**AL-IJTIMA`I:** *International Journal of Government and Social Science* **p-ISSN: 2467-9029**

**Vol. 9, No. 1, Oktober 2023** **e-ISSN: 2549-6921**

# FONDASI KEMANANAN SIBER UNTUK LAYANAN PEMERINTAH

**Dhanang Ksatrio Witjaksono [1]; Arimurti Kriswibowo[2]**
[1,2]*Universitas Pembangunan Nasional Veteran, Jawa Timur, Indonesia*
[1]*Contributor Email: 19041010104@student.upnjatim.ac.id*

**Abstract**

*The use of the internet in the current government environment continues to grow. The increasingly complex use of the internet can cause vulnerabilities to cyber attacks in information security, which include aspects of confidentiality, integrity, and service availability, so that it can disrupt the performance of public service delivery. The systematic literature review research method was carried out because of the large amount of information and data regarding cyber security strategies. This can be traced through various information in books, scientific journals, newspapers, magazines, as well as sources of information from web pages/websites via the internet. This method is important in analyzing the concept of cyber security strategy in Indonesia. The obstacles that the government has are expired devices that are still used on local government networks, which may not have the latest updates, security devices such as antiviruses have expired, human resources have not fully supported this cybersecurity. Indonesia needs policies that regulate all elements related to cyber security. This infrastructure standard must comply with international standards for dealing with cyber warfare.*

**Keywords:** *Cybersecurity, Electronic-Based Government System, Cyber Crime, Human Resources.*

## A. Pendahuluan

Pergerakan dunia menuju era yang serba digital menjadikan kebutuhan akan strategi keamanan siber berskala nasional yang komprehensif hangat diperbincangkan di kalangan pemerhati keamanan siber nasional. Dengan pemanfaatan Teknologi Informasi dan Komunikasi (TIK) yang semakin menjamur, hal ini mendorong terbentuknya Cyberspace. Menurut Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber, ruang siber (cyberspace) atau siber merupakan ruang dimana komunitas saling terhubung menggunakan jaringan (misalnya internet) untuk melakukan berbagai kegiatan sehari-hari.

Penggunaan internet di lingkungan pemerintahan saat ini terus mengalami pertumbuhan. Selaras dengan kebutuhan penyediaan layanan pemerintahan yang cepat dan aman, penggunaan internet yang makin kompleks dapat menyebabkan kerentanan akan serangan siber dalam keamanan informasi, yang meliputi aspek kerahasiaan, keutuhan, dan

ketersediaan layanan, sehingga dapat mengganggu kinerja penyelenggaraan pelayanan publik. Kementerian Pertahanan RI mendefinisikan serangan siber sebagai tindakan, kata-kata, atau pikiran yang disengaja atau tidak disengaja oleh para pihak, terlepas dari motivasi, latar belakang, atau tujuannya, di lokasi manapun, yang ditujukan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apapun, terhadap obyek vital maupun nonvital dalam lingkup militer dan nonmiliter, yang berpotensi mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa.

Tak dapat disangkal bahwa perkembangan teknologi informasi dan komunikasi telah berkontribusi secara positif terhadap perkembangan ekonomi global dan berdampak pada produktivitas, persaingan, dan keterlibatan warga negara yang lebih tinggi. Dengan mengingat hal di atas, pertahanan siber membantu menghindari peluang yang dapat merugikan individu dan negara. Pertahanan siber (cyber defense) merupakan upaya penanggulangan serangan cyber yang mengganggu penyelenggaraan pertahanan negara. Istilah pertahanan siber ini muncul sebagai upaya untuk memproteksi diri dari segala ancaman dan gangguan tersebut.

Keamanan siber nasional mencakup semua upaya untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi, serta semua lembaga pendukung lintas sektoral tingkat nasional. Untuk memperoleh keamanan siber, diperlukan pertahanan siber bertingkat mulai dari lingkup perorangan kelompok kerja, organisasi sampai dengan skala nasional (dalam Pedoman Pertahanan SIber). Sektor-sektor utama yang mengelola infrastruktur kritis seperti pertahanan dan keamanan, energi, sistem keuangan, transportasi dan berbagai layanan publik lainnya mendapat perhatian khusus dalam hal ini. Salah satu alasan yang mendasarinya adalah gangguan dalam sistem elektronik pada sektor - sektor ini dapat menyebabkan turunnya tingkat kepercayaan pada pemerintah, kerugian ekonomi, terganggunya ketertiban masyarakat dan masih banyak lainnya. Risiko ini menjadi dasar pertimbangan pentingnya mencapai keamanan siber yang kuat dalam suatu negara (Pertahanan Siber, 2014.).

Pemerintah telah melakukan upaya untuk meningkatkan keamanan siber di Indonesia, namun upaya tersebut masih perlu ditingkatkan mengingat dalam

pemeringkatan Indeks keamanan Siber Global (Global Cybersecurity Index - GCI), Indonesia menempati peringkat 77 dari 193 anggota. (Aptika dan IKP et al., n.d.)

Tantangan terbesar saat ini adalah penguatan kelembagaan keamanan siber di Indonesia, Kurangnya dasar hukum yang optimal untuk keamanan siber, dan kurangnya staf profesional dan kerjasama dengan komunitas nasional dan internasional. Oleh karena itu, penting bagi pemerintah untuk memperkuat keamanan siber dan mempersiapkan masyarakat yang dibutuhkan di dunia yang semakin digital. Pada dasarnya, praktik penerapan keamanan siber tidak dapat dilaksanakan secara optimal tanpa landasan hukum yang optimal, sehingga UU Keamanan Siber meluncurkan upaya keamanan nasional Indonesia terhadap maraknya serangan siber di era Society 5.0 saat ini (Budi et al., 2021)

Berlandaskan fakta pada latar belakang masalah keamanan siber tersebut, kajian ini ditujukan untuk menjawab masalah terkait kerentanan serangan siber di layanan pemerintah Indonesia sehingga kebutuhan akan strategi keamanan siber berskala nasional di Indonesia sebagai fondasi untuk layanan pemerintah yang lebih kuat perlu segera ditemukan solusinya. Pembahasan dan diskusi dalam studi ini difokuskan untuk menyoroti dan menjelaskan berbagai persoalan yang berkaitan dengan serangan siber yang rentan terjadi di Indonesia khususnya dalam lingkup pemerintahan serta peranan stakeholder vital dalam upaya perbaikan ini sehingga ditemukan pemahaman atas kebutuhan yang harus dipenuhi dalam menguatkan fondasi keamanan siber di Indonesia.

