Sriwijaya Journal of International Relations

Vol 1 No. 1, Juni 2021
Halaman 18-33

ANCAMAN SIBER DI TENGAH PANDEMI COVID-19 : TINJAUAN TERHADAP KEAMANAN NON-TRADISIONAL DAN KEAMANAN SIBER DI INDONESIA

Al Bahits Annef[1]

[1]*Jurusan Ilmu Hubungan Internasional, Universitas Pembangunan Nasional Vetera, Jakarta, Indonesia*

SUBMISION TRACK

Recieved: 17 Maret 2021
Final Revision: 25 Mei 2021
Available Online: 31 Juni 2021

KEYWORD

COVID-19, Cyberattack, Non-Traditional Security, Cyber Security

ABSTRACT

Several policies made by country during pandemic related to restriction and prohibition of public mobility implicated to cyberspace activities. Internet Users in Indonesia increased significantly by 17% in 2020 compared to 2019. Internet Users escalation during pandemic reciprocal with the rise of cyberattacks. By using qualitative methods, this paper aims to explain the phenomenon using two approaches, non-traditional security and cybersecurity. The author's findings show that cyberattacks in Indonesia elevated by 5 times in 2020. Some of these cyberattacks include phishing emails, ransomware and disinformation. These cyberattacks potentially threaten human security in various sectors such as personal, community, health, and economic security. Author also tries to elaborate the cyberattack with the National Cyber and Crypto Agency's (BSSN) responses as a state entity.

KATA KUNCI

COVID-19, Serangan Siber, Keamanan Non-Tradisional, Keamanan Siber.

CORRESPONDENCE

Email : albahitsannef@upnvj.ac.id

ABSTRAK

Sejumlah kebijakan negara di masa pandemi terkait pembatasan dan pelarangan mobilitas masyarakat berimplikasi pada aktivitas di dunia maya. Terjadi peningkatan signifikan pengguna internet di Indonesia hingga mencapai 17% pada tahun 2020 dibanding tahun 2019. Ekskalasi pengguna internet di Indonesia selama pandemi sejalan dengan terjadinya peningkatan serangan siber. Dengan menggunakan metode kualitatif, tulisan ini bertujuan untuk menjelaskan fenomena ini menggunakan dua pendekatan, yaitu keamanan non-tradisional dan keamanan siber. Hasil temuan Penulis ialah, serangan siber di Indonesia meningkat sebesar 5 kali lipat pada tahun 2020. Beberapa serangan siber tersebut di antaranya phising emails, ransomware dan disinformation. Serangan siber tersebut berpotensi mengancam keamanan manusia di berbagai sektor seperti keamanan personal, komunitas, kesehatan dan ekonomi. Penulis juga berusaha mengelaborasikan respon serangan siber oleh BSSN sebagai entitas negara yang bergerak di bidang siber.

PENDAHULUAN

Deklarasi COVID-19 sebagai pandemi global pada Maret 2020 lalu, menandakan babak awal dari krisis global terbesar dekade ini yang berdampak pada status quo manusia. Secara global, pandemi COVID-19 telah memberikan tekanan dan ancaman keamanan bagi manusia di berbagai aspek fundamental kehidupan, seperti pada aspek sosial-ekonomi dengan terjadi peningkatan PHK, sulitnya akses kesehatan, penurunan ekspor impor serta

peningkatan inflasi (Marpaung, 2020; Yamali & Putri, 2020). Sejak kasus pertama ditemukan pada Desember 2019 hingga Januari 2021, total kasus terkonfirmasi telah mencapai 99,363,967 kasus dengan total kematian mencapai 2,135,959 jiwa (WHO, 2021). Secara partikular di Indonesia total kasus yang berhasil diidentifikasi hampir menyentuh 1 juta kasus dengan tingkat kematian sebesar 2.8% atau sekitar 28 ribu jiwa (WHO, 2021).

Faktanya pasca COVID-19 menginfeksi dunia selama lebih dari satu tahun, varian jenis baru dari COVID-19 menuntut manusia untuk sekali lagi berevolusi demi beradaptasi dengan situasi yang ada. Sebagai virus yang mudah menyebar melalui kontak antar manusia, sejumlah negara melakukan kebijakan adaptasi dengan memberlakukan pembatasan mobilitas masyarakat sebagai kontrol penyebaran COVID-19. Pembatasan tersebut secara domestik diberlakukan untuk membatasi akses ke tempat-tempat publik yang memiliki eksposur besar dalam interaksi manusia seperti sekolah, perkantoran, tempat ibadah dan pusat perbelanjaan. Sementara itu dalam cakupan internasional beberapa negara pernah memberlakukan kebijakan *lockdown* untuk mencegah warga negara asing masuk ke negaranya, seperti Spanyol, Italia, Denmark, Jerman, juga Indonesia (Business Insider, 2020). Sementara itu di Indonesia, kebijakan pembatasan tersebut terimplementasi melalui kebijakan Pembatasan Sosial Berskala Besar (PSBB) sejak April 2020. Sayangnya kebijakan tersebut dinilai kurang efektif sehingga ditransformasikan menjadi kebijakan Pembatasan Kegiatan Masyarakat (PPKM) pada 11 Januari 2021 dengan harapan dapat menjadi langkah efektif untuk mengendalikan penyebaran COVID-19 (Kompas, 2021).

Sebagai implikasi dari pembatasan aktivitas masyarakat di luar rumah, masyarakat mengalihkan berbagai aktivitas lanskap *offline* menjadi *online*. Berbagai aktivitas mengalami adaptasi, seperti skema kerja *work from home*, pembelajaran berbasis kelas *online,* hingga aktivitas jual-beli *online* pun meningkat. Faktanya terjadi peningkatan pengguna internet pada tahun 2020 sebesar 10% dibanding tahun 2019 lalu, hingga Juli lalu tercatat pengguna internet dunia mencapai angka 3.96 Miliar (Datareportal, 2020b). Peningkatan eksposur dan penggunaan internet secara masif tentu menjadi suatu potensi ancaman keamanan tersendiri, terutama dalam ancaman serangan siber. Serangan siber melalui domain internet berpotensi mengancam keamanan manusia di sektor lainnya secara lebih luas.

