Konsensus : Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi
Volume. 2 Nomor. 3 Juni 2025
e-ISSN : 3048-1325, p-ISSN : 3048-4405, Hal. 01-16
DOI: https://doi.org/10.62383/konsensus.v2i3.831
Available online at: https://journal.appisi.or.id/index.php/konsensus

Kerja Sama Indonesia dan Inggris dalam Upaya Meningkatkan Kapabilitas Keamanan Siber

Nawwar Shafwan Mudlaffar Aksah[1*], Imam Fadhil Nugraha[2]
[1-2]Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Indonesia

Alamat: Jl. Perintis Kemerdekaan No.KM.10, Tamalanrea Indah, Kec. Tamalanrea, Kota Makassar, Sulawesi Selatan, Indonesia
*Korespondensi penulis: nafwanma@gmail.com**

Abstract*. This paper analyzes bilateral cooperation between Indonesia and the UK in the field of cybersecurity. Cyber threats are increasingly complex and require a collaborative approach that cannot be addressed independently by each country. Indonesia as a developing economy with high internet faces significant cyber dynamics, while the UK has technological advantages and mature cybersecurity experience. Using a descriptive qualitative analysis approach, this paper examines bilateral agreements, data, and related literature to understand the dynamics of this cooperation. Therefore, this paper shows that this cooperation is based on the strategic interests of both countries in maintaining regional and global security stability, as well as the rampant cyber threats in the current digital era. Indonesia chose the UK as its main partner because of its technological advantages in AI and digital innovation. This cooperation is implemented through personnel exchange mechanisms, technical training, and research and development collaboration.*

Keywords: *Cyber Security, Indonesia, Securitization, United Kingdom.*

Abstrak. Tulisan ini menganalisis kerja sama bilateral Indonesia-Inggris di bidang keamanan siber. Ancaman siber yang semakin kompleks dan memerlukan pendekatan kolaboratif yang tidak dapat diatasi secara mandiri oleh masing-masing negara. Indonesia sebagai ekonomi berkembang dengan internet tinggi menghadapi dinamika siber yang signifikan, sementara Inggris memiliki keunggulan teknologi dan pengalaman keamanan siber yang matang. Menggunakan pendekatan analisis kualitatif deskriptif, tulisan ini mengkaji perjanjian bilateral, data, dan literatur terkait untuk memahami dinamika kerja sama ini. Oleh karena itu, tulisan ini menunjukkan bahwa kerja sama ini didasari oleh adanya kepentingan strategis kedua negara dalam menjaga stabilitas keamanan regional dan global, serta maraknya ancaman siber di era digital saat ini. Indonesia memilih Inggris sebagai mitra utama karena keunggulan teknologi dalam AI dan inovasi digital. Kerja sama ini diimplementasikan melalui mekanisme pertukaran personel, pelatihan teknis, dan kolaborasi penelitian pengembangan.

Kata kunci: Keamanan Siber, Indonesia, Sekuritisasi, Inggris.

1. LATAR BELAKANG

Tulisan ini bertujuan untuk mengeksplorasi secara mendalam terkait kerja sama Indonesia dan Inggris dalam upaya meningkatkan kapabilitas keamanan siber serta mengkaji hal-hal yang perlu menjadi perhatian Indonesia dengan mencontoh Inggris sebagai negara maju. Mengingat ruang siber saat ini telah menjadi wilayah kedaulatan negara, hal ini memungkinkan negara dapat mengatur aktivitas siber terkait keamanan nasional melalui penggunaan teknologi dan informasi. Keberadaan teknologi dan informasi saat ini telah mengalami perkembangan yang cukup pesat. Hal tersebut telah membawa dampak yang besar di berbagai aspek kehidupan manusia. Perkembangan ini tentunya perlu mendapat perhatian agar tidak menimbulkan permasalahan yang tidak diinginkan. Salah satu permasalahan yang

Received: April 21,2025; Revised:Mei 19, 2025; Accepted: Juni 05, 2025; Published: Juni 07, 2025

dapat timbul yakni meningkatnya tantangan dan tuntutan terkait keamanan siber (Lumintosari & dkk, 2024, p. 747).

Keamanan siber dapat diartikan sebagai serangkaian upaya yang dilakukan untuk melindungi kerahasiaan data, integritas, dan informasi (Rizki, 2022, p. 57). Tidak dapat dipungkiri, mudahnya mobilisasi dan pertukaran informasi menjadikan manusia sebagai makhluk informatif yang mampu memberi dan menerima informasi dengan instan. Ungkapan yang mengatakan bahwa orang yang menguasai dunia adalah mereka yang menguasai informasi, tidak lagi menjadi kiasan belaka, namun hal tersebut sudah menjadi hukum yang nyata (Siagian & dkk, 2018, p. 2). Dan hal ini juga menjadi aspek yang krusial dalam konteks pertahanan negara di era modern saat ini. Siber dapat menjadi faktor ancaman bagi keamanan dan kedaulatan suatu negara yang dapat terjadi karena lingkup dari ruang siber berpotensi digunakan untuk mencuri informasi, menyebarkan ide yang bersifat merusak, mencuri informasi, dan juga melakukan penyerangan infrastruktur penting di berbagai bidang, seperti jaringan militer, data perbankan, hingga sistem pertahanan negara (Weu, 2020, p. 155).

Di era digital saat ini, setiap negara akan mengintegrasikan kecanggihan teknologi dalam upaya memperkuat kemampuan pertahanan nasional mereka. Penggunaan teknologi seperti kecerdasan buatan akan sangat membantu dalam menganalisis dan mengidentifikasi ancaman potensial sebelum berkembang menjadi permasalahan yang kritis. Saat ini, dunia maya telah berkembang menjadi medan perang baru yang tidak memiliki batasan, yang mana sumber ancaman sulit untuk ditebak apakah berasal dari individu, negara, atau aktor non negara yang bekerja secara rahasia (Aditya & dkk, 2022, p. 37).