## B. Metode

Penelitian ini menggunakan metode penelitian *Systematic Literature Review* dan Observasi dengan metode pengumpulan data berupa dokumen publik. *Systematic Literatur Review* merupakan sebuah metode pebnelitian yang mana merupakan sebuah cara untuk indentifikasi, evaluasi, dan interpretasi semua ketersediaan penlitian yang relevan terhadap rumusan masalah atau area topik yang diteliti (Calderon, 2015). *Systematic Literature Review* (SLR) didefinisikan sebagai proses mengidentifikasi, menilai, dan menafsirkan semua bukti penelitian yang tersedia dengan tujuan untuk menyediakan jawaban untuk pernyataan penelitian secara spesifik (Kitchenham et al., 2009).

Tujuan dari studi literatur ini adalah untuk membuat kerangka kerja untuk ini. Sebuah teori yang membantu memecahkan masalah yang sedang dipelajari Pengungkapan konsep yang secara khusus terkait dengan kasus Studi ini akan mempelajari lebih lanjut tentang faktor-faktor yang berpengaruh terhadap keamanan siber pada layanan pemerintah.

**C. Hasil dan Pembahasan**

Serangan siber adalah serangan terhadap sistem komputer atau jaringan yang mengendalikan sistem komputer target atau mendapatkan akses tidak sah ke sistem komputer target. (Maurer & Morgus, 2014; Marshall & Saulawa, 2015). Disisi lain, Cybercrime adalah kegiatan ilegal yang menargetkan pada suatu sistem atau jaringan komputer (ITU, 2012) Dalam arti lain, cybercrime merupakan sebutan yang merujuk pada kegiatan kriminal dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan (Abidin, 2017) yang dapat menimbulkan kerugian materiil atau immateriil pada pihak yang menjadi sasaran (Wilson, 2008).

Cybercrime atau kejahatan dunia maya biasanya mengacu pada kegiatan kriminal yang melibatkan komputer atau jaringan komputer sebagai bagian yang tidak terpisahkan. Istilah ini juga digunakan dalam kegiatan kriminal tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan tindak kriminal itu terjadi (Saragih & Azis, 2020). Pada dasarnya, tidak semua serangan dunia maya didefinisikan sebagai kejahatan, tetapi baik serangan dunia maya maupun kejahatan dunia maya dianggap sebagai ancaman dunia maya. Ancaman dunia maya adalah aktivitas yang dapat terjadi, menyebabkan masalah serius pada jaringan atau sistem komputer dan mempengaruhi semua aspek. (CIPS, 2019).

Untuk melindungi dan meminimalkan dunia maya dari ancaman dunia maya, keamanan dunia maya diperlukan agar ruang maya dapat terus berfungsi. Keamanan siber terdiri dari praktik, tindakan, dan penanggulangan untuk melindungi ekosistem siber dan aset perusahaan serta pengguna dari serangan jahat yang bertujuan untuk mengurangi kerahasiaan, integritas, dan ketersediaan informasi dan data. (Fischer, 2005; ITU, 2012). Data Global Cyber Security Index 2020 didasarkan pada konsep lima kategori evaluasi atau

disebut lima pilar kerangka GCI: hukum, teknologi dan prosedur, organisasi, peningkatan kapasitas, kerja sama internasional, siber Indonesia. posisi keamanan di 24 's. Skor 94 dan 88 jauh di belakang Singapura dan Malaysia yang masing-masing berada di peringkat ke-4 dan ke-5.

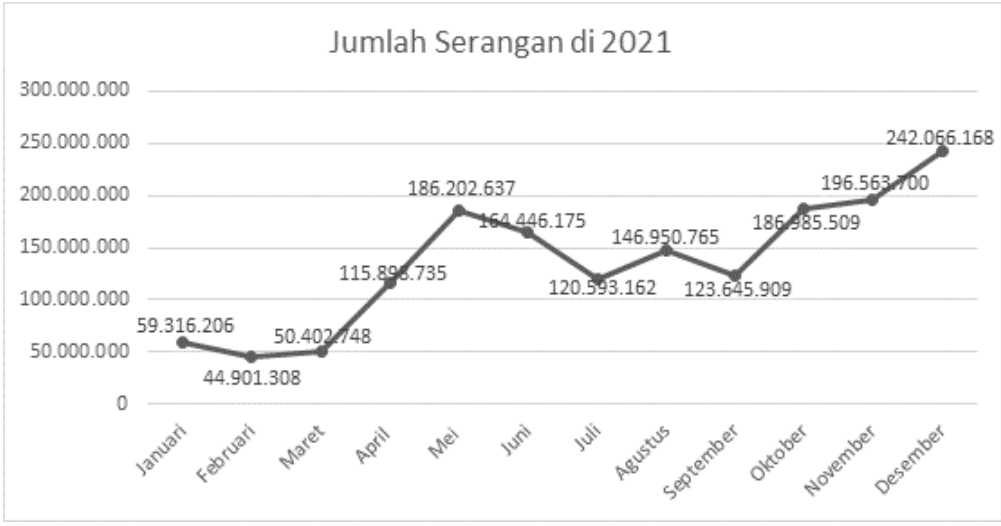
| Country Name | Score | Rank |
|---|---|---|
| United States of America** | 100 | 1 |
| United Kingdom | 99,54 | 2 |
| Saudi Arabia | 99,54 | 2 |
| Estonia | 99,48 | 3 |
| Korea (Rep. of) | 98,52 | 4 |
| Singapore | 98,52 | 4 |
| Spain | 98,52 | 4 |
| Russian Federation | 98,06 | 5 |
| United Arab Emirates | 98,06 | 5 |
| Malaysia | 98,06 | 5 |
| Lithuania | 97,93 | 6 |
| Japan | 97,82 | 7 |
| Canada** | 97,67 | 8 |
| France | 97,6 | 9 |
| India | 97,5 | 10 |
| Turkey | 97,49 | 11 |
| Australia | 97,47 | 12 |
| Luxembourg | 97,41 | 13 |
| Germany | 97,41 | 13 |

| Country Name | Score | Rank |
|---|---|---|
| Portugal | 97,32 | 14 |
| Latvia | 97,28 | 15 |
| Netherlands** | 97,05 | 16 |
| Norway** | 96,89 | 17 |
| Mauritius | 96,89 | 17 |
| Brazil | 96,6 | 18 |
| Belgium | 96,25 | 19 |
| Italy | 96,13 | 20 |
| Oman | 96,04 | 21 |
| Finland | 95,78 | 22 |
| Egypt | 95,48 | 23 |
| Indonesia | 94,88 | 24 |
| Viet Nam | 94,59 | 25 |
| Sweden | 94,55 | 26 |
| Qatar | 94,5 | 27 |
| Greece | 93,98 | 28 |
| Austria | 93,89 | 29 |
| Poland | 93,86 | 30 |