Diskursus mengenai COVID-19 dan ancaman keamanan menjadi satu bahasan yang cukup sering dibahas di kalangan akademik dan peneliti dari berbagai latar belakang dalam satu tahun terakhir. Secara spesifik, pembahasan mengenai ancaman siber di saat pandemi COVID-19 menjadi satu topik yang cukup relevan dengan situasi global. Terdapat tiga literatur ekstensif yang substansial dan relevan yang Penulis gunakan sebagai tinjauan pustaka. Literatur tersebut mencakup pembahasan mengenai COVID-19 sebagai ancaman keamanan non-tradisional terhadap keamanan manusia (Nurhasanah, 2020), dampak COVID-19 terhadap ancaman keamanan siber secara general (Mouton, 2020), serta dampak pandemi COVID-19 spesifik di Indonesia yang ditinjau dari sudut pandang keamanan siber (Hadi et al., 2020).

Literatur pertama berjudul "*Covid-19 As A Non-Traditional Threat To Human Security"* oleh Siti Nurhasanah (2020). Diskusi difokuskan pada COVID-19 yang mengancam keamanan dari perspektif keamanan non-tradisional terhadap ancaman keamanan manusia. Nurhasanah juga berusaha mengelaborasikan ancaman keamanan manusia mampu menciptakan ancaman keamanan nasional. Hasil temuan dari diskusi ini mengacu pada perubahan ancaman keamanan dari yang sebelumnya terlihat menjadi tidak terlihat. Hal ini dideskripsikan dengan situasi di mana manusia memiliki kesadaran dan cenderung tahu tindakan apa dalam melawan suatu entitas militer, sedangkan saat melawan ancaman tidak terlihat seperti *bioweapon* manusia perlu beradaptasi secara signifikan untuk melawan ancaman tersebut. Terlepas dari apakah COVID-19 merupakan sebuah *bioweapon* atau memang fenomena alam, Nurhasanah menjelaskan bahwa COVID-19 lebih dari sekedar krisis kesehatan karena memengaruhi sektor kehidupan lainnya termasuk krisis sosial, ekonomi, dan politik secara massif (Nurhasanah, 2020).

Literatur kedua berjudul *"COVID-19 : Impact on the Cyber Security Threat Landscape"* oleh Francois Mouton (2020). Literatur ini secara eksplisit mendiskusikan lanskap ancaman keamanan siber selama pandemi COVID-19. Hasil temuan dari literatur ini berupa sejumlah serangan siber seperti *phising*, *fake urls*, penyebaran misinformasi, *malicious website*, dll. Mouton mengungkapkan serangan siber saat COVID-19 berdampak besar pada beberapa aspek, yaitu informasi, bisnis, dan ekonomi secara lebih luas. Kesadaran akan teknologi masih menjadi hal yang terbatas di masyarakat, dengan demikian edukasi terkait siber diperlukan (Mouton, 2020).

Literatur ketiga berjudul "*Analisis Dampak Pandemi Covid 19 di Indonesia Ditinjau dari Sudut Pandang Keamanan Siber"* oleh Hadi, dkk (2020). Literatur ketiga bersinggungan dengan literatur kedua, namun yang membedakan ialah bahasan literatur ketiga secara spesifik menggunakan perspektif keamanan siber dan berdasarkan studi kasus di Indonesia. Hasil temuan dari literatur ketiga sejalan dengan premis Penulis di mana kondisi nasional yang memaksa agenda masyarakat menjadi terbatas meningkatkan pengguna internet di Indonesia. Peningkatan penggunaan internet oleh masyarakat kemudian berpotensi pada peningkatan serangan siber, hal ini terbukti dari peningkatan serangan siber dari bulan ke bulan. Jenis-jenis serangan siber yang dilancarkan di Indonesia berupa *malware, phising, ransomware*, informasi palsu, situs web berbahaya, dll (Hadi et al., 2020).

Dengan menggunakan metode kualitatif Penulis berusaha mendiskusikan dua hal, pertama terkait serangan siber dan kaitannya dengan keamanan non-tradisional disertai sejumlah contoh kasus relevan. Kedua, Penulis berusaha menjelaskan serangan siber di Indonesia dari kacamata peran negara dalam proteksi keamanan siber.

KERANGKA TEORI

Penulis menggunakan dua konsep sebagai instrumen analisis tulisan ini, yaitu keamanan non-tradisional dan keamanan siber.

Keamanan Non-Tradisional

Definisi keamanan secara sederhana dapat dikatakan sebagai perasaan aman dari bahaya, ketakutan, kecemasan, penindasan, bahaya, kemiskinan, pertahanan, perlindungan dan pelestarian nilai-nilai inti dari ancaman (Smith & Brooks, 2013). Konsep keamanan mengalami perkembangan dan pedalaman definisi dan perluasan ruang lingkup bahasan seiring berkembangnya zaman. Sejak berakhirnya Perang Dingin, perluasan konsep keamanan dibedakan menjadi ancaman keamanan "*hard* / tradisional" dan "*soft* / non-tradisional". Keamanan non-tradisional tidak terkonsentrasi pada negara sebagai objek referen melainkan pada dimensi keamanan manusia sebagai entitas (Nurhasanah, 2020). Ketika konsep keamanan tradisional berbau militeristik, keamanan non-tradisional bersifat lebih humanisme dengan memperhatikan keamanan manusia. Hal ini kemudian mencakup seluruh area terkait kebutuhan manusia sebagai entitas seperti ekonomi, pangan, kesehatan, lingkungan, personal, komunitas dan politik (Smith & Brooks, 2013). Dengan demikian Penulis berusaha berfokus mengelaborasikan serangan siber

melalui kacamata ancaman keamanan non-tradisional yang mengancam berbagai aspek kehidupan. Secara spesifik Penulis akan fokuskan pada keamanan personal, ekonomi dan komunitas.