Konsep pertahanan nasional saat ini memiliki cakupan yang lebih luas, mencakup ancaman fisik dan non-fisik, seperti ancaman siber yang berpotensi membahayakan keamanan negara. Globalisasi dan kemajuan teknologi telah memunculkan potensi ancaman baru yang lebih kompleks, salah satunya adalah peperangan siber (*cyber warfare*) yang memanfaatkan teknologi informasi di dunia maya untuk melakukan serangan atau sabotase terhadap infrastruktur penting suatu negara. Ancaman ini memerlukan perhatian serius dan strategi pertahanan yang adaptif untuk menghadapinya.

Dalam informasi yang disampaikan Media Informasi Direktorat Jenderal Pertahanan Kementerian Pertahanan RI pada 2013, Indonesia telah melakukan perang siber dengan negara lain sejak 1998. Hal ini terjadi akibat permasalahan sosial dan politik pada kerusuhan rasial, Indonesia berperang dengan *hacker* dari China dan Taiwan melalui ruang siber. Sementara pada tahun 1999 timbul permasalahan di dunia maya antara Indonesia dan Portugal

menyangkut kasus Timor-Timur. Dan ketika berseteru dengan Portugal, saling serang terjadi hingga masuk ke dalam sistem dan mampu menghapus data yang ada (Soewardi, 2013).

Data serangan siber di Indonesia pada Desember 2024 menunjukkan peningkatan yang cukup siginfikan.

Tabel 1. Data serangan siber di Indonesia pada akhir tahun 2024

Periode/Bulan	Jumlah Serangan	Sektor vital yang diserang
Oktober	20.285.001	Pemerintahan, Layanan Komunikasi, Kesehatan, Energi, dan Transportasi
November	49.429.682	
Desember	112.085.045	

Sumber: Data diolah dari https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html ID-SIRTII/CC (2024)

Hal ini menunjukkan kondisi pertahanan siber Indonesia yang masih berada dalam tahap pengembangan meskipun telah menghadapi ancaman siber selama lebih dari dua dekade. Di samping itu, pembentukan lembaga seperti Badan Siber Sandi Negara (BSSN) menjadi salah satu hal yang kemajuan siginifikan. Indonesia masih menghadapi tantangan dalam mengintegrasikan sistem pertahanan siber yang komprehensif, terutama dalam konteks negara kepulauan dengan ketidakseimbagan digital yang tinggi antar wilayah.

Keterbatasan sumber daya manusia yang memiliki keahlian di bidang keamanan siber juga menjadi hambatan serius, di mana jumlah tenaga profesional keamanan siber berkualitas belum sebanding dengan kebutuhan nasional yang semakin meningkat. Pada tahun 2023, kepala Pusat Pengembangan Profesi dan Sertifikasi Kementerian Komunikasi dan Informatika, Hedi M. Idris, menyatakan bahwa Indonesia masih kekurangan tenaga ahli di bidang *information technology* (IT) hingga tahun 2030 mendatang (Yulianti, 2023). Hal ini tentunya perlu menjadi perhatian serius bagi pemerintah dan seluruh lapisan masyarakat.

Oleh karena itu, penanganan kejahatan siber dalam lingkup hubungan internasional memerlukan kerja sama yang efektif serta upaya diplomatik untuk meminimalisir dampak yang akan terjadi. Indonesia dan Inggris merupakan dua negara yang memiliki hubungan kerja sama yang kuat di berbagai bidang, salah satunya dalam bidang keamanan siber (Ashartati & dkk, 2024, p. 3). Indonesia dan Inggris menandatangani MoU tentang keamanan siber pada tahun 2018. Kerja sama ini mencakup pelatihan dalam bidang keamanan siber, upaya penanganan serangan siber, serta pengembangan strategi. Inggris dipilih karena reputasinya yang kuat, termasuk dalam menangani serangan *Ransomware WannaCry* pada 2017 (Nurdiyanto & dkk, 2024, p. 340). Dengan banyaknya kasus serangan siber yang juga berdampak pada kepentingan nasionalnya, semakin meningkatkan upaya kerja sama internasional yang dilakukan oleh Inggris. Hubungan kerja sama ini dilanjutkan hingga tahun 2027 guna menghadapi tantangan siber di masa mendatang.

Dengan demikian, kolaborasi ini menunjukkan keseriusan dan komitmen kedua negara dalam memperkuat kapabilitas keamanan siber mereka, serta menjalin kerja sama internasional dalam upaya mengatasi ancaman kejahatan siber yang semakin kompleks. Berdasarkan uraian latar belakang di atas, maka penulis berusaha untuk menganalisis kerja sama Indonesia dan Inggris dalam upaya meningkatkan kapabilitas keamanan siber serta mengkaji hal-hal yang perlu menjadi perhatian Indonesia dengan mencontoh Inggris sebagai negara maju.

2. KAJIAN TEORITIS

Konsep keamanan siber merupakan upaya pencegahan dari segala ancaman digital yang dapat mengganggu keamanan negara atau masyarakat (Rachman, 2021, p. 2). Konsep keamanan siber merupakan evolusi dari pemahaman keamanan tradisional yang telah diperluas ke dalam domain digital. Dalam konteks *securitization theory* menekankan bahwa keamanan siber telah mengalami transformasi dari isu teknis menjadi isu keamanan nasional yang memerlukan perhatian serius dari negara. Ancaman siber memiliki karakteristik unik karena dapat bersifat transnasional, sulit diidentifikasi pelakunya, dan mampu menimbulkan dampak yang meluas pada infrastruktur kritis suatu negara. Konsep keamanan siber juga mencakup dimensi sosial dan politik, dimana ancaman tidak hanya berupa serangan teknis terhadap sistem komputer, tetapi juga manipulasi informasi yang dapat mempengaruhi stabilitas sosial dan legitimasi politik. Dalam era digital, batas antara keamanan internal dan eksternal menjadi kabur, sehingga memerlukan pendekatan keamanan yang lebih kolaboratif antar negara untuk menghadapi tantangan keamanan siber yang semakin kompleks.

