ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.2 No.1 Tahun 2023
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-2 2023
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2023

Pentingnya Pengetahuan *Cyber security* Untuk Publik Dan Negara

The Importance of Cyber security Knowledge for the Public and the Country

Abdul Aziz
Program Studi, Fakultas Teknik Informatika, Universitas Pelita Bangsa
Ajizabdul116@gmail.com

Abstract

The global Cyber security phenomenon represents a complex socio-technical challenge for governments, but requires the involvement of every individual. There has been a significant increase in community online activities for work, study, transactions, socializing, etc. This increase in online activity is also in line with the increase in cyber crime, knowledge of cyber attacks except for systems owned by the Government. An incident management system is needed to be able to quickly detect and handle information security incidents, minimize losses, reduce exploitable vulnerabilities and restore infrastructure including services and improve internet availability for people in environments that have an impact on online internet risks, as well as policies taken by governments and the effects that will occur.

***Keywords**: Cyber security, cyber attack, cyber impact*

Abstrak

Fenomena global *Cyber security* yang mewakili tantangan sosio-teknis yang kompleks bagi pemerintah, tetapi membutuhkan keterlibatan tiap individu. Adanya peningkatan yang signifikan pada aktivitas online masyarakat baik untuk bekerja, belajar, transaksi, bersosialisasi, dan sebagainya. Dunia saat ini sangat bergantung pada teknologi elektronik, dan melindungi data ini dari serangan dunia maya merupakan masalah yang menantang. Tujuan dari serangan *cyber* adalah untuk merugikan secara finansial,militer,maupun politik. Peningkatan aktivitas media sosial ini juga seiring dengan peningkatan kejahatan *cyber*, pengetahuan tentang penyerangan *cyber* tak terkecuali pada sistem yang dimiliki Pemerintah. Dibutuhkan sistem manajemen insiden untuk dapat mendeteksi dan menangani insiden keamanan informasi dengan cepat, meminimalkan kerugian, mengurangi kerentanan yang dieksploitasi dan memulihkan infrastruktur termasuk layanan serta meningkatnya ketersediaan internet untuk masyarakat di lingkungan berdampak pada risiko online internet,serta kebijakan yang diambil oleh pemerintah memunculkan efek paradoks dan dampak yang akan terjadi.

Kata kunci: *Cyber security*, serangan *cyber*, dampak *cyber*

Pendahuluan

Cyber security didefinisikan sebagai sekelompok perangkat, kebijakan, pengaturan, upaya perlindungan, pendekatan manajemen risiko, jaminan keamanan, pelatihan, praktik terbaik serta teknologi yang bisa dimanfaatkan untuk mengamankan aset organisasi terutama data dan informasi yang ada pada ruang *cyber* [1]. *Cyber security* awareness sebagai metodologi untuk mendidik pengguna internet agar peka terhadap berbagai ancaman dunia maya dan kerentanan komputer dan data terhadap ancaman tersebut dan mendefinisikan kesadaran keamanan *cyber* sebagai tingkat pemahaman pengguna tentang pentingnya keamanan informasi dan tanggung jawab mereka untuk melaksanakan tingkat kontrol informasi yang memadai untuk melindungi data dan jaringan organisasi[2]. Meskipun kebanyakan orang tampaknya menganggap Internet sebagai lingkungan yang aman dan menggunakannya setiap hari menggunakan ponsel pintar, tablet, dan komputer mereka, ada sejumlah besar serangan setiap hari. Serangan dunia maya, peretasan, dan pelanggaran keamanan di Internet tidak lagi menjadi pengecualian.[3].Namun faktanya masih banyak kejahatan yang terjadi setiap hari di dalam lingkungan bahkan insiden keamanan siber kecil, seperti infeksi malware, dapat menjadi masalah yang lebih besar yang pada akhirnya menyebabkan pelanggaran data,

kehilangan data, dan operasi bisnis yang terganggu.[4]. Seperti peretasan pencurian data, manipulasi data pencurian identitas atau bahkan mengambil alih system dan membahayakan dunia fisik, dampak terbesar terjadi ketika seorang penyusup mendapatkan akses ke akses kontrol pengawasan dan meluncurkan tindakan kontrol yang dapat menyebabkan kerusakan besar[5]. Kesulitan definisi akhirnya membocorkan kurangnya pemahaman umum. Pelaku yang berbeda memahami keamanan dunia maya secara berbeda dalam situasi yang berbeda[5] keamanan *cyber* sebagai akses tindakan yang diambil untuk melindungi komputer atau sistem komputer (seperti di Internet) dari akses atau serangan yang tidak sah[6]