Gambar 1. Peringkat Keamanan Siber di Dunia Tahun 2020 (Global Cybersecurity Index, 2020)

Berdasarkan data A.T. Kearney (2018) Indonesia belum memiliki sektor yang didedikasikan untuk keamanan siber di Indonesia. Terkait strategi nasional, Indonesia baru mulai mewujudkan peningkatan kesadaran, peningkatan kapasitas dan legislasi. Hal ini sama dengan hasil laporan data National Cyber Security Index (2021), yang menempatkan Indonesia pada peringkat ke-5 dari 10 negara ASEAN dan peringkat ke-77 dari 160 negara yang masuk dalam NCSI 2020 dengan skor indeks sebesar 38,96. Selain melindungi layanan yang penting bagi keamanan siber, Indonesia menyatakan bahwa regulasi, undang-undang, dan regulasi masih lemah. Hal ini juga ditandai dengan landasan hukum pengelolaan keamanan siber Indonesia. Hal itu hanya terlihat dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) Nomor 11 Tahun 2008 dan kemudian direvisi menjadi Undang-Undang ITE Nomor 19 Tahun 2016. Undang-undang tersebut berisi aturan untuk beberapa pelanggaran, termasuk distribusi konten, pelanggaran data ilegal, akses tidak sah ke sistem komputer untuk memperoleh informasi, penyalahgunaan ilegal dan tidak sah atau pencurian komputer lain atau sistem elektronik.

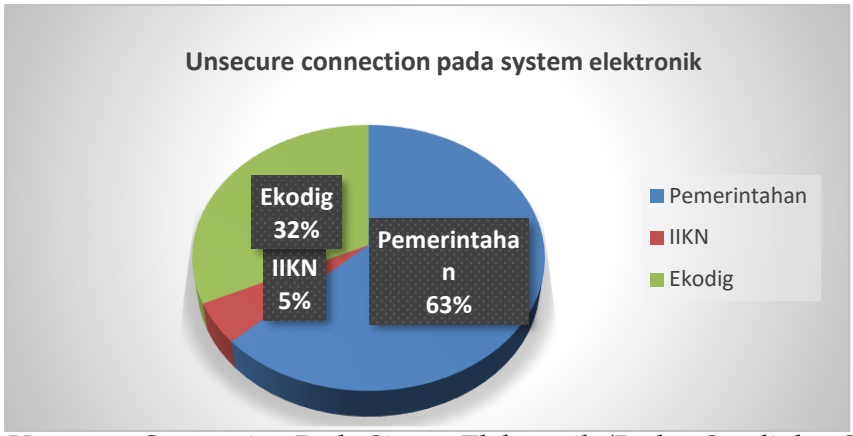
1. Jumlah Serangan Siber di Indonesia




Gambar 2. Jumlah Serangan Tahun 2021 di Indonesia (Badan Sandi dan Siber Negara, 2022)

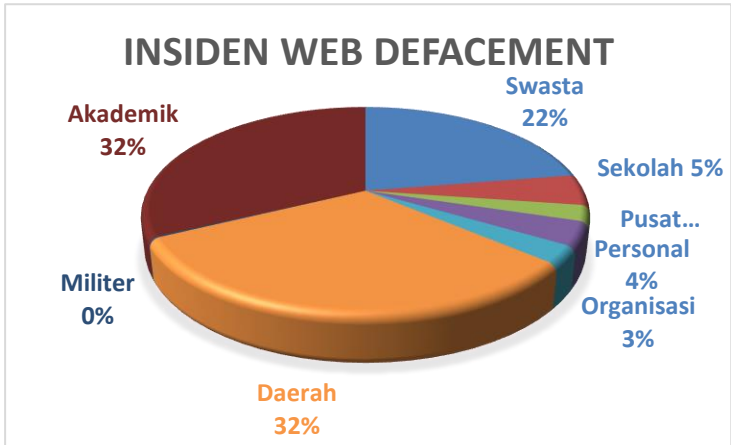
Berdasarkan data yang diperoleh di Indonesia terdapat 1,6 miliar atau lebih tepatnya 1.637.973.022 serangan siber yang terjadi di seluruh wilayah indonesia, Sebagian besar kategori anomali: malware, aktivitas Trojan horse, dan pengumpulan intelijen (mengumpulkan informasi untuk mencari kerentanan keamanan). Pada tahun 2021, setidaknya 44,62% dari anomali lalu lintas akan didominasi oleh botnet MyloBot. Selain botnet MyloBot, beberapa anomali dalam kategori Top 10 Anomaly juga menyertakan tautan ke botnet lain seperti ZeroAccess dan DiscoverUsingSocksAgent dalam serangan tersebut. Botnet adalah jaringan komputer yang terinfeksi malware yang dikendalikan oleh satu penyerang. Botnet dapat dirancang untuk spam, pencurian data, ransomware, penipuan klik, penolakan layanan (DoS), dan banyak lagi. Dalam periode tersebut, sektor pemerintah merupakan sektor tertinggi yang mengalami kebocoran data akibat malware pencuri informasi yakni dengan sebaran 45,5%, yang kemudian disusul oleh sektor keuangan (21,8%), telekomunikasi (10,4%), penegakan hukum (10,1%), transportasi (10,1%), dan BUMN lainnya (2,1%).

2. Sektor yang rentan akan ancaman Siber di Indonesia




Gambar 3. Unsecure Connection Pada Sistem Elektronik (Badan Sandi dan Siber Negara, 2022)

Koneksi tidak aman sistem elektronik dalam grafik adalah bahwa pemerintah menyumbang hingga 63% dari sistem koneksi tidak aman, yang kedua adalah ekonomi digital sebesar 32%, dan tempat ketiga adalah infrastruktur informasi kritikal nasional sebesar 5%. Hambatan yang dimiliki oleh pemerintah adalah perangkat kedaluwarsa yang masih digunakan di jaringan pemerintah daerah dan mungkin tidak memiliki pembaruan terbaru. Perangkat keamanan seperti program antivirus telah kedaluwarsa dan sumber daya manusia tidak sepenuhnya mendukung keamanan siber ini. Web defacement adalah peretasan yang mengubah konten website, misalnya mengganti layout, font, memunculkan iklan, sampai perubahan konten keseluruhan. Peretasan ini juga bisa masuk lebih jauh hingga mencuri data dan sebagainya.




Gambar 4. Insiden Web Defacement 2021 (Badan Sandi dan Siber Negara, 2022)

Beberapa faktor yang menyebabkan sebuah situs diserang diantaranya adalah mulai dari aplikasi yang tidak dilakukan update, tidak memiliki keamanan yang baik hingga aplikasi generik yang rentan. Sektor yang paling banyak mengalami insiden web defacement yakni situs pemerintah daerah sebanyak 32,57 persen dan situs pemerintah pusat sebanyak 2 persen.

Peretas sering mengeksploitasi kerentanan dalam aplikasi umum. Misalnya framework aplikasi yang digunakan oleh pemilik website. Kerentanan tersebut kemudian dimanfaatkan oleh para hacker untuk melakukan web tampering. Pemangku kepentingan juga tidak memiliki batas keamanan yang tepat, visibilitas ke firewall aplikasi web, atau visibilitas ke aktivitas anomali yang terjadi di situs web yang mereka kelola. Akibatnya, kebanyakan orang tidak tahu apakah situs tersebut telah direfas hingga mereka tidak dapat memblokir aktivitas serangan. Peretasan dapat terjadi atau dapat terjadi berulang kali. Aplikasi yang tidak diperbarui secara berkala oleh pemilik sistem juga rentan diretas. Inilah salah satu penyebab website hacks yang terjadi. Selain itu, administrator situs web tidak sepenuhnya menyelesaikan kasus penyusupan, sehingga aplikasi dan situs web sering diretas oleh peretas. Ini karena seorang peretas dapat memasang pintu belakang dan mengakses server untuk mengakses situs.

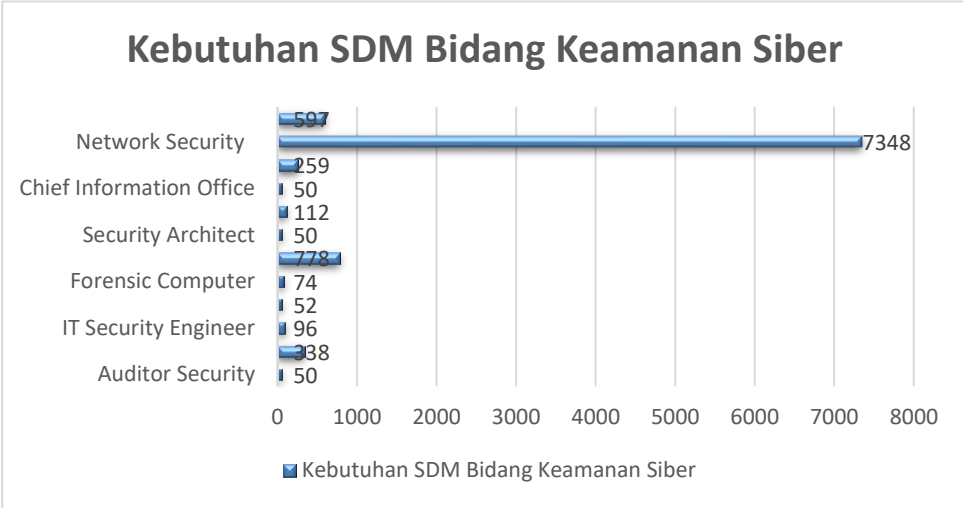
Oleh karena itu, pihak yang berkepentingan atau memiliki kewenangan untuk mengelola website suatu institusi untuk keamanan tambahan. Melakukan uji keamanan secaraberkali pada system elektronik layanan publik pun menjadi langkah untuk mencegah peretasan. Selain itu, sistem yang diretas harus responsif.

3. Kebutuhan SDM Bidang Keamanan Siber di Indonesia

Sumber daya manusia merupakan salah satu faktor terpenting dalam memastikan implementasi keamanan siber sesuai dengan pedoman yang telah ditetapkan. Pengetahuan dan keterampilan khusus perlu tersedia dan dipelihara karena keamanan perlu berubah. Rekrutmen diwujudkan dalam bentuk program rekrutmen, pembinaan, dan pemisahan terkait dengan peraturan yang berlaku.

Terkadang manusia merupakan mata rantai terlemah dalam rantai keamanan. Tidak peduli seberapa hati-hati, manusia dapat tergelincir dan membuat kesalahan di beberapa titik. Karena itu kesadaran sangat penting dalam keamanan siber. Dalam

manajemen sumber daya manusia, teknologi, serta penelitian dan pengembangan (Research and Development) untuk memperkuat keamanan siber, Pemerintah dalam hal ini Kementerian Pendidikan, Kebudayaan, Ristek bekerjasama dengan BSSN dan Kementerian Komunikasi dan Informatika harus melakukan upaya terobosan untuk mendidik dan merekrut profesional keamanan teknologi informasi yang memiliki integritas dan etika yang sempurna untuk mendukung mengembangkan dan menjalankan keamanan siber.




Gambar 5. Data Kebutuhan SDM Bidang Keamanan Siber (Jobstreet.co.id, 2022)

Berdasarkan data asal BSSN tahun 2020, diperoleh data sebesar 9804 lowongan di Industri bagi sumber daya insan bidang Keamanan SIber di Indonesia. Sekurang-kurangnya ada 650 Instansi Penyelenggara Negara serta 1000 Instansi Penyelenggara Layanan Publik. apabila diasumsikan masing-masing Instansi membutuhkan paling sedikit lima orang yg memiliki kompetensi di bidang keamanan Siber, maka total sdm yang diharapkan merupakan 18.054 orang.

Hal ini harus sebagai perhatian terbesar pemerintah, karena global teknologi ketika ini tidak terlepas berasal revolusi Teknologi gosip dan Komunikasi (TIK). Revolusi Teknologi isu serta Komunikasi (TIK) ialah Sistem Pemerintahan Berbasis elektronika (SPBE) atau eGovernment, pemerintahan yg menggunakan TIK buat melayani instansi pemerintah, pejabat, pengusaha, masyarakat, dan pemangku kepentingan lainnya. SPBE mempromosikan serta menerapkan pemerintahan yg terbuka, partisipatif, inovatif dan

akuntabel, memperkuat kolaborasi antara lembaga pemerintah pada aplikasi operasi serta tugas pemerintah buat mencapai tujuan beserta, serta komunitas yg lebih luas, meluas ke ketidakpuasan elektronika dan publik serta menaikkan kualitas serta jangkauan pelayanan publik.

Waktu memasuki dunia teknologi, elemen kunci yang nantinya dimasukkan dalam Sistem Pemerintahan Berbasis elektro (SPBE) paling penting adalah integritas serta autentifikasi, mengenali menggunakan siapa berinteraksi di global maya, BSSN harus membentuk budaya keamanan siber secara nasional dan dituangkan pada seni manajemen keamanan siber nasional , yg terakhir merupakan Human Capital yang sedang dilaksanakan oleh pihak BSSN berafiliasi menggunakan pihak akademisi, komunitas, dan industri untuk menciptakan kapasitas sdm pada Indonesia melalui pengembangan standar kompetensi kerja nasional Indonesia. Hal ini berhubungan dengan teknologi yang dikembangkan sesuai dengan jaringan yang dimiliki oleh BSSN. Namun, saat ini sedang teknologi cloud meluas di perusahaan bahkan industri sehingga menjadikan pendekatan keamanan melalui cloud. Dalam teknologi cloud sendiri terdapat self responsibility yang harus dikenali masyarakat, begitu juga dengan tren mikro yang harus diselaraskan. Untuk mengurangi berbagai macam risiko dari lingkungan pemerintah maka BSSN membangun Sistem Pemerintahan Berbasis Elektronik Nasional.

4. Peran BSSN Dalam SPBE Nasional

Peran BSSN pada SPBE Nasional merupakan pada penyususunan arsitektur SPBE, penerapan keamanan, aplikasi keamanan audit, pertimbangan kelayakan keamanan pada pembangunan infrastruktur misalnya sentra data nasional, sistem jaringan pemerintah, & badan penghubung layanan pemerintah, kiprah terakhir merupakan manajemen keamanan yang berfungsi buat memudahkan melakukan kontrol dalam sistem pemerintahan yang mempunyai ribuan aplikasi. Sistem pemerintahan berbasis elektronik (SPBE) diterapkan untuk membangun pemerintahan yang cepat dan efisien. Namun, pada kenyataannya, berbagai institusi membuat aplikasi dengan-fungsionalitas-yang-tumpang tindih,-meskipun tidak relevan-dengan kebutuhan mereka. Oleh karena-itu, arsitektur SPBE diperlukan-sebagai pedoman dalam-membangun-dan menyempurnakan aplikasi baik untuk instansi pemerintah pusat maupun daerah.

Arsitektur SPBE merupakan kerangka dasar untuk mengintegrasikan proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menciptakan layanan SPBE yang terintegrasi. Arsitektur SPBE adalah alat yang mendukung pengambilan keputusan manajemen dan pembuatan kebijakan untuk tata kelola dan manajemen manajer teknologi informasi dan komunikasi (TIK). Namun hingga saat ini, baik arsitektur SPBE nasional maupun model referensi arsitektur belum tersedia. Situasi saat ini adalah penurunan infrastruktur dan sistem aplikasi, serta kesenjangan keamanan yang masih tersebar di seluruh kementerian dan daerah. Arsitektur SPBE memberikan dampak positif bagi masyarakat dan pemerintah karena memberikan kemudahan operasional, penyederhanaan struktur, dan penghematan anggaran. Sementara itu, masyarakat memiliki pemerintahan yang kredibel dan kredibel, meningkatkan kualitas hidup dan meningkatkan pelayanan.

Tujuan dari arsitektur SPBE adalah untuk mengurangi duplikasi fungsi bisnis negara, mengurangi duplikasi infrastruktur dan sistem informasi, menerapkan standarisasi TIK, dan berbagi data dan informasi. SPBE dengan integrasi layanan SPBE. Selain itu, dengan menerapkan arsitektur SPBE, setiap instansi dapat menghilangkan aplikasi yang tidak berfungsi dan aplikasi yang tumpang tindih dengan aplikasi lain.

Arsitektur SPBE memiliki enam keunggulan, antara lain penghapusan duplikasi fungsi bisnis pemerintah. Menghilangkan duplikasi aplikasi dan infrastruktur teknologi informasi dan komunikasi (TIK) dan meningkatkan keamanan informasi. Implementasi standarisasi TIK dan standarisasi kualitas nasional layanan digital. Berbagi data dan informasi sesuai kebijakan OneData Indonesia. Memfasilitasi integrasi layanan pemerintah, sehingga memfasilitasi inovasi proses bisnis baru dan pengembangan layanan. Meningkatkan koordinasi perencanaan dan penganggaran SPBE untuk meningkatkan efisiensi dan efektivitas pelaksanaan SPBE. Infrastruktur SPBE Nasional

Infrastruktur SPBE mencakup semua perangkat keras, perangkat lunak, dan fitur yang memberikan dukungan utama untuk menjalankan sistem, aplikasi, komunikasi data, pemrosesan dan penyimpanan data, perangkat terintegrasi / terhubung, dan perangkat elektronik lainnya. Aplikasi SPBE adalah seperangkat program komputer atau program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE. Aplikasi Generik adalah aplikasi SPBE yang memenuhi standar yang sama dan digunakan

untuk penggunaan bersama oleh otoritas pusat dan/atau pemerintah daerah. Aplikasi Khusus adalah aplikasi SPBE yang dibuat, dikembangkan, digunakan, dan dipelihara oleh pemerintah pusat atau daerah tertentu untuk memenuhi kebutuhan khusus yang tidak dibutuhkan oleh pemerintah pusat atau daerah lainnya. Peran BSSN dalam evaluasi SPBE dapat dibagi menjadi tiga indikator: peningkatan keamanan kebijakan internal terkait pengelolaan keamanan informasi, peningkatan maturitas penerapan manajemen keamanan informasi, dan peningkatan maturitas audit keamanan SPBE.

5. Hambatan Terkait Cyber Security yang Harus Diatasi

Menurut Hasyim Gautama, ada beberapa kendala yang harus kita hadapi terkaitperkembangan cyber security dalam skala nasional, seperti (Ardiyan, 2014) :

a. Kurangnya pemahaman pejabat negera terkait keamanan siber,

Berawal dari kurangnya pemahaman pejabat negara terkait keamanan siber dapat menyeababkan kurangnya dukungan anggaran yang dimuntahkan sang pemerintah. Maju serta canggihnya keamanan siber berkorelasi dengan belanja keamanan siber yang dimuntahkan (Qamar, 2020). Sepanjang tahun 2011 hinga 2021 anggaran pada lembaga BSSN, dimana artinya lembaga yg mempunyai tugas utama pada bidang keamanan siber cenderung mengalami fluktuatif, dimana pada tahun 2019 merupakan kenaikan anggaran tertinggi sepanjang tahun tersebut.

Anggaran penindakan tidak pidana siber di Kepolisian mencapai Rp43,53 miliar pada tahun 2020, dimana penanganan tindak pidana siber adalah salah satu tugas dan tanggungjawab Kepolisian RI. aturan ini dipergunakan untuk mewujudkan stabilitas politik serta keamanan melalui penegakan hukum yang professional, proporsional, dan akuntabel serta menjunjung tinggi hak asasi insan khususnya dalam keamanan siber (Kepolisian RI, 2020). Tetapi jika dilakukan perbandingan antara anggaran penindakan tindak pidana siber tersebut menggunakan jumlah masalah tindak pidana siber yang sebanyak 12.197 di tahun yang sama, maka diperoleh bahwa aturan penanganan perkara kejahatan siber rata rata sebesar Rp3,57 juta. Nilai ini jauh asal istilah ideal, mengingat aturan tindak pidana umum dengan indikator kinerja perkara simpel di tingkat POLSEK memerlukan aturan sebesar Lima Juta per perkara (Kepolisian Resot Sumbawa, 2019).

Sedangkan buat penanganan perkara tindak pidana umum menggunakan indikator kinerja perkara sedang pada taraf POLSEK memerlukan anggaran sebanyak Rp15 juta per masalah (Kepolisian Resot Sumbawa, 2019). Sedangkan anggaran penyidikan taktis inteligen pada lingkungan Baintelkam Mabes Polri, besaran aturan yang penyidikan mencapai Rp20 juta per kasus. dalam proses penyidikan masalah kasus tindak pidana siber metode yang dipergunakan hamper sama menggunakan penyelidikan pada menangani kejahatan narkotika, terutama pada undercover serta control delivery. Hal ini dapat diartikan bahwa penanganan tindak pidana siber memiliki kompleksitas yg lebih dibandingkan menggunakan tindak pidana awam. Hal ini menunjukkan bahwa dukungan anggaran bagi penindakan tindak pidana siber masih kurang. Minimnya dukungan anggaran tadi bisa mengakibatkan di tidak tertanganinya laporan rakyat atas tindak pidana siber yg terjadi, yg dalam jangk panjang jua mengakibatkan pada menurunnya agama warga terhadap aparat penegak aturan.

b. Server layanan yang beberapa masih ada di luar negeri,

Perangkat teknologi informasi yang digunakan hampir sebagian besar merupakan produk dari luar negeri. Belum terdapat start up local yang berkecimpung dalam bidang keamanan siber (BSSN, 2020). Hal ini sebagai tantangan tersendiri bagi pembangunan keamanan siber di Indonesia. menjadi contoh, guna membangun stabilitas keamanan nasional dalam penguatan keamanan siber, salah satu upaya yg dilakukan dari pihak Kepolisian adalah-membuatkan intelijen media. Sistem intelijen media yg digunakan Polisi Republik Indonesia-waktu ini mengumpulkan data-dari pemberitaan 6000 media online (nasional, lokal, dan internasional asal 132 negara),-165 media cetak (nasional, lokal dari 10 provinsi sampai saat ini), 11 media televisi nasional,-media umum Twitter, Facebook, Instagram, dan Youtube (Herlambang, 2019). dengan menggunakan teknologi AI (Artificial Intellegence) pada intelijen media, dibutuhkan Kepolisian dapat mencegah post truth yang berpotensi buat merusak stabilitas-keamanan nasional.

Terkait-menggunakan hal tersebut sistem intelijen media yg digunakan sang Kepolisian saat ini-artinya perangkat teknologi informasi yg dibeli asal luar negeri. Mengingat alat-alat yang-dipergunakan oleh Kepolisian pada menjaga keamanan nasional merupakan teknologi-yang dikembangkan sang pihak ketiga, terlebih lagi transfer

teknologi yg dilakukan waktu-pembelian teknologi informasi, sporadis diikuti menggunakan-transfer knowledge.-Tentunya hal ini menjadi satu hambatan pada upaya mempertinggi-keamanan siber.

c. Undang undang siber yang hingga saat ini belum disahkan,

Indonesia sendiri, sejauh ini memang belum memiliki suatu grand design kebijakan keamanan siber yang komprehensif dan integratif buat menghadapi aneka macam ancaman siber yg ada (BSSN, 2020). sesuai laporan BSA The software Alliance (2015), Indonesia sedang dalam tahap awal mengembangkan strategi keamanan siber nasional. Kerangka hukum buat keamanan siber di Indonesia masih tergolong lemah, bahkan tidak adanya undang undang atau kebijakan keamanan misteri yang jelas, dan praktik keamanan beredar di banyak sekali undang undang. Selain itu pula tidak ada ketentuan keamanan siber spesifik yang berlaku.

Peraturan yang ada waktu ini hanya terkait Undang Undang nomor 19 Tahun 2016 wacana isu serta Transaksi elektronika (UU ITE) serta Peraturan Pemerintah No. 71 Tahun 2019 perihal Penyelenggaraan Sistem dan Transaksi elektro (PP PSTE), RUU tentang proteksi Data pribadi pun masih dalam proses pembahasan sang dewan perwakilan rakyat, sementara RUU tentang Keamanan dan Ketahanan Siber juga belum ada pembahasan lebih lanjut. UU ITE sendiri menyampaikan perlindungan aturan buat konten sistem elektronik serta transaksi elektronika. tapi, UU ini tidak meliputi aspek krusial keamanan siber, mirip infrastruktur isu dan jaringan, serta sumber daya insan dengan keahlian di bidang keamanan siber (CIPS, 2019).

d. Tata Kelola kelembagaan siber yang masih bermasalah,

Penanganan tindak pidana siber di Indonesia bisa dilakukan oleh pihak Kepolisian Republik Indonesia dan Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). Hal ini dimungkinkan terjadi, mengingat di Kominfo ada Penyidik Pegawai Negeri Sipil (PPNS) yg bisa membatu menyelidik serta menyampaikan bukti jejak digital pada penanganan berbagai kasus kejahatan siber. Tetapi tanpa adanya komunikasi serta sinergitas yg baik antara Kepolisian serta Kominfo, penangan tindak pidana siber di Indonesia bisa menjadi kurang optimal. sehingga perlu adanya pembagian sektor yang jelas antara jenis tindak pidana siber yang akan dilakukan sang Kepolisian atau Kominfo.

Tanpa adanya pembagian sektor penanganan tindak pidana siber yg kentara, akan berakibat di adanya beberapa sektor kasus tindak pidana siber yang akan ditangani oleh Kepolisian dan Kominfo. Hal ini bisa mengakibatkan adanya permasalahan kepentingan antara ke 2 instansi tadi. tetapi pada sisi lain, akan terdapat sektor tindak pidana siber yang tak tertangani sang ke 2 forum. sebagai akibatnya koordinasi dan sinergitas antara Kepolisian serta Kominfo pada hal ini PPNS ialah keharusan. Hal ini bertujuan agar tertanganinya tindak pidana siber yang terjadi pada Indonesia secara optimal.

e. Minimnya kesadaran akan ancaman internasional dari serangan dunia maya yang dapat melumpuhkan infrastruktur vital suatu negara.

Kesadaran keamanan siber dimasyarakat masih tergolong rendah, selain berdasarkan atas laporan A.T Kearney (2018) yg menyebutkan bahwa pencerahan rakyat atas keamanan siber masih dalam kategori nascent (baru lahir/terbentuk) hal ini jua ditunjukkan berdasarkan penelitian yg telah dilakukan oleh *Communication and Information System Security Research Center* (CISSReC) (2017) di sembilan kota besar tanah air (DKI Jakarta, Bandung, Semarang, Yogyakarta, Surabaya, Medan, Palembang, Bali serta Makasar), bahwa hanya sebesar 33 persen masyarakat sadar akan pentingnya melakukan keamanan siber. Hal ini membagikan bahwa sebagian besar masyarakat masih enggan untuk melakukan pengamanan pada aset yang terkoneksi ke wilayah siber.

Penanganan cybercrime bersifat parsial dan cenderung menyebar karena kurangnya koordinasi yang baku. Ini sangat berbahaya karena serangan siber dapat melumpuhkan infrastruktur penting negara. Misalnya, sistem radar di Bandara Internasional Soekarno Hatta beberapa kali terputus. Serangan siber selalu mungkin terjadi pada infrastruktur penting negara itu. Indonesia membutuhkan kebijakan yang mengatur semua elemen terkait keamanan siber. Dalam semua kebijakan yang mengatur sistem TIK, komunikasi yang digunakan mencakup semua peraturan yang memerlukan dokumentasi standar sebagai acuan pelaksanaan semua proses yang terkait dengan keamanan informasi. Standar infrastruktur ini harus sesuai dengan standar internasional untuk menghadapi perang cyber. kita memerlukan perlindungan perimeter yang tepat dan sistem pemantauan jaringan. Selain itu, kebijakan sistem TIK memerlukan manajemen kejadian dan sistem informasi yang dapat memantau insiden keamanan jaringan saat mengakses komunikasi keamanan. Anda juga memerlukan penilaian keamanan jaringan untuk mengontrol dan mengukur keamanan.

Dari aspek proses GCI, kurangnya bukti hukum untuk keamanan siber mempengaruhi struktur organisasi yang mengatur keamanan siber. Di bawah dasar hukum ini, tidak mungkin menerapkan praktik keamanan siber di tingkat nasional. Ini juga membingungkan koordinasi tanggung jawab yang terkait dengan keamanan siber itu sendiri. Draf terbaru dari Cyber Security Act saat ini tidak diterbitkan dan hanya RUU versi Mei 2019 yang tersedia, tetapi teks ilmiah RUU tersebut tersedia. Kemampuan BSSN juga dikritik karena banyak tumpang tindih dengan lembaga-lembaga seperti Kementerian Komunikasi dan Informatika, Unit Kejahatan Siber Polri, dan Pusat Operasi Siber Kementerian Pertahanan. Kedepannya, Indonesia perlu mempercepat penerapan undang-undang keamanan siber untuk memberikan landasan hukum. Keberadaan undang-undang tersebut juga dapat memfasilitasi strategi keamanan siber nasional yang komprehensif yang dapat lebih mendefinisikan fungsionalitas BSSN.

## D. Penutup

Hambatan-hambatan yang dimiliki pemerintah adalah perangkat-perangkat yang sudah kadaluarsa yang masih digunakan di jaringan-jaringan pemerintah daerah yang mungkin update terbarunya sudah tidak ada, perangkat keamanannya seperti antivirus sudah kadaluarsa, dari sumber daya manusia belum mendukung sepenuhnya pada keamanan siber ini.

Sistem pemerintahan berbasis elektronik (SPBE) diterapkan untuk membangun pemerintahan yang cepat dan efisien. Namun, pada kenyataannya, berbagai institusi membuat aplikasi dengan fungsionalitas yang tumpang tindih, meskipun tidak relevan dengan kebutuhan mereka. Oleh karena itu, arsitektur SPBE diperlukan sebagai pedoman dalam membangun dan menyempurnakan aplikasi baik untuk instansi pemerintah pusat maupun daerah.