Sejalan dengan teori di atas, teori sekuritisasi dalam domain siber yang dikembangkan oleh Buzan, Waever, dan de Wilde, terdapat tiga model keamanan yang mengkaji bidang siber yaitu *Hyper securitization*, *Everyday Security Practice*, dan *Technotification* (Buzan & al, 1998). Ancaman siber mengalami proses transformasi dari isu teknis biasa menjadi isu keamanan yang memerlukan tindakan darurat dan luar biasa. Dalam konteks ini, securitization merupakan proses dimana aktor keamanan (*securitizing actors*) seperti pemerintah, militer, atau lembaga keamanan nasional berhasil meyakinkan masyarakat bahwa suatu objek referensi seperti infrastruktur kritis, data pemerintah, atau sistem informasi nasional menghadapi ancaman eksistensial yang memerlukan tindakan segera di luar prosedur politik normal. Proses *securitization* dalam domain siber memiliki karakteristik unik karena ancaman siber seringkali bersifat tidak terlihat, sulit diverifikasi, dan dapat menimbulkan efek psikologis yang signifikan pada masyarakat. Keberhasilan mengamankan ancaman siber ditentukan oleh kemampuan aktor keamanan dalam menciptakan wacana kuat tentang bahaya ancaman,

memungkinkan alokasi sumber daya besar untuk pertahanan siber dan pembatasan kebebasan sipil demi keamanan nasional. Dalam praktiknya, banyak negara termasuk Indonesia dan Inggris telah mengalami proses *securitization* ancaman siber, yang tercermin dalam pembentukan strategi keamanan siber nasional, pendirian lembaga khusus keamanan siber, dan peningkatan anggaran pertahanan siber sebagai respons terhadap persepsi ancaman yang telah berhasil disekuritisasi.

3. METODE PENELITIAN

Tulisan ini menggunakan jenis kualitatif dengan desain studi kasus dalam menganalisis kerja sama Indonesia dan Inggris dalam upaya meningkatkan kapabilitas keamanan siber. Pendekatan ini dipilih guna memungkinkan eksplorasi yang mendalam terhadap dinamika dan hubungan bilateral kedua negara, implementasi program kerja sama keamanan siber yang dilakukan, serta peluang dan tantangan yang muncul dari proses tersebut. Tulisan ini menerapkan pendekatan kualitatif deskriptif guna menguraikan dan menganalisis secara mendalam data sekunder yang bersumber dari berita, jurnal ilmiah, serta sumber lain yang relevan, sehingga memberikan pemahaman yang lebih komprehensif dan mendalam tentang fenomena yang menjadi objek kajian, serta implikasinya dalam konteks yang lebih luas.

Teknik pengumpulan data yang digunakan dalam tulisan ini menggunakan studi pustaka. Teknik pengumpulan data studi pustaka melibatkan pengumpulan dan analisis data sekunder dari sumber-sumber tertulis seperti buku, jurnal ilmiah, artikel, laporan penelitian, dan dokumen lainnya yang sesuai dengan topik bahasan. Proses ini dimulai dengan identifikasi sumber, yaitu mencari dan mengidentifikasi sumber-sumber yang relevan, diikuti dengan menyeleksi sumber untuk memastikan kredibilitas dan relevansi.

4. HASIL DAN PEMBAHASAN

Transformasi digital yang berlangsung pesat dalam dua dekade terakhir telah mengubah cara negara-negara mengelola kedaulatan dan keamanan nasionalnya. Domain siber kini menjadi arena strategis baru yang menentukan daya saing dan ketahanan suatu bangsa, di mana ancaman siber tidak lagi mengenal batas geografis dan dapat melumpuhkan infrastruktur kritis dalam hitungan detik. Indonesia sebagai negara kepulauan terbesar di dunia dengan populasi digital yang terus berkembang, menghadapi tantangan unik dalam membangun kapabilitas keamanan siber yang memadai untuk melindungi aset digital nasional dan infrastruktur kritisnya. Di sisi lain, kompleksitas ancaman siber modern memerlukan pendekatan kolaboratif yang melampaui kemampuan domestik semata, mendorong perlunya kerja sama strategis

dengan negara-negara yang memiliki keunggulan teknologi dan pengalaman dalam menghadapi ancaman siber tingkat tinggi.

Dalam konteks inilah kerja sama Indonesia dengan Inggris dalam bidang keamanan siber menjadi relevan untuk dikaji secara mendalam. Inggris, sebagai salah satu kekuatan siber global dengan reputasi dalam *intelligence* dan teknologi keamanan siber canggih, menawarkan potensi transfer pengetahuan dan teknologi yang signifikan bagi Indonesia. Namun demikian, efektivitas kerja sama bilateral ini tidak dapat dinilai secara terbatas, melainkan perlu pemahaman komprehensif tentang kondisi awal kedua negara, kesenjangan kapabilitas yang ada, serta karakteristik program kerja sama yang telah dan sedang diimplementasikan. Analisis berikut ini akan menguraikan secara sistematis kondisi keamanan siber Indonesia dan Inggris sebagai *baseline assessment*, kemudian mengkaji program-program kerja sama yang telah berlangsung untuk mengevaluasi dampak, tantangan, dan prospek pengembangan kerja sama bilateral ini dalam meningkatkan kapabilitas keamanan siber Indonesia.

Kondisi Keamanan Siber Indonesia

Indonesia saat ini telah menjadikan keamanan siber sebagai salah satu aspek yang perlu diperhatikan dalam hal menjaga kedaulatan negara. Berdasarkan data dari situs Kementerian Komunikasi dan Digital, data pengguna siber di Indoensia di awal tahun 2025 telah mencapai 221 juta pengguna, setara dengan 79,5 persen dari jumlah penduduk di Indonesia (Komdigi, 2025). Dengan tingginya pengguna internet aktif yang ada, tingkat ancaman dan risiko dalam penyalahgunaan teknologi informasi tentu akan menjadi semakin kompleks. Infrastruktur siber negara juga akan menjadi sasaran yang rentan terhadap serangan. Menyikapi kondisi tersebut, guna menciptakan kondisi ruang siber yang aman dan penyelenggaraan sistem elektronik yang andal, transparan, dan terpercaya, pemerintah telah membentuk Badan Siber Sandi Negara (BSSN) sebagai lembaga terpercaya yang menjaga keamanan siber dan sandi negara, serta bersinergi dengan pemangku kepentingan guna mewujudkan keamanan nasional (Ginanjar, 2022, p. 305).

