Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 283-290

PARTISIPASI INDONESIA DALAM UNITED NATION GROUP GOVERMENTAL

Sry Wahyu Ningsih Waruwu [1], Astroviska Dayantresya Sabea [2]
Universitas Kristen Indonesia
srywaruwu15@gmail.com, viskasabea07@gmail.com

Abstract (English)

Indonesia's participation in the United Nations Group of Governmental Experts (UN GGE) for the 2019-2021 period focuses on the cyber security challenges faced by the country. Along with the increasing use of Information and Communication Technology (ICT), the threat of cyberattacks has become a significant global issue. Indonesia, as a country with a high vulnerability to cybercrime, needs to strengthen its national cyber security policy through international cooperation. Through UN GGE, Indonesia seeks to contribute to formulating international cyber norms, improving regional cyber security, and representing the interests of developing countries. In this research, researchers discovered the urgency of Indonesia's participation in the UN GGE, the benefits obtained, and the role of cyber diplomacy as a means of building multilateral cooperation to create a safe and stable cyber space. In conclusion, although the challenges in cyberspace are complex, continued international collaboration is essential to achieve effective cybersecurity.

Article History
Submitted: 13 Oktober 2024
Accepted: 16 Oktober 2024
Published: 23 Oktober 2024

Keywords:
Cyber Security, Cyber Diplomacy, International Cooperation, International Norms.
.

Abstrak (Indonesia)

Prtisipasi Indonesia dalam *United Nations Group of Governmental Experts* (UN GGE) periode 2019-2021, berfokus pada tantangan keamanan siber yang dihadapi negara. Seiring dengan meningkatnya penggunaan Teknologi Informasi dan Komunikasi (TIK), ancaman serangan siber telah menjadi isu global yang signifikan. Indonesia, sebagai salah satu negara dengan kerentanan tinggi terhadap kejahatan siber, perlu memperkuat kebijakan keamanan siber nasionalnya melalui kerjasama internasional. Melalui UN GGE, Indonesia berupaya berkontribusi dalam merumuskan norma-norma siber internasional, meningkatkan keamanan siber regional, dan mewakili kepentingan negara-negara berkembang. Dalam penelitian ini peneliti menemukan urgensi partisipasi Indonesia dalam UN GGE, manfaat yang diperoleh, serta peran diplomasi siber sebagai sarana untuk membangun kerjasama multilateral demi menciptakan ruang siber yang aman dan stabil. Kesimpulannya, meskipun tantangan di ruang siber kompleks, kolaborasi internasional yang berkelanjutan sangat diperlukan untuk mencapai keamanan siber yang efektif.

Sejarah Artikel
Submitted: 13 Oktober 2024
Accepted: 16 Oktober 2024
Published: 23 Oktober 2024

Kata kunci:
Keamanan Siber, Diplomasi Siber, Kerja sama Internasional, Norma Internasional.

PENDAHULUAN

Saat ini, Teknologi Informasi dan Komunikasi (TIK) telah menjadi elemen yang esensial dalam setiap aspek kehidupan masyarakat. Salah satu penemuan paling signifikan dalam era informasi adalah internet. Kehadiran internet sebagai inovasi teknologi telah membuat manusia tak mungkin terpisah dari aliran komunikasi dan informasi. Hal ini sangat relevan mengingat pemanfaatan teknologi kini semakin bervariasi dan meluas. Dengan munculnya komunikasi daring, batasan-batasan konvensional yang sebelumnya diakui oleh konsensus internasional kini menjadi semakin kabur.

Dalam hampir satu dekade terakhir, perdebatan mengenai perang siber (*cyber war*) terus mencuat, bahkan diperkirakan dapat memicu ketegangan antara negara-negara, yang berpotensi mengancam perdamaian global. Bersamaan dengan itu, kemajuan teknologi juga tidak terlepas dari konsekuensi berupa ancaman dan serangan di dunia maya. Serangan siber dapat berakibat fatal, mulai dari kerugian ekonomi, gangguan stabilitas politik, hingga hilangnya nyawa manusia. Kejahatan siber menjadi ancaman serius seiring dengan

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 283-290

perkembangan teknologi dan globalisasi, menimbulkan risiko yang signifikan bagi banyak negara.