Keamanan Siber

Isu mengenai keamanan siber mulai mendapat perhatian lebih setelah berakhirnya Perang Dingin. Hal ini disebabkan kemunduran minat negara dalam memperkuat nuklir dan ingin memperkuat teknologi di sektor lainnya. Ancaman dunia siber kemudian menjadi perhatian kebijakan politik dan pertahanan (Kshetri, 2016). Keamanan siber didefinisikan sebagai sebuah rangkaian aktifitas dan pengukuran yang dimaksudkan untuk melindungi dari serangan, disrupsi, atau ancaman yang lainnya melalui elemen-elemen *cyberspace* (*hardware, software, computer network*) (Fischer et al., 2005). Sementara itu Schaeffer dkk (2019) mendefinisikan keamanan siber sebagai perlindungan sistem komputer, program perangkat lunak, dan data apa pun terhadap penggunaan, pengungkapan, transfer, modifikasi, atau perusakan yang tidak sah, baik yang tidak disengaja atau disengaja (Schaeffer et al., 2009). Dalam penyelenggaraan keamanan siber tentu berkaitan erat dengan serangan siber, yang secara konvensional digambarkan sebagai aktivitas kriminal yang diarahkan untuk menyerang teknologi informasi dan komunikasi tertentu yang menggunakan medium komputer (Smith, 2014). Nye dalam Valeriano (2018) menambahkan domain siber tidak hanya terbatas pada internet namun juga intranet, teknologi selular, kabel fiber-optik, dll (Valeriano & Maness, 2018). Penulis kemudian berusaha mengelaborasikan serangan siber di Indonesia seperti *phising, malware,* dan miss informasi menggunakan pendekatan keamanan siber, termasuk di dalamnya bagaimana aktor negara melawan serangan siber secara formal dan praktikal.

METODE PENELITIAN

Penulis menggunakan metode kualitatif sebagai metodologi fundamental penelitian. Metode kualitatif merupakan metode yang dirasa tepat untuk mendeskripsikan, mengeksplorasi serta memahami suatu permasalahan. Moeleong (2014) mendefinisikan metodologi kualitatif sebagai posedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan atau dari bentuk tindak kebijakan. Dalam proses pengumpulan data-data utama dan penunjang penelitian, Penulis menggunakan metode berbasis *internet-based research* atau penelitian berbasis internet. Tulisan ini memanfaatkan teknologi internet dengan mencari sejumlah literatur yang relevan dalam bentuk artikel

buku, artikel jurnal, artikel internet, berita dan laporan penelitian. Peneliti kemudian memanfaatkan berbagai sumber dari internet seperti artikel, artikel jurnal, artikel buku, berita daring, maupun statistik daring. Peneliti memfokuskan pencarian dan temuan terkait topik yang berkaitan dengan beberapa kata kunci seperti *cyberatack, phising emails, misinformation, cybersecurity* dengan rentan waktu spesifik sejak COVID-19 dideklarasikan sebagai pandemi global. Interpretasi data temuan kemudian ditinjau menggunakan konsep keamanan non-tradisional sebagai salah satu fokus bahasan dalam studi Hubungan Internasional bersama dengan konsep keamanan siber disertai sejumlah contoh kasus. Sebagai tambahan, Penulis mendeskripsikan sejumlah langkah strategis BSSN sebagai entitas negara dalam merespons eskalasi ancaman siber di Indonesia.

HASIL DAN PEMBAHASAN

Ancaman Serangan Siber dan Keamanan Non-Tradisional

Pandemi COVID-19 menjadi ancaman keamanan terbesar dekade ini karena berhasil mengancam berbagai aspek kehidupan manusia, termasuk di antaranya sosial, kesehatan, ekonomi, dan politik. Meskipun virus ini mengacaukan dan mengancam eksistensi negara, ancaman yang diberikan tidak bisa dikategorikan sebagai bentuk jenis ancaman keamanan tradisional. Hal ini dikarenakan COVID-19 bukanlah suatu entitas yang mengancam dalam konteks 'militeristik' seperti ancaman keamanan tradisional. Hal ini lebih tepat dikategorikan sebagai lebih tantangan keamanan yang berefek pada kesehatan masyarakat yang mampu menimbulkan bahaya bagi lanjutan bagi keamanan manusia (Nurhasanah, 2020).

Sebagaimana situasi pandemi yang tidak bisa dikategorikan sebagai ancaman keamanan tradisional, serangan siber pun tidak bisa dikategorikan demikian. Serangan siber juga tidak bisa dikategorikan sebagai sebuah ancaman keamanan tradisional karena tidak adanya penggunaan konteks militeristik dalam penyelesaiannya. Serangan siber bergerak melalui *cyberspace* dengan memberikan tekanan, ancaman dan serangan terhadap entitas digital lainnya. Kendati demikian, dewasa ini sejumlah serangan siber mulai menyerang domain militer dengan melakukan serangan siber langsung dan spionase terhadap militer (Juncun, 2018). Meskipun demikian hal ini tetap tidak bisa dikategorikan sebagai ancaman keamanan tradisional karena serangan siber tidak mengakibatkan 'membahayakan fisik' manusia (Kshetri, 2016).

