JOURNAL SYNTAX IDEA
p–ISSN: 2723-4339 e-ISSN: 2548-1398
Vol. 6, No. 02, Februari 2025

Ancaman Keamanan Siber dan Peran Aktor Non-Negara di Dunia Digital

Serly Sintia Saramuke, Vianna Antoneta Putri, Agnes Marianti Sormin*, Muthia Nugraha
Universitas Komputer Indonesia, Indonesia
Email: agnesmariantisormin27@gmail.com*

Abstrak

Seiring dengan kemajuan teknologi digital dan internet yang semakin pesat dimana masyarakat global sangat bergantung dengan teknologi dan internet, seluruh dunia dihadapi dengan tantangan yang sangat serius dalam bentuk kejahatan siber. Tantangan tersebut tidak hanya memerlukan peran aktor negara dalam menghadapinya, namun aktor non-negara juga memegang peranan penting. Penelitian ini bertujuan untuk mengidentifikasi apa saja bentuk ancaman keamanan siber yang dihadapi saat ini serta menganalisis peran aktor non-negara dalam menghadapi ancaman keamanan siber. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur untuk menganalisis ancaman siber dan peran aktor non-negara dalam menghadapi hal tersebut melalui data non-numerik dari sumber tertulis yang terpercaya. Hasilnya mmenunjukkan bahwa ancaman keamanan siber semakin meningkat seiring dengan pertumbuhan pengguna internet global yang mencakup berbagai jenis seperti cyber crime, cyber warfare, dan cyber terrorism, yang semakin diperburuk oleh adanya pandemi COVID-19. Dalam menghadapi ancaman ini, aktor non-negara seperti organisasi internasional, perusahaan teknologi, dan Lembaga Swadaya Masyarakat berperan penting dalam edukasi publik, kerjasama antarnegara, serta penguatan kebijakan dan pertahanan siber, terutama melalui media sosial sebagai saluran komunikasi yang efektif.

Kata kunci: Aktor non-negara, keamanan siber, kejahatan siber, teknologi digital.

Abstract

Along with the rapid advancement of digital technology and tnternet where the global community is highly dependent on technology and imternet, the whole world is faced with very serious challenges in the form of cybercrime. These challenges not only require the role of state actors in dealing with them, but non-state actors also play an important role. Therefore, this article aims to identify what forms of cybersecurity threats are faced today and analyze the role of non-state actors in dealing with cyber security threats. This article uses a qualitative approach with a literature study method to analyze cyber threats and the role of non-state actors in dealing with them through non-numerical data from reliable written source. The results show that cyber security threats are increasing along with the growth of global internet users which include various types such as cyber crime, cyber warfare, and cyber terrorism, which are further exacerbated by the COVID-19 pandemic. In dealing with these threats, non-state actors such as international organizations, technology companies, and non-governmental organizations play an important role in public education, cooperation between countries, and strengthening cyber policies and defenses, especially through social media as an effective communication channel.

Keywords: *Non-state actors, cyber security, cybercrime, digital technology.*

PENDAHULUAN

Perkembangan dan kemajuan teknologi digital mengakibatkan perubahan yang signifikan terhadap peradaban manusia (Alimin & Islami, 2022). Tidak hanya dalam sektor industri, teknologi juga turut andil dalam perubahan cara hidup manusia (Aji, 2023). Teknologi memungkinkan manusia untuk terhubung secara global, berkomunikasi tanpa batas, serta mengakses informasi hanya dalam hitungan detik (Nasional, 2021). Kemajuan internet sebagai salah satu produk dari teknologi memiliki segudang manfaat bagi keberlangsungan hidup manusia. Internet dan teknologi menawarkan berbagai kemudahan bagi manusia (Rosy, 2020). Kemudahan tersebut membuat manusia hidup bergantung pada teknologi sehingga di era *society 5.0* ini tidak dapat dipungkiri bahwa teknologi menjadi salah satu infrastruktur penting bagi kemajuan kehidupan masyarakat secara global tanpa terkecuali.