Menurut laporan data anomali grafik dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2021, Indonesia mengalami serangan siber yang mencapai 495,3 juta kasus sepanjang tahun 2020, meningkat 41 persen dari 290,3 juta serangan di tahun 2019. Puncak anomali trafik terjadi pada 10 Desember 2020, dengan total mencapai 7.311.606 anomali (DPR, 2015). Data ini menunjukkan betapa mendesaknya perlunya perhatian dan langkah-langkah preventif untuk menghadapi ancaman yang terus berkembang di ranah siber.

Gambar 1: Sektor data yang diretas di Indonesia
Sumber:https://bssn.go.id/

Berdasarkan data diatas dinyatakan bahwa tidak ada negara yang kebal dari ancaman, masalah, dan tantangan di ruang siber. Saat ini, konflik di ruang siber menjadi tantangan bagi komunitas internasional. Sebagai domain baru, ruang siber memerlukan aturan agar tidak terjadi perang. Ruang Siber menjadi arena konflik berbagai kepentingan sehingga unsur politis di ruang siber tidak dapat diabaikan. Penting bagi Indonesia untuk memperhatikan keamanan siber baik itu infrastruktur "lunak" maupun "keras" karena di era digitalisasi ini metode dan jenis serangan siber yang memanfaatkan kelengahan teknologi, sistem informasi, dan instalasi sebuah negara semakin beragam. Pada dasarnya *cyber attack* itu sendiri (yang biasanya dilakukan dengan teknologi) bisa menyebabkan secara tepatnya dampak yang besar, karena adanya problema tersebut ini akan mengancam pada keamanan suatu negara. Dalam konteks ini dinamakan *Cyber Security*.Keamanan siber menjadi penting karena ancaman siber (*Cyber threats*) dan serangan siber (*Cyber Attack*) menuju pada infrastruktur kritis negara.

TINJAUN PUSTAKA

Keamanan selalu menjadi konsep yang terkait dengan objek tertentu, baik di lokasi eksternal maupun internal, serta berhubungan dengan berbagai sektor. Dengan semakin beragamnya ancaman, perluasan konsep keamanan menjadi sangat penting. Keamanan Siber (cyber security) merujuk pada upaya melindungi sistem komputer dari berbagai ancaman atau akses ilegal. Ini mencakup praktik yang bertujuan untuk menjaga sistem, jaringan, dan program dari serangan digital. Keamanan siber melibatkan alat, kebijakan, dan prinsip yang digunakan untuk melindungi aset organisasi dan penggunanya. Dengan demikian, keamanan siber berfungsi untuk mengurangi risiko ancaman terhadap sistem komputer. Isu keamanan siber telah menjadi prioritas bagi negara-negara di seluruh dunia sejak teknologi informasi dan komunikasi digunakan dalam berbagai aspek kehidupan, termasuk sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, dan pertahanan.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 283-290

PEMBAHASAN

I. Cybersecurity

Dewasa ini, kekhawatiran telah meningkat di kalangan pakar keamanan tentang kerentanan terhadap serangan terhadap sistem komputer dan infrastruktur terkait. Namun, meskipun ada peningkatan perhatian dari pemerintah federal dan negara bagian serta organisasi internasional, pertahanan terhadap serangan terhadap sistem ini tampaknya secara umum terfragmentasi dan efektivitasnya sangat bervariasi. Kekhawatiran telah berkembang bahwa yang dibutuhkan adalah kerangka kerja keamanan siber nasional serangkaian upaya sektor publik dan swasta yang terkoordinasi dan koheren yang diperlukan untuk memastikan tingkat keamanan siber yang dapat diterima oleh negara (Fischer, 2005)

