JURNAL KEBANGSAAN
Universitas Pradita
Volume 1, Issue 1,Oktober 2020, pp.1-9

Analisis Dampak Pandemi Covid 19 di Indonesia Ditinjau dari Sudut Pandang Keamanan Siber

Martanto Dwi Saksomo Hadi[1],Pujo Widodo[2],Resmanto Widodo Putro[3]
[1,2,3]Universitas Pertahanan Indonesia

ABSTRAK

Seperti yang kita ketahui saat ini, masyarakat dikejutkan dengan merebaknya pandemi virus Covid-19 diseluruh dunia. Penyebaran Covid-19 sangat masif dan berdampak hampir diseluruh sektor kehidupan masyarakat, bahkan Indonesia telah menerapkan kebijakan pembatasan sosial berskala besar (PSBB) untuk mencegah penyebaran Covid-19. Selama masa tersebut penggunaan internet melonjak tajam, karena kebijakan tentang bekerja dari rumah dan belajar dari rumah. Kondisi tersebut dimanfaatkan oleh penjahat siber untuk melancarkan serangan melalui dunia maya. Fenomena yang menonjol adalah meningkatnya serangan siber selama pandemi Covid-19 dibandingkan bulan sebelumnya. Artikel ini mencoba menganalisis dampak Covid-19 ditinjau dari sudat pandang keamanan siber dan juga membahas serangkaian serangan siber yang terjadi selama pandemi serta upaya yang telah dilakukan untuk mencegahnya. Pendidikan tentang pengetahuan keamanan siber sudah menjadi kebutuhan yang utama bagi masyarakat, untuk mengamankan diri-sendiri dari serangan siber.

Kata Kunci: Covid-19, Keamanan Siber, Serangan Siber

ABSTRACT

As we all know, the public was shocked by the outbreak of the Covid-19 virus, which then became a major pandemic around the world. The spread of Covid-19 has had a profound impact on almost all sectors of human life. In fact, Indonesia has implemented a large-scale social restriction policy (PSBB), to prevent the spread of the Covid-19 virus. During a pandemic in which people work and study strictly from home, internet usage has soared pretty high sharply. This condition is then used by cybercriminals to launch their attacks through cyberspace. A prominent phenomenon is the increase in cyber attacks during the Covid-19 pandemic compared to the previous month. This article attempts to analyze the impact of Covid-19 from a cybersecurity point of view, and also discusses the series of cyber attacks that occurred during the pandemic and the prevention efforts that have been taken. Education about what cybersecurity is, has become the main necessity for people to protect themselves from cyber attacks.

***Keywords**: Covid-19; Cyber Security; Cyber attacks*

1. Pendahuluan

Awal tahun 2020, dunia dikejutkan dengan wabah virus corona (Covid-19) yang merebak hampir di seluruh dunia. Virus ini membawa dampak yang cukup besar dalam kehidupan sehari-hari. Covid-19 pertama kali teridentifikasi di kota Wuhan, China pada bulan November 2019. Organisasi kesehatan dunia (WHO) kemudian mengumumkan bahwa virus corona sebagai Pandemi Global pada Maret 2020 . Terjadinya pandemi ini merupakan fenomena luar biasa yang terjadi di abad 21, karena hampir semua aktivitas manusia diseluruh dunia dibatasi. Kebijakan beberapa negara dalam mengatasi penyebaran Virus memaksa warga negara untuk lebih banyak berdiam diri dan melaksanakan aktivitas di rumah . Hingga bulan Agustus 2020, jumlah kasus orang yang terinfeksi virus corona sudah mencapai 22,6 juta jiwa, 14,5 juta jiwa dinyatakan sembuh dan 792 ribu jiwa meninggal dunia (WHO,2020).

