Journal of Peace, Security and Democracy

eISSN: 0000-0000
**Journal Homepage:**
journal.unhas.ac.id/index.php/jpsd
Volume 1, No. 1, January 2025

# *The Dynamics of Cyber Security Cooperation Between Countries: A Case Study of Indonesia and the Netherlands*

Muhammad Faiq Qushayyi[1]

[1]*Bachelor Program of International Relations, Universitas Hasanuddin, Makassar, Indonesia*
*Correspondent author: muhammadfaiqq0@gmail.com*

**ARTICLE INFO**

***Keywords:***

*Cyber Security, Bilateral Cooperation, Security Cooperation, Indonesia, Netherlands*

***Kata Kunci:***

*Keamanan Siber, Kerja Sama Bilateral, Kerja Sama Keamanan, Indonesia, Belanda*

***How to cite:***

Qushayyi, *F. M., (2025). The Dynamics of Cyber Security Cooperation Between Countries: A Case Study of Indonesia and the Netherlands. Journal of Peace, Security and Democracy, 1(1), 37-56*

Copyright: © 2025 Muhammad Faiq Qushayyi.
This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/4.0/

**ABSTRACT**

*The rapid development of information technology in the era of globalization has brought new challenges in the field of cybersecurity. As a country with a high internet adoption rate, Indonesia faces various cyber threats that can damage critical infrastructure and threaten socio-political stability. In the face of these challenges, international cooperation is becoming increasingly important, and one significant form of cooperation is between Indonesia and the Netherlands. This article examines the impact of cybersecurity cooperation between the two countries in improving Indonesia's capacity to deal with cyber threats. Through a qualitative approach, it explores the various initiatives that have been implemented, including training programs, information exchange, and joint policy development to improve Indonesia's cyber resilience. It found that this cooperation not only strengthens the technical aspects, but also facilitates the formation of more holistic policies in addressing cyber challenges. The article also discusses the obstacles faced in this collaboration, including differences in infrastructure, human resource capacity, and political and legal aspects that may affect the effectiveness of this collaboration. Finally, the article offers strategic recommendations for both countries to strengthen their cooperation, with a focus on strengthening Indonesia's national capacity and integrating cybersecurity policies at the international level.*

## Pendahuluan

Perkembangan teknologi informasi dalam era globalisasi ini membawa perubahan besar dalam kehidupan manusia. Adanya internet menjadikan hubungan komunikasi antar manusia di seluruh dunia kini semakin mudah dan cepat tanpa dipengaruhi oleh ruang dan waktu. Dunia Internet (*cyberspace*) ini menawarkan berbagai kesenangan, keuntungan, serta kemudahan tanpa perlu susah payah menggerakkan badan ataupun berpergian untuk memperoleh sesuatu. Seperti hal nya memperoleh informasi, menikmati musik, mencari literatur, *teleshopping*, *teleconference*, *e-commerce* dan lain sebagainya (Fuady, 2005). Penggunaan internet ini telah memasuki berbagai bahkan hampir keseluruhan lini kehidupan manusia seperti kehidupan sosial masyarakat, Kesehatan, pendidikan, termasuk pemerintahan atau pengurusan negara. Pada tahun 2020, pengguna internet di seluruh dunia mencapai lebih dari 4,5 miliar jiwa dari total jumlah penduduk sekitar 8 miliar, lebih dari setengah populasi manusia di dunia telah terhubung ke internet. Pengguna internet juga terus meningkat di seluruh bagian dunia, khusunya di Asia yang meningkat tajam sejak tahun 2006 (Our World In Data, 2022).

Namun, keberadaan internet atau *cyberspace* ini juga memunculkan berbagai macam penyimpangan seperti kejahatan yang memanfaatkan internet atau juga disebut sebagai kejahatan siber atau kejahatan dunia maya (*cybercrime*). *Cyber Crime* merupakan aktivitas kejahatan yang dilakukan dengan menggunakan komputer atau jaringan komputer baik itu dari segi alat yang digunakan, sasaran kejahatan, ataupun tempat berlangsungnya kejahatan (Basmatulhana, Cyber security atau Keamanan Siber: Pengertian, Jenis, dan Ancamannya, 2022). Penggunaan internet yang terus meningkat di seluruh sektor kehidupan manusia yang kemudian disertai dengan ancaman kejahatan siber dan juga kerugian yang dihasilkannya, tentunya menjadikan kejahatan ini menjadi salah satu isu yang penting untuk dibahas dalam isu-isu keamanan nasional setiap negara di dunia. Negara saat ini tidak lagi hanya perlu untuk memiliki keamanan di sektor militer, politik, ekonomi, lingkungan dan lain sebagainya, namun sektor keamanan siber ini pun juga merupakan hal yang perlu diperhatikan. *Conference of States Parties* UNTOC pada tahun 2010 juga telah mengidentifikasi bahwa kejahatan siber ini termasuk sebagai salah satu dari *New Emerging Crimes* dan bahkan juga telah berkembang menjadi salah satu ancaman utama dari kesejahteraan masyarakat di seluruh dunia (Rosy, 2020). Negara-negara saat ini juga telah banyak yang mengkoneksikan data-data dan kontrolnya terhadap beberapa sektor melalui internet, sehingga selain menghadapi ancaman secara fisik, negara pun juga menghadapi ancaman yang berasal dari ruang siber sehingga negara perlu untuk juga mengembangkan kekuatan dalam bidang teknologi dalam hal ini teknologi siber atau bisa juga kita katakan bahwa negara juga perlu untuk memastikan keamanannya di ruang siber. Oleh karena itu, diperlukan upaya peningkatan keamanan siber oleh pemerintah sebagai bagian dari penjagaan keamanan

nasional dikarenakan untuk menangani kejahatan siber diperlukan keamanan siber yang mumpuni.

Kejahatan siber ini bersifat global dan sering kali terjadi melintasi batas negara atau bersifat transnasional sehingga kejahatan siber ini terkadang begitu sulit untuk dideteksi termasuk bagaimana penentuan hukum yang berlaku terhadap pelakunya (Harruma, 2022). Transnasionalisme dari kejahatan siber menjadikan kejahatan ini pada dasarnya begitu sulit bahkan terkadang tidak dapat diselesaikan tanpa adanya kerja sama dengan negara-negara lainnya. Kerja sama internasional baik yang sifatnya bilateral maupun multilateral dapat memberikan kemudahan dalam penanganan kejahatan siber yang terjadi baik di suatu negara maupun kawasan.

Indonesia sendiri saat ini merupakan negara dengan penggunaan internet yang sangat tinggi. Pengguna internet Indonesia pada Maret tahun 2021 telah mencapai 212,35 juta, angka ini menjadikan Indonesia berada di urutan ketiga pengguna internet terbanyak di Asia (Kusnandar, 2021). Penggunaan internet yang begitu tinggi, termasuk letak negara Indonesia yang strategis dan masyarakatnya yang banyak dan beragam, menjadikan peluang ancaman terjadinya kejahatan siber di Indonesia tentunya juga akan sangat tinggi. Pemerintah Indonesia pun juga menyadari akan hal ini, sehingga pemerintah Indonesia juga melakukan berbagai langkah guna meningkatkan keamanan siber di Indonesia.