Perkembangan ini juga berimplikasi pada berkembangnya kajian dalam Hubungan Internasional (Indarta et al., 2022). Seiring dengan kemajuan teknologi, pola keamanan internasional pun terjadi pergeseran dimana konsep keamanan dalam hubungan internasional tidak lagi hanya membahas mengenai isu *high politics*, namun berkembang menjadi isu-isu *low politics* (Barisione & Michailidou, 2017). Isu keamanan *high politics* yang juga disebut sebagai keamanan tradisional membahas mengenai upaya-upaya pengamanan negara yang dilakukan oleh negara dan mencakup kekuatan militer (Trihartono, Indriastuti, & Nisya, 2020). Sedangkan isu keamanan *low politics* atau yang disebut sebagai *Non-Traditional Security* (NTS) lebih mengarah kepada keamanan yang melibatkan aktor non-negara dan ancaman yang ada berasal dari kekuatan non-miiter. Karena cakupan ancaman yang luas tersebut, bukan hanya keamanan negara dan teritorial saja yang terancam, namun juga keamanan seluruh lapisan masyarakat ikut terancam (Trihartono et al., 2020)

Cyber security atau keamanan siber merupakan salah satu bentuk konsep keamanan non-tradisional. *Cyber security* merupakan upaya strategis yang sangat penting dalam melindungi data dan informasi di dunia digital (Indah, Sidabutar, & Nasution, 2023);(Aji, 2023). Hal ini melibatkan berbagai tindakan untuk menjaga keamanan data yang tersimpan di media penyimpanan, serta memastikan bahwa data yang dikirimkan melalui jaringan tetap aman dari potensi gangguan (Rahmawati, 2017). Perkembangan teknologi yang semakin maju memunculkan kejahatan dalam bentuk baru yang disebut sebagai *cyber crime*, kejahatan ini dilakukan secara kasat mata dimana ancaman yang timbul dari kejahatan ini tidak berbentuk fisik. Para pelaku *cyber crime* ini memanfaatkan jaringan internet yang terkoneksi secara global sehingga dapat mengancam keamanan nasional suatu negara (Maskun, 2022). *Cyber crime* saat ini telah diakui sebagai salah satu bentuk kejahatan transnasional yang serius. Pada *Conference of states Parties* UNTOC tahun 2010, *cyber crime* diidentifikasi sebagai *New Emerging Crimes*. Julian Droogan juga menyatakan bahwa *cyber crime* kini menjadi salah satu ancaman utama terhadap kesejahteraan masyarakat global (Rosy, 2020).

Dikutip dari majalah Forbes, pada tahun 2023, serangan siber di seluruh dunia meningkat tajam dengan mencatat lebih dari 2 ribu serangan siber yang mengakibatkan jumlah korban lebih dari 343 juta. Serangan ini mengalami kenaikan sebesar 72 persen dibandingkan tahun 2021 dimana pada tahun itu serangan siber mencatat rekor tertinggi sepanjang masa dengan vektor serangan yang paling umum terjadi pada email dimana sekiitar 35 persen *malware* dikirim melalui email pada tahun 2023 dan 94 persen

organisasi melaporkan mengalami insiden tersebut. dampak finansial dari inisiden ini sangat besar dengan rata-rata biaya kebocoran data mencapai 4,88 juta USD per Agustus 2024. Serangan yang menyasar email bisnis menyebabkan kerugian lebih dari 2,9 miliar USD. *Cyber crime* menjadi ancaman ekonomi global yang cukup serius dimana Cybersecurity Ventures dalam Cybercrime Magazine memperkirakan kerugian akibat kejahatan ini mencapai 9,5 triliun USD di tahun 2024 dan diproyeksikan meningkat menjadi 10,5 triliun USD pada tahun 2025. Angka ini menjadikan kejahatan siber sebagai "ekonomi terbesar ketiga" di dunia setelah Amerika Serikat dan China dengan pertumbuhan kerugian sebesar 15 persen per tahun.

Rumusan penelitian ini bagaimana bentuk ancaman keamanan siber yang dihadapi dunia digital saat ini; Bagaimana peran aktor non-negara dalam menghadapi ancaman keamanan siber. Penelitian ini bertujuan untuk mengidentifikasi berbagai bentuk ancaman keamanan siber yang semakin berkembang seiring dengan pesatnya penggunaan teknologi digital serta menganalisis peran aktor non-negara dalam menanggulangi ancaman tersebut. Adapun manfaat penelitian ini adalah memberikan wawasan akademis dan praktis mengenai strategi keamanan siber yang dapat diterapkan oleh berbagai pemangku kepentingan, termasuk pemerintah, organisasi internasional, dan masyarakat luas. Selain itu, penelitian ini diharapkan dapat menjadi referensi dalam perumusan kebijakan yang lebih efektif dalam menghadapi tantangan keamanan siber global serta meningkatkan kesadaran publik terhadap pentingnya literasi digital dan perlindungan data di era digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif. Pendekatan ini dipilih karena memungkinkan peneliti untuk mengeksplorasi ancaman siber dan dinamika peran aktor non-negara dalam dunia digital secara mendalam melalui analisis data non-numerik. Metode yang digunakan dalam artikel ini adalah studi literatur (*literature review*) yang melibatkan pengumpulan data dari berbagai sumber tertulis seperti buku, artikel jurnal, laporan penelitian, dokumen, serta publikasi dari sumber yang terpercaya. Metode penelitian ini diharapkan dapat memberikan landasan yang kuat untuk analisis dan diskusi terkait dengan topik yang dibahas, serta membantu pembaca dalam memahami ancaman yang dihadapi di era digital dan strategi yang diperlukan untuk mengatasinya.