Indonesia membutuhkan kebijakan yang mengatur semua elemen terkait keamanan siber. Dalam semua kebijakan yang mengatur sistem TIK, komunikasi yang digunakan mencakup semua peraturan yang memerlukan dokumentasi standar sebagai acuan pelaksanaan semua proses yang terkait dengan keamanan informasi. Standar infrastruktur ini harus sesuai dengan standar internasional untuk menghadapi perang cyber.

**Referensi**

Abidin, D. Z. (2017). Kejahatan dalam Teknologi Informasi dan Komunikasi. JurnalProcessor, 10(2), 509 516.

Alrubaiq, Abdullah, and Talal Alharbi. "Developing a Cybersecurity Framework for e Government Project in the Kingdom of Saudi Arabia." *Journal of Cybersecurity and Privacy* 1, no. 2 (2021): 302–18. https://doi.org/10.3390/jcp1020017.

Ardiyanti, Handrin. "Cybersecurity Dan Tantangan Pengembangannya Di Indonesia." *Jurnal Politica*, 1, 5 (August 2014): 95–110.

Ayu, Mathilda Gian. "BSSN Tingkatkan Sistem Pelayanan Berbasis Elektronik Yang Aman Bagi Masyarakat." Cloud Computing Indonesia, 2020. https://www.cloudcomputing.id/berita/bssn tingkatkan spbe aman bagi masyarakat.

Budi, Eko, Dwi Wira, and Ardian Infantono. "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0." *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)* 3 (2021): 223–34. https://doi.org/10.54706/senastindo.v3.2021.141.

BSA The Software Alliance. 2015. Asia Pacific Cyber Security Dashboard – A Path to a Secure Global; Cyberspace.

BSSN. 2020. Renstra BSSN Tahun 2020 2024.

BSSN. 2021. Laporan Tahunan: Monitoring Keamanan Siber 2020.

CIPS. 2019. Ringkasan Kebijakan: Perlindungan Keamanan Siber di Indonesia.

Calderón, A., & Ruiz, M. (2015). A systematic literature review on Serious games evaluation: An application to software project management. *Computers & Education, 87*, 396 422. Https://doi:10.1016/j.compedu.2015.07.011.

Fitriati, Rachma. *Membangun Model Kebijakan Nasional Keamanan Siber Dalam Sistem Pertahanan Negara*. 2nd ed. Universitas Pertahanan Indonesia, 2018.

Hilmy, Muhammad, and Rama Azmi. "Konstruksi Pertahanan Dan Keamanan Negara Terhadap Perlindungan Data Dalam Cyberspace Untuk Menghadapi Pola Kebiasaan Baru." *Jurnal Lemhannas RI*, 1, 9 (March 31, 2021): 579–91.

Islami, Maulia Jayantina. "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia DITINJAU Dari Penilaian Global Cybersecurity Index." *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi dan Komunikasi* 8, no. 2 (2018): 137. https://doi.org/10.17933/mti.v8i2.108.

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology, 51*(1), 7 15. doi:10.1016/j.infsof.2008.09.009.

Nagaraju, Regonda, Selvanayaki Kolandapalayam Shanmugam, Sivaram Rajeyyagari, Jupeth Toriano Pentang, B Kiran Bala, Arjun Subburaj, and M.Z.M. Nomani. "Analysis of Cyber Security in e Governance Utilizing Blockchain Performance," 2021. https://doi.org/10.21203/rs.3.rs 938929/v1.

Nasional Cyber Security Index, (2021). Diambil dari: https://ncsi.ega.ee/country/id/

Parulian, Sahat, Devi Anassafila Pratiwi, and Meiliya Yustina. "Ancaman Dan Solusi Serangan Siber Di Indonesia." *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, 2, 1 (December 15, 2021): 85–92.

Kementerian Pertahanan RI. (2014). *Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber*.

Rahmawati, Dwi. "BSSN Temukan 1,6 Miliar Serangan Siber Sepanjang 2021, Mayoritas Malware." detiknews, March 2022. https://news.detik.com/berita/d 5972491/bssn temukan 16 miliar serangan siber sepanjang 2021 mayoritas malware#:~:text=BSSN%20Temukan%201%2C6%20Miliar%20Serangan%20Siber% 20Sepanjang%202021%2C%20Mayoritas%20Malware, Dwi%20Rahmawati%20%2D%20detikNews&text=Badan%20Siber%20dan%20Sand i%20Negara,yang%20ditemukan%20antara%20lain%20Malware.

Rizki, Makbull. "Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia Dalam Menghadapi Tantangan Perkembangan Teknologi Dan Informasi." *Politeia: Jurnal Ilmu Politik* 14, no. 1 (2022): 54–62. https://doi.org/10.32734/politeia.v14i1.6351.

Saragih, Y. M., & Azis, D. A. (2020). Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi. Soumatera Law Review, 3(2), 265 279.

Setiawan, Ahmad Budi. "Kajian Kesiapan Keamanan Informasi Instansi Pemerintah Dalam Penerapan E Government." *Jurnal Masyarakat Telematika dan Informasi* 4, no. 2 (November 2, 2013): 109–26.

Shafira, Irnasya. "Menganalisis Strategi Keamanan Siber Nasional Indonesia." Research Associate Center for Digital Society Universitas Gadjah Mada, June 2021. https://cfds.fisipol.ugm.ac.id/id/2021/07/28/menganalisis strategi keamanan siber nasional indonesia/.

Telang, R., & Wattal S. (2007). An empirical analysis of the impact of software vulnerability announcement on firm stock price. IEEE Transactions on Software Engineering, 33. Doi: 10.1109/TSE.2007.70712.

Timur, Fauzia Gustarina, and Muh. Fachrul Febriansyah. "Pemanfaatan IT DRC Sebagai Implementasi Cyber Security Pada Sistem Pemerintahan Berbasis Elektronik." *Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU)* 1, no. 1 (September 2019): 307–14.

Waranggani, Arundati Swastika. "BSSN : Spbe Harus Didukung Keamanan Siber Yang Kuat." Cloud Computing Indonesia, April 2021. https://www.cloudcomputing.id/berita/bssn spbe harus didukung cybersecurity kuat.