Pengembangan keamanan siber di Indonesia di inisiasi pada tahun 2007 yang diwujudkan melalui kebijakan yang memberikan adanya kepastian hukum dengan dikeluarkannya peraturan Menteri komunikasi dan informatika No.26/PER/M.Kominfo/5/2007/21 tentang Pengamanan Pemanfaatan Jarijngan Telekomunikasi Berbasis Protokol Internet. Peraturan tersebut mengalami beberapa kali revisi yang pada akhirnya kemudian menghasilkan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010. Dalam peraturan tersebut, turut diatur terkait pembentukan *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII), yakni tim yang bertugas untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet.

Namun, tidak hanya sampai disitu, berbagai serangan siber yang terjadi secara global terkhusus kepada Indonesia termasuk serangan terhadap institusi pemerintah Indonesia menjadikan Indonesia perlu untuk lebih waspada terhadap isu keamanan siber ini dikarenakan telah terkait dengan keamanan nasional. Sehingga kemudian melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) (Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara, 2017) dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 (Peraturan Presiden Republik Indonesia Nomor 133 Tahun 2017 Tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara, 2017), pemerintah membentuk Badan Siber dan Sandi Negara (BSSN) yang kemudian menjadi garda terdepan dalam membangun kesadaran dan kepekaan terhadap ketahanan dan keamanan nasional di bidang keamanan siber, yang kemudian bertugas

menyelenggarakan keamanan siber secara efektif dan efisien dengan menggunakan, mengembangkan, dan memantapkan seluruh elemen yang terkait dengan keamanan siber nasional. Dalam strategi keamanan siber nasional BSSN, terdapat 7 fokus area kerja yang salah satunya ialah kerja sama internasional (Materi Strategi Keamanan Siber Nasional). Indonesia merupakan negara yang aktif dalam berbagai forum PBB termasuk dalam Konferensi Anggota PBB khususnya yang membahas terkait Kejahatan Transnasional Terorganisir yang menetapkan lima unsur kejahatan baru yang harus mendapat perhatian termasuk kejahatan siber. Indonesia sendiri juga melalui BSSN telah melakukan berbagai kerja sama keamanan siber baik yang sifatnya bilateral maupun multilateral seperti di ASEAN Regional Forum, dengan Department of Foreign Affairs and Trade (DFAT) Australia, Pemerintah kerajaan Inggris dan termasuk pula pemerintah Belanda.

Belanda sendiri merupakan sebuah negara dengan pertukaran internet terbesar di dunia yaitu *Amsterdam Internet Exchange* (AMS-IX) dan Belanda juga salah satu negara dengan tingkat konektivitas internet tertinggi di dunia dan salah satu pasar internet paling kompetitif di dunia. Oleh karena itu, kejahatan dunia maya, gangguan layanan online serta spionase digital juga menjadi perhatian utama bagi pemerintah Belanda. Pemerintah Belanda berusaha tidak hanya membangun kesadaran keamanan siber tetapi juga secara aktif memerangi ancaman siber (Privacy Shield Framework, 2017).

Hubungan antara Indonesia dan Belanda memiliki latar belakang dan sejarah yang unik, mulai dari zaman kolonialisme sampai saat ini banyak dinamika yang terjadi antar kedua negara ini. Hubungan bilateral Indonesia dan Belanda secara umum mulai menguat sejak adanya pengakuan oleh belanda secara moral dan politik atas proklamasi kemerdekaan Republik Indonesia 17 Agustus 1945 yang disampaikan melalui pernyataan menteri luar negeri Ben Bot pada tahun 2005. Sejak saat itu, terjadi peningkatan intensitas kerja sama bilateral kedua negara di berbagai bidang, terjadi peningkatan tren nilai perdagangan antara kedua negara selama 5 tahun terakhir (2006-2010) adalah 8.46 % total nilai perdagangan selama periode tersebut mencapai US 18,68 Milyar atau rata-rata per tahun US 3,73 Miliar (Badan Pembinaan Hukum Nasional & Manusia, 1945).

Hingga saat ini, Kerja sama antara Indonesia dan Belanda banyak dilakukan mulai dari bidang Transportasi, perdagangan, investasi, infrastruktur, maritim, pertanian, pariwisata, Pendidikan, termasuk juga khususnya dalam bidang pertahanan dan keamanan. (Kementerian Perhubungan Republik Indonesia, 2019). Kita bisa melihat bahwa Kerja sama antara Indonesia dan Belanda sampai saat ini terus meningkat dan mengikuti perkembangan daripada isu-isu serta tantangan era yang terus berubah sampai saat ini. Di era Globalisasi dengan hadirnya teknologi internet yang kemudian memberikan tantangan yaitu dunia siber yang terus menerus berkembang dan juga mempengaruhi berbagai kehidupan sosial lainnya, tentunya Kerja sama di bidang siber menjadi bidang

Kerja sama yang perlu untuk diperhatikan oleh kedua negara demi lancarnya keberlangsungan Kerja sama antara kedua negara ini.

Kerja sama siber antara Indonesia dan Belanda sendiri, dimulai sejak LOI ditandatangani oleh kepala BSSN Djoko Setiadi sebagai representatif dari pemerintah Indonesia dan Stephanus Abraham perwakilan Menteri Luar Negeri Belanda, di Jakarta pada tahun 2018. Setelah penandatanganan LOI tersebut beberapa kerja sama kemudian dilakukan oleh Indonesia dan Belanda, yang Kerja sama ini tentunya akan memberikan manfaat kepada kedua negara khususnya Indonesia dalam hal peningkatan keamanan siber. Berdasarkan pada hal tersebut, penelitian mengajukan pertanyaan sebagai berikut: Bagaimana pelaksanaan kerja sama keamanan antara Indonesia dan Belanda terhadap peningkatan keamanan siber Indonesia?.

## Metode Penelitian

Penelitian ini menggunakan metode kualitatif. Metode penelitian kualitatif ini merupakan metode penelitian dimana prosedur statistik dan bentuk-bentuk hitungan lainnya tidak digunakan dalam menemukan hasil penelitian. Dan penelitian kualitatif ini berusaha menafsirkan makna daripada sesuatu peristiwa interaksi tingkah laku manusia dalam situasi tertentu menurut perspektif daripada peneliti sendiri.

Penelitian kualitatif dimulai dengan gagasan yang dinyatakan dengan pertanyaan penelitian. Pertanyaan penelitian ini menentukan bagaimana data dikumpulkan dan dianalisis. Metode kualitatif bersifat dinamis, sehingga perubahan, penambahan, dan penggantian selalu memungkinkan selama proses analisis (Wibisono, 2019). Penelitian dengan metode kualitatif ini adalah untuk menggambarkan Dampak kerja sama bilateral antara Indonesia dan Belanda dalam bidang keamanan siber terhadap peningkatan keamanan siber di Indonesia.