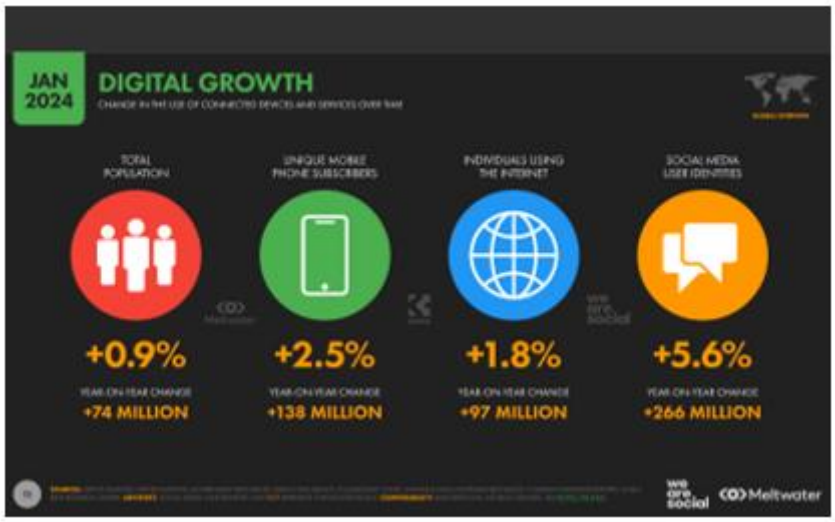
HASIL DAN PEMBAHASAN

Bentuk Ancaman Keamanan Siber



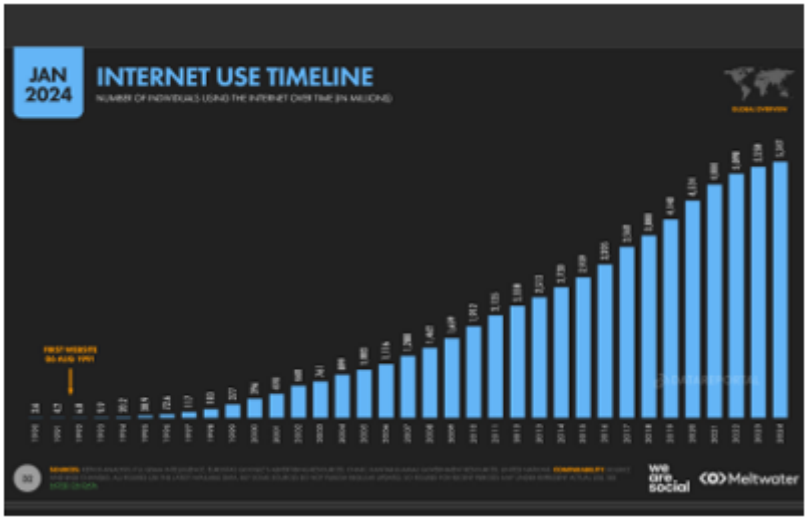
Gambar 1. Ancaman Keamanan Siber
Sumber: We Are Social (2024)

Berdasarkan data yang dilaporkan oleh *We Are Social* per Januari 2024 di atas, jumlah pengguna internet di dunia telah mencapai angka yang cukup tinggi, yakni 5,35 miliar dari total populasi global sebanyak 8,08 miliar. Angka ini menunjukkan bahwa sekitar 66,2% dari populasi dunia kini terhubung dengan internet.



Gambar 2. Pertumbuhan Digital
Sumber: We Are Social (2024)

Data dari gambar di atas memberikan gambaran tentang pertumbuhan digital secara global pada Januari 2024. Jumlah individu yang menggunakan internet naik sebesar 1,8% dari tahun sebelumnya dimana pertumbuhan tersebut menambahkan jumlah pengguna internet baru sebanyak 97 juta, seiring dengan meningkatnya jumlah populasi di dunia sebesar 0,9% dari tahun ke tahun yang berjumlah sekitar 74 juta orang.



