

INTERPOL, *INTERPOL Report Charts Top Cyberthreats in Southeast Asia,* 22 January 2021, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-

report-charts-top-cyberthreats-in-Southeast-Asia

INTERPOL, *INTERPOL Report Highlights Key Cyberthreats in Southeast Asia*, 17 February 2020, pol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-key-cyberthreats-in-Southeast-Asia

Kaspersky, *What is Cryptojacking?-Definition and Explanation*, https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking

Kementerian Luar Negeri Republik Indonesia, *Isu Khusus Kejahatan Lintas negara*, Kejahatan Lintas Negara | Portal Kementerian Luar Negeri Republik Indonesia (kemlu.go.id), https://kemlu.go.id/portal/id/read/89/halaman_list_lainnya/kejahatan-lintas-negara

Kinza Yasar, *Command and Control Server*, https://www.techtarget.com/whatis/definition/command-and-control-server-CC-server, diakses pada 27/02/2023

OECD, *Cybersecurity Policy Making at a Turning Point: Analysing New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD Digital Economy Papers, No.211 (2012). EOCD Publishing, Paris, 2012, p. 4.

Patipon Wongsrikul, *Cybercrime in Thailand*, https://www.interriskthai.co.th/wp-content/uploads/2022/06/22-02-InterRisk-Thai-Report-Cybercrime-in-Thailand-EN-1.pdf