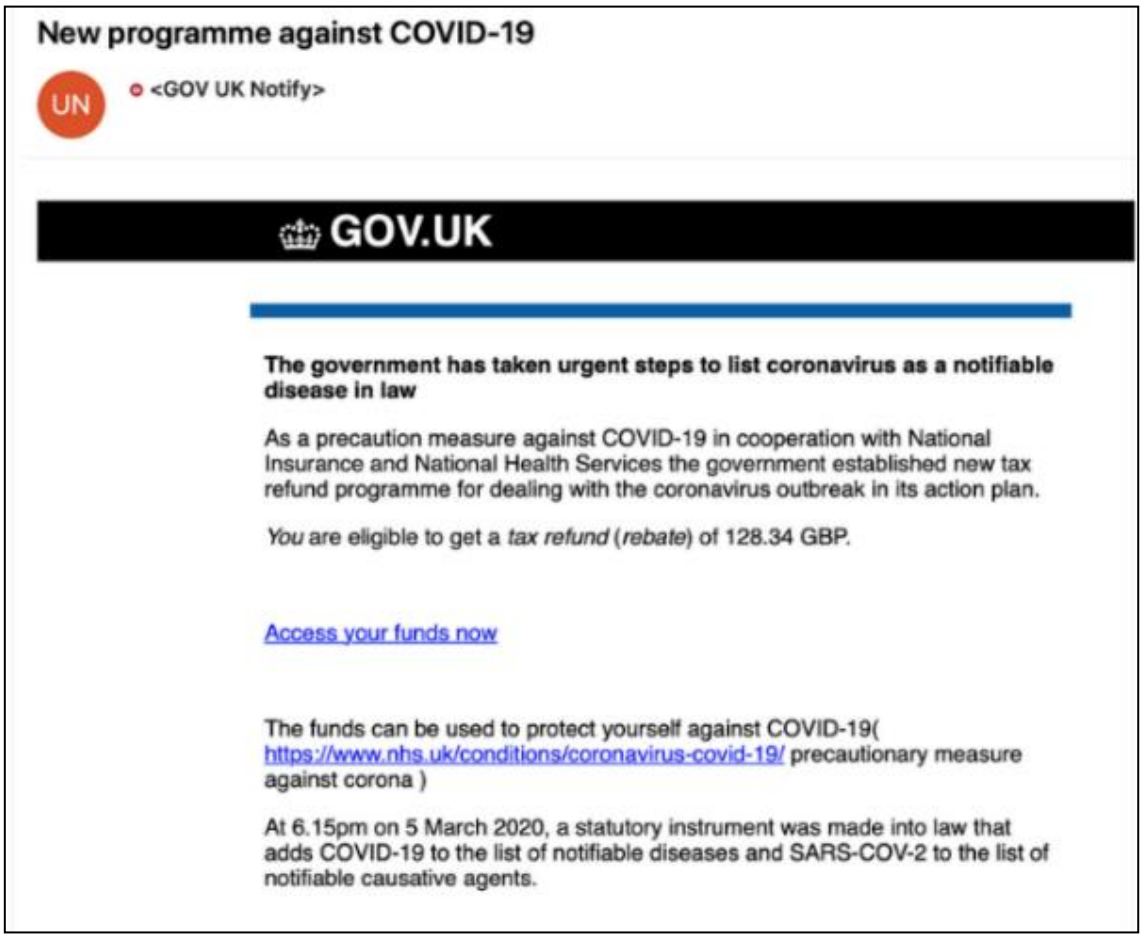
Ironinya, serangan siber semasa pandemi menjadi tantangan ganda yang

cukup signifikan bagi masyarakat Indonesia. Terjadi peningkatan pengguna internet di Indonesia sebesar 17% atau sekitar 25 juta pengguna pada tahun 2020 (Datareportal, 2020a). Lebih lanjut pengguna sosial media juga mengalami peningkatan sebanyak 12 juta pengguna atau pertambahan sebesar 8.1% (Datareportal, 2020a). Hal ini kemudian menjadikan internet sebagai arena substitusi untuk melakukan aktivitas manusia di masa pandemi. Peningkatan secara massif tersebut kemudian menjadi sasaran empuk bagi para pelaku serangan siber selama masa pandemi. UNODC menguatkan argumen dengan menyatakan bahwa setiap kali krisis baru muncul, pelaku kriminal akan melihat celah kesempatan untuk mengeksploitasi korban yang rentan karena dihadapi situasi ketakutan, ketidakpastian dan keraguan (UNODC, 2020).

Serangan siber secara konvensional digambarkan sebagai aktivitas kriminal yang diarahkan untuk menyerang teknologi informasi dan komunikasi tertentu yang menggunakan medium komputer (Smith, 2014). UNODC merilis beberapa ancaman siber yang secara signifikan mengancam keamanan manusia. Di antaranya ialah *malicious campaigns*, *phising emails*, *malicious domains*, dan *disinformation* (UNODC, 2020). Di dunia internasional terdapat beberapa serangan siber signifikan yang tercatat selama pandemi, di antaranya *scam* pendaftaran vaksin palsu NHS via email di Inggris, serangan siber terhadap 600 entitas perusahaan di Jepang, serta 61 serangan *ransomware* terhadap bisnis di Singapura (BBC, 2021; New Strait Times, 2020; The Strait Times, 2020). Lebih lanjut, FBI melaporkan serangan siber mencapai 4,000 kasus perhari dengan peningkatan persentase serangan siber sebesar 400% dari kondisi sebelum pandemi (PRNewswire, 2020). Selain itu isu konspirasi menciptakan disinformasi di masyarakat juga tersebar di internet yang mengaitkan teknologi 5G sebagai penyebab kasus COVID-19 (BBC, 2020).

Menurut Setiawan (Direktur Proteksi Ekonomi Digital Badan Siber dan Sandi Negara (BSSN) praktik *phising emails* menjadi salah satu serangan siber yang paling sering dilakukan di Indonesia (Liputan 6, 2020a). Setidaknya *phising emails* berpotensi mengancam pada dua aspek keamanan manusia, yaitu personal dan ekonomi. *Phising emails* merupakan tindakan penipuan berbasis email yang bertujuan untuk mencuri data informasi target melalui beberapa cara yang terlihat ‘menjanjikan’. Bagi keamanan personal, *phising emails* berpotensi mengancam keamanan privasi individu dengan mencuri data-data penting yang kemudian bisa

dimanfaatkan untuk praktik kriminal *online* lainnya, seperti peminjaman *online* atau penipuan menggunakan data yang dicuri.