Pada awal kasus virus ini merebak di Indonesia, pemerintah telah membentuk Gugus Tugas Percepatan Penanganan Corona Virus Disease 2019 (Covid-19) melalui Keputusan Presiden Nomor 7 tahun 2020 pada tanggal 13 Maret 2010 di Jakarta . Pemerintah juga telah mengeluarkan status darurat bencana terhitung mulai tanggal 29 Februari 2020 hingga 29 Mei 2020 terkait pandemi ini . Langkah-langkah yang telah dilakukan pemerintah untuk mengurangi penularan virus ini, antara lain dengan sosialisasi cara pencegahan agar terhindar dari virus corona. Adapun cara yang dapat dilakukan untuk mencegah terjangkit virus corona antara lain rajin mencuci tangan, hindari kontak, *sosial distancing*, gunakan masker, dan *stay at home* .

Dengan ditetapkannya status darurat bencana, maka pemerintah menerbitkan Peraturan Pemerintah Nomor 21 Tahun 2020 tentang Penetapan pembatasan sosial dalam skala besar (PSBB) untuk mencegah penyebaran virus corona (Covid-19) . Akibat diterapkannya peraturan tersebut adalah pembatasan aktivitas keseharian masyarakat diluar rumah. Salah satu contoh adalah penerapan *work from home* bagi para pekerja baik pegawai negeri dan swasta, serta pembelajaran jarak jauh bagi pelajar dan mahasiswa. Dengan beralihnya sistem tatap muka menjadi sistem online, maka penggunaan internet melonjak dratis. Hal tersebut berdampak pada banyaknya serangan *cyber* yang terjadi pada pengguna internet di Indonesia (BSSN,2020).

Banyaknya serangan *cyber* yang terjadi disaat kondisi dunia dilanda pandemi Covid-19 saat ini, memicu peneliti untuk menganalisis lebih jauh mengapa hal tersebut dapat terjadi di saat kondisi negara sedang dalam keadaan bencana dan bagaimana cara mengatasinya.

2. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah studi kepustakaan, yaitu studi yang objek penelitiannya berupa karya-karya kepustakaan, baik berupa jurnal ilmiah, buku, artikel dalam media massa, maupun data-data statistik. Kepustakaan tersebut akan digunakan untuk menjawab permasalahan penelitian yang diajukan oleh penulis yang dalam hal ini adalah mengapa terjadi

banyak serangan *Cyber* disaat pandemi virus Covid-19 dan bagaimana mengatasinya. Adapun sifat dari studi yang dilakukan adalah deskriptif analisis yaitu memberikan edukasi dan pemahaman kepada pembaca, serta jenis data yang digunakan dalam penelitian ini adalah data sekunder.

3. Pembahasan

Irregular Warfare atau yang lebih dikenal dengan sebutan perang tak beraturan adalah suatu bentuk peperangan yang tujuannya adalah kredibilitas atau legitimasi otoritas politik yang relevan, dengan tujuan untuk merongrong atau mendukung otoritas tersebut (USAF,2013). *Irregular warfare* juga sebagai perjuangan kekerasan antara aktor negara dan non-negara untuk mendapatkan legitimasi dan pengaruh atas populasi yang relevan (US DoD, 2007) . *Cyber Warfare* atau perang siber adalah penggunaan teknologi untuk menyerang suatu negara, menyebabkan kerusakan yang sebanding dengan peperangan yang sebenarnya (Relia.S, 2015). Perang siber bisa dikategorikan sebagai perang hibrid yang merupakan salah satu bagian dari bentuk *irregular warfare* (Otaiku, 2018).

Pandemi Covid 19 telah membuat panik seluruh dunia, beberapa negara menetapkan kebijakan yang berbeda dalam mengatasi penyebaran dan penularan virus covid 19. Italia dan Spanyol telah melakukan *lockdown*, sehingga memaksa masyarakat untuk tetap tinggal di rumah. Indonesia sendiri menerapkan kebijakan PSBB yang membatasi aktivitas masyarakat di luar rumah. Beberapa organisasi dan perusahaan telah menerapkan ketentuan untuk bekerja dari rumah, dan sekolah juga menerapkan ketentuan untuk belajar dari rumah. Hal inilah yang menyebabkan masyarakat sangat tergantung pada teknologi internet untuk berkomunikasi, bekerja, belajar dan berinteraksi sosial.