Tingginya angka aktif pengguna internet seharusnya juga dibarengi dengan tingkat keamanan *cyber* itu sendiri, sehingga aktivitas di dunia internet tersebut dapat terjamin keamanan dan kerahasiannya. Sementara kondisi *Cyber security* di Indonesia masih sangat lemah dan buruk [7] Pembuatan kebijakan di bidang keamanan *cyber* saat ini menghadapi banyak paradoks, pemilihan satu arah dapat mengorbankan arah lain, sedangkan ada argumen untuk berjalan dua arah.[8] Kemajuan teknologi, peperangan kini telah merambah dunia maya yang mengakibatkan munculnya medan *cyber*,pun ujungnya adalah tetap mengarah pada perang fisik. Dan, perang fisik yang paling berbahaya di abad 21 adalah Perang Nuklir yang melibatkan teknologi *cyber* [9]. *Cyber security* juga melakukan tinjauan tentang aktivitas internet dan motivasi penggunaan oleh anak-anak dan mengidentifikasi beberapa risiko yang mereka hadapi. Mereka mengklasifikasikan risiko menjadi lima kategori: (i) risiko konten, (ii) risiko kontak, (iii) anak-anak yang ditargetkan sebagai konsumen, (iv) risiko ekonomi, dan (v) risiko privasi online[10].

*cyber*space juga menjadi sumber dari berbagai ancaman, kerentanan, dan ketidakamanan. Menurut Smith ancaman tersebut dapat bersumber dari pemerintah, organisasi, individu, atau pengusaha, baik secara disengaja maupun tidak demi mendapatkan keuntungan secara finansial, militer, politik, maupun tujuan lainnya[11]. Kasus *cyber*crime, baik korban maupun pelaku tidak berhadapan langsung dalam 1 (satu) tempat dimana kejadian perkara terjadi, bahkan dapat terjadi antar negara. Hal ini membuktikan bahwa *cyber*crime merupakan salah satu bentuk kejahatan lintas negara (transnational crime), tanpa batas (borderless), tanpa kekerasan (non violence), tidak ada kontak fisik (non phisically contact) dan tiada nama[12]. Saat ini, sebagian besar kegiatan dan interaksi ekonomi, komersial, budaya, sosial dan pemerintahan negara-negara, di semua tingkatan, termasuk individu, organisasi non-pemerintah dan lembaga pemerintah dan pemerintah, dilakukan di dunia maya[13].

Metode Penelitian

Metode sumber data jurnal ini menggunakan sumber data sekunder, data ini diperoleh melalui hasil studi literasi jurnal. Dalam penelitian ini penulis menggunakan jurnal yang berkaitan yang relevan, lalu melakukan pembanding, meringkas dan menganalisis secara sistematis terhadap karya-karya hasil penelitian melalui referensi jurnal nasional dan internasonal.