Gambar 3. Jumlah pengguna internet
Sumber: We Are Social (2024)

Data diatas menggambarkan tren jumlah pengguna internet dari tahun ke tahun hingga Januari 2024. Grafik ini menunjukkan pertumbuhan signifikan dalam jumlah individu yang menggunakan internet secara global sejak awal keberadaan internet hingga tahun 2024. Grafik tersebut menyoroti bahwa internet pertama kali digunakan secara umum pada tahun 1991 dengan situs web pertama diluncurkan pada 6 Agustus 1991. Pada fase ini jumlah pengguna internet sangat sedikit karena teknologi baru muncul sehingga infrastrukturnya pun terbatas. Seiring berkembangnya teknologi dan infrastruktur, pengguna internet mulai meningkat pesat dari tahun ke tahun. Mulai dari tahun 2010 ke atas, grafik menunjukkan lonjakan jumlah pengguna internet yang tajam. Hingga pada tahun 2024, jumlah pengguna internet telah mencapai lebih dari 5,35 miliar individu.

Data-data di atas memberikan bukti kuat bagaimana internet telah berevolusi menjadi bagian penting dari kehidupan manusia. Dengan lebih dari separuh populasi dunia terhubung secara digital, internet tidak hanya memfasilitasi komunikasi dan informasi, tetapi juga mendorong transformasi di berbagai aspek kehidupan baik sosial, ekonomi, maupun budaya secara global. Namun, peningkatan jumlah pengguna internet yang tidak dapat terhindarkan ini menghadirkan tantangan yang sangat serius bagi masyarakat global dimana risiko ancaman keamanan siber semakin meningkat. Ancaman keamanan siber dapat dibedakan menjadi beberapa jenis berdasarkan modus operasinya (Ginanjar, 2022).

Cyber Crime merupakan kejahatan siber yang melibatkan akses ilegal ke sistem atau data dengan tujuan menciptakan gangguan atau memperoleh keuntungan finansial. Jenis ancaman ini pertama kali muncul pada era 1960-an di Amerika dengan berbagai kasus seperti manipulasi transkrip akademik, penyalahgunaan komputer oleh karyawan, hingga pembobolan database bank yang mengakibatkan kerugian besar. *Cyber crime* meliputi aktivitas seperti pencurian identitas (*identity theft*), pembobolan kartu kredit (*carding*), hingga mata-mata siber (*cyber espionage*) yang sering dilakukan oleh sekelompok atau individu ahli menggunakan teknik hacking canggih.

Cyber Warfare, merujuk pada perang di ranah siber yang dilakukan antarnegara, dengan tujuan mengganggu stabilitas dan kedaulatan negara tertentu. *Cyber warfare* memanfaatkan komputer dan internet untuk menyerang objek di *cyberspace*, seperti infrastruktur teknologi, sistem pertahanan, atau komunikasi strategis, yang dikuasai oleh suatu negara. Contoh nyata dari ancaman ini adalah kasus pada tahun 2008 ketika Amerika Serikat merusak sistem sentrifugal di Pembangkit Listrik Tenaga Nuklir milik Iran. Ancaman ini tidak hanya berbahaya bagi keamanan nasional tetapi juga berpotensi untuk merusak hubungan antarnegara.

Cyber Terrorism, melibatkan jaringan atau kelompok teroris yang menggunakan internet untuk menciptakan ketakutan dan kepanikan di masyarakat. Ancaman ini ditujukan untuk menyerang keamanan sosial, politik, dan ekonomi suatu negara. Ancaman ini dapat mengguncang stabilitas nasional dan menimbulkan efek domino pada berbagai sektor.

Dalam Peraturan Menteri Pertahanan Republik Indonesia No. 82 Tahun 2014 tentang Pedoman Pertahanan Siber dijelaskan mengenai beberapa bentuk ancaman siber, yaitu:

a. *Advanced Persistent Threats* (APT), *Denial of Service* (DoS), dan *Distributed Denial of Service* (DDoD)
   Serangan ini bertujuan untuk membebani kapasitas sistem sehingga mencegah pengguna sah untuk mengakses layanan. Akibatnya, sistem menjadi *crash* dan tidak dapat beroperasi. Ancaman ini sangat berbahaya bagi organisasi yang sangat bergantung pada internet untuk menjalankan aktivitasnya
b. *Defacement*
   Serangan ini dilakukan dengan mengubah atau memodifikasi halaman web sehingga isi web berubah sesuai dengan motif penyerang.
c. *Phising*
   Penyerang dalam serangan ini membuat situs web palsu yang menyerupai situs asli untuk mencuri informasi sensitif, seperti *username*, *password*, atau data pribadi lainnya.
d. *Malware*
   Merupakan program berbahaya yang mengganggu operasi sistem komputer. Tujuannya dapat berupa keuntungan finansial atau lainnya. Jenis *malware* yang umum terjadi mencakup virus, *ransomware*, *spyware*, dan trojan. Serangan ini sering menyebar melalui perangkat lunak berbahaya atau spam.
e. Penyusupan siber
   Serangan ini dilakukan dengan berbagai metode untuk mendapatkan akses ilegal ke sistem, seperti menebak *password*, menggunakan akun yang tidak terlindungi, rekayasa sosial atau berpura-pura menjadi administrator untuk meminta data pribadi, penyadapan komunikasi yang tidak terenkripsi, menggunakan program palsu untuk mencuri kredensial pengguna, serangan *brute force* atau serangan kamus untuk memecahkan *password* yang terenkripsi, serta pemantauan aktivitas menggunakan *spyware* untuk merekam parameter koneksi pengguna.
f. Spam
   Merupakan pengiriman email massal yang tidak diinginkan dengan tujuan seperti promosi komersial, Penyebaran *malware*, virus, atau upaya *phishing*
g. Penyalahgunaan Protokol Komunikasi