Keamanan Siber dan Pertahanan Siber memiliki hubungan yang erat, yaitu keduanya bertujuan untuk melindungi dan mempertahankan kerahasiaan, integritas, dan ketersediaan informasi elektronik atau Sistem Elektronik. Upaya yang dilakukan oleh negara dalam bidang Keamanan Siber dan Pertahanan Siber bertujuan untuk melindungi informasi penting bagi negara dan keamanan nasional, serta menjaga Sistem Elektronik yang kritis untuk pelayanan publik dan kelangsungan negara (Kominfo, 2015).

Secara umum, keamanan diartikan sebagai "kualitas atau kondisi aman dari bahaya". Keamanan informasi merujuk pada perlindungan informasi, termasuk sistem dan perangkat yang digunakan untuk menyimpan dan mengirimkan data. Ancaman dan kejahatan yang ada perlu diantisipasi, salah satunya melalui Keamanan Siber. Keamanan Siber dapat dianggap sebagai serangkaian aktivitas dan langkah-langkah yang bertujuan untuk melindungi dari gangguan, serangan, atau ancaman lain yang berasal dari elemen-elemen di dunia maya, baik berupa perangkat lunak, perangkat keras, maupun jaringan komputer (Nganda, 2017).

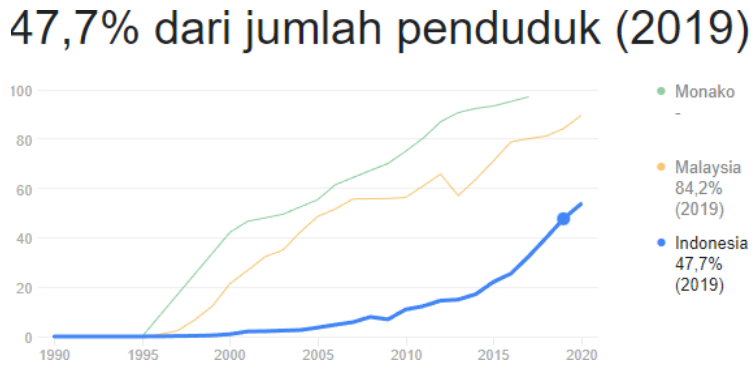
Seperti yang biasa digunakan, *"cybersecurity"* mengacu pada tiga hal: langkah-langkah untuk melindungi teknologi informasi; informasi yang dikandungnya, diproses, dan ditransmisikan, serta elemen fisik dan virtual terkait; tingkat perlindungan yang dihasilkan dari penerapan langkah-langkah tersebut; dan bidang terkait usaha profesional. Hampir semua elemen dunia maya dapat berisiko, dan tingkat interkoneksi elemen-elemen tersebut dapat mempersulit untuk menentukan sejauh mana kerangka kerja keamanan siber yang dibutuhkan. Namun, beberapa komponen tampaknya menjadi sumber risiko yang berpotensi signifikan karena kerentanan besar telah teridentifikasi atau dampak besar dapat dihasilkan dari serangan yang berhasil. Ada beberapa opsi untuk mengatasi kelemahan keamanan siber secara luas.

Diplomasi siber didefinisikan sebagai penggunaan upaya dan kinerja fungsi diplomatik untuk mengamankan kepentingan nasional di ruang siber. Kepentingan ini diidentifikasi sebagai strategi keamanan siber nasional yang diproyeksikan ke dalam agenda diplomatik. Diplomasi siber termasuk ke dalam agenda keamanan siber, kejahatan di ruang siber, pembangunan kepercayaan antar negara, serta kebebasan dan tata kelola ruang siber. Diplomasi siber juga dapat dikatakan sebagai upaya komunikasi, negosiasi, perjanjian, pengumpulan informasi antarnegara dalam rangka mengatasi konflik di ruang siber (Nadhifah, 2020).