1. Peran Badan Siber Sandi Negara (BSSN) Sebagai Lembaga Keamanan Siber

Badan Siber dan Sandi Negara (BSSN) yang dibentuk melalui Peraturan Presiden Nomor 53 Tahun 2017 merupakan institusi sentral dalam konteks keamanan siber Indonesia yang bertugas untuk melindungi infrastruktur dan informasi vital negara. Sebagai lembaga non-kementerian yang berada langsung di bawah koordinasi Presiden, BSSN memiliki kewenangan luas dalam penyelenggaraan keamanan siber nasional, mulai dari pengembangan kebijakan, standardisasi sistem keamanan, hingga koordinasi respons insiden siber lintas sektor. Kehadiran BSSN sebagai lembaga siber berperan dalam menjalin koordinasi di antara lembaga

dan pemangku kepentingan bidang siber di Indonesia, di antaranya Kepolisian Republik Indonesia, Tentara Nasional Indonesia, Kementerian Luar Negeri, Kementerian Komunikasi dan Digital, dan lembaga lainnya (Chotimah, 2019, p. 122).

Transformasi kelembagaan keamanan siber Indonesia melalui pembentukan BSSN mencerminkan pengakuan pemerintah terhadap urgensi ancaman siber sebagai risiko keamanan nasional yang memerlukan penanganan khusus dan terpusat. Sebelum terbentuknya BSSN, fungsi keamanan siber tersebar di berbagai lembaga dengan koordinasi yang minim. BSSN hadir dengan tujuan untuk mengintegrasikan seluruh ekosistem keamanan siber nasional melalui fungsi koordinasi yang diperkuat dengan kewenangan regulasi dan operasional.

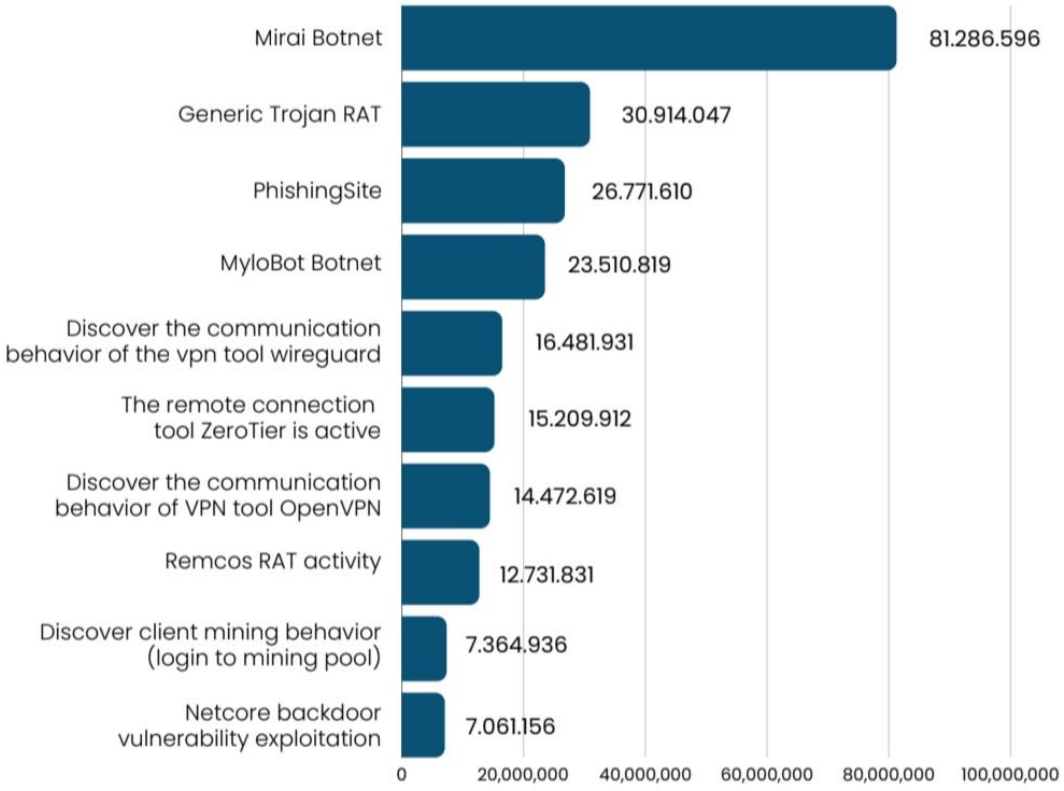
BSSN telah menunjukkan komitmen kuat dalam pengembangan kapabilitas keamanan siber melalui berbagai inisiatif riset dan pengembangan teknologi dalam negeri. Selain itu, BSSN bekerja sama dengan Microsoft dalam mengembangkan program *Cyber Threat Intelligence Platform* (CTIP), sebagai salah satu upaya dalam meningkatkan keamanan siber (Sayekti, 2022). Dalam menghadapi tantangan dinamika keamanan siber yang semakin kompleks, BSSN diharapkan dapat terus berinovasi dan meningkatkan kemampuannya untuk menghadapi ancaman siber.

2. Isu Serangan Siber di Indonesia Pada Tahun 2024

Serangan siber terhadap sistem informasi Indonesia masih kerap terjadi akibat kurangnya kesadaran akan dampak dari ancaman siber serta regulasi dan kebijakan yang belum kuat di Indonesia (Vimy & dkk, 2022, p. 2325). Hal ini membuat ruang siber di Indonesia memiliki celah yang sangat memungkinkan untuk diserang. Sistem manajemen keamanan siber juga masih dapat dikatakan belum mampu untuk berperan sebagaimana mestinya dalam mengontrol pengguna maupun ruang siber. Terkait hal tersebut, pengetahuan terntang ancaman siber perlu dipelajari dan dipahami bersama, bahkan sejak masa sekolah. Proses ini bertujuan guna menambah kesadaran masyarakat akan ancaman siber dan kemungkinan terjadinya *cyber war*, sehingga di masa mendatang akan bertambah pula sumber daya manusia yang memiliki kemampuan yang mumpuni dalam bidang siber.