Penyerang memanfaatkan kelemahan protokol komunikasi seperti *Transmission Control Protocol* (TCP). Salah satu contohnya adalah serangan *spoofing* nomor port TCP, yang memungkinkan penyerang melewati *firewall* untuk membuat koneksi antara sistem target dan penyerang.

Ancaman siber semakin meningkat dengan munculnya pandemi COVID-19. Dengan adanya pandemi tersebut, mengharuskan masyarakat di seluruh dunia untuk beradaptasi dengan cara-cara baru dalam bekerja, belajar, dan berinteraksi dimana masyarakat melakukan hal-hal tersebut secara *online* yang akhirnya menyebabkan ketergantungan yang lebih besar pada teknologi dan platform digital. Akibatnya, serangan siber semakin meningkat secara signifikan karena para pelaku serangan ini memanfaatkan perubahan perilaku tersebut untuk mengeksploitasi kerentanan data pribadi masyarakat. Dalam masa pandemi setidaknya terdapat lima ancaman siber yang terjadi menurut (Silalahi, 2022):

1. *Malicious Domains*
   Dalam laporan Palo Alto Networks, tercatat bahwa domain baru mengenai 'COVID' dan 'corona' meningkat sejumlah 2.022 domain berbahaya dan 40.261 domain beresiko tinggi per Maret 2020
2. Penipuan *online* dan *phishing*
   Pelaku serangan ini menciptakan situs web mengenai COVID-19 dimana situs web tersebut adalah palsu dengan tujuan menjerat para korban agar mereka membuka *link phishing.*
3. *Data-harvesting Malware*
   Beberapa bentuk *malware* penyimpanan yang berkaitan dengan COVID-19 menyebar serta masuk ke sistem elektronik untuk mencuri data, mendapatkan keuntungan, serta membangun *botnet.*
4. *Ransomware* dan DDoS
   Infrastruktur medis seperti rumah sakit dan pusat-pusat kesehatan menjadi target serangan *ransomware* oleh para pelaku serangan dengan tujuan untuk mengganggu pekerjaan para tenaga medis dan meminta tebusan.
5. Kerentanan bekerja dari rumah
   Para pelaku serangan memanfaatkan perubahan sistem kerja masyarakat yang dilakukan secara *online* dimana mereka mengeksploitasi kerentanan sistem *online* dan kelemahan masyarakat sebagai pengguna layanan *online* untuk bekerja.

Peran Aktor Non-Negara dalam Menghadapi Ancaman Keamanan Siber

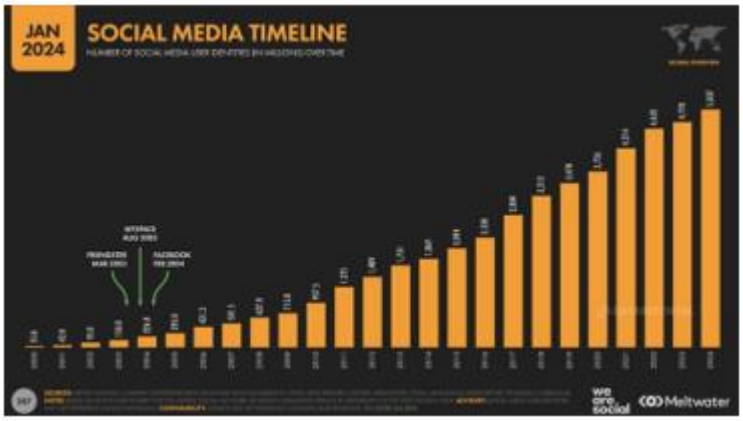
Berkembangnya konsep keamanan non-tradisional yang meliputi ancaman terhadap sektor non-militer seperti keamanan siber, peran aktor yang terlibat menjadi lebih beragam. Keamanan siber kini menjadi perhatian utama tidak hanya bagi negara, tetapi juga bagi berbagai aktor non-negara. Munculnya peran aktor non-negara dalam keamanan siber juga didorong oleh faktor lain dimana ancaman siber di dunia digital juga tidak hanya mengancam infrastruktur negara, tetapi juga mengancam kesejahteraan dan keamanan hidup masyarakat luas. Hal tersebut diakibatkan oleh semakin bergantungnya masyarakat pada teknologi digital.