Sumber : BBC, 2020

Gambar 1. Contoh *phising email* dengan menyamar sebagai Pemerintah Inggris yang beredar di *United Kingdom*.

Sementara itu bagi keamanan ekonomi, *phising emails* berpotensi mencuri data dan informasi kritikal pelaku bisnis, pemangku kepentingan ekonomi, hingga pemerintahan. *Phising emails* biasanya berkedok pesan/*email* dengan judul yang 'memancing' korban untuk membuka pesan/*email* tersebut. Hal ini biasanya berkaitan dengan konteks finansial, periklan, berita penting, dan penawaran dengan sisipan file *attachment* atau *link* berbahaya. Kasus *phising emails* di Indonesia terjadi pada kasus penipuan pembelian ventilator dan monitor virus COVID-19 pada tahun lalu (Media Indonesia, 2020). Kasus yang ditafsir merugikan lebih dari 3,6 juta Euro tersebut menggunakan modus *phising emails.* Para pelaku berasal dari Indonesia yang behasil melakukan 'bypass' komunikasi e-mail

antara perusahaan pembeli ventilator, Althea Italy dengan penjual, yaitu Perusahaan Shenzen, China.

Selain itu Perusahaan Anti-Virus Global, *Kapersky* melaporkan terdapat upaya serangan *phising* yang menargetkan UKM Indonesia yang terbilang masih rentan terhadap ancaman serangan digital. *Kapersky* berhasil mendeteksi setidaknya 190 ribu serangan siber terhadap pelanggannya di Indonesia yang terjadi pada kuartal pertama tahun 2020 (Suara.com, 2020). Tidak bisa dipungkiri bahwa infrastruktur digital Indonesia masih cukup jauh tertinggal dengan negara-negara maju. Kendati demikian, infrastruktur digital yang belum optimal bukanlah satu-satunya tantangan bagi Indonesia. UKM Indonesia yang rentan terhadap bahaya laten serangan digital juga diakibatkan rendahnya literasi digital masyarakat Indonesia terhadap bahaya serangan siber.

Serangan siber lainnya yang turut berperan dalam mengancam keamanan personal maupun ekonomi Indonesia ialah *ransomware*. *Kapersky* melaporkan berhasil mengidentifikasi dan mencegah sebanyak lebih dari 800 ribu serangan *ransomware* di Asia Tenggara sejak awal tahun hingga Agustus 2020 (Tempo, 2020). Di Indonesia, serangan *ransomware* tersebut dikalkulasikan sebanyak 49,35% ditujukan pada sektor perusahaan. *Ransomware* sendiri merupakan perangkat lunak berjenis *malware* yang memiliki kemampuan untuk meretas, mengakses bahkan mengambil alih komputer targetnya. Meskipun secara konvensional ancaman keamanan bagi ekonomi meliputi kemiskinan, pengangguran atau rendahnya pendapatan (Smith & Brooks, 2013), hal seperti serangan siber juga berpotensi meningkatkan kerugian tinggi bagi para pelaku ekonomi. Tindakan militeristik apa pun tidak mampu menyelesaikan masalah *ransomware* maupun *phising* dalam penyebarannya.

Serangan siber selain mengancam keamanan personal dan ekonomi, juga memiliki potensi ancaman terhadap keamanan kolektif manusia. Kasus *ransomware* yang terjadi selama pandemi berhasil melumpuhkan aktivitas fasilitas kesehatan *Universal Health Service* (UHS) di Amerika Serikat (Liputan 6, 2020b). Hal ini kemudian tidak menutup kemungkinan untuk terjadinya ancaman serangan siber maupun fisikal di fasilitas-fasilitas kesehatan di Indonesia. Fasilitas kesehatan merupakan entitas kritikal di masa pandemi. Terhambatnya atau bahkan lumpuhnya fasilitas digital suatu institusi kesehatan bisa mengakibatkan ancaman keamanan terhadap kesehatan masyarakat.

Lebih lanjut, serangan siber tidak hanya menyasar masyarakat melalui penipuan

yang bertujuan untuk menguntungkan ekonomi para pelaku. Serangan siber juga dapat dilakukan melalui penyebaran informasi palsu yang bertujuan untuk memanipulasi persepsi masyarakat terhadap suatu isu tertentu. UNODC menjelaskan intensi dari serangan jenis ini ialah mengelirukan untuk merusak lembaga, entitas, atau orang, dan / atau mendapatkan keuntungan finansial atau politik (UNODC, 2020). Kominfo melaporkan ditemukan berita hoaks sebanyak 1.125 kasus yang beredar di berbagai *platform* digital (Kominfo, 2020). Lebih detail terdapat 785 kasus hoaks melalui *facebook*, 10 kasus via *Instagram*, 324 kasus via *twitter* 324, dan 6 kasus via *youtube*. Selama pandemi, misinformasi setidaknya berkaitan dengan hal-hal kritikal seperti COVID-19, Status infeksi individu terkena COVID-19, pendekatan Pemerintah terhadap isu COVID-19, serta obat dari COVID-19 (Mouton, 2020). Missinformasi yang dipercaya oleh masyarakat secara luas berpotensi menciptakan kebingungan publik dan mengancam keamanan dalam tatanan yang lebih luas.

Serangan Siber dan Respons Entitas Keamanan Siber

Dengan terjadinya peningkatan serangan siber di Indonesia secara drastis pada masa pandemi, keamanan siber menjadi perhatian banyak pihak terkait. Badan Siber dan Sandi Negara (BSSN) melaporkan serangan siber di Indonesia yang berhasil terdeteksi pada semester pertama tahun 2020 mengalami peningkatan luar biasa, yaitu sebesar 5 kali lipat dari tahun sebelumnya dengan total 149,78 juta kali (Cyberthreat, 2020)**.** Tren serangan siber yang terus meningkat terjadi selama pandemi setelah sejumlah kebijakan yang membatasi mobilitas masyarakat diberlakukan. Individu, Organisasi serta Pemerintah ketiganya merupakan entitas yang menjadi sasaran bagi para pelaku penyerangan siber. Hal serupa dikemukakan oleh Shaeffer, dkk yang mengatakan bahwa entitas organisasi terutama perusahaan yang akan berdampak dalam bidang ekonomi sangat disarankan untuk memiliki kebijakan yang berkaitan dengan perlindungan data, penyimpanan data, penghancuran data, privasi, dan penyangkalan kepada para pelanggan (Schaeffer et al., 2009).

Lebih lanjut, Schaeffer, dkk (2009) mengformulasikan skala ancaman dalam keamanan siber sebagai "*Chan Scale of Cyber In-Security"*. Skala ancaman ini dikategorikan berdasarkan dampak yang dihasilkan. Skala ancaman tersebut dibagi menjadi 5 tahapan, yaitu; pertama, risiko rendah yang ditimbulkan akibat peretas yang berhasil meretas sistem dan menciptakan kerusakan minor yang berdampak pada bisnis semisal; kedua,

risiko sedang yang ditimbulkan akibat ditanamkannya *malware* pada jaringan yang bisa menyebabkan malfungsi dan berpotensi menciptakan kerusakan signifikan dalam kerugian finansial; ketiga, risiko sedang-tinggi ketika peretas berhasil mendapatkan data dan informasi berupa *personally identifiable information (PII)*; keempat, risiko tinggi yang digambarkan sebagai serangan dari 'orang dalam', serangan jenis ini berpotensi mengakibatkan kebocoran informasi krusial organisasi; kelima, risiko kritikal, diilustrasikan dengan peretas yang berhasil masuk ke sistem dan dapat mengakses PII serta informasi keuangan dan informasi rahasia organisasi (Schaeffer et al., 2009). Skala ancaman Schaeffer dapat berguna sebagai acuan bagi para pemangku kebijakan dan praktisi keamanan siber dalam merespon serangan siber selama pandemic.

Berdasarkan laporan Pusat Operasi Keamanan Siber Nasional, serangan siber sejak Januari 2020 hingga April 2020 didominasi oleh serangan *Trojan activity* sebesar 56% dan *information gathering* 43% (Tobing, 2013). *Trojan activity* merupakan aktivitas serangan siber yang memanfaatkan perangkat lunak yang 'menyamar' dengan tujuan memperoleh data dan informasi target atau bahkan merusak sistem dan jaringan. China dan Italia pernah menghadapi kasus terkait *Trojan* dengan modus penyebaran melalui email berbentuk dokumen yang berasal dari otoritas *WHO* (Tobing, 2013). Eksploitasi *Trojan* sendiri memiliki risiko kritikal bagi target jika para peretas berhasil masuk ke sistem dan mengakses informasi krusial. Selain *Trojan, information gathering* juga berpotensi mengancam keamanan data privasi masyarakat. *Information gathering* dilakukan melalui beberapa cara seperti *phising, keylogger,* dan *malicious website.* Para pelaku memanfaatkan kebingungan masyarakat yang belum akrab dengan teknologi untuk mencuri informasi dan data melalui perantara seperti *email* atau *malicious website* yang kemudian dimanfaatkan untuk aktivitas kriminal lainnya.

Serangan siber pada dasarnya tidak terbatas pada suatu negara saja karena lanskap yang dilindungi bersifat *intangible landscape* sehingga tidak ada batasan negara dalam bertindak. Kendati demikian, negara tetap memiliki kewajiban untuk melindungi masyarakatnya dari berbagai serangan siber. Di Indonesia, ruang lingkup keamanan siber masuk ke dalam domain BSSN sebagai pembuat, pelaksana, dan pemantau kebijakan siber. Secara formal legalitas, BSSN dalam operasinya memiliki Strategi Keamanan Siber Nasional (SKSN) yang berlandaskan pada Pasal 94 ayat (1)

huruf a Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Merdeka, 2020). Strategi ini berfungsi sebagai cetak biru negara dalam melakukan proteksi keamanan siber.

Tujuan strategis dari SKSN ialah mencapai ketahanan siber, pelayanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber pada ekonomi digital (BSSN, 2020). Dengan tingginya tren serangan siber selama pandemi keamanan siber yang meliputi perangkat keras, perangkat lunak dan data dalam jaringan juga membutuhkan perlindungan yang adaptif. Dalam upaya mitigasi serangan siber yang terjadi di Indonesia selama pandemi, BSSN merilis Buku Putih Mitigasi Insiden Siber saat Pandemi COVID-19 (BSSN, 2020). Dalam Buku Putih BSSN kemudian mendeskripsikan setidaknya terdapat tiga elemen penting sebagai langkah persiapan dan perlawanan terhadap serangan siber selama pandemi COVID-19 yang bisa dilakukan oleh Organisasi dan Pemerintah (BSSN, 2020).

Elemen pertama ialah perencanaan penanganan serangan siber yang komprehensif. Perencanaan penanganan insiden siber perlu dipersiapkan oleh Organisasi dan Pemerintah sebagai langkah preventif terhadadp serangan siber jika benar-benar terjadi. Perencanaan meliputi beberapa persiapan seperti mempersiapkan delegasi personil ketika terjadi serangan siber, tim identifikasi, mekanisme pencegahan penyebarluasan, mekanisme penyelesaian masalah, mekanisme pemulihan data yang terdampak , serta evaluasi sebaga data pembelajaran untuk kedepannya (BSSN, 2020).