II. Kerentanan Ruang *Cyber* di Indonesia

Jumlah pengguna internet aktif saat ini menunjukkan peningkatan yang signifikan, dengan persentase penduduk yang mengakses internet naik dari sekitar 21,98 persen pada tahun 2015 menjadi 47,69 persen pada tahun 2019 (BPS, 2019). Para pengguna melakukan berbagai aktivitas seperti menonton video di YouTube, melihat vlog, mendengarkan musik secara streaming, mengikuti siaran radio online, hingga menikmati podcast. Namun, semua aktivitas daring ini juga membuka peluang bagi tindak kejahatan siber.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 283-290



Gambar 2: Grafik pengguna internet di Indonesia tahun 2019
Sumber: shorturl.at/iFHL9

Laporan tahunan tentang kejahatan siber menunjukkan angka yang tinggi, dengan beberapa kasus telah diselesaikan sementara yang lainnya masih dalam proses penanganan. Berdasarkan data yang dirilis oleh Kominfo, Indonesia menduduki peringkat kedua di dunia dalam hal kasus kejahatan siber, bukan hanya di kawasan ASEAN. Di tengah tahun 2020, terdapat 5.093 aduan kasus kejahatan siber yang mengakibatkan total kerugian mencapai Rp17,69 miliar. Dalam kategori kejahatan siber, lima jenis konten negatif paling banyak dilaporkan selama tahun 2020 adalah penipuan, pengancaman, pemerasan, penghinaan, dan pencemaran nama baik. Platform yang paling sering dilaporkan terkait kejahatan ini adalah WhatsApp, Instagram, Facebook, dan SMS. Pelanggaran yang terjadi mencakup pelanggaran privasi, pelanggaran hak kekayaan intelektual, akses tidak sah ke sistem dan layanan komputer, serta konten ilegal, termasuk sabotase dan pemerasan siber.

Gambar 2: *Study case Cybercrime* 2020-2022
Sumber: shorturl.at/nJYZ4

Indonesia hingga saat ini belum memiliki suatu desain kebijakan keamanan siber yang komprehensif dan terintegrasi untuk menghadapi berbagai ancaman siber yang ada. Menurut laporan BSA The Software Alliance, Indonesia masih berada di tahap awal dalam mengembangkan strategi keamanan siber nasional. Kerangka hukum untuk keamanan siber di Indonesia masih tergolong lemah, dengan tidak adanya undang-undang atau kebijakan yang jelas mengenai keamanan siber, serta praktik keamanan yang tersebar di berbagai peraturan. Di samping itu, belum ada ketentuan khusus yang mengatur keamanan siber (Wahidin, 2022).

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 283-290

III. Urgensi Partisipasi Indonesia Bergabung di UN GGE (United Nation Groups of Govermental Experts

Indonesia masih dihadapkan dengan masalah kerentanan siber yang tinggi disertai dengan tata kelola siber nasional yang masih tumpang tindih. Selain itu, Indonesia juga memiliki kepentingan untuk melindungi masyarakat sipil jika sewaktu waktu perang siber terjadi sehingga hal ini tentu menjadi fokus Indonesia dalam mengambil posisinya di UN GGE.Hal ini dapat dilihat dalam langkah yang diambil oleh Majelis Umum PBB yang membentuk UN GGE sebagai pengemban rezim siber internasional untuk menjadi wadah bagi setiap anggota untuk mengambil posisinya terhadap pengembangan TIK mereka untuk mencapai keamanan siber bersama.