Neoliberalisme memiliki pandangan dalam politik internasional yang percaya bahwa hubungan antarnengara tidak hanya ditentukan oleh kekuatan militer, tetapi juga oleh aturan dan norma internasional. Pendekatan ini mengakui bahwa dunia menjadi lebih beragam karena berbagai aktor, termasuk aktor-aktor non-negara seperti organisasi internasional, perusahaan transnasional, serta Lembaga Swadaya Masyarakat (LSM). Neoliberalisme menyetejui bahwa dunia internasional tidak memiliki "pemerintah pusat"

yang mengatur seluruh negara atau yang disebut anarki. Paradigma neoliberalisme percaya bahwa kondisi anarki tidak selalu buruk dimana kondisi tersebut dapat menjadi media bagi negara-negara untuk dapat bekerja sama dalam mencapai tujuan bersama. Dalam perspektif ini, para aktor non-negara dapat memberikan informasi serta pengaruh politik yang dapat membantu negara dalam membuat kebijakan luar negeri yang lebih baik (Anggraini & Widarjo, 2020).

Dari penjelasan tersebut dapat dilihat bahwa perspektif neoliberalisme menganggap penting peran aktor non-negara dalam menghadapi ancaman keamanan siber. Organisasi internasional dapat berperan dalam memfasilitasi kerjasama antarnegara untuk berbagi informasi mengenai kejahatan siber. Selain itu, perusahaan transnasional yang bergerak di bidang teknologi seperti perusahaan penyedia layanan internet dan perangkat lunak dapat memberikan bantuan berupa keahlian untuk membantu negara dalam mengidentifikasi dan mencegah serangan siber. Seperti yang terlihat dalam kemitraan antara Badan Siber dan Sandi Negara (BSSN) dengan perusahaan teknologi global, Microsoft. Sebagai perusahaan yang telah lama berpengalaman dalam industri siber, Microsoft memberikan dukungan serta bantuan dalam memperkuat pertahanan siber Indonesia. Peran aktor non-negara ini mencakup penyediaan intelijen ancamann siber melalui program *Cyber Threat Intelligence Program* (CTIP) yang memungkinkan BSSN untuk mendapatkan informasi ancaman siber serta data *feeds* terkait infeksi *malware* dan infratsruktur yang terkompromi.

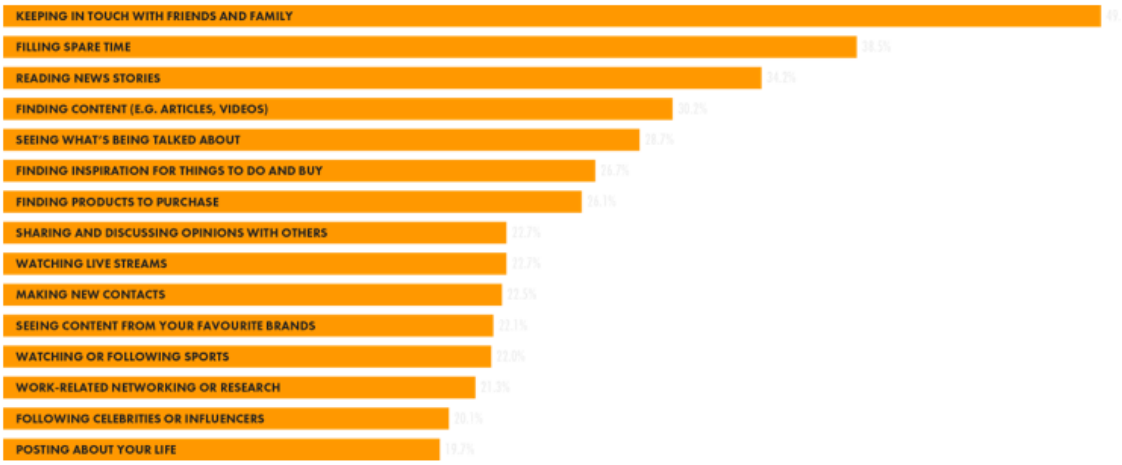
LSM serta organisasi non-negara juga memainkan penting dalam mengedukasi publik tentang resiko ancaman keamanan siber kepada masyarakat serta mengadvokasi kebijakan yang dapat meningkatkan kesadaran masyarakat serta perlindungan terhadap ancaman keamanan siber yang ada. LSM dan organisasi dapat memanfaatkan perkembangan media sosial yang juga mengalami peningkatan akibat perkembangan internet.