Tahun 2024 menjadi tahun yang cukup menantang bagi kondisi keamanan siber di Indonesia. Serangan siber menjadi semakin meningkat dan beragam, dengan menyasar lembaga pemerintahan hingga sektor swasta. Ancaman ini tidak hanya berdampak pada keamanan data, tapi juga berdampak pada kepercayaan masyarakat dan stabilitas ekonomi. Berdasarkan data serangan siber di Indonesia, total trafik anomali di Indonesia pada tahun 2024 mencapai 330.527.636 anomali. Angka tertinggi terjadi di Bulan Desember dengan total 112.085.045 anomali, sedangkan angka terendah terjadi di Bulan Mei dengan total 12.273.078

anomali. Aktivitas ini dapat menyebabkan penurunan kualitas perangkat dan jaringan, pencurian data sensitive, hingga perusakan reputasi dan menurunkan kepercayaan terhadap suatu organisasi (Direktorat Operasi Keamanan Siber, 2024).



Gambar 1. Grafik jenis serangan siber di Indonesia pada tahun 2024
Sumber: Data diakses dari https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html ID-SIRTII/CC (2024)

Berdasarkan data yang disajikan dalam grafik di atas, dapat dilihat bahwa ancaman siber menunjukkan pola distribusi yang sangat tidak merata, dengan Mirai Botnet mendominasi secara signifikan sebagai ancaman terbesar.

a). Dominasi Mirai Botnet

Mirai Botnet mencatat angka tertinggi dengan 81.286.596 insiden, menjadikannya ancaman siber yang paling dominan. Angka ini hampir tiga kali lipat lebih besar dibandingkan ancaman kedua terbesar, menunjukkan betapa masifnya serangan yang dilakukan oleh botnet ini. Dominasi *Mirai* dapat dijelaskan oleh kemampuannya menginfeksi perangkat IoT (*Internet of Things*) yang seringkali memiliki keamanan lemah dan tersebar luas.

b). Kategori Ancaman Menengah

Kategori ancaman dengan tingkat sedang terdiri dari *Generic Trojan RAT* (30.914.047), *PhishingSite* (26.771.610), dan *MyloBot Botnet* (23.510.819). Ketiganya menunjukkan angka yang relatif berimbang, berkisar antara 23-31 juta insiden. *Trojan RAT* dan botnet lainnya

mengindikasikan tingginya aktivitas malware yang dirancang untuk akses jarak jauh dan kontrol sistem, sementara PhishingSite menunjukkan masih tingginya upaya penipuan melalui situs palsu.

c). Ancaman Spesifik dengan Volume Menengah

Dua ancaman terkait VPN tool, yaitu *Wireguard* dan *OpenVPN*, mencatat angka masing-masing 16.481.931 dan 14.472.619. Ini menunjukkan adanya aktivitas mencurigakan atau penyalahgunaan terhadap alat-alat komunikasi yang seharusnya meningkatkan keamanan. *ZeroTier* sebagai *remote connection tool* juga menunjukkan pola serupa dengan 15.209.912 insiden.

d). Ancaman dengan Volume Rendah

Kategori terakhir terdiri dari Remcos RAT (12.731.831), aktivitas *client mining* (7.364.936), dan eksploitasi *backdoor Netcore* (7.061.156). Meskipun angkanya lebih rendah, ancaman-ancaman ini tetap signifikan dan menunjukkan keragaman metode yang digunakan oleh pelaku kejahatan siber.

Data ini menggarisbawahi pentingnya fokus keamanan yang proporsional, di mana *Mirai Botnet* memerlukan perhatian khusus mengingat skala serangannya yang cukup luas, sementara ancaman lainnya tetap memerlukan perhatian dan monitoring yang berkelanjutan.

Kondisi Keamanan Siber Inggris

Pemerintah Inggris menyadari bahwa kemakmuran ekonomi dan kesejahteraan sosial sangat bergantung pada keterbukaan dan keamanan jaringan. Oleh karena itu, kerja sama internasional menjadi sangat penting bagi pemerintah Inggris untuk memastikan keamanan siber dan dunia maya (Weu, 2020, p. 155). Kerja sama ini dapat dilakukan melalui berbagai cara, seperti kerja sama bilateral, multilateral, atau bahkan mendukung organisasi internasional yang berfokus pada keamanan siber. Dengan demikian, pemerintah Inggris dapat melindungi perekonomian dan kesejahteraan negaranya dari ancaman siber yang dapat berdampak langsung pada stabilitas ekonomi dan sosial.

Inggris menghadapi ancaman siber yang semakin kompleks pada tahun 2024, dengan serangan yang tidak hanya meningkat dalam frekuensi tetapi juga dalam tingkat kecanggihan teknologinya. Negara ini menjadi target utama kelompok *cybercriminal* internasional dan aktor negara yang memanfaatkan posisi Inggris sebagai pusat keuangan global dan ekonomi digital yang maju. Meskipun menghadapi tantangan yang berat, Inggris telah menunjukkan komitmen serius dalam memperkuat pertahanan sibernya melalui investasi besar-besaran dalam teknologi keamanan, pelatihan personel, dan kerja sama internasional.

1. Peran National Cyber Security Centre (NCSC) Sebagai Lembaga Keamanan Siber

National Cyber Security Centre (NCSC) hadir sebagai benteng pertahanan siber utama Inggris, berdiri pada tahun 2016 sebagai bagian dari *Government Communications Headquarters* (GCHQ). Lembaga ini lahir dari kebutuhan mendesak untuk mengkonsolidasikan upaya keamanan siber nasional di bawah satu atap yang terpadu dan responsif. NCSC mengemban misi krusial untuk melindungi infrastruktur digital Inggris dari ancaman siber yang semakin kompleks, sekaligus menjadi pusat koordinasi antara pemerintah, sektor swasta, dan masyarakat dalam menghadapi tantangan keamanan digital.

