Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 759-767

Peran Organisasi Internasional Dalam Memperkuat Pertahanan Siber Global Pada Negara Berkembang

Muhammad Darrell Damareka[1], Levi Christopher Ilyas[1], Rasya Arafah[1], Rifky Justicyo[1], Irwan Triadi[2]
[1]Mahasiswa Fakultas Hukum Universitas Pembangunan Nasional "Veteran"
[2]Fakultas Hukum Universitas Pembangunan Nasional "Veteran" Jakarta
Jakarta e-mail: 2310611349@mahasiswa.upnvj.ac.id, irwantriadi1@yahoo.com

Abstrak: Perkembangan teknologi informasi dan komunikasi telah membawa dampak besar terhadap transformasi global, termasuk dalam aspek keamanan siber. Negara berkembang seperti Indonesia menghadapi tantangan serius dalam membangun kapasitas pertahanan siber yang andal, akibat keterbatasan sumber daya, infrastruktur, serta regulasi yang belum harmonis. Dalam konteks ini, peran organisasi internasional menjadi sangat penting untuk membantu negara-negara berkembang dalam meningkatkan kesiapan dan ketahanan terhadap ancaman siber. Artikel ini membahas kontribusi organisasi internasional, khususnya International Telecommunication Union (ITU), dalam membangun kapasitas siber negara berkembang melalui kerja sama teknis, pelatihan sumber daya manusia, dan advokasi kebijakan keamanan siber. Melalui metode yuridis normatif dan studi pustaka, artikel ini menelusuri bagaimana ITU menjalankan perannya melalui berbagai inisiatif, seperti pengembangan broadband, pelatihan mitigasi kejahatan siber, serta kolaborasi dengan organisasi lain seperti IMPACT dan INTERPOL. Di sisi lain, Indonesia juga telah membentuk Badan Siber dan Sandi Negara (BSSN) sebagai langkah strategis untuk mengoordinasikan keamanan siber nasional. BSSN menerapkan strategi berdasarkan lima pilar Global Cybersecurity Index (GCI), yakni aspek hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama. Penelitian ini menyimpulkan bahwa kolaborasi internasional menjadi kunci dalam menciptakan ekosistem keamanan siber yang tangguh dan adaptif. Oleh karena itu, diperlukan sinergi berkelanjutan antara pemerintah, organisasi internasional, sektor swasta, akademisi, dan masyarakat guna meningkatkan daya saing digital negara berkembang di tengah tantangan dunia maya yang semakin kompleks.

Article History
Received: May 25, 2025
Revised: June 14, 2025
Published: June 17, 2025

Kata Kunci:
keamanan siber, organisasi internasional, ITU, BSSN, kerja sama global, negara berkembang

https://doi.org/10.5281/zenodo.15684567

PENDAHUUAN

Abad 21 merupakan abad yang dimana seluruh kegiatan dapat dilakukan melalui teknologi. Abad ini sudah memasuki era globalisasi. Globalisasi dalam bidang teknologi informasi telah menjadikan masyarakat Indonesia sebagai bagian dari komunitas global pengguna teknologi informasi dan komunikasi melalui jaringan internet. Internet merupakan jaringan luas komputer yang sering disebut sebagai jaringan dunia (worldwide network). Internet sendiri adalah sistem komputer yang saling terhubung melalui berbagai media komunikasi, seperti kabel telepon, serat optik, satelit, atau gelombang radio. Jaringan komputer ini dapat memiliki skala kecil, seperti Jaringan Area Lokal (LAN) yang umumnya digunakan secara internal di kantor, bank, atau perusahaan yang dikenal dengan istilah intranet, maupun berskala sangat besar seperti internet. [1]

[1] Agus Raharjo, Cybercrime, Bandung: Citra Aditya Bakti, 2002, hal. 59.

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 759-767

Masuknya dunia dalam era globalisasi memberikan dampak positif apabila dapat ditanggapi dan diatasi dengan baik. Namun, apabila disikapi tidak tepat maka dampak positif tersebut akan berbalik menjadi dampak negatif. Era globalisasi, selalu bersinggungan dengan dunia siber. Siber merupakan sebuah hal yang berhubungan dengan mekanisme sistem komputer dan informasi dunia internet. Dalam dunia siber, terdapat sebuah perkumpulan yang saling berkomunikasi apabila terhubung dengan internet. Dengan begitu, siber tersebut adalah wadah dimana seluruh orang di dunia yang saling berhubungan melalui jaringan internet. Berdasarkan pengertiannya, siber dapat dimanfaatkan menjadi hal yang positif yang dapat dirasakan oleh khalayak manusia. Akan tetapi, perlu kita sadari bahwa siber juga merupakan salah satu hal yang rentan untuk terjadi sebuah kejahatan.