Gambar 4. Perkembangan Media Sosial
Source: We Are Social (2024)

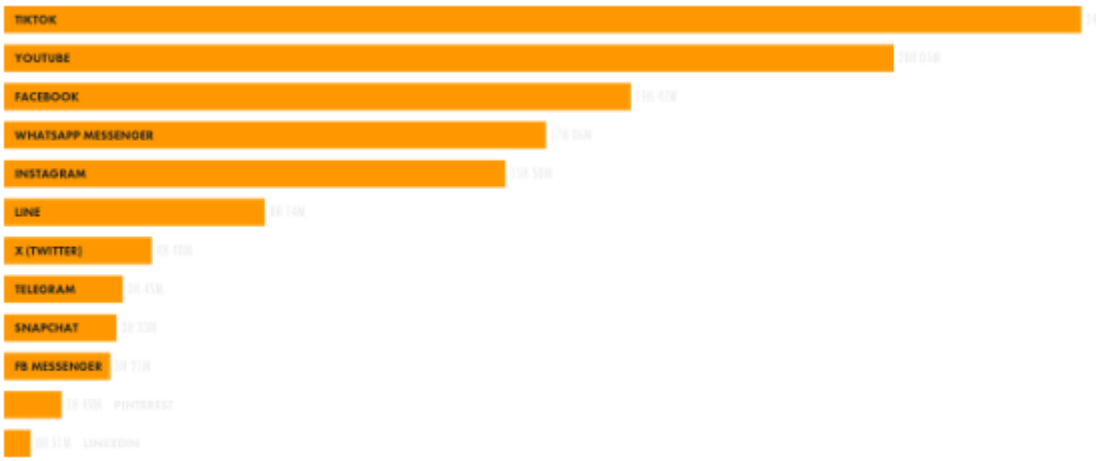
Berdasarkan laporan data yang dikeluarkan oleh We Are Social per Januari 2024, tercatat bahwa sebanyak 5,04 miliar penduduk global aktif menggunakan media sosial. kehadiran media sosial mulai berkemmbang sejak tahun 2004 dimana media sosial

Facebook menjadi pelopornya. Seiring berjalannya waktu, jumlah pengguna media sosial semakin meningkat.



Gambar 5. Pengguna Aktif
Source: We Are Social (2024)

Dari data diatas dapat dilihat bahwa 49,5% dari total 5,04 miliar pengguna aktif media sosial menggunakan waktunya untuk berkomunikasi dengan kerabatnya dalam media sosial. sebanyak 38,5% dari total pengguna menggunakan waktunya dalam media sosial untuk mengisi waktu luang. Sedangkan 30,2% menggunakan media sosialnya untuk membaca berita.



Gambar 6. Pengguna Media Sosial
Source: We Are Social (2024)

Dari sejumlah media sosial yang ada, dalam data diatas dapat dilihat bahwa TikTok, Youtube, dan Facebook menempati posisi media sosial yang paling banyak dipakai oleh para pengguna. Rata-rata pengguna media sosial menghabiskan waktu sebanyak 34 jam untuk menggunakan media sosial TikTok, 28 jam 5 menit untuk menggunakan Youtube, dan 19 jam 47 menit untuk menggunakan Facebook. Artinya,

mayoritas waktu yang dimiliki para pengguna dihabiskan untuk menggunakan ketiga media sosial tersebut.

Dari data tersebut dapat dilihat bahwa media sosial memiliki potensi besar untuk mengedukasi dan mengadvokasi masyarakat luas mengenai keamanan siber. Dengan 5,04 miliar pengguna aktif media sosial di seluruh dunia, platform-platform seperti TikTok, Youtube, dan Facebook dapat menjadi saluran yang cukup efektif bagi aktor non-negara khususnya Organisasi Internasional dan LSM untuk mennyampaikan pesan-pesan terkait keamanan siber. LSM serta organisasi internasional dapat bekerja sama dengan media untuk menyebarkan informasi-informasi mengenai tren ancaman siber serta langkah-langkah mitigasi yang harus diambil oleh individu maupun komunitas.

KESIMPULAN

Dari pembahasan di atas, dapat disimpulkan bahwa ancaman keamanan siber merupakan isu global yang semakin meningkat seiring dengan berkembangnya teknologi dan internet. Dengan meningkatnya jumlah pengguna internet yang kini mencapai lebih dari 5 miliar, bentuk ancaman siber seperti *cyber crime*, *cyber warfare*, *dan cyber terrorism* semakin beragam dan kompleks. Ancaman ini tidak hanya mengancam infrastruktur negara, tetapi juga kesejahteraan dan kehidupan masyarakat di seluruh dunia. Sehingga keamanan siber menjadi salah satu aspek penting yang harus diperhatikan dalam menjaga stabilitas nasional.