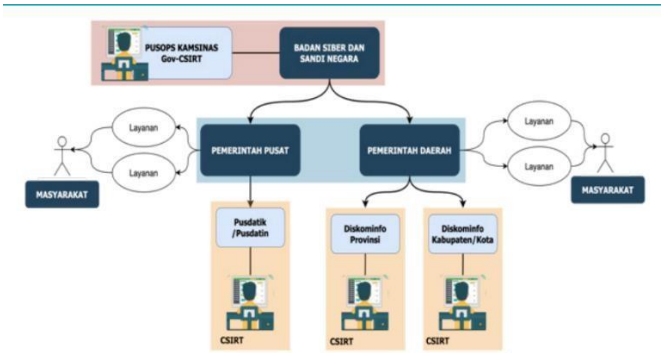
Hasil dan Pembahasan

Kebutuhan keamanan siber menjadi semakin penting karena ketergantungan kita pada Teknologi Informasi dan Komunikasi (TIK) di semua aspek masyarakat siberfisik kita. Keamanan dunia maya sangat penting bagi individu, untuk organisasi publik dan non-publik, tetapi menjamin keamanan seringkali terbukti sulit. Situs web banyak pemerintah memiliki keamanan terbatas ,dan mungkin mudah diretas. Masalah keamanan tidak terbatas pada kekuasaan eksekutif, tetapi juga relevan dengan partai politik dan spionase,sedangkan virus Stuxnet ditujukan untuk merusak infrastruktur nuklir. Dengan demikian, pelanggaran keamanan siber dapat dikatakan berdampak pada semua pemangku kepentingan di masyarakat kita. Pembuatan kebijakan di bidang keamanan siber saat ini menghadapi banyak paradoks. Pemilihan satu arah dapat mengorbankan arah lain, sedangkan ada argumen untuk berjalan dua arah. Politik dan pembuatan kebijakan keamanan siber terjadi dalam ekosistem yang kompleks di mana pemangku kepentingan dari masyarakat yang beragam, bidang kebijakan, dan pemerintah harus berinteraksi satu sama lain. Salah satu paradoks tersebut adalah bahwa pemerintah ingin memastikan keamanan dunia maya, tetapi pada saat yang sama mereka menginginkan akses ke data individu dan organisasi untuk tujuan pengawasan. Seluruh diskusi tentang akses 'pintu belakang' ke data mengungkapkan paradoks yang dihadapi oleh pemerintah. Di satu sisi, pemerintah ingin perusahaan dan warga

negara melindungi diri mereka sendiri, tetapi di sisi lain, mereka tidak ingin mereka menggunakan enkripsi dan tindakan keamanan dunia maya lainnya, karena hal ini memungkinkan teroris dan penjahat menyembunyikan jejak mereka.

Tabel 1 Tinjauan *Cyber security*

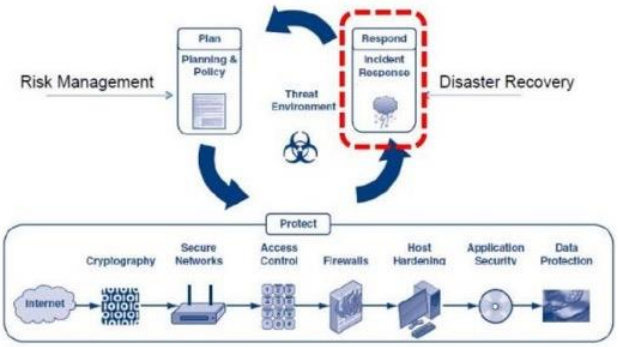
No	Pertanyaan kebijakan *Cyber* security	Deskripsi pembahasan
1	Apa tingkat perlindungan sistem yang diinginkan?	Pemerintah ingin perusahaan dan warga negara melindungi diri mereka sendiri. Namun demikian, pemerintah ingin memiliki pintu belakang untuk mengontrol dan mendeteksi kriminalitas dan terorisme.
2	Berapa banyak kolaborasi (lintas batas) yang diperlukan untuk memerangi keamanan siber?	Negara-negara perlu berkolaborasi karena keamanan dunia maya adalah fenomena global, namun mereka tidak saling percaya karena mereka mungkin aktif dalam meretas satu sama lain.
3	Kepada siapa harus berjuang?	Meskipun dampak serangan itu sering terlihat, serangan dan penjahatnya sulit ditentukan.
4	Berapa jumlah pengeluaran yang tepat untuk keamanan siber?	Pengeluaran yang terlalu sedikit untuk keamanan siber mungkin mengindikasikan bahwa mereka tidak terlindungi dengan baik, sementara pengeluaran yang terlalu banyak dapat mengirimkan pesan bahwa mereka terlalu khawatir dan mungkin ada sesuatu yang salah.
5	Apa tingkat visibilitas yang tepat?	Organisasi tidak mendapat manfaat dari membuat masalah dan serangan terlihat oleh pelanggan mereka karena dapat menurunkan keyakinan dan kepercayaan. Namun, visibilitas ini diperlukan untuk menciptakan rasa urgensi yang lebih besar dan memulai tindakan.
6	Bagaimana data akan digunakan?	Data yang sama yang dapat digunakan untuk meningkatkan kualitas hidup juga dapat digunakan terhadap warga negara.
7	Siapa yang harus memastikan keamanan siber sistem?	Organisasi yang menyediakan atau yang dapat menyediakan keamanan mungkin tidak akan terpengaruh oleh dampaknya.



