OPTIMALISASI LAYANAN PUBLIK BADAN INTELIJEN NEGARA DALAM PERSPEKTIF *GLOBAL CYBERSECURITY INDEX*

M. Yusuf Samad[1)]
[1]*Preinexus Indonesia, Gedung Guru Indonesia, Jalan Tanah Abang III Nomor 24, Jakarta Pusat, DKI Jakarta*
Email: ahmadyusad@gmail.com

ABSTRACT

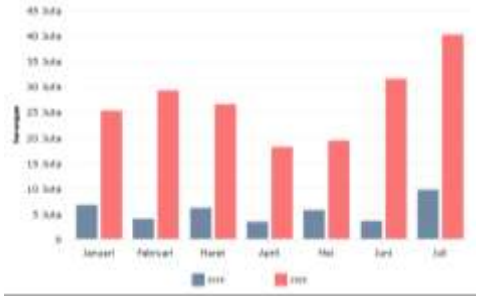
Indonesia is currently ranked 24th in the Global Cybersecurity Index (GCI) 2020. Indonesia's ranking can be improved by improving the assessment pillars of the GCI survey, one of the efforts is to improve the cyber security system of government agencies through Security Assessment. For this reason, the purpose of this study is to provide alternative solutions in order to optimize the public services of the State Intelligence Agency (BIN) in the form of Security Assessment in the perspective of the GCI 2020 survey. This research is a qualitative research using data related to BIN public services and then juxtaposed with data from the Global Cybersecurity survey. Index 2020 as a reference. The results of the study indicate that the optimization of the Security Assessment can be done by implementing cyber counterintelligence and optimizing the publication of services by paying attention to the rules of intelligence secrecy. With the optimization of the Security Assessment, it will affect the assessment of the Technical, Cooperation and Organizational pillars in the GCI survey so that it is expected that Indonesia's ranking will increase in the next survey.

Keywords: Public Service, Cyber Attack, State Intelligence Agency, Global Cybersecurity Index.

PENDAHULUAN

Perkembangan era digitalisasi secara global mengalami percepatan yang pesat hingga mencapai 4,66 miliar pengguna internet. Hal tersebut ditandai dengan pengguna internet di tahun 2021 mengalami peningkatan 316 juta atau 7,3% jika dibandingkan dengan tahun 2020. (We are Social & Hootsuite, 2021). Sedangkan di Indonesia, terdapat 202,6 juta pengguna internet di Indonesia pada Januari 2021. Selain itu, jumlah pengguna internet di Indonesia meningkat 27 juta atau bertambah 16% antara tahun 2020 dan 2021 dan penetrasi internet di Indonesia mencapai 73,7% pada Januari 2021. (Kemp, 2021).

Peningkatan pengguna internet di dunia dan di Indonesia tidak hanya memberikan dampak positif terhadap layanan telekomunikasi dan informatika, tetapi juga berdampak negatif peningkatan serangan siber. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber di Indonesia mengalami peningkatan hampir lima kali lipat dengan rentan waktu Januari hingga Juli 2019. Jika ditotal, serangan siber mencapai 39,3 juta. Adapun jenis serangan siber yang paling sering ditemukan berupa situs internet, trojan, pengumpulan informasi. (Pusparisa, 2020).



Gambar 1. Jumlah Kejahatan Siber di Indonesia (2019-2020).
Sumber: https://databoks.katadata.co.id/datapublish/2020/11/20/tren-serangan-siber-meningkat-selama-pandemi-covid-19, diakses pada 27 Juni 2021.