Peran aktor non-negara, seperti organisasi internasional, perusahaan transnasional, dan Lembaga Swadaya Masyarakat (LSM), semakin penting dalam menghadapi ancaman siber. Aktor-aktor tersebut dapat memanfaatkan perkembangan media sosial yang pesat untuk mengedukasi masyarakat mengenai resiko ancaman siber serta langkah mitigasi yang dapat dilakukan. Dengan 5,04 miliar pengguna aktif media sosial, platform seperti TikTok, Youtube, serta Facebook dapat menjadi saluran yang efektif untuk menyebarkan informasi dan meningkatkan kesadaran masyarakat akan pentingnya keamanan siber.

Dalam menghadapi ancaman keamanan siber yang semakin kompleks, kolaborasi antara aktor negara dan aktor non-negara harus ditingkatkan. Kerjasama ini tentunya penting dalam pengembangan kebijakan untuk melawan serangan siber. Dengan adanya kerjasama dari para aktor non-negara yang mampu *me-reach out* masyarakat lebih dalam, maka upaya-upaya yang dilakukan oleh para aktor negara akan semakin efektif. Selain itu, pemanfaatan media sosial sebagai platform edukasi mengenai keamanan strategis juga harus lebih digembor, karena hal tersebut merupakan salah satu langkah strategis dalam menjaga keamanan siber. Informasi yang disebarkan melalui media sosial ini dapat dilakukan melalui konten yang menarik dan mudah untuk dipahami, guna meningkatkan kesadaran masyarakat tentang ancaman siber dan langkah mitigasi nya. Dengan upaya-upaya tersebut, diharapkann masyarakat dapat lebih siap dalam menghadapi tantangan yang ditimbulkan akibat perkembangan teknologi digital.

BIBLIOGRAFI

Aji, Muhammad Prakoso. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238.

Alimin, Fahira, & Islami, Adelia Nurul. (2022). *Teknologi Digital dalam Komunikasi*. OSF Preprints.

Anggraini, Yety, & Widarjo, Wahyu. (2020). Political connection, institutional ownership and tax aggressiveness in Indonesia. *European Journal of Business and Management Research*, *5*(5). https://doi.org/10.24018/ejbmr.2020.5.5.528

Barisione, Mauro, & Michailidou, Asimina. (2017). *Social media and European politics: Rethinking power and legitimacy in the digital era*. Springer.

Ginanjar, Yusep. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui Badan Siber dan Sandi Negara. *Dinamika Global: Jurnal Ilmu Hubungan Internasional*, *7*(02), 295–316.

Indah, Febyola, Sidabutar, Arista Quera, & Nasution, Nurul Annisa. (2023). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 57–64.

Indarta, Yose, Ranuharja, Fadhli, Ashari, Ilham Firman, Sihotang, Jay Idoan, Simarmata, Janner, Harmayani, Harmayani, Algifari, M. Habib, Muslihi, Muhammad Takdir, Mahmudi, A. Aviv, & Fatkhudin, Aslam. (2022). *Keamanan Siber: Tantangan di Era Revolusi Industri 4.0*. Medan: Yayasan Kita Menulis.

Maskun, S. H. (2022). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media.

Nasional, Pusat Operasi Keamanan Siber. (2021). Laporan Tahunan Hasil Monitoring Keamanan Siber 2020. *Buletin Jendela Data Dan Informasi Kesehatan*.

Rahmawati, Ineu. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan Dan Bela Negara*, *7*(2), 35–50.

Rosy, Afifah Fidina. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber: Indonesia's International Cooperation: Strengthening National Security in the Field of Cyber Security. *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan*, *1*(2), 118–129.

Silalahi, Fujiama Diapoldo. (2022). Keamanan Cyber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–285.

Trihartono, Agus, Indriastuti, Suryani, & Nisya, Chairun. (2020). *Keamanan dan Sekuritisasi dalam Hubungan Internasional*.

Yanuar, A. P. (2021). Cyber War : Ancaman Baru Keamanan Nasional dan Internasional. Jurnal Keamanan Nasional, 7(1), 23-35.

We Are Social. (2024, Januari 31). Digital 2024: 5 billion social media users. Retrieved from wearesocial.com: https://wearesocial.com/id/blog/2024/01/digital-2024-5-billion-social-media-users/

Copyright holder:
Serly Sintia Saramuke, Vianna Antoneta Putri, Agnes Marianti Sormin, Muthia Nugraha (2025)

First publication right:
Syntax Idea

This article is licensed under:

