Strategi Penguatan *Cyber Security* Guna Mewujudkan Keamanan Nasional di Era *Society 5.0*

(Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0)

Eko Budi[1*], Dwi Wira[2], Ardian Infantono[3]

[1,2] Prodi Ilmu Kepolisian, Akademi Kepolisian, Semarang
E-mail: ekobudi76120885@gmail.com, wira712017@gmail.com
[3] Prodi Teknik Aeronautika Pertahanan, Akademi Angkatan Udara, Yogyakarta
E-mail: ardian.infantono@aau.ac.id

Abstract— ***The concept of Society 5.0 is human-centered and technology-based. Where the main drivers of industry are technology and modern society. In the era of technology and information growing rapidly, it has an impact on all aspects of life. One of them is the security aspect in the form of cyber crime threats. Therefore, cyber security has a vital role to prevent the occurrence of cyber crime. The purpose of this study is to obtain an overview of cyber crime and its challenges in the future, cyber security strategies in Indonesia and strengthening cyber security in Indonesia in order to realize national security in the era of society 5.0. The research method used is a qualitative and descriptive analytical approach with data collection techniques using literature studies from previous studies and other secondary data. The result of this study is that the Covid-19 pandemic is the main topic in cybersecurity trends. Hackers took advantage of public unrest as a loophole to launch various attacks, ranging from phishing to ransomware, the data leak of 91 million users of the online shopping site Tokopedia and the data leak of 1.2 million users of the Bhinneka site. Indonesia has also been affected by global cybersecurity cases such as Coronavirus Ransomware, Covidlock Malware, Border Gateway Protocol hacking, vulnerabilities in Draytek Vigor router products, Remote Code Execution on several versions of Windows operating system products, vulnerabilities in Arbitrary Code Execution on all Google Android operating systems, to exploitation of Solar Winds Orion Platform products. The conclusion is that currently Indonesia is in a state of cyber security emergency and has reached an alarming stage. Cyber security strategies that must be carried out by Indonesia to realize national security in the era of society 5.0, are 1) capacity building, 2) Formation of special laws on cyber crimes, 3) Increasing human resources, 4) Domestic stakeholder cooperation and international cooperation cyber security sector to realize national security in society 5.0.***

Keywords— **Strategy, cyber security, cyber crime, society 5.0**

Abstrak**—** ***Konsep Society 5.0 berpusat pada manusia dan berbasis teknologi. Dimana penggerak utama industri adalah teknologi dan masyarakat modern. Di era teknologi dan informasi berkembang dengan pesat memiliki dampak terhadap seluruh aspek kehidupan. Salah satunya adalah aspek keamanan berupa ancaman cyber crime. Oleh karena itu cyber security mempunyai peran vital untuk mencegah terjadinya cyber crime. Tujuan dari penelitian ini adalah untuk memperoleh gambaran tentang cyber crime dan tantangannya kedepan, strategi cyber security di Indonesia serta penguatan cyber security di Indonesia dalam rangka mewujudkan keamanan nasional di era society 5.0. Metode penelitian yang digunakan adalah pendekatan kualitatif dan deskriptif analitis dengan teknik pengumpulan data menggunakan studi pustaka dari penelitian sebelumnya dan data sekunder***

**Penulis Korespondensi (Eko Budi)*
E-mail: ekobudi76120885@gmail.com

p-ISSN 2086-5805
e-ISSN 2808-2540

lainnya. Hasil dari penelitian ini adalah pandemi Covid-19 menjadi topik utama dalam tren keamanan siber. Para peretas memanfaatkan keresahan masyarakat sebagai celah dalam meluncurkan berbagai serangan, mulai dari phishing hingga ransomware, kasus kebocoran data 91 juta pengguna situs belanja online Tokopedia dan kebocoran data 1,2 juta pengguna situs Bhinneka. Indonesia pun terdampak oleh kasus keamanan siber global seperti Coronavirus Ransomware, Covidlock Malware, peretasan Border Gateway Protocol, kerentanan pada produk router Draytek Vigor, adanya Remote Code Execution pada beberapa versi produk sistem operasi Windows, kerentanan terjadinya Arbitrary Code Execution pada seluruh sistem operasi Google Android, hingga eksploitasi produk Solar Winds Orion Platform. Kesimpulannya adalah saat ini Indonesia tengah dalam keadaan darurat cyber security dan sudah mencapai tahap memprihatinkan. Strategi cyber security yang harus dilakukan Indonesia untuk mewujudkan keamanan nasional di era society 5.0, adalah 1) capacity building, 2) Pembentukan undang-undang khusus tentang tindak pidana siber, 3) Peningkatan sumberdaya manusia, 4) Kerjasama stakeholder di dalam negeri dan kerjasama internasional bidang cyber security untuk mewujudkan keamanan nasional di era society 5.0.

Kata Kunci— **Strategy, cyber security, cyber crime, society 5.0**

I. PENDAHULUAN

Society 5.0 lahir sebagai solusi dari Revolusi 4.0 yang ditakutkan akan mendegradasi umat manusia dan karakter manusia. Di era Society 5.0 ini nilai karakter harus dikembangkan, empati dan toleransi harus dipupuk seiring dengan perkembangan kompetensi yang berfikir kritis, inovatif, dan kreatif. Society 5.0 bertujuan untuk mengintegrasikan ruang maya dan ruang fisik menjadi satu sehingga semua hal menjadi mudah dengan dilengkapi *artificial intelegent.* Pada Era Society 5.0 pekerjaan dan aktivitas manusia akan difokuskan pada *human centered* yang berbasis pada teknologi. Namun, jika manusia tidak mengikuti perkembangan teknologi dan pengetahuan maka Society 5.0 masih sama saja dengan era disrupsi yang seperti pisau bermata dua. Pada satu sisi dapat menghilangkan lapangan kerja yang telah ada, namun juga mampu menciptakan lapangan kerja baru serta menimbulkan dampak lainnya, yaitu berupa kejahatan di dunia maya akibat perkembangan teknologi yang semakin tidak terbendung.

Saat keprihatinan melanda dunia akibat pandemi COVID-19, para *threat actor* justru seperti memperoleh durian runtuh. Tak disangka-sangka, ada peluang-peluang baru untuk melancarkan ancaman-ancaman maya, baik kepada pengguna individu, perusahaan, maupun institusi pemerintahan. Di sisi user, pandemi telah mengaburkan batas antara kerja dan kehidupan pribadi. Sementara perusahaan harus menghadapi cara kerja *hybrid* di saat bisnis juga tengah berupaya mempercepat melakukan migrasi ke *cloud.* Dan pemerintah di berbagai negara di dunia pun dipusingkan oleh urusan data dan privasi, terutama terkait aktivitas *tracing* dalam upaya menangani COVID-19.

Dalam beberapa dekade terakhir ini, perkembangan teknologi informasi dan komunikasi secara positif telah berkontribusi terhadap perkembangan ekonomi global dan berdampak pada produktivitas, persaingan, dan keterlibatan warga negara yang lebih tinggi. Akan tetapi, karena pihak pemerintah, pengusaha, dan masyarakat kini jauh lebih terkoneksi di dunia maya, beberapa tantangan terkait ancaman dunia maya membutuhkan lebih banyak perhatian untuk mengembangkan keamanan dunia maya *(cyber security)* yang lebih kuat. Menurut ISO *(International Organization for Standardization),* ISO/IEC 27032 mengutip dari sejumlah sumber, *cyber security* atau *cyberspace security* adalah preservasi dari kerahasiaan, integritas, dan ketersediaan informasi di *cyberspace* [1]. Adapun *cyberspace* merujuk pada lingkungan yang kompleks dan merupakan hasil dari interaksi antara orang, peranti lunak, dan layanan-layanan internet melalui penggunaan aneka perangkat teknologi dan berbagai koneksi jaringan dan lingkungan yang tidak memiliki wujud.

Sementara menurut Kaspersky, *cyber security* adalah suatu praktik melindungi para komputer, server, perangkat mobile, sistem elektronik, jaringan, dan data dari serangan-serangan jahat [2]. Begitu pula *Cisco* yang mendefinisikan *cyber security* sebagai praktik

melindungi berbagai sistem, jaringan, dan program dari serangan-serangan digital [3]. Jadi, *cyber security* atau keamanan siber merupakan tindakan untuk melindungi informasi di dunia maya dari aneka serangan. *Cyber security* makin populer berhubung makin banyaknya penggunaan komputer seperti desktop, laptop, smartphone, server, dan perangkat IoT *(internet of things)* serta penggunaan jaringan komputer seperti internet dalam kehidupan umat manusia sehari-hari.

Menurut World Bank dalam infokomputer oleh cakrawala, berdasarkan data ITU *(International Telecommunication Union)*, misalnya porsi pengguna internet di dunia adalah sekitar 49% populasi pada tahun 2017. Porsi tersebut meningkat pesat dibandingkan tahun 2000 yang hanya sekitar 6,7%. Serupa halnya menurut *Internet World Stats* yang memperkirakan porsi pengguna internet di dunia adalah sebesar 64,2% populasi pada kuartal pertama tahun 2021. Adapun jumlah pengguna internet yang diperkirakan itu adalah sebanyak lebih dari 5 miliar. Jumlah tersebut meningkat sekitar 1.300% dibandingkan tahun 2000.

Tak hanya itu, jumlah serangan juga meningkat. Menurut Deep Instinct misalnya, jumlah *cyber attack* atau serangan siber menggunakan *malware* mengalami peningkatan sebesar 358% pada tahun 2020 dibandingkan tahun 2019. Sementara, khusus *ransomware*, peningkatannya sebanyak 435% pada tahun 2020 dibandingkan tahun sebelumnya. Adapun besarnya peningkatan yang disebutkan Deep Instinct tersebut berdasarkan basis data Deep Instinct yang menerima data dari berbagai sumber, termasuk pihak ketiga dan yang didapatkan dari konsumen Deep Instinct. Data yang dikumpulkan pun diklaim merefleksikan ratusan juta kejadian pada tahun 2020.

Secara nasional, menurut Hasyim Gautama terdapat sejumlah permasalahan terkait dengan strategi penguatan *cyber security* di antaranya: 1) Lemahnya pemahaman penyelenggara negara atas security terkait dengan dunia cyber yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya penggunaan *secured system*, 2) Legalitas penanganan penyerangan di dunia siber, 3) Pola kejadian *cyber crime* sangat cepat sehingga sulit ditangani, 4) Tata kelola kelembagaan *cyber security* nasional masih terbatas, 5) Rendahnya awareness atau kesadaran akan adanya ancaman *cyber attack* internasional yang dapat melumpuhkan infrastruktur vital suatu negara dan 6) Masih lemahnya industri dalam negeri untuk memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi informasi yang merupakan celah yang dapat memperkuat maupun memperlemah keamanan dalam dunia siber [4].

Untuk di Indonesia, menurut BSSN (Badan Siber dan Sandi Negara) menyatakan sepanjang bulan Januari sampai Agustus tahun lalu, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibandingkan periode yang sama pada tahun 2019 yang sekitar 39 juta. Pada tahun 2021 ini sejumlah pihak menilai pula serangan siber belum akan mereda. Kaspersky misalnya menyebutkan bahwa pandemi COVID-19 bisa membuat munculnya berbagai gelombang kemiskinan yang kemungkinan meningkatkan kejahatan, termasuk melakukan *cyber attack.*

Indonesia sangat membutuhkan strategi keamanan siber nasional era *society 5.0* saat ini. Jika suatu keamanan sebagai kebebasan dari ancaman atau bahaya, salah satu pendorong yang terpenting dalam mengelola *cyber security* adalah bagaimana ancaman dipahami dalam ruang siber kemudian dicari solusinya. Tanpa upaya *cyber security* yang tepat, kemungkinan ancaman akan meningkat.