Penggunaan internet dalam menunjang aktivitas masyarakat sehari-hari, merupakan kontribusi utama terhadap peningkatan ancaman serangan *Cyber (*Bruijn.H & Janssen.M, 2017). Hal itu terlihat dengan beberapa fakta yang ada, antara lain ; 1) Masyarakat memiliki ketergantungan yang tinggi terhadap infrastruktur digital. 2) belum semua organisasi terbiasa dengan pelaksanaan bekerja dari rumah. 3) Ketergantungan yang sangat besar terhadap konektivitas online dan infrastruktur jaringan yang ada. 4) Masyarakat menghabiskan sebagian besar waktunya untuk mengkonsumsi layanan online. 5) Masyarakat yang awalnya "gagap teknologi", dipaksa untuk menggunakan teknologi dalam kehidupan sehari-hari.

4. Hasil

Pandemi Covid 19 merupakan peristiwa luar biasa yang telah merubah kehidupan masyarakat secara global, hal tersebut telah menghasilkan apa yang disebut *new normal* yaitu norma-norma baru masyarakat dalam hidup dan bekerja. Pandemi ini telah memaksa jutaan orang untuk beraktivitas dari rumah, bekerja dari rumah dan belajar dari rumah. Kondisi ini tidak pernah dihadapi sebelumnya yang menimbulkan kerawanan terhadap keamanan dunia maya. Para penjahat

cyber telah memanfaatkan situasi ini untuk mengembangkan diri dan melakukan serangan *cyber*, dengan memanfaatkan kondisi masyarakat yang mengalami kehawatiran dan kecemasan.

Badan Siber dan Sandi Negara (BSSN) mencatat total kasus serangan siber di Indonesia selama pandemi virus corona (Covid-19) sejak bulan Januari sampai Maret 2020 berjumlah 80.837.445. Selama periode 1 Januari hingga 12 April 2020, ada 159 kasus web defacement (perusakan website) pada situs web pemerintah. Sedangkan serangan siber secara global yang memanfaatkan isu Covid-19 ada 25 kasus. Adapun jenis-jenis serangan yang dilancarkan ialah *malware*, *phising*, dan *ransomware* (BSSN, 2020). Selain serangan melalui dunia maya, para penjahat siber juga memanfaatkan beberapa cara untuk mengambil keuntungan pribadi. Terkait hal diatas, penulis mencoba menganalisa terkait serangan siber di Indonesia selama terjadinya pandemi Covid-19.

4.1. Phising

Phising adalah suatu metode untuk melakukan penipuan dengan mengelabui target dengan maksud untuk mencuri akun target. Phising mungkin merupakan serangan cyber yang mengalami peningkatan selama masa-masa sulit ini (Shu, Tian, Ciambrone, & Yao, 2017). Kebutuhan masyarakat akan informasi atau karena tuntutan pekerjaan yang memaksa mereka lebih intens menggunakan email, sehingga phising akan jauh lebih berhasil selama masa-masa ini. Para penjahat akan menyebarkan spam email, dengan tujuan untuk mendapatkan data pribadi yang berkaitan dengan transaksi keuangan. Pelaku kejahatan cyber sering kali mengambil keuntungan dari peristiwa besar, seperti pandemi saat ini untuk mengirim email phishing dalam upaya memanfaatkan potensi keingintahuan, kepanikan atau peristiwa tertentu.

4.2. URL Palsu

Sejak terjadinya pandemi, telah terjadi peningkatan dalam pengadaan URL palsu terkait dengan Covid 19. Palo Arto Network menyatakan hingga akhir Maret, telah mengidentifikasi 116.357 nama domain baru terkait virus Corona yang telah terdaftar. Dari seluruh domain baru tersebut, 2.022 domain dinilai berbahaya, sedangkan 40.261 lainnya berisiko tinggi (Szurdi, Chen, Starov, McCabe, & Duan, 2020). Biasanya modus operandi adalah penipu mengambil banyak domain terkait Covid 19 atau Coronavirus, dan mengubahnya kedalam situs injeksi malware yang berbahaya. Sehingga dalam situasi seperti ini banyak situs yang telah diambil alih oleh individu dengan niat yang jahat, dimana seharusnya web tersebut bisa digunakan untuk tujuan yang baik dan memungkinkan seseorang menemukan informasi yang benar dan akurat.

4.3. Serangan Fisik

Ketika berbicara tentang ancaman keamanan cyber, kita sering kali melupakan serangan fisik yang masih berlangsung. Jenis serangan ini masih mengandalkan rekayasa sosial, faktanya bahwa manusia dalam keadaan histeris dan membutuhkan bantuan, tidak akan berpikir panjang dan cenderung panik. Hal itulah yang dimanfaatkan oleh para penjahat untuk menyebarkan berita melalui dunia maya, tentang bantuan dengan menawarkan berbagai kebutuhan masker, penutup

wajah, hand sanitizer dan produk lain yang persediaannya sudah habis selama terjadinya krisis. Dengan menggunakan teknik ini, mereka bisa mendapatkan akses fisik untuk kerumah korban, bahkan menawarkan sterilisasi melalui penyemprotan disinfektan didalam rumah dan meminta pemilik rumah untuk berada diluar selama proses berlangsung.

4.4. Memanfaatkan Kebaikan orang

Para penipu memanfaatkan situasi yang terjadi saat ini dengan membuka halaman web donasi dalam rangka membantu penanganan pandemi Covid 19, dimana orang dapat menyumbang untuk membantu penelitian dalam menemukan obat untuk Covid 19. Dalam kenyataannya, halaman web tersebut tidak dikelola dengan benar dan dipergunakan untuk kepentingan individu dengan mengambil keuntungan dari penggalangan dana.

4.5. Mengambil Keuntungan Pribadi

Pandemi Covid 19 telah menyebabkan kekhawatiran hampir di seluruh masyarakat, ketakutan akan terbatasnya bahan makanan dan alat kesehatan telah terjadi di masa-masa sulit sekarang ini. Keadaan itu dimanfaatkan oleh sebagian individu yang mencoba mengambil keuntungan dengan menimbun beberapa produk yang dibutuhkan masyarakat dan akan menjual kembali dengan nilai yang lebih tinggi . Pemanfaatan dunia maya memungkinkan para penjahat ini melakukan operasinya, penyebaran melalui perdagangan online dan menggunakan media sosial sebagai sarana transaksi. Untungnya pemerintah Indonesia sudah bergerak cepat dengan menghentikan tindakan para penjahat ini, melalui ultimatum yang dibuat Polri tentang hukuman bagi para penimbun sembako dan alat kesehatan.

4.6. Menyebarkan Informasi Palsu

Informasi palsu dan berita Hoax adalah salah satu musuh terbesar bagi masyarakat selama pandemi ini. Maraknya pemberitaan palsu dan berita hoax yang menyebar dengan cepat melalui dunia maya, telah menimbulkan kekhawatiran dan cukup meresahkan masyarakat. Sampai dengan bulan juni 2020, Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo RI) menemukan 800 berita bohong yang menyebar di sejumlah media sosial terkait Covid-19 . Hoaks atau berita palsu bisa berdampak parah bila ada kelompok yang menjadi sasaran. Di sisi lain, berita dari sumber yang dipercaya justru tenggelam akibat hoaks yang menyebar cepat. Informasi yang salah dapat berdampak buruk bagi masyarakat luas dan berimbas kepada sektor lain, seperti kerugian di sektor ekonomi dan konflik SARA. Langkah yang diambil pemerintah/POLRI terkait berita palsu dan Hoaks adalah dengan melakukan penyelidikan terhadap kasus ini dan menghukum pelakunya .

4.7. Situs Web yang Berbahaya

Seiring dengan penyebaran virus Covid 19 yang begitu cepat, para penjahat cyber juga memanfaatkan situasi ini dengan menyebarkan malware terkait virus corona di dunia maya. Penyebaran malware ini bisa dibilang sangat cepat, karena setia harinya diperkirakan ada ribuan situs scam dan malware terkait Corona yang diaktifkan. Situs-situs ini tak cuma menargetkan

konsumen biasa, melainkan juga korban di kelas industri. Kebanyakan dari situs ini dipakai untuk melakukan serangan phishing, mendistribusikan file malware, ataupun melakukan penipuan finansial, seperti menipu pengguna dengan menjual barang yang diklaim sebagai obat, suplemen, ataupun vaksin untuk mengatasi COVID-19 . Hal ini menunjukkan bahwa seluruh masyarakat harus waspada terhadap serangan malware yang ditujukan kepada pengguna dengan berpura-pura sebagai situs yang memberikan informasi terkait virus corona.

4.8. Serangan Cyber di masa datang

Pertumbuhan jenis serangan siber di masa datang akan lebih kompleks dari sebelumnya. Perkembangan teknologi informasi akan membawa dampak terhadap kemampuan penjahat siber dalam melakukan aksinya, semakin canggih teknologinya maka akan semakin canggih juga celah kejahatannya. Ditinjau dari perspektif keamanan siber, beberapa tren perkembangan serangan siber di masa datang yang terus mengancam didunia maya adalah ; 1) Serangan Phishing akan lebih menakutkan dari sebelumnya, Phishing telah berkembang ke berbagai versi seperti Smishing (phishing melalui SMS) atau Vishing (phishing melalui panggilan langsung), yang menjebak korbannya untuk memberikan informasi pribadi seperti username dan password untuk keperluan login, atau OTP untuk melakukan transaksi. ; 2) Serangan yang berasal dari teknologi berkekuatan AI (Kecerdasan Buatan), yaitu dengan memanfaatkan teknologi AI untuk serangan Phishing yang canggih, di samping serangan malware ; 3) Resiko pada perangkat IoT (Internet of Think) yang digunakan untuk mencuri informasi pribadi dan data lainnya yang berguna bagi hacker untuk mendapat keuntungan.

4.9. Dampak Covid 19 Dan Upaya Pencegahannya

Pandemi covid 19 telah berdampak luas di dunia, wabah ini juga telah memberikan pelajaran yang sangat berharga bagi umat manusia, sehingga kita bisa menggunakan pengetahuan selama pandemi untuk menghadapi kehidupan masa datang yang lebih baik. Pandemi Covid 19 adalah contoh bagaimana masyarakat mengabaikan peringatan yang ada dan tidak siap untuk menghadapi wabah yang terjadi dengan cepat. Disamping berdampak pada kehidupan bermasyarakat, pandemi Covid 19 juga telah membawa dampak di dunia maya. Ditinjau dari sudut pandang ancaman cyber, beberapa bidang kegiatan yang memanfaatkan dunia maya sebagai sarana utama secara tidak langsung akan terpengaruh.

Berita palsu dan Hoaks akan menjadi salah satu permasalahan yang paling serius selama pandemi, banyaknya informasi yang tidak akurat memiliki dampak negatif dalam kehidupan bermasyarakat. Bukan hanya para penjahat cyber yang akan menyebarkan berita palsu dan hoaks, tetapi para aktor yang punya kepentingan tertentu akan mencoba memanfaatkan berita palsu tersebut. Berita palsu yang beredar luas dikalangan masyarakat akan meningkatkan keresahan dan kekhawatiran, hal itu dapat berdampak pada menurunnya tingkat kepercayaan pada pemerintah. Oleh sebab itu pemerintah harus membuat sebuah keputusan yang cepat dan tepat, dan meyakinkan kepada masyarakat akan informasi atau berita yang benar karena tidak semua informasi dapat

dipercaya. Dibutuhkan tenaga yang ekstra dan mental yang cukup kuat untuk meyakinkan tentang kebenaran sebuah berita atau informasi, dimana orang sudah terlanjur percaya terhadap berita palsu. Beredarnya berita palsu juga menyebabkan banyak waktu yang terbuang percuma selama pandemi.

Dunia usaha juga mengalami dampak yang sangat serius, adanya pemberhentian operasional maupun pembatasan tenaga kerja, tentu saja akan menurunkan produksi sebuah perusahaan. Dunia usaha juga dipaksa untuk menerapkan kebijakan bekerja dari rumah, sesuatu hal yang tidak pernah disiapkan sebelumnya dan tidak semua usaha bisa dijalankan dari rumah. Bagi perusahaan atau organisasi yang bisa menerapkan kebijakan bekerja dari rumah, ketergantungan terhadap koneksi data atau internet menjadi sangat besar. Mekanisme kerja antara karyawan yang berada di rumah dan perusahaan sepenuhnya menggantungkan adanya ketersediaan koneksi internet, tetapi hal ini tidak dibarengi dengan peningkatan keamanan jaringan atau firewall untuk melindungi mereka. Selain itu tidak semua karyawan yang bekerja dari rumah memiliki tingkat kemampuan yang sama dalam bidang teknologi informasi. Hal inilah yang menjadi sasaran para hacker untuk menjalankan aksinya seperti meretas situs perusahaan, pengiriman phising dan malware, dengan tujuan untuk mendapatkan keuntungan pribadi.

Gangguan yang terjadi pada dunia usaha, secara tidak langsung memberikan tekanan pada perekonomian. Dari perspektif awam kerugian finansial tampaknya menjadi salah satu tren utama dampak dari Covid 19 di masyarakat. Wisata merupakan salah satu sektor yang sangat terpukul akibat pandemi ini, kebijakan pemerintah untuk menutup sementara tempat wisata merupakan pukulan berat bagi sektor wisata. Hal tersebut juga berimbas kepada sektor penerbangan yang terpaksa mengurangi atau bahkan meniadakan rute penerbangan akibat tidak adanya penumpang.

Semua dampak negatif yang kita alami, memberikan sebuah pelajaran berarti tentang konsep menghadapi sebuah ancaman yang bisa datang secara tiba-tiba. Para penjahat dunia maya memanfaatkan kondisi Pandemi ini untuk melancarkan aksinya dan mereka bisa dikatakan berhasil. Keamanan dunia maya hingga saat ini masih merupakan krisis besar yang perlu ditangani secara serius dan teruss menerus. Semua yang terjadi saat ini, ketika dimana semua orang secara tiba-tiba dipaksa untuk merangkul dan bersentuhan langsung dengan teknologi, bekerja dari rumah dan sekolah dari rumah. Bagaimananpun tidak semua masyarakat familiar dengan teknologi internet, masih banyak masyarakat yang awam terhadap teknologi internet dan terpaksa harus menggunakannya. Disaat hampir semua masyarakat memanfaatkan teknologi internet untuk memenuhi kebutuhan mereka, para penjahat dunia maya bersuka cita karena mereka dapat melakukan serangan siber secara masif.

Pendidikan tentang keamanan siber merupakan salah satu kemampuan yang harus dimiliki oleh setiap organisasi. Tidak mungkin kita mengharapkan setiap karyawan untuk selalu waspada terhadap serangan siber, jika mereka belum dibekali tentang hal itu. Jawaban dari masalah itu adalah pendidikan, semua karyawan harus menerima pelatihan tentang tata cara melindungi akun

mereka sendiri di internet dari serangan siber. Dalam sebuah organisasi, karyawan merupakan salah satu titik lemah yang harus dilindungi. Saat ini karyawan sedang menghadapi masalah yang berkaitan dengan keamanan duni maya yang belum pernah mereka hadapi sebelumya. Hal itu memberikan pelajaran berharga bagi sebuah organisasi dalam menyiapkan karyawannya secara lebih baik lagi, setiap karyawan harus menerima pelatihan tentng bagaimana meningkatkan kewaspadaan dari serangan siber dalam kehidupan sehari-hari. Seorang karyawan yang mengerti bagaimana agar tetap aman bekerja dari rumah, akan selalu menerapkan prinsip yang sama dalam kehidupan berorganisasi.

5. Kesimpulan

Pandemi Covid-19 telah membawa dampak yang sangat luas, dan masyarakat akan membutuhkan waktu yang cukup lama agar pulih dari trauma pandemi Covid-19. Disaat yang sama Covid-19 telah membawa serta serangan siber yang sangat masif, sehingga berdampak pada kehidupan masyarakat. Ada peningkatan serangan siber yang signifikan di dunia maya yang memanfaatkan kondisi saat ini, dimana para pemimpin negara sedang bekerja keras untuk membuat keputusan yang sulit dalam menentukan masa depan mereka menghadapi covid-19. Kondisi masyarakat sedang mengalami tekanan, banyaknya berita palsu yang beredar di dunia maya menyebabkan masyarakat tidak yakin dengan apa yang terjadi saat ini. Perekonomian negara juga berada dalam keadaan yang cukup sulit akibat berhentinya operasional dunia usaha.

Dalam kondisi yang seperti ini, sudah saatnya para ahli dalam keamanan siber untuk bersatu dan berusaha melindungi masyarakat dari serangan siber didunia maya. Ketidaksiapan masyarakat dan kurangnya kesadaran tentang keamanan dunia maya, adalah permasalahan yang sangat serius dan perlu perhatian khusus. Pendidikan tentang keamanan siber bagi masyarakat dan karyawan sudah menjadi kebutuhan utama saat ini. Organisasi perlu mulai berinvestasi terhadap pendidikan bagi karyawan tentang keamanan dunia maya, sehingga mereka mampu untuk melindungi diri mereka sendiri.

REFERENSI

Bruijn.H & Janssen.M (2017) *Building cybersecurity awareness: The need for evidence-basedframing strategies*.Government Information Quarterly 34 (2017) 1–7. Diunduh dari http://dx.doi.org/10.1016/j.giq.2017.02.007

BSSN. (2020).*Rekapitulasi Insiden Web Defacement Januari-April 2020 dan Serangan Siber di Indonesia.* Pusat Operasi Keamanan Siber. Jakarta

Otaiku,AA. (2018). *A Framework for Hybrid Warfare: Threats, Challenges and Solutions*.J Def Manag 8: 178. doi:10.4178/2167-0374.1000178

Relia,S. (2015). *Cyber Warfare Its Implications on National Security*. United Service Institution of India. New Delhi

Sekertariat Negara RI. (2020). *Kepres No 7 Tahun 2020 Tentang Gugus tugas Percepatan Penanganan Corona Virus Disease 2019 (COVID-19).* Jakarta.

Sekertariat Negara RI. (2020).*Perpres Nomor 21 Tahun 2020 tentang Penetapan pembatasan sosial dalam skala besar (PSBB) untuk mencegah penyebaran virus corona (Covid-19).* Jakarta.

Shu,X., Tian,K., Ciambrone,A., & Yao,D., (2017). *Breaking the Target: An Analysis ofTarget Data Breach and Lessons Learned.* Diunduh dari http://arXiv:1701.04940v1

Szurdi,J., Chen,Z., Starov,O., McCabe,A.,&Duan,R. (2020). *Studying How Cybercriminals Prey on the COVID-19 Pandemic*. Paloalto Network. Diunduh dari https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

USAF. (2013). *Irregular Warfare ; Air Force Doctrine Document 3-2.* New York.

US DoD. (2007). *Irregular Warfare (IW); Joint Operating Concept (JOC) V-1*. New York WHO. (2020, Agustus 20). *WHO Coronavirus Disease (COVID-19) Dashboard*. World Health Organization (Online). https://covid19.who.int/

.