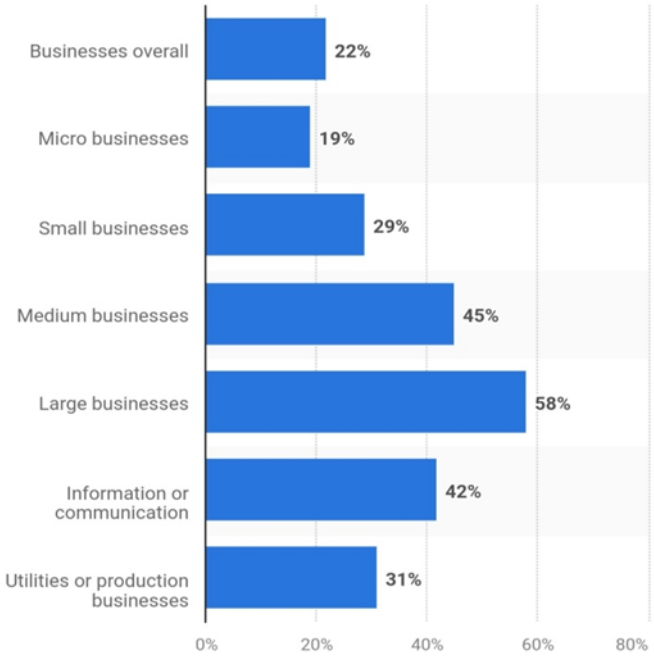
Pada tahun 2018, kepala NCSC menyatakan bahwa NCSC memiliki tujuan untuk menjadikan Inggris sasaran yang tidak menarik bagi penjahat siber dan negara tertentu (The Guardian, 2018). Dalam menjalankan fungsinya, NCSC mengadopsi pendekatan yang mencakup pencegahan, deteksi, respons, dan pemulihan terhadap insiden siber. Selain itu, mereka juga mengembangkan standar keamanan siber nasional, menyediakan layanan konsultasi, dan mengoordinasikan respons terhadap insiden siber berskala besar yang dapat mengancam stabilitas nasional. Melalui program seperti *Cyber Security Information Sharing Partnership* (CiSP) dan berbagai program penelitian, NCSC tidak hanya berfungsi sebagai pengawas, tetapi juga sebagai pendorong inovasi dalam bidang keamanan siber.

2. Isu Serangan Siber di Inggris Pada Tahun 2023 Hingga 2024

Kompleksitas dinamika digital Inggris semakin bertambah dengan adanya keterhubungan yang tinggi antara sektor publik dan swasta, di mana layanan-layanan penting saling bergantung pada sistem digital yang terintegrasi. Kondisi ini menciptakan efek domino yang berpotensi merusak ketika satu sektor mengalami serangan siber, karena dapat dengan cepat menyebar dan mempengaruhi sektor-sektor lainnya. Setiap hari, jutaan transaksi digital dan aktivitas lainnya mengalir melalui jaringan digital Inggris, menciptakan ruang pertempuran siber yang tidak ada habisnya.

Dalam situasi seperti ini, keamanan siber bukan lagi hanya menjadi prioritas, tetapi menjadi kebutuhan mendesak yang harus dipenuhi. Serangan siber dapat memiliki dampak yang sangat luas dan merusak, sehingga perlu dilakukan upaya pencegahan dan penanggulangan yang sangat efektif dan cepat. Jika tidak ditangani dengan serius, serangan siber dapat menyebabkan kerugian yang sangat besar. Hal ini tentunya perlu menjadi prioritas Inggris untuk menjaga stabilitas dan keamanan nasional.

Pada tahun 2024 pula, ancaman siber di Inggris menjadi semakin serius. Pada periode ini serangan siber menjadi lebih terarah, dengan penggunaan kecerdasan buatan dalam serangan dan koordinasi yang lebih baik antara kelompok-kelompok kriminal siber internasional yang menargetkan aset-aset strategis Inggris. Pangsa perusahaan di Inggris juga mengalami berbagai kejahatan siber dengan data berikut:



Gambar 2. Grafik kejahatan siber pada perusahaan di Inggris

Sumber: Data diakses dari https://www.statista.com/statistics/1426513/uk-businesses-encountered-cybercrime-within-year-by-business-size/ Statista.com (2024)

Survei yang dilakukan pada September 2023 hingga Januari 2024 menunjukkan distribusi kejahatan siber berdasarkan ukuran perusahaan di Inggris (GOV.UK, 2024). Secara keseluruhan, 22% dari seluruh perusahaan di Inggris melaporkan mengalami serangan siber, namun angka ini menunjukkan variasi yang signifikan ketika dianalisis berdasarkan ukuran bisnis. Temuan ini mengindikasikan bahwa risiko kejahatan siber tidak terjadi secara merata, melainkan menunjukkan hubungan yang kuat dengan operasional perusahaan.

Analisis berdasarkan ukuran perusahaan menunjukkan tren yang konsisten dimana semakin besar ukuran perusahaan, semakin tinggi kemungkinannya mengalami serangan siber. *Micro businesses* mencatat tingkat kejadian terendah sebesar 19%, diikuti oleh *small businesses* dengan 29%, *medium businesses* mencapai 45%, dan *large businesses* menunjukkan angka tertinggi yaitu 58%. Pola ini cukup masuk akal karena perusahaan besar biasanya memiliki sistem komputer yang lebih rumit, data yang lebih banyak dan berharga, serta lebih banyak titik yang bisa diserang. Selain itu, perusahaan besar juga lebih menarik perhatian pelaku kejahatan siber karena potensi keuntungan yang lebih besar.

Analisis berdasarkan sektor industri menunjukkan bahwa sektor informasi dan komunikasi mencatat prevalensi tertinggi dengan 42% perusahaan mengalami insiden siber. Sebaliknya, sektor utilities dan produksi menunjukkan tingkat kejadian 31%, yang meskipun relatif lebih rendah namun tetap memiliki dampak kritis mengingat peran vital infrastruktur tersebut dalam mendukung stabilitas ekonomi dan sosial masyarakat.

Data serangan siber tahun 2024 tidak hanya menunjukkan volume dan intensitas ancaman, tetapi juga menunjukkan perubahan signifikan dalam taktik penyerang yang lebih berfokus pada dampak terhadap stabilitas ekonomi dan sosial negara. Berdasarkan data yang diperoleh dari *Cyber Security Breaches Survey* 2024, jenis serangan yang paling umum terjadi yaitu phising, penipuan melalui email, dan virus atau malware (GOV.UK, 2024).

Program Kerja Sama Indonesia dan Inggris di Bidang Siber

Adanya kepentingan nasional membuat setiap negara harus mampu memenuhi segala aspek yang dapat menjadi penunjang terpenuhinya kepentingan nasional tersebut, salah satunya adalah aspek pertahanan negara. Kepentingan pertahanan dan keamanan merupakan peran negara dalam memberikan perlindungan terhadap masyarakat dari ancaman yang berasal dari luar.

Indonesia memilih untuk bekerja sama dengan Inggris di bidang siber karena berbagai keunggulan yang ditawarkan oleh Inggris dianggap mampu untuk bersaing di era saat ini. Pertama, Inggris memiliki teknologi dan keahlian yang unggul sebagai salah satu negara pelopor yang mengembangkan strategi keamanan siber nasional., termasuk penggunaan kecerdasan buatan dan inovasi digital lainnya. Kedua, Inggris telah menghadapi berbagai serangan siber tingkat tinggi dan mampu untuk mengatasinya, sehingga dianggap mampu menjadi *role model* Indonesia dalam meningkatkan keamanan sibernya. Tidak hanya itu, Inggris menawarkan model kemitraan yang lebih setara yang memungkinkan Indonesia tidak hanya menjadi penerima bantuan teknis, tetapi juga berkontribusi aktif dalam pengembangan solusi keamanan siber.

Indonesia secara spesifik memilih Inggris sebagai mitra kerja sama dibanding negara maju lainnya karena melihat kualitas Inggris dalam ekosistem keamanan siber global. Inggris memiliki NCSC sebagai bagian dari otoritas teknis nasional untuk ancaman siber, dengan akses ke beberapa *tools* dan teknologi keamanan siber paling canggih di dunia, memberikan Indonesia akses ke keahlian dan teknologi yang tidak tersedia dari kebanyakan negara lain. Cukup berbeda dengan pendekatan dari negara-negara seperti Amerika Serikat atau Cina yang sering mengaitkan kerja sama dengan agenda geopolitik yang kompleks, Inggris menawarkan

pendekatan kemitraan yang lebih fleksibel berdasarkan prinsip "*mutual respect and cooperation*" tanpa tekanan politik berlebihan.

Selain itu, sebagai kekuatan maritim yang memiliki pengalaman panjang dalam mengelola keamanan infrastruktur maritim, Inggris memiliki pemahaman mendalam mengenai tantangan keamanan siber yang dihadapi negara kepulauan seperti Indonesia, yang tidak dimiliki oleh negara-negara kontinental seperti Jerman atau Prancis. Sejalan dengan hal tersebut, penelitian yang dilakukan Ashartati (2024) menyatakann bahwa Indonesia dan Inggris melakukan kerja sama khususnya di bidang siber dengan dua kepentingan pertahanan dan keamanan, yaitu manajemen insiden dan pengembangan kapasitas (Ashartati & dkk, 2024, p. 3).

1. Manajemen Insiden

Manajemen insiden menjadi fokus utama dalam kerja sama keamanan siber antara Indonesia dan Inggris, sebagaimana tertulis dalam MoU yang ditandatangani kedua negara. Strategi ini dirancang untuk meningkatkan respons cepat dan efektif terhadap ancaman siber, serta menjadi pendorong utama peningkatan keamanan siber di Indonesia. Dalam implementasinya, manajemen insiden melibatkan evaluasi menyeluruh terhadap upaya keamanan siber yang telah dilakukan sebelumnya. Evaluasi ini mencakup peninjauan insiden siber sebelumnya, identifikasi kelemahan dan kekuatan respons, dan juga perbaikan untuk meningkatkan kesiapan di masa mendatang.

Kerja sama antara Indonesia dan Inggris juga melibatkan pertukaran informasi dan rekomendasi dari ahli internasional, dengan tujuan Indonesia dapat memperkuat sistem keamanannya dan meningkatkan efektivitas manajemen insiden. Selain itu, pelatihan dan pengembangan kapasitas untuk personel keamanan siber di Indonesia juga menjadi bagian penting dari kerja sama ini. Pelatihan ini bertujuan meningkatkan keterampilan teknis dan mempersiapkan personel untuk menghadapi berbagai jenis ancaman siber.

Implementasi strategi manajemen insiden ini diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan keamanan siber di Indonesia, serta menunjukkan komitmen kedua negara dalam membangun lingkungan siber yang lebih aman dan stabil. Dengan kerja sama ini, Indonesia dapat meningkatkan kapabilitasnya dalam menanggulangi ancaman siber dan melindungi infrastruktur kritis, serta memastikan keamanan data di dunia digital yang semakin kompleks.

2. Pengembangan Kapasitas

Kerja sama keamanan siber antara Indonesia dan Inggris memiliki fokus pada pengembangan kapasitas, yang sejalan dengan teori neorealis tentang hubungan kerja sama internasional. Teori ini menyatakan bahwa kerja sama antarnegara muncul sebagai respons terhadap anarki dalam sistem internasional. Dalam konteks ini, Indonesia memperoleh keuntungan relatif dari kerja sama keamanan siber dengan Inggris. Inggris memiliki kemampuan yang sangat baik dalam menjaga keamanan siber, dengan struktur yang terorganisir dengan baik dan potensi sumber daya manusia serta teknologi yang besar. Sementara itu, Indonesia masih memiliki kekurangan dalam aspek pertahanan siber, baik dalam persiapan, sumber daya manusia, maupun teknologi. Oleh karena itu, Indonesia menekankan pada implementasi kerja sama dengan Inggris untuk meningkatkan kapasitas keamanan siber.

Salah satu implementasi kerja sama ini adalah melalui "*Practical Exchange*" dalam antisipasi dan keamanan siber. Indonesia mengembangkan program pelatihan untuk meningkatkan kapasitas keamanan siber melalui pertukaran informasi dan tenaga terlatih. Hal ini bertujuan untuk mencegah tindak kejahatan siber dan meningkatkan kesadaran akan pentingnya keamanan siber di Indonesia Program pelatihan ini merupakan salah satu upaya dalam meningkatkan kemampuan Indonesia menghadapi ancaman siber dan meningkatkan keamanan siber di negara. Dengan demikian, kerja sama ini dapat membantu Indonesia meningkatkan kapabilitasnya dalam menjaga keamanan siber dan melindungi infrastruktur kritis.

5. KESIMPULAN

Ancaman siber yang semakin meluas membuat setiap negara terus berupaya menjaga lingkup keamanan sibernya. Lemahnya infrastruktur keamanan siber dan kurangnya sumber daya manusia yang mumpuni membuat Indonesia menjalin kerja sama dengan Inggris yang memiliki kemampuan yang unggul dalam bidang siber. Kemitraan ini mencakup berbagai aspek, seperti pengembangan kapasitas melalui pelatihan dan pertukaran informasi, serta implementasi strategi manajemen insiden yang responsif. Hal ini menunjukkan pentingnya memahami kondisi setiap negara yang akan dijadikan mitra dalam kerja sama dalam memenuhi kepentingan nasional.

Melalui kerja sama dengan Inggris, indeks keamanan siber di Indonesia mengalami peningkatan peringkat dari posisi 41 di tahun 2018 menjadi peringkat 24 dari 194 negara dalam *Global Cybersecurity Index* (GCI) di tahun 2020. Dalam tingkat regional pula, Indonesia

berada pada peringkat enam di Asia Pasifik dan peringkat tiga di Kawasan Asia Tenggara setelah Singapura dan Malaysia. Namun di samping itu, meskipun Indonesia telah menjalin kerja sama siber dengan Inggris sejak tahun 2018, peningkatan signifikan belum terlihat secara konsisten. Indonesia masih perlu banyak berbenah untuk mampu bersaing dalam lingkup keamanan siber global.

DAFTAR REFERENSI

Aditya, A. R., & dkk. (2022). Serangan Hacking Tools Sebagai Ancaman Siber Dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, 37.

Ashartati, A. D., & dkk. (2024). Kerja sama Indonesia-Inggris Dalam Mengatasi Kejahatan Siber Tahun 2018-2022. *Global Insight Journal*, 3.

Buzan, B., & al, e. (1998). *Security: A New Framework For Analysis.* London: Lynne Rienner Publishers.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Jurnal Politica*, 122.

Direktorat Operasi Keamanan Siber. (2024). *Lanskap Keamanan Siber Indonesia 2024.* Jakarta Selatan: Deputi Bidang Operasi Keamanan Siber.

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. *Jurnal Dinamika Global*, 305.

GOV.UK. (2024, April 9). *Cyber security breaches survey 2024*. Retrieved Mei 24, 2025, from GOV.UK: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

GOV.UK. (2024, April). *Share of companies in the United Kingdom (UK) having experienced cybercrime in the last year as of 2024, by business size*. Retrieved Mei 25, 2025, from Statista.com: https://www.statista.com/statistics/1426513/uk-businesses-encountered-cybercrime-within-year-by-business-size/

Komdigi. (2025, Februari 27). *Komitmen Pemerintah Melindungi Anak di Ruang Digital*. Retrieved Mei 23, 2025, from Komdigi.go.id: https://www.komdigi.go.id/berita/artikel/detail/komitmen-pemerintah-melindungi-anak-di-ruang-digital

Lumintosari, F. R., & dkk. (2024). Peluang dan Tantangan Diplomasi Digital dalam Meningkatkan Keamanan Siber Indonesia. *Journal of Social Science Research*, 747.

Nurdiyanto, R. A., & dkk. (2024). Kerjasama Keamanan Siber Indonesia-Inggris Pada Periode 2018-2028. *Diplomacy and Global Security Journal*, 340.

Rachman, F. M. (2021). Modal Sosial Masyarakat Digital dalam Diskursus Keamanan Siber. *Jurnal Indonesia Maju*, 2.

Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *POLITEIA: Jurnal Ilmu Politik*, 57.

Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *POLITEIA: Jurnal Ilmu Politik*, 57.

Sayekti, I. M. (2022, Agustus 10). *BSSN & Microsoft Jalin Kemitraan Perangi Peningkatan Kejahatan Siber di Indonesia*. Retrieved Mei 23, 2025, from Pressrelease.id: https://pressrelease.kontan.co.id/news/bssn-microsoft-jalin-kemitraan-perangi-peningkatan-kejahatan-siber-di-indonesia

Siagian, L., & dkk. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Prodi Perang Asimetris*, 2.

Soewardi, B. A. (2013, Maret). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang Tangguh Bagi Indonesia.

The Guardian. (2018, April 10). *UK businesses face growing threat from cyber-attacks – report*. Retrieved Mei 24, 2025, from The Guardian.com: https://www.theguardian.com/technology/2018/apr/10/uk-businesses-face-growing-threat-from-cyber-attacks-report

Vimy, T., & dkk. (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan*, 2325.

Weu, M. R. (2020). Kerjasama Pemerintah Indonesia dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber. *Global Political Studies Journal*, 155.

Yulianti, C. (2023, September 16). *Kominfo: Indonesia Masih Kekurangan 9 Juta Talenta IT di Tahun 2030*. Retrieved Mei 21, 2025, from detikcom: https://www.detik.com/edu/edutainment/d-6934224/kominfo-indonesia-masih-kekurangan-9-juta-talenta-it-di-tahun-2030