UN GGE siber didirikan pada 2004 oleh Majelis Umum PBB. Kerangka UN GGE menjadi arena untuk memperluas diskusi mengenai keamanan siber internasional. UN GGE menjadi wadah bagi setiap anggota untuk mendeliberasikan posisi nasionalnya mengenai pengembangan TIK mereka Setiap GGE dibangun di atas pekerjaan yang dilakukan oleh yang sebelumnya, membuat kemajuan kumulatif yang signifikan pada masalah yang dihadapi.
Secara umum, topik yang dibahas dalam The Groups of Governmental Experts terdiri atas beberapa bahasan berikut:

1. Potensi dan Ancaman yang ada di ruang siber
2. Bagaimana aplikasi hukum internasional berlaku dalam penggunaan TIK
3. Norma, aturan, dan prinsip perilaku negara yang bertanggung jawab
4. Confidence Building Measures (CBMs)
5. Pengembangan Kapasitas. (UN,2018)

Dalam sidang UN GGE, kelompok ahli ini mengidentifikasi masalah yang ada dan yang akan muncul di ruang siber. UN GGE juga mendiskusikan bagaimana hukum internasional yang ada dapat berlaku dan diterapkan dalam ruang siber. UN GGE merekomendasikan langkah-langkah untuk negara dalam menciptakan keamanan siber internasional seperti langkah saling membangun kepercayaan dan saling mendukung pengembangan kapasitas terutama untuk negara-negara yang masih tertinggal.

Norma juga hadir sebagai langkah-langkah untuk memastikan internet yang bebas, dapat dioperasikan, dapat diandalkan, serta mencakup pendekatan tata kelola pemangku kepentingan. Keinginan Indonesia lewat Kementerian Luar Negeri yaitu meningkatkan peran Indonesia dalam forum multilateral.

Di Indonesia menjadi sangat penting bahwa Regulasi norma dalam konteks keamanan cyber menjadi sangat penting karena dilihat dari mulai meluas di ruang siber baik itu sebagai larangan atas perilaku seperti cybercrime atau hal-hal penggunaan kekuatan di ruang siber. (Azmi, 2012).
Berikut beberapa tujuan Indonesia ikut serta dalam UN GGE:

1. Politik Luar Negeri Indonesia Sebagai Landasan Diplomasi Siber

Kebijakan luar negeri juga merupakan pedoman dasar bagi para pembuat keputusan dalam menghadapi kondisi eksternal menyebutkan bahwa ancaman dan serangan siber yang dialami Indonesia mengalami kenaikan setiap tahunnya. Hal ini menandakan bahwa dari segi kapasitas, Indonesia masih tergolong negara dengan kerentanan siber yang tinggi. Dari sebab-sebab tersebut, keamanan siber menjadi salah satu kepentingan nasional Indonesia. Dalam melindungi kepentingan nasional Indonesia membutuhkan norma yang mengatur perilaku negara bertanggung jawab di ruang siber.

Selanjutnya, pelaksanaan diplomasi siber Indonesia didasarkan pada pelaksanaan politik luar negeri Indonesia yang memiliki dua spektrum utama, yaitu mendukung pencapaian kepentingan nasional dan sebagai upaya untuk berkontribusi terhadap kemaslahatan dunia pertama dasar politik Indonesia yang bebas aktif cocok dengan UN

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 283-290

GGE, Indonesia terpilih kembali menjadi salah satu dari 25 negara yang duduk di UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE Siber) periode 2019-2021. Posisi ini merupakan kesempatan bagi Indonesia untuk mengambil peran dalam penciptaan norma siber, mendukung kerja sama internasional, dan terlibat dalam regulasi senjata siber.

Kebijakan luar negeri Indonesia dalam pembangunan ruang siber Indonesia dipengaruhi oleh faktor internal dan eksternal. Dilihat dari faktor internal, Indonesia sedang memasuki tahap digitalisasi. Pemanfaatan teknologi internet merubah cara jalannya berbagai sektor pelayanan di Indonesia dimana semua mekanisme kerja saling terhubung baik itu di sektor pemerintah maupun swasta Indonesia juga perlu melindungi masyarakat sipil sebagai pengguna internet yang rentan terkena serangan siber

2. **Ketidakhadiran Kerangka Hukum yang Mengatur Ruang Siber**

Indonesia membutuhkan aturan perilaku negara. Indonesia membutuhkan UN GGE sebagai salah satu pengemban bertanggung jawab di ruang siber dalam rangka melindungi negaranya dari konflik terbuka UN GGE sebuah forum yang dibangun untuk mencapai kesepakatan bersama mengenai aturan perilaku negara yang bertanggung jawab di ruang siber. UN GGE dibentuk sukarela di antara sejumlah negara untuk mempermudah koordinasi.

Ancaman siber merupakan masalah lintas negara sehingga kerjasama adalah hal yang penting untuk mendapatkan keamanan siber bersama. Norma keamanan siber dunia yang dicanangkan oleh UN GGE selaras dengan tujuan rezim internasional yaitu tidak hanya mengatur anggota di dalamnya tetapi juga negara yang berada di luar keanggotaan. Dalam hal ini, Indonesia mengutamakan kerja sama dengan negara-negara kawasan karena dampak dari serangan siber akan dirasa oleh negara-negara yang lebih dekat. Indonesia mendorong ASEAN untuk sepakat dalam melihat isu siber dan ingin membawa kultur CBMs untuk terhubung dengan negara- negara kawasan.

3. **Mewakili Kepentingan Negara Kawasan**

Kemudian, dasar diplomasi siber Indonesia tidak lepas dari kepentingan kawasan, ASEAN, sebagai pilar utama politik luar negeri Indonesia. Indonesia hadir dalam GGE untuk memonitor norma keamanan siber yang mewakili kepentingan negara- negara berkembang.Indonesia menjadi salah satu ahli perwakilan dari negara-negara ASEAN.Norma keamanan siber dunia yang dirancangkan oleh UN GGE selaras dengan tujuan rezim internasional yaitu tidak hanya mengatur anggota di dalamnya tetapi juga negara yang berada di luar keanggotaan.

Manfaat Keikutsertaan Indonesia di UN GGE

Melalui UN GGE, Indonesia dapat saling berbagi Informasi dengan negara lainnya tentang isu-isu siber dan mempelajari sistem yang berlaku di negara lain sehingga hal-hal tersebut dapat dipelajari untuk kemudian diadopsi dan disesuaikan dengan kebutuhan nasional. Beberapa hal yang Indonesia dapat dari GGE:

a. Adanya kesepakatan bahwa hukum internasional dan piagam PBB yang ada juga berlaku di ruang siber.
b. Indonesia mendirikan *Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center* (Id/SIRTII/CC) yang dibawahi oleh kemkominfo
c. Hadirnya infrastruktur berstandar internasional yang berfungsi memantau berbagai kejadian di jaringan yang berkaitan insiden keamanan.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2024), 1 (6): 283-290

KESIMPULAN

Indonesia masih dihadapkan dengan masalah kerentanan siber yang tinggi di bidang teknologi dan informasi hal tersebut mencoba untuk mereduksi ketidakpastian yang ada di ruang siber dengan mendukung rezim siber dunia, UN GGE. Hal ini merupakan bagian dari proses kebijakan luar negeri Indonesia dalam rangka mencapai keamanan siber yang sesuai dengan landasan politik luar negeri Indonesia. GGE merupakan wadah untuk pelaksanaan kebijakan luar negeri Indonesia di ruang siber dengan cara-cara diplomatik.Hal ini bertujuan untuk meningkatkan peran Indonesia dalam forum multilateral dengan mewakili negara kawasan untuk menciptakan norma di ruang *cyber*.

GGE menjadi forum yang penting bagi Indonesia karena sejalan dengan keinginan Indonesia yang dibangun lewat Kementerian Luar Negeri untuk meningkatkan peran Indonesia dalam forum multilateral dan praktik diplomasi Indonesia yang mengedepankan institusi berbasis norma. Kemudian, Indonesia juga tentu memiliki tujuan-tujuan yang ingin dicapai sebagai hasil dari keamanan siber itu sendiri. Dilihat dari tujuannya sendiri yaitu untuk mencegah praktik TIK yang berbahaya atau mungkin menimbulkan ancaman terhadap perdamaian dan keamanan internasional.