Gambar 1. Evaluasi Kebijakan Pembentukan Tim Tanggap Insiden Siber Pada Sektor Pemerintah

Dari tujuan ini dapat dijelaskan bahwa kepentingan yang terpengaruh adalah seluruh sektor pemerintah dan masyarakat umum sebagai penerima layanan, implikasi dari adanya kebijakan ini adalah seluruh sektor khususnya sektor pemerintah harus segera membentuk CSIRT nya dalam kurun waktu sampai dengan tahun 2024. Namun dalam perjalanannya tidak sedikit kendala dan resistensi yang terjadi. Dari hasil analisa, ditemukan fakta bahwa sebelumnya, penanganan insiden masih belum terorganisir dan masih dijalankan

secara manual per kasus, juga dilakukan mandiri tanpa adanya koordinasi dengan instansi lainnya.[2]. Dan berdasarkan hasil manfaat yang didapatkan bahwa yang dihasilkan dari kebijakan pembentukan CSIRT pada sektor pemerintah adalah instansi pemerintah mampu menangani insiden *cyber* yang terjadi di ruang lingkup tanggung jawab mereka secara sistematis dan terorganisir melalui mitigasi awal, dan pengoordinasian dalam jangka waktu tertentu. Sementara manfaat yang dirasakan bagi masyarakat adalah pelayanan publik yang dapat diakses setiap saat, andal dan bebas gangguan atau hambatan. Pada dasarnya biaya investasi yang dianggarkan untuk pembentukan CSIRT akan jauh lebih murah jika dibandingkan dengan potential loss dan penurunan tingkat kepercayaan masyarakat yang mungkin terjadi jika suatu insiden siber melumpuhkan layanan pemerintah. Jika website atau aplikasi milik pemerintah dapat diretas maka masyarakat akan merasa khawatir data mereka bisa disebarluaskan dan disalah gunakan, sebagaimana yang pernah terjadi pada sistem milik BPJS Kesehatan tahun 2021 silam menyebabkan turunnya tingkat kepercayaan publik kepada pemerintah selaku pengelola data *public*.

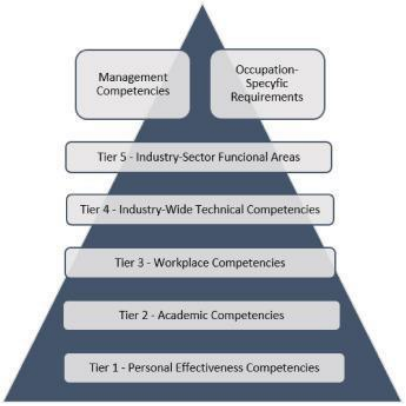


Gambar 2. Urgensi Penanganan Insiden Keamanan Informasi

Pengetahuan dalam penanganan insiden keamanan informasi diperoleh dari capture tacit knowledge dari ahli yang sudah memperoleh pengetahuan dan pengalaman serta trick-trick dalam menangani dan merespon insiden. Knowledge atau pengetahuan dalam menangani insiden adalah salah satu sumber daya yang penting bagi Bidang Siber & Sandi dalam mengemban misi terciptanya sistem keamanan informasi yang handal di lingkungan pemerintah[3]. Fakta menarik lainnya yang diperoleh dari hasil wawancara adalah bahwa kebanyakan penanganan insiden hanya bergantung pada satu orang admin yang dianggap menguasai sistem. Terkadang dikarenakan keterbatasan pengetahuan dan kapabilitas maka sering kali suatu aplikasi yang terkena serangan siber bukannya dilakukan prosedur penanggulangan dan pemulihan alih-alih dilakukan penonaktifan atau take down, sambil menunggu "bala bantuan" datang, baik menggunakan konsultan keamanan IT atau dari pihak yang dianggap lebih berkompeten. terkait SDM, terdapat kesenjangan yang cukup lebar antara jumlah dan kompetensi SDM yang dibutuhkan untuk mengelola tenaga ahli dengan apa yang tersedia di lapangan saat ini. Sekurang-kurangnya terdapat 650 Instansi Penyelenggara Negara dan 1000 Instansi Penyelenggara Layanan Publik. Apabila diasumsikan masing-masing instansi membutuhkan paling sedikit lima orang yang memiliki kompetensi di bidang Keamanan Siber. Serangan siber secara nyata telah memberikan dampak yang besar bagi negara terserang, terkhusus Indonesia, berdasarkan data yang ada telah menjadi negara dengan urutan tertinggi menjadi sasaran penyerangan siber oleh para hacktivist. Total kerugian yang sangat besar patut menjadi sebuah bahan evaluasi bagi bidang keamanan dan pertahanan terkhsusus pada bagian *cyber*space.

Gambar 3. Total Kebutuhan Jfs Dan Jfmi Tahun 2019, 2020, Dan 2021 Berdasarkan Hasil Validasi

Meningkatnya jumlah serangan siber yang mengeksploitasi kerentanan faktor manusia menentukan kebutuhan untuk meningkatkan kompetensi di bidang keamanan siber. Selain itu, kompetensi digital merupakan elemen penting dalam mengimplementasikan ide pembangunan berkelanjutan.Bahwa peningkatan pengetahuan dan kompetensi sangat penting untuk peningkatan keamanan *cyber*.
Posisi serupa dapat diamati dalam kegiatan NATO, yang menciptakan Pusat Kolaborasi Keamanan Siber, untuk bertukar pengalaman dan pelatihan. Kompetensi didefinisikan secara berbeda tergantung pada disiplin ilmu. Selain itu, dalam satu disiplin, seseorang juga dapat menemukan interpretasi yang berbeda dari kategori yang dibahas. Dalam literatur tentang subjek, beberapa definisi menghubungkan kompetensi dengan efektivitas tindakan di bidang tertentu. Dalam pendekatan lain, kompetensi terkait dengan mengumpulkan banyak kemampuan, keterampilan, dan sifat yang berbeda , keamanan siber terkait dengan kombinasi pengetahuan, keterampilan, dan sikap untuk memastikan keamanan siber. Memiliki kompetensi di bidang yang dibahas menentukan efektivitas tindakan unit dalam situasi pengambilan keputusan terkait dengan memastikan keamanan siber dan meminimalkan risiko insiden keamanan. Model Kompetensi Keamanan Siber, yang merupakan upaya untuk mendefinisikan, mengklasifikasikan, dan menormalkan pengetahuan, keterampilan, dan sikap terkait keamanan siber Model.



Gambar 4. Model Kompetensi Keamanan Siber

Tabel 2 Pengetahuan Publik Tentang Ancaman Terkait Dunia Maya Negara.

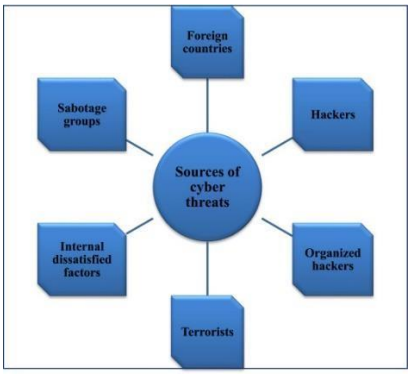
Ancaman	Memiliki pengetahuan	Tidak memiliki pengetahuan	Σ
Tindakan karyawan organisasi	329	1191	1520
Rekayasa sosial	281	1239	1520
Kejahatan dunia maya	822	698	1520
Mata-mata dunia maya	619	901	1520
*Cyber*terrorism	1115	405	1520
Perang dunia maya	597	923	1520
Σ	3763	5357	1520

5
2
0

Berdasarkan tabel di atas, pengetahuan responden tentang ancaman mungkin kurang dinilai. Sebagian besar responden tidak mengetahui skala insiden keamanan yang disebabkan oleh aktivitas karyawan organisasi atau rekayasa sosial. Hasil penelitian juga menunjukkan bahwa banyak responden yang tidak mengetahui secara spesifik ancaman seperti *cyber*war atau *cyber* spying. Sebagian besar responden menyadari ancaman *cyber*terrorism dan *cyber*crime dan dapat menilai skala dampak potensial dari kegiatan tersebut. Analisis karakteristik sosiodemografi dan hasil yang diberikan memungkinkan kita untuk berasumsi bahwa ada hubungan antara pendidikan, usia dan pengetahuan tentang ancaman negara dunia maya. Membandingkan data kuantitatif dalam kelompok individu dari struktur pendidikan, 85% orang dengan gelar atau gelar akademis mengetahui ancaman terhadap dunia maya negara.