Elemen kedua ialah tim penanganan serangan siber. Sama halnya seperti para Dokter dan Perawat yang menjadi garda terdepan dalam penanganan kasus COVID-19. Tim penanganan serangan siber merupakan garda terdepan yang sangat penting yang dibutuhkan oleh tiap organisasi. Maka dari itu tim penanganan serangan siber dituntut responsive dan haruslah terdiri dari orang-orang yang kompeten di bidang terkait. BSSN memberikan gambaran setidaknya dalam tim penanganan serangan siber terdiri dari beberapa anggota funadamental, yaitu; kepala tim penanganan siber; analis keamanan siber; peneliti ancaman keamanan siber; petugas penanganan awal; serta koordinator komunikasi (BSSN, 2020). Lebih lanjut, bila diperlukan investigasi dan penyelesaian lebih lanjut dalam bidang hukum, setidaknya diperlukannya analis forensic *digital* dan perwakilan digital hukum.

Elemen ketiga ialah perangkat bantu proteksi serangan siber. Alat bantu dimanfaatkan untuk proses penanganan serangan siber dan jenisnya beragam tergantung jenis serangan siber yang dihadapi. Secara umum dalam proses mendeteksi dan menganalisis serangan siber terdapat beberapa perangkat umum yang bisa dimanfaatkan, seperti *system log, antivirus,* dan *security information and event management (SIEM).* Semisal dalam perangkat SIEM, BSSN memberikan contoh produk teknologi yang bisa digunakan oleh organisasi seperti *IBM Qradar* dan *Security-Onion*. SIEM sendiri bisa dimanfaatkan untuk pengumpulan dan pengangregasian data pada infrastruktur teknologi informasi, perangkat keamanan serta jaringan (BSSN, 2020)

KESIMPULAN

Situasi pandemi COVID-19 merupakan jenis keamanan non-tradisional yang memiliki dampak luas terhadap berbagai aspek kehidupan manusia. Di saat banyak negara merespon situasi pandemic dengan berbagai kebijakan pembatasan hingga pelarangan mobilisasi, masyarakat beradaptasi dengan beralih ke lanskap baru dalam beraktivitas. Dunia siber kemudian dimanfaatkan oleh masyarakat untuk terus menjalankan produktifitas. Hal ini kemudian berimplikasi kepada peningkatan pengguna internet secara global, termasuk Indonesia. Pengguna internet di Indonesia meningkat sebanyak 17% sebagai jawaban adaptif masyarakat terhadap kebijakan pembatasan pemerintah. Aktivitas seperti *work from home*, kelas berbasis *online*, serta praktik jual-beli menjadi beberapa pemanfaatan ruang siber selama pandemi. Fenomena ini kemudian memberikan tantangan tersendiri bagi keamanan siber dengan terjadinya pengingkatan serangan siber secara massif pada tahun 2020 dibanding tahun sebelumnya. BSSN mencatat peningkatan serangan siber di Indonesia sebanyak 5 kali lipat lebih tinggi selama pandemi. Penulis berhasil menemukan beberapa serangan siber yang berhasil mengancam keamanan bagi manusia di berbagai sektor.

Sebagaimana keamanan non-tradisional merupakan jenis sekuritisasi keamanan yang tidak menggunakan militer sebagai instrument penyelesaiannya, begitupula dengan serangan siber yang menimpa Indonesia. Beberapa serangan tersebut meliputi praktik *phising emails* yang menargetkan entitas individu dan perusahaan, *ransomware* yang menargetkan fasilitas kesehatan dan perusahaan, serta *disinformation* yang menargetkan masyarakat luas dengan tujuan memanipulasi persepsi dan pemahaman masyarakat. BSSN sebagai institusi yang berwenang dalam domain

siber merilis Buku Putih yang berisi panduan dan rekomendasi mitigasi serangan siber di masa pandemic COVID-19. Beberapa rekomendasi tersebut di antaranya ialah menyarankan penerapan tiga elemen perlawanan terhadap serangan siber. Elemen tersebut kemudian dapat dimanfaatkan baik oleh Organisasi maupun Pemerintah sebagai upaya preventif proteksi keamanan siber dari serangan siber.

Dalam upaya perlawanan serangan siber selama pandemic COVID-19 di Indonesia sebetulnya Penulis menemukan masih minimnya data sekunder yang bisa didapatkan. Laporan serangan siber komprehensif oleh pihak BSSN pun terbatas dan cenderung sejumlah data yang Penulis dapatkan berasal dari informan BSSN yang melakukan seminar *online.* Hal ini kemudian memberikan asumsi bagi Penulis, BSSN memanglah berhasil mengidentifikasi serangan siber tetapi dalam implementasi dan praktiknya dipertanyakan, apakah hanya semata-mata dalam konteks normatif seperti pembentukan kebijakan atau memberikan edukasi masyarakat melalui seminar semata. Penulis kemudian mengakui masih adanya *gap* data dan informasi yang Penulis temukan dalam tulisan ini terkait keamanan siber. Hal ini kemudian memberikan peluang bagi Penelitian selanjutnya untuk mengeksplorasi penelitian mengenai serangan siber saat pandemic dari sudut pandangan implementasi terhadap keamanan siber.

DAFTAR PUSTAKA

BBC. (2020). *Coronavirus: 5G and microchip conspiracies around the world*. https://www.bbc.com/news/53191523

BBC. (2021). *Beware fake Covid vaccination invites, NHS warns*. https://www.bbc.com/news/technology-55811161

BSSN. (2020). *Mitigasi Insiden Siber*. *15*, 431–432.

Business Insider. (2020, September). *Our ongoing list of how countries are reopening, and which ones remain under lockdown*. https://www.businessinsider.com/countries-on-lockdown-coronavirus-italy-2020-3?r=US&IR=T

Cyberthreat. (2020). *Semester Pertama 2020, Serangan Siber di Indonesia Naik 5 Kali Lipat*. https://cyberthreat.id/read/8167/Semester-Pertama-2020-Serangan-Siber-di-Indonesia-Naik-5-Kali-Lipat

Datareportal. (2020a). *Digital 2020 : Indonesia*. https://datareportal.com/reports/digital-2020-indonesia

Datareportal. (2020b). *Digital 2020: July Global Statshot*. https://datareportal.com/reports/digital-2020-july-global-statshot

Fischer, E. A., Ave, I., & Washington, S. E. (2005). *CRS Report for Congress Received through the CRS Web Creating a National Framework for Cybersecurity : An Analysis of*.