Pada akhirnya, diplomasi siber multilateral memang akan mengalami proses yang cukup panjang. Merumuskan aturan di ruang siber juga bukan hal yang mudah. UN GGE telah bekerja selama beberapa tahun dalam membentuk norma siber dan kemungkinan tidak akan selesai dalam waktu yang singkat. Namun, Indonesia tidak dapat membangun keamanan siber internasional sendiri, dibutuhkan kerjasama yang memiliki kontinuitas dan banyak negara yang terlibat seperti yang ada dalam GGE untuk dapat mencapai tujuan tersebut.

DAFTAR PUSTAKA

Buku

Iswardhana, M. R., & Widiono, S. (2021). *Diplomasi Siber dan Teknologi Mobile Pada Multidisiplin.* Jakarta: PACE.

Jurnal

Arianto, A. R., & Anggraini, G. (2019). Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indoonesia Security Incident Response Team On Internet Infrastructure (ID- SIRTII). *Jurnal IDU , 9* (1).

BPD. (2019). *Statistik Telekomunikasi Indonesia 2019.* Jakarta: Badan Pusat Stastistik.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica , 10* (2).

DPR. (2015). Analisis RUU Tentang APBN: Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan. Jakarta: DPR.

Fischer, E. A. (2005). Creating a National Framework for Cybersecurity: An Analysis of Issues and Options.

Islami, M. J. (2018). Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index.

Jurnal Penelitian Teknologi Informasi dan Komunikasi.

Kaljurand, M. (2016). United Nations Group of Governmental Experts: The Estoninans Perspective. *International Cyber Norms: Legal, Policy, Industry Perspective* .

Nadhifah, H. N. (2020). Diplomasi Siber Indonesia dalam (United Nations Group Of Governmental Experts Development In The Field Of Information And Telecommunications In The Context Of International Security 2012-2019. *Repository Universitas Islam Syarif Hidayatullah* .

ISSN: 3032-7482
(2024), 1 (6): 283-290

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tanggung bagi Indonesia. *Media Informasi DITJEN POTHAN KEMHAN* .

Windriya, D. R. (2013). TA: Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002. *Repository Stkiom Surabaya* .

Website

Azmi, A. (2012). Indonesia on ASEAN Cyber Security Cooperation.

Retrieved November 18, 2022, from Academia: https://www.academia.edu/11985777/Indonesia_on_ASEAN_Cyber_Security_ Cooperation accesed 16 October 14:22

Febriyani, C. (2021, Agustus 17). Waduh! Indonesia Peringkat Kedua Kejahatan Siber di Dunia. Retrieved November 18, 2022, from industrycoid: https://www.industry.co.id/read/91328/waduh-indonesia-peringkat-kedua-kejahatan-siber-di-dunia accesed 17 October 16:30

KOMINFO. (2015, April 10). Indonesia Peringkat Ke-2 Dunia Kasus Kejahatan Siber. Retrieved November 18, 2022, from kominfo: https://www.un.org/disarmament/ict-security/ accesed 17 October 16:35

Kompas. (2020, Oktober 12). Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi. Retrieved November 18, 2022, from tekno: https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di- indonesia-naik-4-kali-lipat-selama-pandemi accesed 15 October 16:30

UN. (n.d.). Developments in the field of information telecommunications in the context of international security. Retrieved November 18, 2022, from un.org: https://www.un.org/disarmament/ict-security/ accesed 15 October 13:30

Wahidin, K. P. (2022, September 15). Kasus-kasus kebocoran data RI.

Retrieved November 18, 2022, fromalinea.id: https://www.alinea.id/infografis/kasus-kasus-kebocoran-data-ri-b2fqz9G8X accesed 14 October 12:35