Kejahatan tersebut dapat beruba penipuan, pengintimidasian kepada seseorang, maupun kejahatan tingkat tinggi yakni peretasan data pribadi seseorang. Kejahatan-kejahatan tersebut, umumnya disebut sebagai *cybercrime.* Pengertian terkait dengan *cybercrime* yang dikemukakan oleh para ahli pada awalnya hanya sebatas pada peranti lunak. Akan tetapi, seiring berkembangnya zaman, pengertian mengenai *cybercrime* mengalami perubahan yakni mengarah pada perlakuan-perlakuan yang menyebabkan kerugian dalam hal ini adalah kejahatan dalam dunia maya. Menurut Barda Nawawi, salah satu dampak negatif adalah terbukanya peluang bagi munculnya perilaku antisosial yang sebelumnya dianggap mustahil atau bahkan tidak pernah terpikirkan akan terjadi. Dalam hal ini, sebuah teori menyebutkan bahwa *crime is product of society itself*, yang secara sederhana dapat diartikan bahwa masyarakat itu sendiri menjadi penyebab munculnya tindak kejahatan.[2]

Menurut Indra Safitri, kejahatan dunia maya adalah bentuk kejahatan yang berkaitan dengan pemanfaatan teknologi informasi tanpa batasan. Kejahatan ini memiliki karakteristik khas yang melibatkan rekayasa teknologi canggih, mengandalkan tingkat keamanan yang tinggi, serta kredibilitas informasi yang diakses atau disampaikan oleh pengguna internet.[3] Sementara itu, kepolisian Inggris mendefinisikan kejahatan siber sebagai segala bentuk pemanfaatan jaringan komputer untuk melakukan tindakan kriminal, atau kejahatan berbasis teknologi tinggi, dengan cara menyalahgunakan kemudahan yang ditawarkan oleh teknologi digital.[4]

Pada dasarnya, cybercrime adalah kejahatan yang memanfaatkan komputer dan sistem telekomunikasi, seperti telepon atau sistem nirkabel dengan antena khusus, sebagai sarana untuk melakukan tindakan ilegal. Fenomena ini sering disebut dengan istilah telematika, yang merujuk pada gabungan antara teknologi telekomunikasi, media, dan informatika yang sebelumnya berkembang secara terpisah. Kejahatan ini muncul sebagai akibat negatif dari perkembangan aplikasi internet dan sering kali dikenal dengan sebutan cybercrime. Dengan demikian, cybercrime mencakup berbagai jenis kejahatan beserta cara-cara pelaksanaannya yang berhubungan dengan penggunaan internet.

Berdasarkan pengertian mengenai *cybercrime,* menandakan bahwa pentingnya sebuah perlindungan terkait dengan siber. Keamanan siber (*cyber security*) merujuk pada berbagai aktivitas, proses, kemampuan, atau kondisi di mana sistem informasi dan komunikasi, termasuk data yang tersimpan di dalamnya, dilindungi dari kerusakan, penyalahgunaan, perubahan, atau eksploitasi oleh pihak yang tidak

berwenang. Pengguna yang mengakses informasi tanpa memanfaatkan alat keamanan siber dianggap melanggar prinsip keamanan informasi.[5] Dalam penerapan sistem keamanan siber, perlindungan biasanya difokuskan pada titik-titik dengan potensi kerentanan tertinggi terhadap

[2] Barda Nawawi Arief, 2007, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Kencana, Jakarta.
[3] Indra Sjafri, 1999, Tindak Pidana di Dunia Siber, dalam insider, Legal Journal From Indonesia Capital & Investment Market.
[4] Abdul Wahid dan Mohammad Labib 2005, Kejahatan Mayantara (Cyber Crime), Jakarta: PT. Refika Aditama, hlm 40

[5] Nurse, Jason & Creese, Sadie & Goldsmith, Michael & Lamberts, Koen. (2011). Trustworthy and Effective Communication of Cybersecurity Risks: A Review. Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011. 10.1109/STAST.2011.6059257.

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 759-767

kejahatan atau serangan siber.[6]

Keamanan terkait dengan perlindungan siber menjadi penting, namun penerapan keamanan siber pada negara berkembang masihlah jauh dari kata sempurna dalam pelaksanaan maupun penerapannya. Berbagai masalah harus dihadapi oleh negara berkembang. Indonesia sebagai negara berkembang, masih kesulitan dalam menerapkan keamanan siber. Salah satu hal yang dapat dibuktikan bahwasannya Indonesia masih memiliki kecacatan dalam menanggulangi keamanan siber adalah dengan adanya serangan siber yang terus menyasar institusi pemerintah di Indonesia. Dalam beberapa tahun terakhir, kasus peretasan berulang kali terjadi pada berbagai lembaga dan perusahaan di tanah air. Pada tahun 2021, situs resmi Badan Siber dan Sandi Negara (BSSN) dengan alamat menjadi korban serangan deface, di mana tampilan halaman utamanya diubah oleh pihak tak bertanggung jawab.[7][8]

Dengan maraknya serangan pada instansi pemerintahan terkait dengan siber, dapat dikatakan Indonesia masih terlalu awam dengan pemahaman mengenai dunia siber. Hal tersebut dapat dilihat dengan faktor-faktor bahwa masih banyaknya Sumber Daya Manusia (SDM) di Indonesia belum memahami pentingnya perlindungan siber. Selain itu, lambatnya perkembangan teknologi pada Indonesia masih menjadi salah satu faktor yang menghambat keamanan siber di Indonesia. Serta belum terharmonisasinya peraturan di Indonesia menyebabkan ketidakpastian hukum yang seharusnya menjadi sebuah penentu keadilan dalam keamanan siber tersebut.

Dengan demikian, perlu adanya kerja sama antarnegara dan organisasi internasional untuk membantu negara-negara berkembang dalam melaksanakan perlindungan terhadap serangan siber. Bantuan ini dapat berupa pelatihan sumber daya manusia, transfer teknologi, hingga penyediaan infrastruktur keamanan siber yang memadai. Selain itu, perlu dibangun sistem deteksi dini untuk mengidentifikasi dan merespons potensi ancaman siber secara lebih cepat dan efektif. Kolaborasi dalam berbagi informasi tentang ancaman siber juga menjadi langkah penting untuk meningkatkan kesiapan dan mitigasi risiko. Kerja sama ini tidak hanya melibatkan pemerintah, tetapi juga sektor swasta, akademisi, dan masyarakat untuk menciptakan ekosistem keamanan siber yang kokoh.

METODE

Dalam penelitian mengenai "Peran Organisasi Internasional Dalam Memperkuat Pertahanan Siber Global," penulis menerapkan metode pendekatan yuridis normatif. Pendekatan ini dilakukan berdasarkan pada peraturan perundang-undangan beserta dengan peraturan lainnya yang mengatur permasalahan tersebut. Pendekatan pengumpulan data dalam artikel ilmiah ini dilakukan melalui studi literatur, yaitu metode yang melibatkan pengumpulan informasi dari berbagai sumber terpercaya, seperti jurnal dan artikel relevan yang telah dipublikasikan sebelumnya. Prosesnya mencakup tahapan mencari, membaca, mencatat, serta menganalisis materi penelitian secara kritis untuk mendapatkan pemahaman yang komprehensif tentang topik yang dibahas.

HASIL DAN PEMBAHASAN

Peran Organisasi Internasional dalam Membangun Kapasitas Siber Negara Berkembang

Hubungan antar negara yang dilandasi oleh kerja sama internasional perlu mengikuti suatu aturan hukum yang mengatur hak dan kewajiban masing-masing pihak, yang diatur dalam apa yang disebut hukum internasional.[8] Hukum internasional memiliki peranan yang krusial guna memecahkan

[6] Mitnick, K. & Simon, W. (2002). The Art of Deception: Controlling the Human Element of Security, diunduh pada 10 Desember 2024 dari,https://portal.abuad.edu.ng/lecturer/documents/1585589655The_Art_of_D eception_by_Kelvin_Mitnick.pdf

[7] Topan Yuniarto, *Tantangan Keamanan Siber Indonesia: Ancaman dan Dampaknya,* kompas.com, diakses,dari,https://kompaspedia.kompas.id/baca/paparan-topik/tantangan-keamanan-siber-indonesia-ancaman-d an-dampaknya, pada 10 Desember 2024.

[8] Chainur Arrasijid. S, Dasar-Dasar Ilmu Hukum, Cetakan Ke -5, Sinar Grafika, Jakarta, 2008, Hal 1

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 759-767

permasalahan global maupun mengatur tingkah laku masyarakat global. Terciptanya sebuah hubungan antar negara dapat melahirkan sebuah organisasi yang menyatukan negara-negara dengan dasar tujuan yang sama. Organisasi internasional merupakan sebuah perkumpulan antar negara-negara yang memiliki tujuan atau cita-cita yang serupa. Lahirnya organisasi internasional, bermula dengan adanya sebuah hubungan antar negara-negara yang didasari dengan perjanjian-perjanjian internasional.

Organisasi internasional adalah salah satu entitas non-negara yang memiliki peran penting dalam hubungan internasional. Munculnya organisasi internasional modern mulai dikenal pada abad ke-19 di negara-negara Barat sebagai sebuah lembaga formal, dan terus berkembang pada abad ke-20 yang kemudian dikenal sebagai era kerja sama internasional.[9] Sebelum terbentuknya organisasi internasional, sudah ada berbagai aliansi militer, organisasi antar pemerintah di negara-negara berdaulat, serta aktor non-negara internasional seperti gereja Katolik dan Kekaisaran Romawi. Namun, organisasi-organisasi tersebut bukanlah organisasi antar pemerintah, melainkan dibentuk oleh negara dan dikelola secara mandiri oleh anggotanya.

Clive Archer mendefinisikan organisasi internasional merupakan sebuah tatanan formal yang berkelanjutan dan dilahirkan berdasarkan adanya kata sepakat dari anggota-anggota terkait, dalam hal ini adalah pemerintah maupun non-pemerintah dari negara-negara yang berdaulat.[10] [10]Terciptanya organisasi internasional yang merupakan subjek dari hukum organisasi internasional memberikan kemudahan bagi terciptanya sebuah pembentukan hukum internasional itu sendiri. Hal itu dikarenakan terciptanya sebuah wadah bagi negara-negara yang memiliki pendirian dan kaidah yang kuat pada negaranya masing-masing untuk sepakat menaati hubungan dengan negara lainnya.[11] Secara umum, organisasi internasional dapat diklasifikasikan menjadi tiga jenis:[12]

1. *Regional Organizations*. Organisasi internasional yang memiliki keanggotaan berdasarkan batasan geografis atau geopolitik berfungsi untuk mempererat kemitraan politik dan ekonomi antarnegara anggotanya. Contoh terkenal dari organisasi semacam ini adalah Uni Eropa dan Uni Afrika.
2. *Multinational Organizations*. Berbeda dengan organisasi regional *regional organizations*, organisasi multinasional memiliki keanggotaan yang lebih luas, melampaui batas geografis atau ekonomi, serta mencakup berbagai kepentingan yang lebih menyeluruh. Contoh penting dari organisasi semacam ini adalah *Commonwealth of Nations* dan *Group of Seven* (G7).
3. *Global Organizations.* Organisasi-organisasi ini benar-benar bersifat internasional dan tidak dibatasi oleh faktor sosial atau geopolitik. PBB, WHO, dan Interpol adalah contoh organisasi global utama.

Dalam hal keamanan siber, terdapat sebuah organisasi internasiona yang termasuk kedalam klasifikasi *Global Organizations* yang bernama *International Telecommunication Union* (ITU). ITU adalah organisasi internasional tertua yang fokus pada pengembangan teknologi informasi dan telekomunikasi di seluruh dunia.[1313] Organisasi ini didirikan pada 17 Mei 1865 di Paris, dengan melibatkan 20 negara yang saat itu sedang mengadakan konvensi untuk mencari solusi atas berbagai kendala dalam layanan telekomunikasi. Tujuan awal pendiriannya adalah untuk menyusun standar peralatan telegraf, menetapkan pedoman operasional yang tepat, serta menentukan tarif dan aturan internasional yang berlaku untuk komunikasi global.[14]

ITU berperan dalam memastikan kenyamanan dan keamanan negara saat menggunakan alat telekomunikasi semakinditegaskan pada pertemuan negara-negara anggota dalam WSIS *(World Summit on the Information Society)* tahun 2013, yang berlandaskan pada hasil Plenipotentiary Conference tahun 2006. Dalam pertemuan tersebut, dijelaskan bahwa ITU berfungsi

[9] Theodore A. Couloumbis and James H. Wolfe . 1981 . Introduction International Relations : Power And Justice. New Delhi : Prentice-Hall of India.
[10] Cliver Archer. International Organizations. 2001.London & New York: Routledge
[11] J.G. Starke, Pengantar Hukum Internasional, Sinar Grafika, Jakarta, 1989, hal.1.
[12] Neethu. N, *Role of International Organisations in Prevention of Cyber Crimes: An Analysis,* Nalsar University, Research Gate, diakses dari https://www.researchgate.net/publication/350525198_Role_of_Internati
[13] ITU, 2015. *International Tellecommunication Union: Regional Presence,* diakses dari https://www.itu.int/en/about/Pages/default.aspx, pada 10 Desember 2024
[14] *Ibid.*

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 759-767

sebagai fasilitator utama untuk membangun inisiatif C5, yang mencakup lima aspek: Keamanan Siber, Kolaborasi, Kerjasama, Perlindungan Anak, dan Ancaman Siber. Sebagai organisasi internasional ITU melakukan segala upaya guna mengatasi kejahatan ancaman siber. Upaya serta peran yang dilakukan oleh ITU diantaranya berupa malakukan advokasi kepada pemerintah dan pihak-pihak terkait di tingkat nasional mengenai kebijakan, peraturan, serta perbaikan hukum untuk memperkuat rencana aksi nasional dalam menangani kejahatan dunia maya (*cyber crime*); mengatur peningkatan kapasitas anggota dan kelompok strategis yang terlibat dalam penanggulangan cyber crime melalui dukungan teknis dan pelatihan; mengumpulkan data mengenai kondisi kejahatan dunia maya global melalui berbagai survei, jajak pendapat, dan penelitian; serta menyebarkan informasi tentang keamanan siber

melalui sosialisasi, seminar, diskusi, dan konferensi.[15]

Untuk meningkatkan kemampuan Indonesia dan negara berkembang lainnya dalam mengembangkan broadband nirkabel, ITU pada tahun 2011 menjalin kerjasama dengan pemerintah Korea untuk melaksanakan program yang disebut *"Master Plan for Wireless Broadband in the Asia Pacific Region."* Program ini berjalan sepanjang tahun 2011 dan berhasil diterapkan pada 2012, yang menghasilkan peningkatan kapasitas broadband di Indonesia dan wilayah Asia Pasifik, serta pengembangan sumber daya yang dilatih untuk mendukung program tersebut. Peningkatan teknologi di Indonesia diikuti dengan pelatihan intensif yang diselenggarakan oleh ITU pada 16-18 September 2012, di mana negara-negara Asia Pasifik mengadakan pelatihan terkait penanggulangan kejahatan siber di Jakarta.[16]

Untuk lebih memperdalam pengetahuan Indonesia dalam menangani cyber crime, ITU bekerja sama dengan IMPACT dan INTERPOL (International Criminal Police Organization) dalam menyelenggarakan workshop di Malaysia pada 19-21 Februari 2014. Workshop ini fokus pada negara-negara di Asia Tenggara, termasuk Indonesia, dengan tujuan untuk bekerja sama dalam mengatasi masalah investigasi internet tingkat tinggi dan teknik-teknik untuk merespons cyber crime. Selain itu, workshop ini juga bertujuan untuk memperkuat hubungan antara penegak hukum dan komunitas CERT (Computer Emergency Response Team) di negara-negara Asia Tenggara

Upaya Indonesia Sebagai Negara Berkembang Dalam Menghadapi Ancaman Keamanan Siber

Belakangan ini, kejahatan siber semakin banyak terjadi dan dapat menyerang siapapun. Meningkatnya kejahatan dunia maya (cyber crime) merupakan dampak dari perkembangan teknologi informasi (TI), yang di satu sisi diakui membawa banyak kemudahan bagi manusia. Namun, di sisi lain, kemudahan ini sering dimanfaatkan sebagai sarana untuk melakukan tindakan kriminal di dunia digital, seperti yang semakin sering kita jumpai akhir-akhir ini. Ancaman serangan siber semakin bertambah, baik terhadap individu maupun organisasi atau instansi pemerintah yang semakin bergantung pada teknologi dan jaringan internet. Jika ditinjau dari tujuannya, serangan atau ancaman siber dapat dikelompokkan ke dalam beberapa kategori berikut:[17]

A. Hacktivism.

Istilah *hacktivism* berasal dari penggabungan dua kata, yaitu *hacking* dan *activism*. Kata *hack* pertama kali mendapatkan popularitas pada tahun 1960-an di Massachusetts Institute of Technology (MIT), yang mengacu pada tindakan kreatif berupa lelucon cerdas dengan gaya tertentu, namun tanpa menimbulkan bahaya bagi siapa pun.[1818] Meski begitu, istilah *hack*, *hacking*, atau bahkan *hacker*

[15] ITU, 2014. Manual for Measuring ICT Access and Use by Households and Individuals, Geneva, Switzerland, hal 16.
[16] ITU iLibrary, *Guidelines for the Preparation of National Wireless Broadband Masterplans for the Asia Pacific Region,* diakses dari https://itu-ilibrary.org/science-and-technology/guidelines-for-the-preparation-of-national-wireless-broadband-ma sterplans-for-the-asia-pacific-region_pub/808e784e-en, pada 11 Desember 2024.

[17] Sugeng Santoso, 2018, *Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional,* Jurnal Kajian Lemhannas RI, hal. 45.
[18] Coleman, E. G. (2012). *Phreaks, hackers, and trolls: The politics of transgression and spectacle*. M. Mandiberg (Ed.), *The social media reader*. New York University Press. hal. 99–119

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 759-767

(sebutan untuk individu yang memiliki kemampuan meretas) seringkali dipahami dalam konteks yang kurang positif. Kata-kata ini kerap dikaitkan dengan hal-hal ilegal atau tindakan yang bertentangan dengan norma hukum, terutama karena dalam pemberitaan media, aktivitas peretasan sering diasosiasikan dengan praktik peretasan komputer yang melanggar hukum.[19]

B. Krimninal.

Jenis serangan siber ini bertujuan untuk melakukan tindakan kriminal, termasuk kejahatan ekonomi. Dalam kasus kejahatan ekonomi bermotif umum, contohnya adalah mendapatkan akses ke situs keuangan guna memperoleh data yang dapat digunakan untuk tindakan kriminal finansial atau menjual data tersebut kepada pihak ketiga. Salah satu contohnya adalah insiden pembobolan data Yahoo pada tahun 2013. Selain itu, serangan siber juga bisa bertujuan untuk memeras dengan cara mengambil data, seperti pada kasus WannaCry di tahun 2017, di mana pemerasan dilakukan dengan mengenkripsi data sehingga tidak dapat diakses. Di Indonesia, salah satu contoh kejahatan siber yang menonjol terjadi pada November 2016, ketika seorang remaja meretas akun di situs tiket.com. Aksi illegal access ini menyebabkan kerugian pada pihak tiket.com sebesar Rp4.124.000.982.[20]

C. Perang Siber.

Serangan siber, atau dalam bahasa Inggris disebut *cyber attack*, secara literal merujuk pada bentuk serangan yang memanfaatkan perangkat elektronik dan digital. Sebelum memahami definisi serangan siber secara mendalam, penting untuk terlebih dahulu memahami konsep ruang siber *cyber space* itu sendiri.[2121] Istilah *cyber attack* kini telah sangat populer. Serangan siber memiliki kemampuan untuk melumpuhkan sentrifugal nuklir, sistem pertahanan udara, hingga jaringan listrik, menjadikannya ancaman signifikan terhadap keamanan nasional.[22] [22]Serangan siber seringkali dipicu oleh motif politik dan melibatkan elemen perintah dari pemerintah suatu negara, yang disertai dengan dukungan serta penyediaan fasilitas guna memastikan kelancaran pelaksanaannya.

D. Spionase.

Cyber espionage dapat dijelaskan secara terpisah dengan memahami arti kata *cyber* dan *espionage*. Kata *cyber* diartikan sebagai dunia maya. Menurut Prof. Barda Nawawi Arief, istilah *cyber* atau siber dapat dijelaskan dengan kata mayantara. Dalam bahasa Inggris, cyber juga merujuk pada sesuatu yang bersifat maya, tidak nyata, tidak terlihat, transparan, atau tanpa bentuk. Untuk memberikan pemahaman yang lebih mendalam tentang *cyber espionage*, perlu juga dipahami pengertian spionase serta elemen-elemen yang menjadi parameter dalam tindakan spionase.[23]

Banyaknya kejahatan siber yang terjadi, maka dibutuhkan strategi untuk mengamankan siber di Indonesia. Keamanan siber telah menjadi salah satu isu prioritas global sejak teknologi informasi dan komunikasi mulai dimanfaatkan dalam berbagai bidang kehidupan, seperti sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan, dan lainnya. Seiring dengan meningkatnya penggunaan teknologi informasi dan komunikasi, risiko dan ancaman penyalahgunaannya juga semakin besar dan kompleks.

Sebagai tanggapan terhadap fenomena ini, pemerintah melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) yang diperbarui dengan Peraturan Presiden Nomor 133 Tahun 2017, membentuk BSSN. Lembaga ini bertugas untuk melaksanakan keamanan siber secara efektif dan efisien melalui pemanfaatan, pengembangan, dan konsolidasi berbagai elemen yang terkait dengan keamanan siber nasional.[2424] BSSN juga menyusun Strategi

[19] Gunkel, D. J. (2005). Editorial: Introduction to hacking and hacktivism. *New Media & Society*.
[20] Sugeng Santoso, *Loc. Cit,* hal.46.
[21] Kuehl, Dann, *From cyberspace to cyberpower:Defining The Problem Information Operations at the National Defense University,* National Defence University,USA, 2013, hal 4.
[22] Oona A. Hathaway, 2012, *The Law Of Cyber Attack,* California Law Review, hal. 826.

[23]Teguh Arifiyadi, *Dunia Siber yang Tidak Maya*, diakses dari https://www.hukumonline.com/berita/a/dunia-siber-yang-tidak-maya-lt59c88b4e7bae6/, pada 11 Desember 2024.
[24] Badan Siber dan Sandi Negara. Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024.

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 759-767

Keamanan Siber Indonesia sebagai pedoman bagi seluruh pemangku kepentingan untuk mengembangkan kebijakan keamanan siber di masing-masing instansi.

Implementasi strategi keamanan siber oleh BSSN mengacu pada lima pilar *Global Cybersecurity Index* (GCI) 2017, yakni aspek hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama. Tujuan dari penilaian berdasarkan GCI 2017 adalah untuk membangun kapasitas keamanan siber di tingkat nasional, regional, maupun internasional.[25]

SIMPULAN

Kesimpulannya, peran organisasi internasional sangat penting dalam membantu negara-negara berkembang, termasuk Indonesia, membangun kapasitas keamanan siber. Organisasi internasional seperti ITU berperan sebagai fasilitator utama dalam mendukung pengembangan teknologi informasi, memberikan pelatihan, meningkatkan kapasitas sumber daya manusia, serta mempromosikan kolaborasi internasional dalam menangani ancaman siber. Selain itu, dengan semakin meningkatnya ancaman keamanan siber, Indonesia telah mengambil langkah strategis melalui pembentukan BSSN yang bertugas untuk mengkoordinasikan keamanan siber secara nasional. Strategi keamanan siber yang dirancang oleh BSSN mengacu pada nilai-nilai dasar kehidupan berbangsa serta lima pilar *Global Cybersecurity Index* (GCI) untuk meningkatkan kapasitas di tingkat nasional, regional, dan internasional. Langkah ini menunjukkan komitmen Indonesia dalam menghadapi ancaman siber yang semakin kompleks dan mendorong kerja sama internasional sebagai bagian integral dari upaya menciptakan lingkungan siber yang aman, andal, dan mendukung pertumbuhan ekonomi digital.

Sebagai saran, untuk menghadapi ancaman keamanan siber yang semakin kompleks, Indonesia perlu memperkuat kolaborasi dengan organisasi internasional seperti ITU, IMPACT, dan INTERPOL guna meningkatkan kapasitas teknis, hukum, dan sumber daya manusia dalam menangani kejahatan siber. Pemerintah juga perlu mempercepat pengembangan infrastruktur teknologi informasi yang aman serta memperkuat regulasi yang mampu menjawab tantangan baru di dunia digital. Selain itu, diperlukan kesadaran dan partisipasi aktif dari seluruh lapisan masyarakat, termasuk sektor swasta, akademisi, dan komunitas, dalam menjaga keamanan siber melalui pelatihan dan edukasi. Pendekatan ini dapat menciptakan ekosistem siber yang lebih tangguh dan adaptif terhadap perubahan serta meningkatkan daya saing Indonesia di tingkat global.

REFERENSI

Abdul Wahid dan Mohammad Labib 2005, Kejahatan Mayantara (Cyber Crime), Jakarta: PT. Refika Aditama, hlm 40

Agus Raharjo, Cybercrime, Bandung: Citra Aditya Bakti, 2002, hal. 59.

Badan Siber dan Sandi Negara. Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024.

Bagian Komunikasi Publik, Biro Hukum dan Hubungan Masyarakat, "*Laporan Tahunan GOVCSIRT Badan Siber dan Sandi Negara Tahun 2019"*.

Barda Nawawi Arief, 2007, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Kencana, Jakarta.

Chainur Arrasijid. S, Dasar-Dasar Ilmu Hukum, Cetakan Ke -5, Sinar Grafika, Jakarta, 2008, Hal 1

Cliver Archer. International Organizations. 2001.London & New York: Routledge.

Coleman, E. G. (2012). *Phreaks, hackers, and trolls: The politics of transgression and spectacle*. M. Mandiberg (Ed.), *The social media reader*. New York University Press. hal. 99–119

Gunkel, D. J. (2005). Editorial: Introduction to hacking and hacktivism. *New Media & Society*.

Indra Sjafri, 1999, Tindak Pidana di Dunia Siber, dalam insider, Legal Journal From Indonesia Capital & Investment Market.

[25] Bagian Komunikasi Publik, Biro Hukum dan Hubungan Masyarakat, "*Laporan Tahunan GOVCSIRT Badan Siber dan Sandi Negara Tahun 2019"*.

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 759-767

ITU, 2015. *International Tellecommunication Union: Regional Presence,* diakses dari https://www.itu.int/en/about/Pages/default.aspx, pada 10 Desember 2024.

ITU, 2014. Manual for Measuring ICT Access and Use by Households and Individuals, Geneva, Switzerland, hal 16.

ITU iLibrary, *Guidelines for the Preparation of National Wireless Broadband Masterplans for the Asia Pacific Region,* diakses dari https://itu-ilibrary.org/science-and-technology/guidelines-for-the-preparation-of-nationa l-wireless-broadband-masterplans-for-the-asia-pacific-region_pub/808e784e-en, pada 11 Desember 2024.

J.G. Starke, Pengantar Hukum Internasional, Sinar Grafika, Jakarta, 1989, hal.1.

Kuehl, Dann, *From cyberspace to cyberpower:Defining The Problem Information Operations at the National Defense University,* National Defence University,USA, 2013, hal 4.

June-2025. Vol. 3, No. 3
e-ISSN: 2442-7667
pp 753-758

Mitnick, K. & Simon, W. (2002). The Art of Deception: Controlling the Human Element of Security, diunduh,pada,10,Desember,2024,dari,https://portal.abuad.edu.ng/lecturer/documents/1585589655The_Art_of_Deception_by_Kelvin_Mitnick.pdf

Neethu. N, *Role of International Organisations in Prevention of Cyber Crimes: An Analysis,*

Nalsar University, Research Gate, diakses dari https://www.researchgate.net/publication/350525198_Role_of_International_Organisations_in_Prevention_of_Cyber-Crimes_An_Analysis, pada 10 Desember 2024.

Nurse, Jason & Creese, Sadie & Goldsmith, Michael & Lamberts, Koen. (2011). Trustworthy and Effective Communication of Cybersecurity Risks: A Review. Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011. 10.1109/STAST.2011.6059257.

Oona A. Hathaway, 2012, *The Law Of Cyber Attack,* California Law Review, hal. 826. Sugeng Santoso, 2018, *Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional,* Jurnal Kajian Lemhannas RI, hal. 45.

Teguh Arifiyadi, *Dunia Siber yang Tidak Maya*, diakses dari https://www.hukumonline.com/berita/a/dunia-siber-yang-tidak-maya-lt59c88b4e7bae6/, pada 11 Desember 2024.

Theodore A. Couloumbis and James H. Wolfe . 1981 . Introduction International Relations : Power And Justice. New Delhi : Prentice-Hall of India.

Topan Yuniarto, *Tantangan Keamanan Siber Indonesia: Ancaman dan Dampaknya,* kompas.com, diakses,dari,https://kompaspedia.kompas.id/baca/paparan-topik/tantangan-keamanan-siber-indonesia-ancaman-dan-dampaknya, pada 10 Desember 2024.