Hadi, M. D. S., Widodo, P., & Putro, R. W. (2020). Analisis dampak pandemi Covid 19 di Indonesia ditinjau dari

sudut pandang keamanan Siber. *Jurnal Kebangsaan*, *1*(1), 1–9.

Juncun, S. (2018). *Militaries Versus Non-Traditional Security Threats*.

Kominfo. (2020). *Kominfo Temukan 1.125 Hoaks di Medsos Terkait Corona*. https://kominfo.go.id/content/detail/25831/kominfo-temukan-1125-hoaks-di-medsos-terkait-corona/0/sorotan_media

Kompas. (2021). *PPKM Mulai Diberlakukan Hari Ini, Simak Berikut Bedanya dengan PSBB*. https://www.kompas.com/tren/read/2021/01/11/141500665/ppkm-mulai-diberlakukan-hari-ini-simak-berikut-bedanya-dengan-psbb?page=all

Kshetri, N. (2016). Cybersecurity in National Security and International Relations. *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, 1–240. https://doi.org/10.1007/978-3-319-40554-4

Liputan 6. (2020a). *BSSN: Phishing Jadi Metode Serangan Siber Terbanyak Selama Pandemi*. https://www.liputan6.com/tekno/read/4281600/bssn-phishing-jadi-metode-serangan-siber-terbanyak-selama-pandemi

Liputan 6. (2020b). *Pandemi Covid-19, DPR Ingatkan Ancaman Serangan Siber pada Fasilitas Kesehatan*. https://www.liputan6.com/news/read/4369780/pandemi-covid-19-dpr-ingatkan-ancaman-serangan-siber-pada-fasilitas-kesehatan

Moleong, L. (2014). *Metodologi Penelitian Kualitatif.* Bandung: PT RemajaRosdakarya

Marpaung, E. W. (2020). Pandemi COVID-19 : Dampak Sosial-Ekonomi , Tantangan , dan Potensi Solusi PANDEMI COVID-19 DALAM SUDUT PANDANG DEMOGRAFI SOSIAL : Ditujukan sebagai Tugas Mata Kuliah Demografi Sosial OLEH KELOMPOK 6 KELAS B : Sherina Anjani Putri Nisa Nurul Asror Muhammad. *Jurnal UI*, *1(1)*(May), 1–15. https://doi.org/10.13140/RG.2.2.35252.68483

Media Indonesia. (2020). *Penipuan Ventilator, Bisa Jadi Pelaku Gunakan Modus Email Phising*. https://mediaindonesia.com/megapolitan/342943/penipuan-ventilator-bisa-jadi-pelaku-gunakan-modus-email-phising

Merdeka. (2020). *Tingkatkan Keamanan Siber Nasional, BSSN Susun Draft SKSN*. https://www.merdeka.com/peristiwa/tingkatkan-keamanan-siber-nasional-bssn-susun-draft-sksn.html

Mouton, F. (2020). *COVID-19 : Impact on the Cyber Security Threat Landscape*. *March*. https://www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

New Strait Times. (2020). *Cyberattacks on Japanese firms increase during pandemic*. https://www.nst.com.my/world/region/2020/12/646036/cyberattacks-japanese-firms-increase-during-pandemic

Nurhasanah, S. (2020). Covid-19 As A Non-Traditional Threat To Human Security. *Journal of Strategic and Global Studies*, *3*(1). https://doi.org/10.7454/jsgs.v3i1.1028

PRNewswire. (2020). *Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic*. https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html

Schaeffer, B. S., Chan, H., Chan, H., Ogulnick, S., Schaeffer, B. S., Chan, H., Chan, H., & Ogulnick, S. (2009). Cyber Crime and Cyber Security : *Whitepaper for Franchisors, Licensors and Others*, 1–17.

Smith, C. L., & Brooks, D. J. (2013). Concept of Security. *Security Science, October 2015*, 1–22. https://doi.org/10.1016/b978-0-12-394436-8.00001-1

Suara.com. (2020). *Targetkan UKM, 192 Ribu Upaya Phising Terdeteksi di Indonesia*. https://www.suara.com/tekno/2020/05/12/140000/targetkan-ukm-192-ribu-upaya-phising-terdeteksi-di-indonesia

Tempo. (2020). *Enterprise Target Utama Serangan Ransomware di Indonesia, WFH Jadi Celahnya*. https://tekno.tempo.co/read/1382050/enterprise-target-utama-serangan-ransomware-di-indonesia-wfh-jadi-celahnya/full&view=ok

The Strait Times. (2020, November). *More Singapore businesses hit by ransomware attacks*. https://www.straitstimes.com/tech/more-spore-businesses-hit-by-ransomware-attacks

Tobing, V. (2013). *Insiden web defacement*. *Juni 2012*(Maret), 4–5.

UNODC. (2020). *COVID-19: Cyber Threat Analysis*. https://www.unodc.org/documents/middleeastandnorthafrica//2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf

Valeriano, B., & Maness, R. C. (2018). International relations theory and cyber security: Threats, conflicts, and ethics in an emergent domain. *The Oxford Handbook of International Political Theory*, *February 2019*, 259–272. https://doi.org/10.1093/oxfordhb/9780198746928.013.19

WHO. (2021). *WHO Corona Virus Disease (COVID-19) Dashboard*. https://covid19.who.int/

Yamali, F. R., & Putri, R. N. (2020). Dampak Pandemi Covid-19 Terhadap Ekonomi Indonesia. *Medcom,Id*, *4*(2), 1. https://doi.org/10.33087/ekonomis.v4i2.179