Cyber telah meningkatkan hasil komunitas dan mendistribusikan informasi secara efektif dari waktu ke waktu. Apa pun aplikasi atau industri *cyber* yang digunakan, peningkatan produksi selalu menjadi pertimbangan. Transfer data yang cepat ke dunia maya sebagian besar menurunkan keamanan sistem secara total. Untuk profesional teknologi yang meningkatkan produksi, indikator keamanan sering bertentangan langsung dengan kemajuan karena indikator pencegahan mengurangi, melarang, atau menunda akses pengguna, menggunakan indikator yang mengidentifikasi sumber daya sistem kritis, dan menanggapi perhatian manajemen

Trojan horse adalah virus yang menyembunyikan kode berbahaya dan biasanya terlihat seperti program bermanfaat yang ingin dijalankan oleh pengguna [14]. Selain itu, virus mengotori file sistem, yang biasanya merupakan program praktis, dengan memasukkan salinannya ke dalam file tersebut. Dengan memuat file yang terinfeksi ke dalam memori, versi ini berjalan dan memungkinkan virus menginfeksi file lain. Tidak seperti worm, virus memerlukan campur tangan manusia untuk menyebar. Di sisi lain, worm adalah program sistem otonom yang meregenerasi dirinya sendiri dengan menyalin dari satu komputer ke komputer lain , terakhir, Botnet adalah jaringan sistem kendali jarak jauh yang terinfeksi, yang digunakan untuk mendistribusikan malware , mengoordinasikan serangan, dan mengirim spam serta mencuri pesan [15]. Botnet biasanya dipasang secara diam-diam di komputer target, memungkinkan pengguna yang tidak sah untuk mengontrol sistem target dari jarak jauh untuk mencapai tujuan jahat mereka. Botnet juga disebut sebagai tentara elektronik



Gambar 5. Sumber ancaman dunia maya

Tabel 3 Perkiraan kerugian akibat *cyber* crime

	Global	Indonesia
GDP		
Percent of global GDP Cost of	USD 71,60 bn	USD 895 bn
Genuine *cyber* crime:	USD 3,457 m	USD 43 bn
Transitional *Cyber* crime	USD 46,600 m	USD 582 m
Cyber criminal infrastructure:	USD 24,840 m	USD 310 m
Traditional crimes becoming *cyber*	USD 150,200 m	USD 2,748 m

Tabel ini mendeskripsikan bahwa perkiraan resiko akibat *Cyber crime* di Indonesia dapat terkomparasi dengan perkiaan kerugian global yang terjadi di dunia, perkiraan ini menjadikan Indonesia menurut data CIA diatas telah mencapai 1,20 % dari tingkat kerugian akibat *cyber crime* yang terjadi di dunia Kasus-kasus diatas tentunya menunjukkan suatu fenomena bahwasannya bagaimana bisa suatu sistem informasi yang dimiliki oleh suatu organisasi/instansi/lembaga elite diretas dan diinfeksi oleh orang-orang yang identitas dan keberadaannya tidak diketahui. Sistem informasi milik organisasi/instansi/lembaga elite sudah pasti dikelola oleh para tenaga ahli yang profesional dibidangnya masing-masing. Namun secara empiris sistem tersebut masih dapat dimasuki dan bahkan dirusak secara permanen oleh para pelaku kejahatan tersebut (hacker). Hal ini tentunya menimbulkan spekulasi apakah organisasi/instansi/lembaga elit yang berada di Indonesia telah menerapkan *Cyber security* compliance dengan baik dan benar

Kesimpulan

Pentingnya pengetahuan *Cyber security* adalah keharusan di era teknologi ini demi menjaga privasi dan keamanan hal tersebut tidak lepas dari peran pemerintahan yang menyediakan ruang internet publik yang bersih, Masyarakat kita berubah menjadi masyarakat yang memiliki ketergantungan pada Teknologi Informasi dan Komunikasi (TIK) di semua aspek kehidupan kita sehari-hari, yang menjadikan kebutuhan akan *Cyber security* sangat penting. Sifat serangan *cyber* yang tidak berwujud namun memiliki dampak yang besar merupakan suatu ancaman yang nyata, dampak yang ambigu dan paradoks. Sebagai rekomendasi ada beberapa hal yang harus dan dapat dilakukan oleh pemerintah Indonesia. Diantaranya adalah Menciptakan dan mengembangkan infrastruktur digital milik negara, hal tersebut dapat mengurangi resiko pemanfaatan data. dalam hal ini akan mengurangi resiko oleh oknum-oknum yang dapat membahayakan keselamatan dan kerahasiaan data.