Laporan penelitian dari Perusahaan Keamanan Siber, Kaspersky menunjukkan bahwa selama tahun kuartal pertama tahun 2021, sebanyak 25,7 persen pengguna komputer di Indonesia menjadi sasaran serangan siber berbasis web, sedangkan lebih dari sepertiga atau 38,3 persen menjadi sasaran ancaman

lokal atau melalui USB, CD, DVD dan metode luar jaringan lainnya. Data tersebut diperoleh dari Kaspersky Security Network (KSN), yakni infrastruktur terdistribusi kompleks yang memproses aliran data jutaan peserta di seluruh dunia terkait keamanan siber. Kaspersky mencatat menangani sebanyak 9.639.740 ancaman siber berbeda yang ditularkan melalui Internet pada komputer pengguna KSN di Indonesia. Angka tersebut mengalami peningkatan sebanyak 20 persen jika dibandingkan dengan periode yang sama dengan tahun sebelumnya, yakni sebanyak 8.026.877 ancaman siber. Berbeda dengan ancaman lokal, ancaman ini mengalami penurunan sebanyak 18 persen dengan periode yang sama, dari 28.885.114 menjadi 23.594.930 ancaman siber. (Alfarizi, 2021).

Berdasarkan laporan tahunan Gov-CSIRT (*Government Computer Security Incident Response Team*) pada 2019, tercatat bahwa sebanyak 105 insiden siber yang diterima oleh Gov-CSIRT dengan rincian serangan jenis *Web defacement* sebanyak 15 insiden (14%), *Phising* sebanyak 10 insiden siber (5%), *Malware* sebanyak 10 insiden siber (9%), dan kerentanan sebanyak 66 insiden siber (63%).

Banyaknya serangan siber yang menargetkan instansi pemerintah menunjukkan bahwa instansi pemerintah Indonesia rentan terhadap serangan siber dan hal tersebut merupakan ancaman bagi Indonesia. Badan Intelijen Negara (BIN) merupakan salah satu instansi pemerintah yang bertugas untuk mendeteksi ancaman, termasuk ancaman siber.

BIN sebagai salah satu penyelenggara intelijen negara sesuai dengan Undang-Undang (UU) Nomor 17 Tahun 2011 tentang Intelijen Negara, memiliki peran untuk mendeteksi ancaman yang dapat mengancam kepentingan dan keamanan nasional. Khusus di bidang siber, BIN melakukan deteksi ancaman melalui layanan publik Deputi Bidang Intelijen Siber BIN berupa *Security Assesment*. Namun, penulis menilai peran dari layanan publik tersebut belum optimal mengingat masih sering terjadi serangan siber di Indonesia, terutama pada instansi pemerintah. Hal ini berdampak pada hasil survei dari *International Telecommunication Union* (ITU) yang tertuang dalam hasil survei Indeks Keamanan Siber Global atau *Global Cybersecurity Index* (GCI) 2020 dengan hasil Indonesia berada pada urutan ke-24. Dengan adanya optimalisasi layanan publik BIN di bidang siber, diharapkan mampu menaikkan peringkat Indonesia pada survei GCI selanjutnya. Untuk itu, tujuan penelitian ini untuk memberikan alternatif solusi dalam rangka mengoptimalisasikan layanan publik BIN berupa *Security Assesment* dalam perspektif *Global Cybersecurity Index*.

METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif, Sukidin dalam Siyoto (Siyoto, 2015) menjelaskan bahwa metode kualitatif berupaya memaparkan sejumlah hal-hal unik yang terdapat dalam individu, kelompok, masyarakat, dan/atau organisasi dalam kehidupan sehari-hari secara menyeluruh, rinci, dalam, dan dapat dipertanggungjawabkan secara ilmiah.

Sumber data penelitian kualitatif secara garis besar dapat dibedakan menjadi dua, yaitu manusia dan bukan manusia. Sementara itu, analisis data yang digunakan adalah analisis data kualitatif, yaitu mekanisme dalam memperoleh serta mengolah data secara sistematis baik dari hasil catatan lapangan, hasil wawancara terhadap narasumber, maupun bahan keterangan lainnya sehingga hasilnya mudah dipahami dan dapat dipublikasikan kepada khalayak. (Sugiyono, 2007).

Dalam penelitian ini, penulis menggunakan data terkait layanan publik BIN kemudian disandingkan dengan data dari survei *Global Cybersecurity Index* 2020 sebagai acuan untuk menjawab tujuan penelitian. Adapun optimalisasi layanan tersebut menggunakan pendekatan teori kontra intelijen siber dan membandingkan layanan publik terkait siber antara BIN dan BSSN dari aspek sosialisasi/publikasi. Selanjutnya dapat dilihat pada gambar dibawah ini.

Gambar 2. Diagram Alir Metode Penelitian.

HASIL DAN PEMBAHASAN

Optimalisasi *Security Assesment* melalui Kontra Intelijen Siber BIN

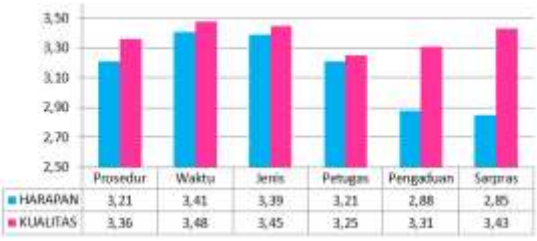
Bentuk pelayanan publik di Badan Intelijen Negara (BIN) terkait siber adalah pelayanan berupa *Security Assesment* (penilaian keamanan) yang dilakukan Deputi Bidang Intelijen Siber BIN (Deputi VI), dalam hal ini Deputi tersebut melakukan penilaian keamanan siber. Dalam situs web yang dikelola Deputi VI, yakni secassiber.bin.go.id, dijelaskan bahwa "*Security Assesment* adalah layanan yang diberikan oleh Deputi Siber Badan Intelijen Negara kepada Kementerian Lembaga yang ada di Indonesia dengan tujuan untuk memberikan pengamanan terhadap jaringan atau server data kementerian lembaga serta melakukan analisa forensik terhadap serangan siber di kementerian lembaga. Sehingga dapat menciptakan keamanan bagi kementerian lembaga dari serangan siber ataupun ancaman pencurian data".

Pelayanan publik *Security Assessment* Deputi VI hanya terbatas pada instansi pemerintah karena berdasarkan Keputusan Kepala Badan Intelijen Negara Nomor 36 Tahun 2019 tentang Standar Pelayanan Badan Intelijen Negara, khususnya lampiran Standar Pelayanan *Security Assessment*, menyatakan bahwa hanya kementerian atau lembaga (K/L) yang dapat menyampaikan surat permohonan untuk melakukan *Security Assessment* pada K/L pemohon.

Jika merujuk pada aturan diatas, *Security Assessment* tidak dijelaskan secara detail sehingga informasi yang diperoleh kementerian/lembaga masih minim dan berpotensi menyebabkan kementerian/lembaga enggan untuk meminta BIN melakukan *Security Assessment* pada sistem siber yang dimiliki oleh kementerian/lembaga. Penulis menilai detail informasi tentang *Security Assessment* dapat dilakukan dengan cara membagi empat layanan tersebut sesuai dengan kategori yang dikemukakan oleh P. D. Beer dan S. v. S. Basie Djoyonegoro (2017), yakni kontra intelijen siber defensif aktif, kontra intelijen siber defensif pasif, kontra intelijen siber ofensif aktif, dan kontra intelijen siber ofensif pasif, bahkan masing-masing kategori tersebut bisa dipadukan satu sama lain atau digabungkan semuanya. Bahkan, informasi terkait alat yang digunakan untuk melakukan *Security Assessment* perlu disertakan sehingga kementerian/lembaga mengetahui sejauh mana perkembangan terkini alat yang digunakan. Namun, penyertaan informasi terkait alat yang digunakan harus mempertimbangkan koridor-koridor sejauh mana informasi tersebut disampaikan dengan mengacu pada Pasal 25, Bab Kerahasiaan Intelijen, UU 17 Tahun 2011 tentang Intelijen Negara. Dengan begitu, kementerian/lembaga dapat dengan mudah mengetahui layanan seperti apa yang disediakan oleh BIN kemudian disesuaikan dengan kondisi atau permasalahan sistem siber yang dihadapi oleh kementerian/lembaga.

Optimalisasi *Security Assesment* melalui Publikasi/Sosialisasi

Dalam pelaksanaan layanan publik, terdapat timbal balik dari penggunaan layanan tersebut, hal itu dapat dilihat dari hasil survei tentang kualitas pelayanan publik Deputi VI BIN.