Tantangan terbesar saat ini adalah penguatan kelembagaan *cyber security*, ketidakadaan dasar hukum untuk keamanan siber dan kurangnya tenaga professional serta kerjasama di dalam negeri maupun dengan dunia internasional. Sehingga, menjadi penting bagi pemerintah untuk penguatan *cyber security* dan mempersiapkan orang-orang yang dibutuhkan di dunia yang semakin digital. UU Keamanan Siber juga harus disahkan secepat mungkin untuk memulai upaya keamanan nasional Indonesia terhadap peningkatan serangan siber di era *society 5.0* sekarang ini.

p-ISSN 2086-5805
e-ISSN 2808-2540

II. LANDASAN TEORI

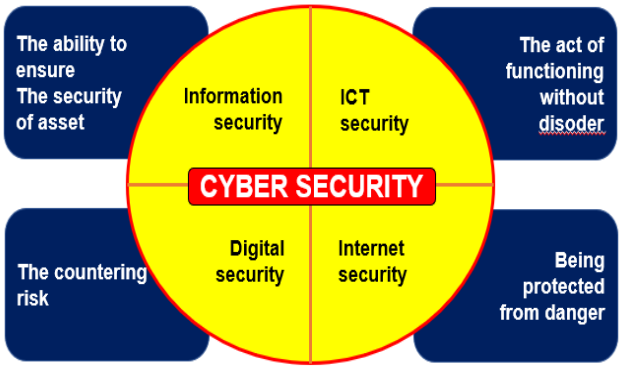
A. Teori Strategi Keamanan

Kajian keamanan telah mengalami perkembangan yang signifikan. Pemahaman konsep keamanan pasca perang dingin tidak lagi sempit sebagai hubungan konflik atau kerjasama antar negara, tetapi juga berpusat pada keamanan untuk masyarakat, kemudian Arnold Wolfers dalam Perwita & Yani mendefinisikan keamanan adalah, *"security, in any objective sense, measures the absence of threats to acquired values and in a subjective sense, the absence of fear that such values will be at tacked*" [5]. Sementara itu, strategi menurut John P. Lovell diartikan sebagai serangkaian langkah-langkah atau keputusan-keputusan yang dirancang sebelumnya dalam situasi kompetititf dimana hasil akhirnya tidak semata-mata bersifat untung-untungan. Strategi adalah cara yang digunakan untuk mencapai suatu tujuan atau kepentingan dengan menggunakan *power* yang tersedia, termasuk juga kekuatan militer [6]. Global *cyber security* menurut Arnold harus dibangun di atas lima bidang kerja: Kepastian Hukum (undang-undang *cyber crime);* teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*).

B. Cyber Security Concept dalam Keamanan Nasional

Ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep *"cyber security"*. Karena *cyber space* merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi [7]. Maka konsep *cyber security* tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional.

Perkembangan teknologi informasi juga telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik tapi juga meluas ke dunia maya. Konsekuensinya, negara harus beradaptasi dengan perkembangan ini, konsep keamanan dunia maya sudah saatnya ditetapkan sebagai salah satu "wilayah" negara yang menjaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan *cyber* tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintah. *Cyber security* ditujukan pada isu keamanan informasi bagi pemerintahan, organisasi dan urusan individual yang dihubungkan dengan teknologi, dan secara khusus dengan teknologi internet. *Cyber security* tidak dapat diabstraksikan terlalu jauh dari wilayah aplikasinya dan lingkungan sosial-kultural, seperti dalam gambar berikut ini:



Gambar 1. Konsep *Cyber Security* [8]

Terminologi "keamanan informasi *(information security)"* dan *cyber security* adalah dua konsep berbeda. Dalam konteks tertentu ada kesamaan pemahaman jika dikaitkan dengan proteksi aset atau perlawanan terhadap spionase industri dan ekonomi, perlawanan terhadap terorisme atau kejahatan ekonomi, perlawanan terhadap konten-konten terlarang.

Dalam konteks lain, dua konsep tadi memiliki perbedaan. *Cyber security* mencakup segala sesuatu berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental. Sedangkan keamanan informasi berhubungan dengan isu-isu yang lebih luas, seperti kedaulatan negara, keamanan nasional, proteksi atas infrastruktur penting, keamanan aset-aset yang terlihat maupun yang tidak terlihat, dan proteksi data personal dan sebagainya.

C. Teori Manajemen Teknologi Informasi

Ada 4 (empat) pondasi utama yang mendukung perkembangan teknologi informasi yaitu: perkembangan perangkat lunak *(software)* seperti sistem dan aplikasi dan perkembangan alat keras (hardware) perkembangan sarana dan prasarana teknologi informasi, manajemen isi *(content management), telecommunication and networking*, perkembangan internet serta perdagangan online atau melalui internet. Sementara untuk pengorganisasian terkait dengan pengunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu: pertama, sistem informasi *(information systems)* dan kedua, kompetisi organisasi *(organizational competition);* ketiga, *information systems* (sistem informasi) dan *organizational decision making* (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan system informasi *(organizational use of information systems).*

D. Teori Cyber Attack

Malware adalah setiap kode komputer yang dapat digunakan untuk mencuri data, melewati kontrol akses, serta menimbulkan bahaya terhadap atau merusak system. Dalam *cyber attack*, selain virus, terdapat beberapa jenis serangan malware antara lain: (1) *Spyware* yang melacak aktivitas, pengumpul penekanan tombol, dan pengambilan data, (2) *Adware* dirancang untuk menampilkan iklan namun juga ditemukan membawa *spyware*, (3) *Bot* yang dirancang otomatis melakukan tindakan tertentu secara online, (4) *Ransomware* yang mengenkripsi data di komputer dengan kunci yang tidak diketahui oleh pengguna [9]. Jenis-jenis malware inilah yang dimanfaatkan sehingga mempengaruhi karakteristik di ruang siber. Menurut Undang-Undang [10], karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar beberapa hal yakni kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan

p-ISSN 2086-5805
e-ISSN 2808-2540

atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja.

III. METODE PENELITIAN

A. Metode Penelitian Yang Digunakan

Penelitian ini menggunakan pendekatan kualitatif yang mengacu pada makna, konsep, definisi, karakteristik, metafora, simbol, dan deskripsi dari suatu hal [11]. Penelitian kualitatif dilakukan melalui pencarian sebuah jawaban dengan memeriksa berbagai pengaturan sosial dan kelompok atau individu di suatu setting sosial.

Dalam hal ini, penelitian kualitatif memahami lingkungan yang diteliti melalui simbol, ritual, struktur sosial, peran sosial, dan sebagainya. Teknik kualitatif di sini memungkinkan peneliti untuk berbagi dalam pemahaman dan persepsi orang lain dan mengeksplorasi bagaimana orang menyusun dan memberi makna pada kehidupan sehari-hari.

B. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah triangulasi, dimana menggunakan kombinasi teknik pengumpulan data secara simultan seperti :

1) Studi Pustaka

Studi Pustaka dilakukan karena banyaknya informasi dan data mengenai Strategi *cyber security*. Hal ini dapat ditelusuri melalui berbagai informasi dalam buku, jurnal ilmiah, koran, majalah, serta sumber informasi dari laman situs/website melalui internet. Studi pustaka menjadi penting dalam menganalisa konsep *strategi cyber security* di Indonesia.

2) Dokumentasi Penelitian.

Teknik ini digunakan untuk menganalisa sumber informasi yang tersedia dari dokumen-dokumen resmi seperti dokumen-dokumen kebijakan mengenai strategi *cyber security* di Indonesia.

IV. HASIL DAN PEMBAHASAN

A. Cyber Crime Dan Tantangannya di Era Society 5.0

1) Cyber Crime di Indonesia

Cyber crime mulai muncul sejak tahun 1988. Pada masa itu, kejahatan ini dikenal dengan sebutan *Cyber Attack*. Waktu itu, pelakunya menciptakan *worm* atau virus untuk menyerang komputer yang mengakibatkan kurang lebih 10 persen komputer di dunia yang terkoneksi internet mengalami mati total [12]. Cyber crime adalah suatu tindakan atau kejadian yang berkaitan dengan teknologi computer, dimana seseorang mendapatkan keuntungan dengan merugikan pihak lain, c*yber crime* juga merupakan kejahatan dunia maya yang dilakukan individu atau sekelompok orang yang menyerang sistem keamanan komputer atau data-data yang ada di dalam komputer. Kejahatan tersebut dilakukan dengan beragam motif, mulai dari kepuasan diri hingga kejahatan yang dapat merugikan ekonomi atau politik.

Adapun contoh *cyber crime* di antaranya, yaitu ancaman *cyber security* seperti rekayasa sosial, eksploitasi kerentanan perangkat lunak, dan serangan jaringan. Jadi secara umum, *cyber crime* adalah perbuatan kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. Dengan kata lain, seseorang memanfaatkan perkembangan teknologi untuk melakukan kejahatan.

Serangan siber (c*yber attacks)* saat ini menjadi momok yang menakutkan bagi sejumlah orang, terutama para pemilik bisnis. Diketahui banyak perusahaan di dunia mengalami kerugian finansial hingga menyentuh angka $1 triliun pada tahun 2020, sebagai dampak dari pandemi virus corona di mana hampir semua perusahaan memberlakukan kebijakan bekerja dari rumah (WFH) yang menyebabkan keamanan digital jadi lebih kendur.

Proyeksi kerugian hingga $945 miliar, dari laporan baru yang dikeluarkan dari Center for Strategic and International Studies (CSIS) dan perusahaan keamanan komputer McAfee, hampir dua kali lipat kerugian moneter dari kejahatan dunia maya yang bernilai $500 miliar pada tahun 2018. Menurut survei yang diadakan oleh Direktorat Tindak Pidana Siber Bareskrim Polri (Dittipidsiber), terdapat 90 juta kasus serangan siber di Indonesia, dan menurut *Financial Services Information Sharing and Analysis Center* (FS-ISAC), Indonesia termasuk dalam daftar negara yang rentan terhadap serangan kejahatan di dunia maya. Indonesia sendiri menduduki posisi ke-9.

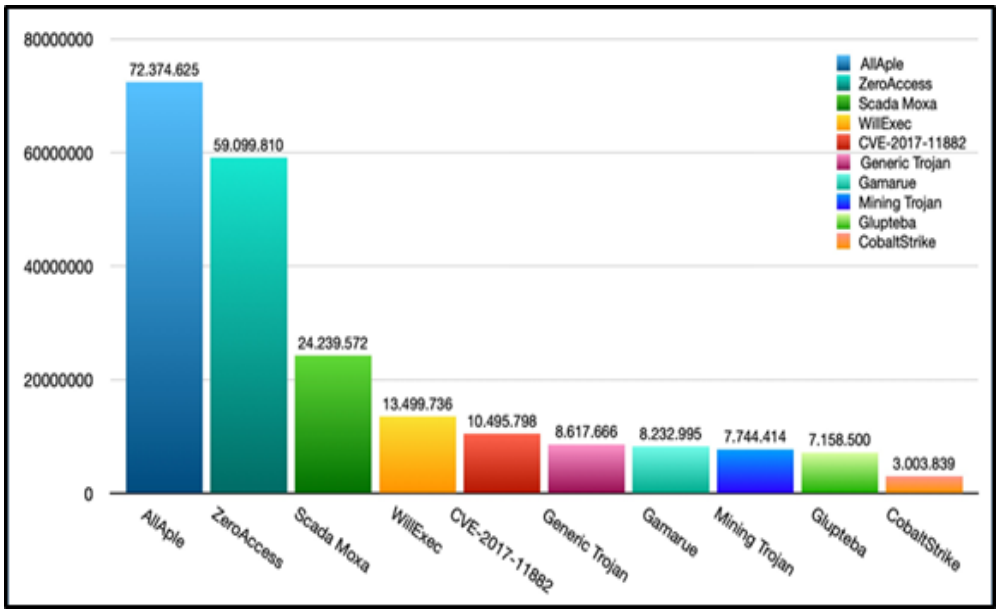
Pandemi Covid-19 menjadi topik utama dalam tren keamanan siber. Para peretas memanfaatkan keresahan masyarakat sebagai celah dalam meluncurkan berbagai serangan, mulai dari phishing hingga ransomware, kasus kebocoran data 91 juta pengguna situs belanja online Tokopedia dan kebocoran data 1,2 juta pengguna situs Bhinneka.

Indonesia pun terdampak oleh kasus keamanan siber global seperti *Coronavirus Ransomware, Covidlock Malware*, peretasan *Border Gateway Protocol*, kerentanan pada produk *router Draytek Vigor*, adanya *Remote Code Execution* pada beberapa versi produk sistem operasi Windows, kerentanan terjadinya *Arbitrary Code Execution* pada seluruh sistem operasi *Google Android*, hingga eksploitasi produk *Solar Winds Orion Platform*.

Masa pandemi juga menjadi sasaran empuk hacker yang terus mencoba menyerobot masuk ke keamanan sistem di perusahaan, karena tingginya penggunaan internet di mana hampir semua orang bekerja dari rumah. Dikutip dari BSSN, serangan paling banyak diterima di bulan Maret 2020, hingga mencapai 22 serangan siber yang menggunakan latar belakang isu pandemi COVID-19, serangan tersebut dengan berbagai jenis serangan diantaranya *Trojan HawkEye Reborn, Blackwater malware, BlackNET RAT, DanaBot Banking Trojan, Spynote RAT, ransomware Netwalker, Cerberus Banking Trojan, malware Ursnif, Adobot Spyware, Trojan Downloader Metasploit, Projectspy Spyware, Anubis Banking Trojan, Adware, Hidden Ad (Android), AhMyth Spyware, Metasploit, Xerxes Bot, dan Covid19 Tracker Apps.*

Pusopskamsinas BSSN melakukan monitoring anomali trafik serangan cyber terhadap Indonesia selama 7/24 jam. Berdasarkah statistik hasil monitoring yang dilakukan mulai 1 Januari 2020 pukul 00:00:00 hingga 31 Desember 2020, diperoleh hasil 495.337.202 anomaly, trafik anomaly tertinggi terjadi pada tanggal 10 Desember 2020 dengan jumlah mencapai 7.311.606 anomali. Anomali trafik tersebut dapat dilihat pada Gambar 2 berikut ini:

p-ISSN 2086-5805
e-ISSN 2808-2540



Gambar 2. Grafik 10 Top Anomaly selama tahun 2020 [13].

Trojan menjadi anomali dengan jumlah tertinggi berdasarkan hasil monitoring Pusopskamsinas BSSN selama tahun 2020. *AllAple, ZeroAccess, WillExec, Glupteba,* dan *CobaltStrike* juga merupakan malware jenis trojan. Trojan merupakan perangkat lunak berbahaya yang dapat merusak sebuah sistem atau jaringan. Berbeda dengan virus ataupun worm, trojan bersifat tidak terlihat, dan seringkali menyerupai program, atau file yang wajar, seperti *file.mp3*, software gratis, antivirus palsu, atau game gratis. Tujuan trojan adalah memperoleh informasi dari target, seperti: *password, log data, kredensial,* dan lainnya tanpa sepengetahuan korban.

Win.Trojan.Allaple merupakan sebuah trojan yang memungkinkan penyerang untuk mengunduh dan mengeksekusi *arbitrary file*, termasuk malware tambahan. Malware ini secara eksklusif dapat dikaitkan dengan *malware family* dari *Net-worm:W32/Allaple. Malware Allaple* adalah jenis *polymorphic malware* yang dirancang untuk menyebar melalui *Local Area Network* (LAN) dan Internet.

Malware ini mencari file dengan ekstensi *.htm/.html*, dan mengunduh alamat e-mail dari file ini. Alamat e-mail yang diambil akan dikirim ke situs milik malicious user. Malware ini juga dapat mengunduh file dari Internet dan meluncurkannya untuk dieksekusi pada komputer milik korban. Malware ini dapat mengakibatkan terjadinya *Denial-of-Service* (DOS) pada sistem korban meskipun eksplotasi tidak sepenuhnya berhasil.

Menurut penelitian yang dilakukan oleh Frost dan Sullivan yang diinisiasikan Microsoft pada tahun 2018, *cyber crime* telah menyebabkan kerugian sebanyak kira-kira 478,8 triliun rupiah atau sebanyak 34,2 milyar US dolar [14]. Hal ini terjadi sebelum pandemi. Pratama Persadha, seorang ahli keamanan siber, telah memprediksi bahwa defisit global akibat serangan siber mungkin akan mencapai 84 ribu triliun rupiah atau sebesar 6 triliun US dolar [15]. Fakta-fakta ini memperlihatkan betapa daruratnya kebutuhan Indonesia akan strategi keamanan siber untuk mewujudkan keamanan nasional di era society 5.0 saat ini.

2) Tantangan Cyber Security di Era Society 5.0

Upaya untuk meningkatkan komitmen dunia terhadap keamanan siber telah dilakukan dengan pemeringkatan Indeks Keamanan Siber Global *(Global Cybersecurity Index*-GCI) oleh Perserikatan Telekomunikasi Internasional (*International Telecommunication Union*-ITU) terhadap 193 negara anggotanya. Peringkat tersebut diberikan dengan dasar 5 pilar, yaitu: 1)

legal/hukum, 2) teknis dan prosedur, 3) struktur organisasi, 4) pembangunan kapasitas, dan 5) kerja sama internasional. Berdasarkan penilaian GCI pada tahun 2020, Indonesia berada di peringkat 77 dari 193 anggota [16]. Hal yang patut dikhawatirkan dari laporan GCI adalah fakta bahwa pengembangan kebijakan keamanan siber di Indonesia berada di angka 0% saat dikonsiderasikan dengan betapa banyaknya serangan siber yang diderita Indonesia selama 5 tahun terakhir.

Tantangan pemerintah di era society 5.0 saat ini dalam penguatan *cyber security* antara lain: tidak cukup tersedianya ahli teknologi dan ahli teknis keamanan untuk merancang dan melaksanakan strategi *cyber security*. Risiko yang terjadi akibat sifat *cyber security* yang lintas-negara, yang membuat negara dengan strategi ketahanan *cyber security* yang lemah dapat mengganggu cybersecurity negara-negara lainnya. Penggunaan alat anonimisasi, misalnya untuk memblokir *chain currencies* atau enkripsi, dalam kejahatan yang menggunakan internet, semakin mempersulit pembuatan kebijakan.

Selalu munculnya teknologi dan sistem baru dari waktu ke waktu memerlukan pemutakhiran sistem pengawasan dilakukan secara berkala. Adanya penyedia layanan komunikasi jenis baru yang seringkali berdomisili di yurisdiksi negara lain serta memerlukan perlakuan berbeda dibandingkan dengan perusahaan telekomunikasi tradisional. Bentuk *cyber crime* baru seperti *ransomware*, pencurian identitas, pendekatan seksual *(grooming)* dan pelecehan seksual melalui ranah siber. Kebutuhan untuk menghadapi *cyber attack* dan bentuk konflik antarnegara lain akibat tidak adanya norma dan peraturan yang berlaku internasional yang mengatur perilaku negara.

Sedangkan tantangan bagi sektor swasta dan bisnis adalah kesulitan untuk beroperasi lintas yurisdiksi, yang berarti dihadapkan pada hukum, penalti maupun rezim regulasi yang berbeda-beda. Berpotensi terkena pencemaran nama baik serius serta gugatan perdata jika terlibat atau bertanggung jawab atas suatu insiden *cyber security*. Tekanan untuk membantu pemerintah dalam menegakkan *cyber security* serta melawan *cybercrime* dan terorisme, yang dapat mencakup pembuatan kebijakan dan pelaporan konten, mematikan jaringan, pemblokiran layanan, bahkan mengkompromikan keamanan produk mereka sendiri untuk membantu pengawasan oleh pemerintah. Keharusan membangun kapasitas internal untuk menjaga keamanan informasi dan jaringan. Dan berupa insentif untuk menjaga kerahasiaan data yang dapat menimbulkan risiko dan serangan siber dengan mengatasnamakan privasi data dan potensi pencemaran nama baik

B. Strategi Penguatan Cyber Security di Indonesia

1) Capacity Building

Program pelatihan dan peningkatan keahlian *cyber security* dilakukan dalam koordinasi Tim Kerja Pusat Operasi Dunia Maya *(Cyber Defence Operation Centre)*. Selain itu diperlukan pembinaan sumberdaya manusia tentang arti pentingnya *cyber security* guna meningkatkan pemahaman langkah-langkah preventif dalam menangkal segala *cyber crime*. Menyusun ulang sistem pertahanan yang berbasis pada *cyber defence* dan *cyber security*, yang tentunya memerlukan persiapan yang matang dan sistematis dengan dukungan dari berbagai pihak. Sinergitas dalam menghadapi ancaman cyber merupakan sebuah keniscayaan dan keharusan bagi Indonesia. Dengan sinergitas dan jalinan komunikasi, koordinasi, jaringan, dan kerja sama teknis harus dilakukan untuk membentuk komunitas keamanan siber *(cyber security community)* yang dapat menangkal, mendeteksi, menangkis, dan mencegah secara dini berbagai potensi serangan ancaman cyber sehingga dapat memperkokoh keamanan dan ketahanan Nasional.

Fungsi BSSN saat ini mendapat kritik karena banyaknya tumpang tindih fungsi dengan lembaga-lembaga seperti Kemenkominfo, Unit Kejahatan Siber Polri, dan Pusat Operasi Siber Kementerian Pertahanan. Di masa depan, Indonesia harus mempercepat pengesahan UU Keamanan Siber untuk memberikan dasar hukum. Keberadaan UU tersebut juga dapat mendorong strategi keamanan siber nasional komprehensif yang dapat mendefinisikan fungsi

p-ISSN 2086-5805
e-ISSN 2808-2540

BSSN dengan lebih baik. Untuk itu perlunya penyelarasan strategi *cyber security* dengan transformasi digital menjadi solusi keamanan berlapis. Di lapisan pertama adalah unit kerja, baik tim teknologi informasi maupun tim bisnis. *Security requirement, security awareness*, kemampuan-kemampuan mendesain solusi yang *secure* sambil mendeliver pengalaman yang menyenangkan, Kemudian di lapisan kedua ada tim manajemen risiko dan kepatuhan. Tim ini harus memiliki visibilitas risiko keamanan siber yang komprehensif dan terbarukan untuk kemudian dibahas Bersama. Di lapis tiga adalah tim audit, untuk melihat apakah kontrol yang terkait *cyber security* ini sudah memadai atau belum, apakah perlu perbaikaan. Tim audit ini harus dibekali dengan kapablitas dan pengetahuan yang memadai untuk menghadapi risiko *cyber security* masa kini. Yaitu kemampuan tentang bagaimana cara mengaudit keamanan *cloud, agile development*, dan lain-lain.

Mengingat pentingnya *cyber security*, terdapat kebutuhan mendesak untuk menguatkan lembaga yang bertanggung jawab melakukan upaya koordinasi ketika diperlukan, dengan dukungan penuh dari seluruh pihak yang terlibat. Lembaga koordinasi tersebut harus terdiri dari individu-individu yang memiliki integritas dan kompetensi tinggi. Di tingkat operasional, setiap sektor harus memiliki tim tanggap daruratnya sendiri untuk menangani insiden di sektor mereka, dengan peran dan tanggung jawab masing-masing yang jelas.

2) Pembentukan Undang-Undang Khusus tentang Tindak Pidana Siber

Ketidakadaan dasar hukum keamanan siber mempengaruhi struktur organisasi yang seharusnya meregulasi keamanan siber. Dalam ketidakadaan dasar hukum tersebut, menjadi mustahil untuk melaksanakan praktik keamanan siber yang berskala nasional. Hal ini juga menciptakan kebingungan dalam mengkoordinasi tanggung jawab mengenai keamanan siber itu sendiri.

Rencana Undang-Undang Keamanan Siber saat ini tidak tersedia untuk publik, dengan RUU versi lama saja yang tersedia, namun teks akademik dari RUU tersebut tersedia. Peraturan perundang-undangan di bidang teknologi informasi yang berlaku di Indonesia saat ini belum mengakomodir seluruh tindak pidana siber, sehingga terdapat beberapa kejahatan siber yang saat ini menjadi persoalan terhadap keamanan dan pertahanan (sebagai faktor dalam menjaga keamanan dan kedaulatan negara) belum diatur dalam regulasi nasional.

Perlu adanya regulasi khusus terkait tindak pidana siber di Indonesia. Dalam regulasi khusus ini dirumuskan aturan umum yang akan berlaku untuk semua tidak pidana di bidang teknologi informasi dan komunikasi, tindak pidana yang berkaitan dengan kerahasiaan, keutuhan, dan ketersediaan data atau system komputer/sistem elektronik, pedoman pemidanaan, hukum acara yang mengatur prosedur penyelidikan dan penyidikan di bidang teknologi informasi dan komunikasi, termasuk penggeledahan dan penyitaan alat bukti digital, kerja sama internasional dalam mengatasi tindak pidana siber.

Hal demikian dikarenakan melihat kondisi Indonesia yang rentan akan serangan siber dan terdapat celah hukum dalam menghadapi hal tersebut. Undang-Undang dan peraturan-peraturan yang berkaitan dengan keamanan siber di Indonesia membagi tanggung jawab ke beberapa kementerian dan hal itu dinilai tidak efektif dalam mencegah ancaman dan kejahatan siber. Oleh karena itu, sebuah peraturan yang komprehensif untuk keamanan siber sangat dibutuhkan di Indonesia.

UU Keamanan Siber nantinya harus dengan jelas mendefinisikan dan menjabarkan peran, tanggung jawab, dan otoritas lembaga terkait dalam mengatasi ancaman keamanan siber. DPR dan BSSN harus terlibat dalam dialog antara Pemerintah dan Swasta atau *Public-Private Dialogue* (PPD) ketika mendiskusikan RUU ini. PPD terbukti membantu pertukaran informasi dan pengalaman yang relevan, membuat kebijakan yang lebih tepat sasaran dan bisa dilaksanakan dengan baik, serta didukung oleh pemangku kepentingan secara luas.

3) Peningkatan Sumberdaya Manusia

Sumberdaya manusia merupakan satu unsur yang terpenting dalam memastikan terlaksananya *cyber security*, sesuai dengan kebijakan-kebijakan yang ditetapkan. Pengetahuan dan ketrampilan khusus harus dimiliki dan dipelihara sesuai dengan perkembangan kondisi kebutuhan keamanan. Sumber daya manusia diwujudkan dalam bentuk program rekruitmen, pembinaan serta pemisahan yang mengacu pada ketentuan yang berlaku.

Dalam rantai keamanan, manusia kerap menjadi mata rantai terlemah. Sehati-hati apapun, suatu saat manusia sebagai pengguna bisa tergelincir dan melakukan kesalahan. Oleh karena itu *awareness* menjadi sangat penting dalam keamanan siber. Dalam pengelolaan sumber daya manusia, teknologi, serta penelitian dan pengembangan *(Research and Development)* untuk penguatan *cyber security*, Pemerintah dalam hal ini Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi bekerjasama dengan BSSN dan Kementerian Komunikasi dan Informatika harus melakukan upaya terobosan untuk mendidik dan merekrut tenaga profesional keamanan teknologi informasi yang memiliki integritas dan etika yang tidak tercela untuk medukung pengembangan dan menjalankan *cyber security.* Salah satu pendekatan teknis misalnya menerapkan ISO 25010 dalam pengujian aplikasi-aplikasi Android atau yang berbasis website untuk mendukung pemantauan keamanan data dan *interface* yang lebih baik[17] dan penapisan konten pornografi[18] di internet. Dengan perencanaan dan pengujian aplikasi yang tepat maka akan mengurangi potensi disalahgunakannya berbagai aplikasi, informasi, dan pusat data di internet oleh peretas.

4) Kerjasama

Masalah *cyber security* sangat kompleks, untuk itu memerlukan pendekatan multidimensional. Karenanya, untuk meningkatkan tata kelola *cyber security*, pelaksanaan prinsip multi pihak (multi stakeholderism) menjadi sangat penting. Tanpa adanya kerja sama dan kolaborasi di kalangan pemangku kepentingan (dari lembaga layanan publik hingga sektor swasta, akademisi dan masyarakat sipil), *problem solving* isu terkait *cyber security* akan terus menjadi satu dimensi dan tidak lengkap. Diperlukan sebuah mekanisme inklusif yang dapat mengesahkan keputusan sekaligus reflektif dan responsif terhadap kepentingan nasional dan populasi yang terdampak.

Kerjasama internasional sangat diperlukan, terkait dengan pengembangan dan penguatan kapasitas kemampuan *cyber security* baik itu untuk infrastruktur, sarana prasarana maupun dalam pengembangan kemampuan SDM dalam bidang *cyber security* baik bilateral antar dua negara maupun regional ataupun internasional. Peningkatan kerja sama teknologi informasi dan *cyber security* selain itu juga diharapkan mampu membuka peluang bagi pengembangan industri media baru terkait dengan teknologi informasi di Indonesia sebagai salah satu bagian dari pengembangan industri strategis Nasional.

V. KESIMPULAN

Dari pembahasan penelitian diatas, dapat disimpulkan bahwa saat ini Indonesia tengah dalam keadaan darurat *cyber security* dan sudah mencapai tahap memprihatinkan. Strategi *cyber security* yang harus dilakukan Indonesia untuk mewujudkan keamanan nasional di *era society 5.0*, adalah dengan: 1) *capacity building* pada semua stakeholder, 2) Pembentukan Undang-Undang Khusus tentang Tindak Pidana Siber agar terwujud kepastian hukum untuk *cyber security* di Indonesia, 3) Peningkatan sumberdaya manusia dengan mendidik dan merekrut tenaga profesional yang memiliki integritas dan etika yang baik untuk mendukung penguatan *cyber security*. 4) Kerjasama stakeholder di dalam negeri melalui multi stakeholderism dan kerjasama internasional dalam pengembangan dan penguatan kapasitas kemampuan *cyber*

p-ISSN 2086-5805
e-ISSN 2808-2540

security baik itu untuk infrastruktur, sarana prasarana maupun dalam pengembangan kemampuan sumberdaya dalam bidang *cyber security*.

Penelitian ini jauh dari sempurna dan perkembangan ancaman *cyber* semakin meluas dan sulit untuk dibendung, untuk itu kiranya ada penelitian yang lebih teknis dalam penguatan *cyber security* untuk menghadapi tantangan dunia global di masa yang akan datang.

UCAPAN TERIMA KASIH

Ucapan terima kasih atas terbitnya naskah ini pada Seminar Nasional Sains Teknologi dan Inovasi Indonesia 2021 sebagai bagian kolaborasi/kerjasama penelitian antara Akademi Kepolisian dengan Akademi Angkatan Udara.

REFERENSI

[1] Cakrawala, Apa Itu Cyber security? Mengapa Cyber security Kini Makin Penting? https://infokomputer.grid.id/read/122710604/apa-itu-cyber-security-mengapa-cyber-security-kini-makin-penting?page=all (Diakses tanggal 2 November 2021)
[2] Dasep Lukiman, Cyber security: Apa Itu Cyber security?, https://wakool.id/blog/582-cyber-security-apa-itu-cyber-security (Diakses tanggal 2 November 2021)
[3] Humaira Aliya, Kupas Tuntas Cybersecurity dan Seluk-beluknya, https://glints.com/id/lowongan/cybersecurity-adalah/#.YYYucmBBzIU (Diakses tanggal 2 November 2021)
[4] Hasyim Gautama, Penerapan Cyber security, http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf. (Diakses tanggal 2 November 2021)
[5] Perwita, Anak Agung Banyu & Yani, Yanyan A. 2005. Pengantar Ilmu Hubungan Internasional. Bandung: Rosdakarya.
[6] Mas'oed, Mochtar. 1989. Studi Hubungan- Internasional, Tingkat Analisis dan Teorisasi. Yogyakarta: Pusat antar Universitas-studi Sosial UGM.
[7] Sitompul, Josua. 2012. Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana. Jakarta: PT. Tatanusa.
[8] Ghernaouti, Solange. 2013. Cyber Power :Crime, Conflict and Security in Cyberspace. Lausanne: EPFL Press.
[9] Koh, B. (t.t.): Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do about It, HarperCollins Publishers, 2010, 290 pages., 3.
[10] T. J. B. H. K. K. dan I. RI, "Undang-Undang Nomor 19 Tahun 2016 tanggal 25 November 2016." https://jdih.kominfo.go.id/produk_hukum/view/id/555/t/undangundang+nomor+19+tahun+2016+tanggal+25+november+2016 (diakses Nov 08, 2021).
[11] B.L. Berg, H. Lune, Qualitative Research methods for The Social Sciences, ninth edition, (England, Essex: Pearson Education Limited, 2017).
[12] "Apa itu Cyber Crime" https://raharja.ac.id/2020/04/29/apa-itu-cyber-crime/ (Diakses tanggal 1 November 2021)
[13] Pusat Operasi Keamanan Siber Nasional, Laporan Tahun 2020 (Monitoring Keamanan Siber). Jakarta: Badan Siber Dan Sandi Negara, 2020.
[14] Kompas.com. 2019. RI Rugi Rp 478,8 Triliun akibat Serangan Siber, DPR Siapkan RUU diakses dari https://nasional.kompas.com/read/2019/08/12/13454311/ri-rugi-rp-4788-triliun-akibat-serangan-siber-dpr-siapkan-ruu-kks?page=all pada 20 Juli 2021
[15] Fikri Kurniawan. 2020. Kerugian Serangan Siber Tahun 2021 Diprediksi RP 84.000 triliun diakses dari https://tekno.sindonews.com/read/284040/207/kerugian-serangan-siber-tahun-2021-diprediksi-rp84000-triliun-1609240357 pada 20 Juli 2021
[16] ITU. 2020. Global Cybersecurity Index 2020. International Telecommunication Unit Indonesia's data accessible and downloadable on https://ncsi.ega.ee/country/id/.
[17] C. Bilah and A. Infantono, "Pengembangan Aplikasi Mobile Kamus Istilah Aeronautika pada Platform Android Sesuai Standar ISO 25010", senastindo, vol. 1, pp. 195-202, Oct. 2021.
[18] A. Infantono, J. Budiarto, A. Persada, F. Azzuhri, and Z. Abidin, "Content Filtering Pornografi Halaman Web Berbasis Citra dan Teks pada Sistem Terintegrasi Server Internet", *AAU-JDST*, vol. 5, no. 2, pp. 125-132, Jan. 2021.