Selanjutnya pihak terkait dapat melakukan peningkatan kapasitas personil dalam bidang pemetaan dan prediksi ancaman, dengan harapan badan keamanan siber memiliki kemampuan pemetaan dan pencegahan sedini mungkin terhadap upaya serangan siber dari pihak manapun. Ketiga, pemerintah indonesia harus membentuk sistem pertahanan keamanan yang lebih mandiri, baik dalam hal pengadaan alat keamanan maupun bidang teknologi informasi, dan tetap terlibat dalam kerjasama internasional dalam bidang keamanan. Terakhir adalah membuat rencana strategi nasional yang tepat dalam bidang keamana dan pertahanan *cyber*.

Daftar Rujukan

[1] P. Prabaswari, M. Alfikri, and I. Ahmad, "Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah," *Matra Pembaruan*, vol. 6, no. 1, pp. 1–14, 2022, doi: 10.21787/mp.6.1.2022.1-14.

[2] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cyber security awareness for children: A systematic literature review," Int. J. Child-Computer Interact., vol. 30, p. 100343, 2021, doi: 10.1016/j.ijcci.2021.100343.

[3] H. de Bruijn and M. Janssen, "Building Cyber security Awareness: The need for evidence-based framing

[4] strategies," Gov. Inf. Q., vol. 34, no. 1, pp. 1–7, 2017, doi: 10.1016/j.giq.2017.02.007.

[5] M. Firmansyah and A. Yuswanto, "Manajemen Pengetahuan Penanganan Insiden Keamanan Informasi Pada Security Operation Center Di Pemerintah Provinsi Dki Jakarta Knowledge Management For Information Security Incident Handling At Security Operation Center Of," Vol. 4, No. 2, Pp. 441–452, 2022.

[6] Indarta, Yose, et al. Keamanan Siber: Tantangan di Era Revolusi Industri 4.0. Yayasan Kita Menulis, 2022.

[7] V. Papakonstantinou, "Cyber security as praxis and as a state: The EU law path towards acknowledgement of a new right to Cyber security?," Comput. Law Secur. Rev., vol. 44, p. 105653, 2022, doi: 10.1016/j.clsr.2022.105653.

[8] Makbull Rizki, "Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi," Polit. J. Ilmu Polit., vol. 14, no. 1, pp. 54–62, 2022, doi: 10.32734/politeia.v14i1.6351.

[9] Suryono, Agus. Teori dan Strategi Perubahan Sosial. Bumi Aksara, 2019.

[10] Arianto, Adi Rio. "Cyber Security: Geometri Politik Dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21." Jurnal PIR: Power in International Relations 1.2 (2018): 108-118.

[11] Amansyah, Munawir. "Ketahanan Masyarakat Menghadapi Bencana (Upaya Preventif Meminimalisir Risiko Kesehatan)." (2021).

[12] A. R. Arianto, "Cyber Security: Geometri Politik Dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21," J. PIR Power Int. Relations, vol. 1, no. 2, p. 108, 2018, doi: 10.22303/pir.1.2.2017.108- 118.

[13] D. P. Setyawan and A. D. W. Sumari, "Diplomasi Pertahanan Indonesia dalam Pencapaian Cyber security Melalui ASEAN Regional Forum On Cyber security Initiatives," J. Penelit. Polit., vol. 13 no 1, no. 726, p. 35, 2016, [Online]. Available: https://www.researchgate.net/profile/Arwin-Sumari/publication/330347859_Diplomasi_Pertahanan_Indonesia_Dalam_Pencapaia N_Cyber Security_Melalui_Asean_Regional_Forum_On_Cyber Security_Initia Tives_Indonesia_Defense_Diplomacy_In_Achieving_Cyber Security_Through

[14] F. Kwarto and M. Angsito, "Pengaruh Cyber crime Terhadap Cyber security Compliance Di Sektor
Keuangan," J. Akunt. Bisnis, vol. 11, no. 2, pp. 99–110, 2018, doi: 10.30813/jab.v11i2.1382.

[15] Pamungkas, Petrus Dwi Ananto. "Analisis Cara Kerja Sistem Infeksi Virus Komputer." Bina Insani ICT Journal 1.1 (2018): 15-40.