Teknik pengumpulan data merupakan bagaimana cara peneliti dalam mengumpulkan data-data penelitian dari sumber data. Adapun Teknik pengumpulan data dalam penelitian ini adalah menggunakan Teknik studi pustaka (*Library Research*) dengan mengumpulkan data dari sumber-sumber bacaan. Adapun data yang dikumpulkan berasal dari buku-buku, jurnal, dokumen, maupun artikel yang berkaitan dengan penelitian (McNabb, 2015)

Jenis data yang dikumpulkan pada penelitian ini ya itu jenis data sekunder yang dimana merupakan data yang telah dikumpulkan atau tersedia untuk peneliti dari pihak lain. Adapun data sekunder didapatkan dari buku, jurnal, website dan sebagainya yang relevan dengan penelitian terkait.

Teknik analisis data yang digunakan dalam penelitian ini adalah teknik analisis data kualitatif dengan menggunakan model Miles dan Huberman yang dapat menganalisis data, menginterpretasikan data, dan menarik kesimpulan. Data yang diperoleh dari pengumpulan data kemudian direduksi terlebih dahulu kemudian disajikan untuk menggambarkan kondisi masalah yang diteliti. Akhirnya, kami menyajikan kesimpulan yang secara singkat menguraikan temuan penelitian (McNabb, 2015).

## Hasil dan Pembahasan

Dalam kerja sama bilateral, tentunya kedua negara memiliki kepentingan nasionalnya masing-masing dan akan mengejar kepentingan nasionalnya sehingga kemudian mendapatkan keuntungan yang maksimal dari adanya kerja sama tersebut (Rana, 2002). Kerja sama keamanan siber antara Indonesia dan Belanda merupakan tindak lanjut daripada Kerja sama-kerja sama keamanan lain sebelumnya yang telah dilakukan oleh kedua negara, Kerja sama keamanan siber ini hadir guna menjawab tantangan era digital yang dihadapi bukan hanya oleh kedua negara namun oleh seluruh dunia saat ini. Dengan adanya Kerja sama keamanan yang dilakukan oleh kedua negara, hal ini tentunya memiliki dampak terhadap peningkatan keamanan siber di Indonesia.

Pemerintah Indonesia juga dalam peraturan presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017, telah menyatakan dengan jelas bahwa pemerintah Indonesia melalui BSSN akan berusaha menciptakan lingkungan siber strategis dan penyelenggaraan sistem elektronik yang aman, andal dan terpercaya; memajukan dan menumbuhkan ekonomi digital dengan meningkatkan daya saing dan inovasi siber; serta membangun kesadaran dan kepekaan terhadap ketahanan dan keamanan nasional dalam ruang siber. Dalam hal ini, Kerja sama yang dilakukan oleh pemerintah Indonesia dengan negara lain dalam bidang siber, termasuk dengan Belanda tentunya adalah untuk meningkatkan keamanan siber di Indonesia.

Pada saat penandatanganan LOI Sendiri, sebagai Langkah awal komitmen Kerja sama dari kedua negara pun, berbagai peluang Kerja sama telah dilihat seperti misalnya berbagi informasi dalam berbagai bidang seperti, hukum, kebijakan nasional, strategi kebijakan manajemen, pertukaran sudut pandang, pengalaman, pembelajaran, penerapan terbaik, penguatan kapasitas dan perbantuan kelembagaan dan juga pengembangan teknologi di bidang keamanan siber melalui berbagai hal seperti jaringan dan program pelatihan dan Pendidikan, pertukaran kunjungan kenegaraan, analisis dan studi lapangan, serta seminar dan konferensi (Fuadona, Indonesia dan Belanda perkuat kerja sama bidang keamanan siber, 2018). Maka setelah penandatanganan LoI tersebut, tentunya kedua negara perlu untuk memaksimalkan peluang-peluang yang ada tersebut dalam program-program Kerja sama.

Dalam *The 1st Cybersecurity Dialogue Indonesia-Belanda* terdapat beberapa pembahasan yang tentunya merupakan berbagi informasi terkait keadaan siber dan hal-hal yang perlu dibahas guna memecahkan masalah-masalah siber yang ada. Dialog dan diskusi dapat menjadi bagian daripada peningkatan keamanan siber dikarenakan dialog ini akan menambah referensi dari kedua negara dalam hal saling tukar menukar persepsi dan solusi dari permasalahan siber yang ada.

### Peningkatan kapasitas hukum dan strategi siber Indonesia

Salah satu diskusi ialah terkait hukum siber internasional. Pesatnya perkembangan dunia siber berbanding lurus dengan munculnya masalah-masalah hukum baru, sehingga beragam kajian hukum terbaru perlu untuk dilakukan guna mengatasi masalah tersebut. Hukum siber, secara sederhana tidak hanya berbicara tentang perlindungan data. namun beberapa aspek juga perlu untuk di kaji diantaranya hukum bisnis yang terkait *e-commerce*, kajian bukti elektronik, perlindungan konsumen, kejahatan pidana berbasis siber, perjanjian kontrak, sampai kepada hal-hal seperti terorisme dan kedaulatan negara (Publik, 2021). Kejahatan siber seperti yang telah kita ketahui merupakan kejahatan yang bersifat transnasional, sehingga dalam penegakan hukum suatu negara, terkadang sulit untuk mengejar pelaku kejahatan transnasional ini dikarenakan perbedaan yurisdksi antar negara, sehingga adanya hukum yang mumpuni baik itu hukum nasional maupun hukum internasional merupakan hal yang penting dalam memastikan keamanan siber dalam suatu negara, Kawasan, maupun global. Adanya pertemuan dan diskusi terkait hukum antara Indonesia dan Belanda ini tentunya dapat menghasilkan adanya suatu promosi hukum yang lebih baik kedepannya khususnya dalam hal hukum internasional. Hukum internasional itu sendiri merupakan bagian dari hukum yang adalah integrasi antara sistem hukum yang berbeda dari berbagai negara. Integrasi yang dimaksud dalam hal ini ialah bahwa hukum internasional secara esensial merupakan kerja sama antar negara.

Adanya kerja sama terkait hukum siber internasional ini juga senada dalam pendekatan hukum yang juga dikatakan bahwa hukum internasional tidak dapat dilindungi dan dipromosikan secara individu melainkan ia harus diupayakan secara bersama-sama (Maskun et al., 2013). Sehingga adanya dialog dan diskusi terkait hukum siber internasional antara Indonesia dan Belanda ini tentunya dapat menghasilkan pandangan-pandangan baru terhadap hukum siber internasional dan juga dapat bersama-sama mempromosikan hal tersebut baik itu di Kawasan maupun secara global.

Indonesia dan Belanda juga termasuk bagian daripada 25 negara anggota PBB yang menjadi anggota daripada United *Nations Group of Governmental Experts (GGE) – Open Ended Working Group (OEWG)* (United Nations, n.d.). Kelompok ini merupakan kelompok ahli pemerintah yang dibentuk guna memajukan perilaku negara yang kemudian bertanggung jawab di dunia maya dalam konteks keamanan internasional. Dalam kelompok negara ini Indonesia aktif dalam proses perumusan normat terkait siber dan pemanfaatan teknologi informasi dan komunifkasi (TIK) dalam kerangka *Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security* (*OEWG Siber*) tersebut. Indonesia telah berkomitmen untuk terus memperkuat pemajuan perdamaian dan perumusan norma siber, dan hali tu juga melalui keanggotaannya dalam *UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE Siber)* periode 2019-2021. (Kemlu.go.id, 2020). Dialog hukum siber internasional yang dilakukan sebelumnya tentunya dapat meningkatkan partisipasi kedua negara dalam forum ini dengan mengangkat ataupun menyampaikan hasil daripada dialog dan

diskusi, pandangan terhadap hukum siber internasional yang telah dilakukan kedua negara dalam program kerja sama bilateral ini

Studi Putra (2014) menjelaskan bahwa dalam mempertahankan keamanan di dunia siber, dapat dilakukan dalam tiga pendekatan, salah satunya ialah dengan pendekatan hukum. Adanya pembahasan dan saling tukar pandangan mengenai hukum siber ini juga tentunya dapat memberikan pandangan-pandangan baru guna meningkatkan aspek *Legal Measures* di Indonesia, yang dimana *Legal Measures* ini merupakan salah satu aspek ataupun pilar yang menjadi penilaian terhadap perkembangan siber di suatu negara (ITU, 2022). Dengan demikian, adanya diskusi dan berbagi informasi serta pandangan terkait hukum dalam keamanan siber merupakan hal yang dapat meningkatkan keamanan siber di suatu negara khususnya di Indonesia.

Dalam hal strategi keamanan siber, dialog yang dilakukan dalam *The 1st Cybersecurity Dialogue Indonesia-Belanda* juga membahas terkait kebijakan dan strategi keamanan siber khusus pada saat pandemic covid-19. Adanya *sharing* mengenai strategi keamanan siber oleh kedua negara ini merupakan hal yang sangat penting khususnya bagi Indonesia, hal ini dikarenakan dalam dunia siber Belanda memiliki keamanan siber yang sangat mumpuni. Belanda ialah negara dengan pertukaran internet terbesar di dunia yaitu Amsterdam Internet Exchange (AMS-IX) dan Belanda juga salah satu negara dengan tingkat konektivitas internet tertinggi di dunia dan salah satu pasar internet paling kompetitif di dunia. Menempati peringkat keenam dalam World Economic Forum's Networked Readiness Index 2016. Wilayah Amsterdan juga menampung hampir sepertiga dari pusat data Eropa, dan kota Groningen dan Middenmeer baru-baru ini mengumumkan pusat data Google dan Microsoft yang baru.

Pemerintah Belanda mendirikan Forum Global untuk Keahlian Siber di Den Haag, yang sudah menjadi rumah bagi Pusat Kejahatan Siber Eropa (EC3) Europol dan Badan Komunikasi dan Informasi (NCI) NATO. Itu juga rumah bagi The Hague Security Delta, kluster keamanan terbesar di Eropa, tempat bisnis keamanan (siber), lembaga pemerintah, dan lembaga pengetahuan bekerja sama. Belanda juga menjadi pemimpin Eropa dalam FinTech, AgTech, dan solusi mobilitas berbasis teknologi, dengan memiliki kelompok usaha rintisan yang cukup besar. Berbagai capaian Belanda terhadap keamanan siber di negaranya tentunya dapat menjadi referensi yang berharga bagi Indonesia untuk dapat diterapkan tidak hanya dalam skala nasional namun juga dapat diterapkan dalam Kawasan.

**Peningkatan kapasitas siber melalui diskusi dan berbagi informasi**

Selain berdampak terhadap peningkatan siber dari segi hukum dan kebijakan siber di Indonesia, kerja sama siber antara Indonesia dan Belanda ini juga berdampak terhadap peningkatan kapasitas siber di Indonesia. Dalam *The 1st Cybersecurity Dialogue Indonesia-Belanda*, beberapa poin yang diangkat dalam diskusi tersebut merupakan hal yang juga menjadi informasi vital yang perlu

untuk diketahui dan yaitu mengenai kejahatan siber multilateral, disinformasi, dan terorisme siber,

Insiden kejahatan siber saat ini telah begitu meningkat dari segi kompleksitas, frekuensi dan termasuk juga tingkat keparahannya, apalagi dengan adanya pandemic covid-19 yang memaksa masyarakat untuk melakukan berbagai kegiatan melalui internet. Pengguna internet di Indonesia pada maret tahun 2021 telah mencapai 212,35 juta, yang ini merupakan angka tertinggi ke-3 pengguna internet terbanyak di Asia (Kusnandar, 2021). Pengguna internet ini merupakan 62,10 persen dari total populasi di Indonesia, dan juga tercatat 90,54 persen dari setiap rumah tangga di Indonesia telah memiliki ataupun menguasai paling tidak minimal satu nomor telepon seluler (Statistik, 2021). Sementara Penggunaan internet yang begitu tinggi tentunya juga berbanding lurus dengan tingginya ancaman terjadinya kejahatan siber, yang dimana juga pada kuartal 1 tahun 2021, lebih dari 9 juta ancaman siber masuk ke Indonesia, hal ini tentunya juga ada kaitannya dengan momentum daripada pandemi covid-19 yang sebagian besar kegiatan dilakukan secara daring (CNN Indonesia, 2021).

Agus Banudi Suyo menyampaikan bahwa jumlah pengguna internet di Indonesia telah mencapai lebih dari 200 juta pengguna, dan menjadi negara keempat dengan pertumbuhan internet tercepat di dunia, yang hal ini menjadikan Indonesia, selain mendapatkan peluang namun juga menghadapi ancaman tantangan kritis dalam mengatasi ancaman serangan siber, yang dimana serangan siber ini yang masuk ke Indonesia tahun 2020 tmencapai sekitar 420 juta serangan (Biro Hukum dan Komunikasi Publik BSSN, 2022). Dalam menangani tantangan ancaman siber yang terus mengikuti perkembangan penggunaan internet di Indonesia, tentunya identifikasi terhadap jenis-jenis atau modus-modus kejahatan siber adalah hal yang termasuk vital untuk dilakukan oleh sebuah negara. Meskipun jenis kejahatan tersebut belum dirasakan di Indonesia, namun tentunya mengetahui adanya suatu jenis kejahatan dan juga penanganan strategis dalam menghadapinya menjadi hal yang harus dilakukan guna jika hal tersebut terjadi maka pemerintah akan lebih sigap dan penanganan bahkan pencegahan dapat dilakukan secepat mungkin, termasuk pada hal-hal seperti disinformasi, dan juga terorisme siber.

Perkembangan teknologi komunikasi yang begitu pesat menjadikan Masyarakat saat ini telah bergerak menuju yang disebut sebagai Masyarakat informasi (*information society*) (Ahmad, 2013). Masyarakat informasi itu sendiri ialah sebuah Masyarakat yang Sebagian besar Angkatan kerjanya adalah pekerja di bidang informasi. Dalam hal ini, menurut Hammer informasi dilihat sebagai sebuah komoditi yang dapat dijual, diberikan, disalin, diciptakan, disalahartikan, didistorsikan dan bahkan dicuri. Informasi telah menjadi salah satu diantara tiga sumber dasar (basic resource) selain potensi material dan energi (Ahmad, 2013). Dunia siber itu sendiri sejatinya dipenuhi oleh informasi-informasi, sehingga juga kemungkinan untuk terjadinya disinformasi pun juga akan semakin mudah terjadi. Saat ini kita lebih mengenal yang dinamakan sebagai Hoax yaitu sebuah kata yang menunjukkan pemberitaan palsu atau usaha untuk menipu atau mengakali pembaca/pendengarnya untuk mempercayai sesuatu yang dibuat

untuk mencapai suatu maksud tertentu yang basisnya saat ini menggunakan media-media sosial seperti facebook, twitter, whatsapp dan lain sebagainya.

Disinformasi atau hoax ini tentunya sangat meresahkan bagi Masyarakat dan bahkan penyalahgunaan daripada informasi-informasi ini bisa jadi terdapat sebuah kepentingan baik di ranah politik, ekonomi (hoaks industry dan bisnis), ideologi, perasaan peribadi dan lain sebagainya. Ancaman terorisme pun juga saat ini, dengan adanya perkembangan lingkungan strategis global telah menjadikan bergesernya kecenderungan ancaman dan konflik yang terjadi dari *inter-state* menjadi *intra-state*. Kemajuan teknologi saat ini juga dimanfaatkan oleh sekelompok teroris untuk kepentingan aksi yang dilakukannya. Internet dapat menjadi media dan pusat kendali daripada Gerakan terorisme, sebagai saran berkomunikasi, melakukan propaganda, ataupun merekrut anggota baru (Dan et al., 2021).

Negara Indonesia dinilai perlu untuk memetakan ancaman-ancaman keamanan siber yang dihadapinya, menguatkan hukum siber nasional, mendirikan koordinasi yang baik antara institusi pemerintahan, mengembangkan infrastruktur digital yang aman termasuk terhadap industri lokal di Indonesia (Chairil, 2019). Dengan adanya diskusi dari kedua negara mengenai kejahatan siber multilateral, disinformasi, dan juga terorisme siber ini, maka tentunya ini akan meningkatkan kapasitas siber di Indonesia yang dalam hal ini, pemerintah lebih banyak mendapatkan referensi tambahan terkait dengan siber.

**Peningkatan kapasitas teknis melalui program pelatihan siber**

Secara teknis, peningkatan kapasitas siber pemerintah Indonesia juga dilakukan melalui *StuNed ScholarshipProgram Evidence-Based Cybersecurity Policy Making Training Program*. Program ini juga merupakan salah satu program yang penting dalam meningkatkan keamanan siber di Indonesia, hal ini dikarenakan yang menjadi sasaran awal daripada program ini yaitu BSSN itu sendiri dengan jabatan fungsional dan dalam program ini mereka memiliki ruang lingkup tugas, tanggung jawab, dan wewenang untuk melakukan studi serta analisis kebijakan keamanan siber. Hal ini tentunya berpengaruh terhadap peningkatan kapasitas teknis dan juga berpengaruh terhadap perumusan kebijakan strategis daripada BSSN sebagai ujung tombak keamanan siber di Indonesia. Dengan Intensnya serangan siber saaat ini, tentunya perumusan kebijakan strategis perlu diperkuat dalam hal ini analisa kebijakan keamanan siber yang berbasis bukti. Sebelum itupun juga salah satu unit kerja BSSN yaitu ortala telah melaksanakan studi banding terkait peyusunan kebijakan keamanan siber di Belanda pada tahun 2019. Tujuan daripada StuNed ini juga selain memperkuat sumber daya manusia dalam organisasi di Indonesia, StuNed juga dapat memperkuat hubungan bilateral antara Indonesia dan Belanda pada saat yang bersamaan.

Kerjasama keamanan siber antara Indonesia dan Belanda ini memberikan pengaruh terhadap peningkatan keamanan siber di Indonesia. Dalam Global Cybersecurity Index (GCI), lima pilar yang menjadi penilaian tingkat

Pembangunan atau keterlibatan setiap negara berdasarkan pada Tindakan hukum, tindakan teknis, tindakan organisasi, pengembangan kapasitas dan juga kerja sama yang dilakukan dengan negara lain. Dalam program kerjasama siber antara Indonesia dan Belanda ini, telah mencakup kelima pilar tersebut sehingga tentunya dalam hal GCI, keamanan siber di Indonesia mengalami peningkatan dan kerjasama yang dilakukan dengan Belanda ini menjadi salah satu faktor penting peningkatan tersebut. Pada tahun 2018, skor GCI Indonesia berada pada angka 17.28, lalu kemudian pada tahun 2022 skor GCI Indonesia meningkat di angka 94,88 yang membuat Indonesia juga berada pada peringkat ke-24 dari 194 negara di dunia (Hariyanto, 2022).

## Kesimpulan

Penelitian ini menunjukkan bahwa kerjasama keamanan siber antara Pemerintah Indonesia dan Pemerintah Belanda memiliki dampak signifikan terhadap peningkatan kapasitas dan ketahanan keamanan siber di Indonesia. Kerjasama ini, yang mencakup pertukaran pengetahuan, pelatihan teknis, serta peningkatan infrastruktur keamanan, telah membantu Indonesia menghadapi tantangan yang muncul seiring dengan berkembangnya ancaman siber. Implikasi teoritis yang dihasilkan dari penelitian ini menunjukkan bahwa kerjasama internasional dalam bidang siber adalah model yang sangat relevan dalam mengatasi ancaman global yang lintas negara. Pendekatan multilateral yang melibatkan berbagai pihak menjadi semakin penting di era digital, di mana ancaman tidak mencapai batas negara.

Dari bidang kebijakan, artikel ini menyoroti pentingnya penguatan kebijakan dalam negeri Indonesia melalui regulasi yang lebih adaptif terhadap perkembangan informasi teknologi serta pembentukan lembaga yang lebih solid dalam menangani ancaman siber. Kerjasama ini memberikan contoh tentang bagaimana negara-negara dengan kapabilitas siber yang lebih maju, seperti Belanda, dapat membantu negara berkembang untuk membangun kemampuan yang serupa. Indonesia, melalui kebijakan yang tepat, dapat memperkuat kerangka regulasi siber, memperbaiki kapasitas lembaga-lembaga operasional terkait, dan meningkatkan kesadaran masyarakat terhadap pentingnya keamanan siber.

Namun, penelitian ini juga menunjukkan keterbatasan dalam hal implementasi dan pengawasan kerjasama ini. Terbatasnya sumber daya dan keahlian yang ada di beberapa sektor, serta tantangan dalam penyamaan standar operasional antara kedua negara, menjadi hambatan yang cukup signifikan. Meskipun kerjasama ini cukup efektif dalam beberapa aspek, tidak semua daerah di Indonesia merasakan dampaknya secara merata, terutama di wilayah dengan infrastruktur yang kurang berkembang. Selain itu, ketergantungan pada pihak luar juga menimbulkan risiko terkait dengan keinginan dan kemandirian Indonesia dalam jangka panjang.

Ke depan, studi ini menyarankan agar dilakukan penelitian lebih lanjut terkait evaluasi mendalam terhadap implementasi kebijakan keamanan siber yang sudah ada serta peran aktor non-pemerintah dalam memperkuat kerjasama ini. Selain itu, perlu adanya model pengembangan kerjasama yang lebih berkelanjutan dengan melibatkan berbagai pihak di luar pemerintahan, seperti sektor swasta dan lembaga pendidikan. Penekanan juga harus diberikan pada penguatan kapasitas lokal, terutama dalam hal pendidikan dan pelatihan yang dapat meningkatkan keahlian teknis di seluruh penjuru Indonesia.

## Referensi

Agita Suryadi. (2015). Kepentingan Indonesia Menyepakati Kerjasama Ekonomi Dengan Slovakia Dalam Bidang Energi Dan Infrastruktur. *Jurnal Online Mahasiswa Bidang Ilmu Sosial dan Ilmu Politik*, 2(2), 1–15.

Ahmad, A. (2013). Perkembangan Media Online dan Fenomena Disinformasi ( Analisis pada Sejumlah Situs Islam ) Online Media Development and Phenomenon of Disinformation ( Analysis of Islamic sites ). *Jurnal Pekommas*, 16(3), 177–186.

Anggoro, D. K. (2013). *Keamanan Nasional, Pertahanan Negara, Dan Ketertiban Umum*. Makalah Pembanding Seminar Pembangunan Hukum Nasional VllI. diselenggarakan oleh Badan Pembinaan Hukum Nasional, Departemen Kehakiman dan HAM RI di Denpasar, 14 Juli 2003. http://www.lfip.org/english/pdf/baliseminar/Keamanan%20Nasional%20Pertahanan%20Negara%20- %20koesnanto%20anggoro.pdf

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Jurnal Politica* 5(1), 95–110. 10.22212/jp.v5i1.336

Arianto, Adi Rio, & Angraini, A. (2019). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan Negara*, 9(1): 13–30.

Azizah, Z. H. (2020). Mendefinisikan Kembali Konsep Keamanan dalam Agenda Kebijakan Negara-Bangsa (Redefining the Concept of Security in the Nation-State Policy Agenda). *Jurnal Diplomasi Pertahanan*, 6(3), 94–104.

Badan Nasional Penanggulangan Terorisme. (2022). Bnpt Dan Nctv Belanda Bahas Kerja Sama Pertukaran Data Informasi Penanggulangan Terorisme. Diambil kembali dari BNPT.GO.ID: https://www.bnpt.go.id/bnpt-dan-nctv-belanda-bahas-kerja-sama-pertukaran-data-informasi-penanggulangan-terorisme

Badan Pembinaan Hukum Nasional (2017) Hasil Penyelarasan Naskah Akademik Rancangan Undang-Undang Tentang Pengesahan Nota Kesepahaman Antara Kementerian Pertahanan Republik Indonesia Dan Kementerian Pertahanan Kerajaan Belanda Tentang Kerjasama Terkait Pertahanan. Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia. https://bphn.go.id/data/documents/na_ruu_ri-belanda_bid_pertahanan.pdf

Badan Siber dan Sandi Negara. (2018, July 3). Badan Siber dan Sandi Negara. Dipetik January 28, 2022, dari Penandatangan Letter Of Intent Kerjasama Bidang Keamanan Siber Kepala Bssn Dengan Menlu Belanda: https://bssn.go.id/penandatangan-letter-of-intent-kerjasama-bidang-keamanan-siber-kepala-bssn-dengan-menlu-belanda/

Badan Siber dan Sandi Negara. (2021, Januari 21). Tingkatkan Kerjasama Bilateral, BSSN Gelar The 1st Cybersecurity Dialogue Indonesia-Belanda. Diambil kembali dari Badan Siber dan Sandi Negara: https://bssn.go.id/tingkatkan-kerjasama-bilateral-bssn-gelar-the-1st-cybersecurity-dialogue-indonesia-belanda/

Badan Pusat Statistik (2021). Statistik Telekomunikasi Indonesia 2021. http://journal.um-surabaya.ac.id/index.php/JKM/article/view/2203

Bakri, U. S. (2017). *Dasar-Dasar Hubungan Internasional*. Depok: Kencana

Basmatulhana, H. (2022). Cyber security atau Keamanan Siber: Pengertian, Jenis, dan Ancamannya: https://www.detik.com/edu/detikpedia/d-6262847/cyber-security-atau-keamanan-siber-pengertian-jenis-dan-ancamannya#:~:text=Keamanan%20Siber%20%28cyber%20security%29%20adalah%20upaya%20yang%20dilakukan,meminimalisir%20masuknya%20risiko%20ancaman%20ke%20dala

Biro Hukum dan Komunikasi Publik – BSSN. (2022, November 9). BSSN dan Kedutaan Belanda Pererat Kolaborasi Kerja Sama Program Beasiswa StuNed untuk SDM Keamanan Siber Indonesia. Diambil kembali dari Badan Siber dan Sandi Negara: https://bssn.go.id/bssn-dan-kedutaan-belanda-pererat-kolaborasi-kerja-sama-program-beasiswa-stuned-untuk-sdm-keamanan-siber-indonesia/

Biro Informasi dan Hukum Kemenko Kemaritiman dan Tim Komunikasi Pemerintah Kemkominfo. (2021). *Tingkatkan Kerjasama Bilateral, BSSN Gelar The 1st Cybersecurity Dialogue Indonesia-Belanda*. https://bssn.go.id/tingkatkan-kerjasama-bilateral-bssn-gelar-the-1st-cybersecurity-dialogue-indonesia-belanda/

Blanchette, J. (2020). *Ideological Security as National Security*. Center for Strategic & International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201202_Blanchette_Ideological_Security_National_Security.pdf

Britto, J. D. (2022). Indonesia-Belanda Tingkatkan Kerja Sama Bidang Keamanan Siber Lewat Beasiswa StuNed untuk BSSN: https://www.kalderanews.com/2022/11/indonesia-belanda-tingkatkan-kerja-sama-bidang-keamanan-siber-lewat-beasiswa-stuned-untuk-bssn/

Caballero, M., & Anthony. (2016). Non-Traditional Security Concept, Issues, and Implications on Security Governance. *Georgetown Journal of Asian Affairs*, 3(1), 5-13.

CNN Indonesia. (2021). *Peta Ancaman Siber RI Kuartal I 2021, Ada 9 Juta Serangan.* https://www.cnnindonesia.com/teknologi/20210607143559-185-651275/peta-ancaman-siber-ri-kuartal-i-2021-ada-9-juta-serangan

Cyberlands. (2022). *Top 15 Cybersecurity Breaches in the Netherlands*. cyberlands.io: https://www.cyberlands.io/topsecuritybreachesnetherlands

Detik.com (2014) *Indonesia dan Belanda Teken Kerjasama Bidang Pertahanan*. https://news.detik.com/internasional/d-2489857/indonesia-dan-belanda-teken-kerjasama-bidang-pertahanan.

Sukoco, A, Syauqillah, M., Ismail, A. U. (2021). Media, Globalisasi dan Ancaman Terorisme. *Journal of Terrorism Studies*, 3(2), 1-15 https://doi.org/10.7454/jts.v3i2.1039

Darmono, B. (2016). Konsep Dan Sistem Keamanan Nasional Indonesia. *Jurnal Ketahanan Nasional*, 15(1): 1–42). https://doi.org/10.22146/jkn.22307

Databooks. (2022). Ad*a 204,7 Juta Pengguna Internet di Indonesia Awal 2022.* Databooks. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/f7af290483a1152/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022

Detik News. (2014). Indonesia dan Belanda Teken Kerjasama Bidang Pertahanan. https://news.detik.com/internasional/d-2489857/indonesia-dan-belanda-teken-kerjasama-bidang-pertahanan

Dewa Web Team. (2022). Pengertian Internet, Sejarah Perkembangan dan Manfaatnya. https://www.dewaweb.com/blog/pengertian-internet/

Diplomat Magazine. (2017, Maret 6). Indonesia-Netherlands' Partnership Beyond 2.0: The Highlights of the Relationship between Indonesia and the Netherlands. https://diplomatmagazine.eu/2017/03/06/indonesie-netherlands-partnership-beyond-2-0-the-highlights-of-the-relationship-between-indonesia-and-the-netherlands/

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science.

Contemporary Security Policy, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Em-Lyon. (2023, Maret 13). What is a tailored program? https://em-lyon.com/en/companies/customized-training-programs/what-is-a-tailored-program#:~:text=A%20tailored%20training%20program%20is%20designed%20specifically%20for,needs%20expressed%20by%20the%20company%20and%20its%20goals

Ezra Natalyn, D. A. (2018, Juli 3). RI-Belanda Teken Kerja Sama Siber, Apa Manfaatnya. Diambil kembali dari Viva.co.id: https://www.viva.co.id/berita/dunia/1050428-ri-belanda-teken-kerja-sama-siber-apa-manfaatnya?page=all

Fisher, L. (2017, Oktober 18). Types of Transnational Crime. Diambil kembali dari Legal Beagle: https://legalbeagle.com/12505445-types-of-transnational-crime.html

Fuadona, F. (2018). Indonesia dan Belanda perkuat kerja sama bidang keamanan siber. https://www.merdeka.com/dunia/indonesia-dan-belanda-perkuat-kerja-sama-bidang-keamanan-siber.html

Fuady, M. E. (2005). "Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia. Mediator: Jurnal Komunikasi, 6(2), 255–264. https://doi.org/10.29313/mediator.v6i2.1194

Hariyanto, P. (2022). Indeks Keamanan Siber Indonesia Peringkat 24 Dunia. Diambil kembali dari SindoNews.com: https://nasional.sindonews.com/read/851697/14/indeks-keamanan-siber-indonesia-peringkat-24-dunia-1660104504#:~:text=Indeks%20Keamanan%20Siber%20Indonesia%20terus%20mengalami%20peningkatan.%20Skor,penilaian%20GCI%20Indonesia%20tahun%202020%20yaitu%20sebesa

Harruma, I. (2022, September 16). Kejahatan Siber: Pengertian, Karakteristik dan Faktor Penyebabnya. Diambil kembali dari Kompas.com: https://nasional.kompas.com/read/2022/09/16/02400071/kejahatan-siber--pengertian-karakteristik-dan-faktor-penyebabnya#:~:text=Karakteristik%20kejahatan%20siber%20Kejahatan%20siber%20atau%20kejahatan%20di,sulit%20untuk%20dideteksi%20dan%20menentukan%20huku

Hasan, M. I. (2018). Kejahatan Transnasional Dan Implementasi Hukum Pidana Indonesia. Lex Crimen, 7(7), 13–20.

Indoworx. (2018, october 13). Indoworx. Dipetik January 17, 2022, dari CyberCrime, 7 Jenis Kejahatan Internet Selain Hacker yang Harus Diketahui: https://www.indoworx.com/kejahatan-internet/

It Governance. (2021). What is Cyber Security? Definition and Best Practices. Dipetik February 2, 2022, dari It Governance: https://www.itgovernance.co.uk/what-is-cybersecurity

ITU. (2022). Global Cybersecurity Index. Diambil kembali dari ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Jelita, A. F., Rizki, K., & Bustami, S. Y. (2020). Analisis Kerja Sama Merida Initiative Antara Meksiko dan Amerika Serikat Dalam Mengurangi Drug Trafficking Organizations di Meksiko. Indonesian Journal of Global Discourse, 2(2), 52–73. https://doi.org/10.29303/ijgd.v2i2.23

Kaspersky. (t.thn.). What is Cyber Security? Diambil kembali dari Kaspersky.com: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kementerian Perhubungan Republik Indonesia. (2019, Mei 1). Indonesia-Belanda Sepakat Pererat Hubungan di Bidang Transportasi.

Kementerian Sekretariat Negara Republik Indonesia. (2016, November 23). Indonesia dan Belanda Perkuat Kerja Sama di Bidang Perdagangan dan Pembangunan Infrastruktur. Diambil kembali dari Kementerian Sekretariat Negara Republik Indonesia: https://www.setneg.go.id/baca/index/indonesia_dan_belanda_perkuat_kerja_sama_di_bidang_perdagangan_dan_pembangunan_infrastruktur

Kemlu.go.id. (2020, Mei 22). Perutusan Tetap Republik Indonesia pada Perserikatan Bangsa-bangsa, New York. Diambil kembali dari Indonesia Suarakan Stabilitas Siber di PBB: https://kemlu.go.id/newyork-un/id/news/6799/indonesia-suarakan-stabilitas-siber-di-pbb

Kemlu.go.id. (t.thn.). Kerajaan Belanda. Diambil kembali dari Kedutaan Besar Republik Indonesia di Den Haag, Belanda: https://kemlu.go.id/thehague/id/pages/belanda/204/etc-menu

Kompas.com (2021, 1 2). Mengapa Setiap Negara Perlu Menjalin Hubungan Internasional?. https://www.kompas.com/skola/read/2021/01/14/144846769/mengapa-setiap-negara-perlu-menjalin-hubungan-internasional?page=all#google_vignette

Kurnia Putra, A. (2014). Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional. Jurnal Ilmu Hukum, 95–109.

Kusnandar, V. B. (2021, october 14). databoks. Dipetik February 4, 2022, dari Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di Asia:

https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internet-indonesia-peringkat-ke-3-terbanyak-di-asia

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. Global Discourse, 8(1), 100–115. https://doi.org/10.1080/23269995.2017.1415082

Marks, J. (2020). The Washington Post. Dipetik January 19, 2022, dari The Cybersecurity 202: Coronavirus crisis spawned more scams than any other event in the last decade: https://www.washingtonpost.com/politics/2020/08/24/cybersecurity-202-coronavirus-crisis-spawned-more-scams-than-any-other-event-last-decade/

Maskun, M., Manuputty, A., Noor, S. M., & Sumardi, J. (2013). Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer. *Masalah-Masalah Hukum*, 42(4), 511–519.

McNabb, D. E. (2015). Research Methods for Political Science. In Research Methods for Political Science. https://doi.org/10.4324/9781003103141

Netherlands and You. (2021). Kingdom of Netherlands. Diambil kembali dari First Indonesia-Netherlands Cyber Policy Dialogue Joint Statement: https://www.netherlandsandyou.nl/latest-news/news/2021/02/10/first-indonesia-netherlands-cyber-policy-dialogue-joint-statement

NL TIMES. (2022). Cyber threat increasing faster than Dutch companies' resilience. Diambil kembali dari NL TIMES: https://nltimes.nl/2022/07/04/cyber-threat-increasing-faster-dutch-companies-resilience

Norton Rose Fulbright. (2017). Data Protection Report. Diambil kembali dari Wannacry Ransomware Attack Summary: https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary

Nuffic. (2023). StuNed. Diambil kembali dari Nuffic: https://www.nuffic.nl/en/subjects/scholarships/stuned

Nugroho, F. T. (2021). Macam-Macam Bentuk Ancaman terhadap Integrasi Nasional di Bidang Pertahanan dan Keamanan. https://www.bola.com/ragam/read/4713336/macam-macam-bentuk-ancaman-terhadap-integrasi-nasional-di-bidang-pertahanan-dan-keamanan

Our World In Data. (2022, Februari 12). Number of people using the Internet. Diambil kembali dari Our World In Data: Number of people using the Internet

Oxial. (t.thn.). Cyberattacks Threaten The Global Economy, As Well As Individual Firms. https://www.oxial.com/grc-blog/cyberattacks-threaten-global-economy-and-individual-firms/

P2K Unkris. (t.thn.). Pengakuan Tanggal Kemerdekaan Indonesia oleh Belanda. Diambil kembali dari Pengakuan Tanggal Kemerdekaan Indonesia oleh Belanda: https://p2k.unkris.ac.id/id3/3065-2962/Penyerahan-Kedaulatan-Kepada-Indonesia_29229_p2k-unkris.html

Petrosyan, A. (2023, Maret 13). IC3 reported cyber crime with the highest amount of victim losses worldwide in 2022, by type. Diambil kembali dari statista: https://www.statista.com/statistics/234987/victim-loss-cyber-crime-type/

Perwita, A. A. B. dan Yani, Y. M. (2005). *Pengantar Ilmu Hubungan Internasional*. Bandung: Rosda Karya

Privacy Shield Framework. (2017, March 4). Netherlands Country Commercial Guide. Dipetik January 28, 2022, dari Netherlands - Cyber Security Services: https://www.privacyshield.gov/article?id=Netherlands-Cyber-Security-Services

Publik, K. K. (2021, Januari 19). Cyber Law Center FH Unpad, Pelopor Kajian Hukum Siber di Indonesia. Diambil kembali dari Universitas Padjajaran: https://www.unpad.ac.id/2021/01/cyber-law-center-fh-unpad-pelopor-kajian-hukum-siber-di-indonesia/

Rana, K. S. ( 2002). *Bilateral Diplomacy*. New Delhi: Manas Publications.

Riana, F. (2021). BIN Sebut 6 Ancaman Keamanan Negara, Termasuk Separatisme Papua dan Radikalisme. https://nasional.tempo.co/read/1472899/bin-sebut-6-ancaman-keamanan-negara-termasuk-separatisme-papua-dan-radikalisme

Rizk, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, 14(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Romm, J. J. (1993). *Defining National Security : The Nonmilitary Aspects*. New York: Council on Foreign Relations Press.

Rosy, A. F. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber. *Journal of Government Science*, 1(2), 118–129. https://doi.org/10.54144/govsci.v1i2.12

Rudy, T. M. (2002). *Studi Strategi Dalam Transformasi SistemInformasi Pasca Perang Dingin*. Bandung: PT Rafika Aditma.

Samuel, R. (2018). Kerjasama Indonesia Belanda Bangun Centre of Excellence Cyber Security & Big Data. https://www.komite.id/2018/10/29/kerjasama-indonesia-belanda-membangun-centre-of-excellence-cyber-security-big-data-dengan-universitas-budi-luhur/

Santosa, E. (2016). *Hubungan RI-Belanda Saat Ini Sangat Baik*. https://news.detik.com/berita/d-3302675/dr-ben-bot-hubungan-ri-belanda-saat-ini-sangat-baik

Security, N. C. (2022). NCTV's Terrorist Threat Assessment: Threats in and to the Netherlands Have Become More Multifaceted and Diffuse. https://english.nctv.nl/latest/news/2022/11/07/nctvs-terrorist-threat-assessment-threat-in-and-to-the-netherlands-has-become-more-multifaceted-and-diffuse

Setyawan, D. P., & Sumari, A. D. W. (2016). Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum on Cybersecurity Initiatives. *Jurnal Penelitian Politik*, 13 (1):1-20

Setyowati, H. E. (2020, Maret 10). *Indonesia-Belanda Sepakat Perkuat Kerja Sama Perdagangan, Investasi, hingga Pariwisata*. Kementerian Koordinator Bidang Perekonomian Republik Indonesia. https://ekon.go.id/publikasi/detail/178/indonesia-belanda-sepakat-perkuat-kerja-sama-perdagangan-investasi-hingga-pariwisata

Statistics Netherlands. (2022). Nearly 2.5 Million People Victims of cybercrime in 202. https://www.cbs.nl/en-gb/news/2022/09/nearly-2-5-million-people-victims-of-cybercrime-in-2021

TechTarget Contributor. (2011). WhatIs.com. https://www.techtarget.com/whatis/definition/letter-of-intent

Tunggal, A. T. (2021). Cyber Security. Dipetik February 4, 2022, dari Why is Cybersecurity Important?: https://www.upguard.com/blog/cybersecurity-important

Tunggal, A. T. (2022). What Is a Cyber Threat. Diambil kembali dari UpGuard: https://www.upguard.com/blog/cyber-threat

United Nations. (t.thn.). *United Nations Office of Disarmament Affairs.* https://www.un.org/disarmament/group-of-governmental-experts/

Utami, M. A. (2022). 5 Kasus Serangan Siber yang Pernah Terjadi di Indonesia. https://techno.okezone.com/read/2022/09/21/54/2672211/5-kasus-serangan-siber-yang-pernah-terjadi-di-indonesia-sebelumnya?page=3.

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P. (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan*, 6(1), 2319–2327.

Yunita. (2016). *Indonesia kekurangan Bakat Cyber Security*. Kementerian Komunikasi dan Informatika Republik Indonesia: https://www.kominfo.go.id/content/detail/8574/indonesia-kekurangan-bakat-cyber-security/0/sorotan_media

Zaimmudin, M. U. (2020). Dinamika Perdagangan Indonesia – Turki dalam kerangka IT-CEPA. *eJournal Ilmu Hubungan Internasional.* 2(1), 118–130.

Zulkifli. (2012). Kerjasama Internasional Sebagai Solusi Pengelolaan Kawasan Perbatasan Negara. *Jurnal Ilmiah Ilmu Administrasi Negara*, 3(2), 1–95.