Gambar 3. Hasil Survei Kualitas Pelayanan Deputi VI BIN.
Sumber: http://secassiber.bin.go.id/Hasil_Survei, diakses pada 29 September 2021.

Pada umumnya, hasil survei menunjukan bahwa persepsi terhadap kualitas pelayanan di Deputi VI BIN telah diatas harapan para responden, dengan tingkat kepuasan paling tinggi berada pada komponen Waktu Pelayanan dengan nilai rata-rata sebesar 3,48 dari skala 4, sedangkan persepsi Kualitas Pelayanan paling rendah berada pada komponen Petugas Pelayanan dengan nilai rata-rata sebesar 3,25.

Harapan responden paling tinggi berada pada komponen Waktu dengan nilai rata-rata sebesar 3,41 dari skala 4, sedangkan harapan responden paling rendah berada pada komponen Sarana dan Prasarana dengan nilai rata-rata sebesar 2,85.

Selisih atau *Gap* antara harapan responden dengan petugas pelayanan yang diselenggarakan

oleh Deputi VI BIN terbesar berada pada komponen Sarana dan Prasarana dengan nilai 0,58 dari skala 4, dan selisih terendah berada pada komponen Jenis Pelayanan dengan nilai 0,07.

Berdasarkan unsur utama proses pelayanan publik, layanan *Security Assessment* telah memenuhi unsur-unsur tersebut, yakni:

1. Penyedia layanan yaitu BIN melalui Deputi Bidang Intelijen Siber atau Deputi VI BIN.
2. Penerima layanan adalah kementerian/lembaga yang telah mendapat layanan *Security Assessment.*
3. Jenis pelayanan berupa pengamanan terhadap jaringan atau server data kementerian lembaga serta melakukan analisa forensik terhadap serangan siber di kementerian lembaga.
4. Kepuasan pelanggan
   Hasil survei merupakan bentuk dari kepuasan pelanggan yang telah mendapat layanan *Security Assessment.*

Selain BIN, terdapat instansi pemerintah lainnya yang juga melakukan *Security Assessment* yaitu Badan Siber dan Sandi Negara (BSSN) dengan layanan publik berupa *Information Technology Security Assessment* (ITSA). Menurut situs web resmi BSSN, layanan ITSA bertujuan meminimalisir celah kerawanan yang terdapat pada sistem informasi pemerintah melalui menguji kerentanan, memberikan saran dan rekomendasi. Kedua layanan publik tersebut cenderung sama namun hasil dari ITSA BSSN dipublikasikan ke internet sehingga mudah diketahui seperti apa hasil ITSA BSSN kepada penerima layanan dan siapa saja penerima layanan ITSA tersebut, seperti contoh penilaian ITSA terhadap aplikasi Pedulilindungi milik Kementerian Kesehatan (Kliwantoro, 2021) dan rekomendasi hasil ITSA pada Dinas Komunikasi dan Informastika Kabupaten Pekalongan (Lubbi, 2020). Sementara *Security Assessment* BIN kepada penerima layanan tidak ditemukan hasilnya di internet. Hal ini menyebabkan minimnya informasi kepada calon penerima layanan *Security Assessment* BIN sehingga tidak mengetahui seperti apa manfaat yang diperoleh jika meminta layanan *Security Assessment* tersebut. Dengan demikian, optimalisasi publikasi penting untuk dilakukan guna mensosilisasikan layanan *Security Assessment* BIN ke publik atau calon penerima layanan (kementerian/lembaga) sehingga calon tersebut memiliki gambaran awal sebelum meminta BIN untuk melakukan *Security Assessment*. Namun, dengan catatan bahwa publikasi tersebut tidak berbenturan dengan asas kerahasiaan yang diatur dalam UU 17 Tahun 2011.

Dampak Optimalisasi *Security Assesment* pada GCI

Optimalisasi *Security Assessment* berdampak pada sejumlah pilar dalam *Global Cybersecurity Index* (GCI). Dengan adanya optimalisasi tersebut, diharapkan kementerian/lembaga yang memanfaatkan layanan *Security Assessment* dapat bertambah dan pada akhirnya dapat mempengaruhi penilaian pada pilar GCI. Hal tersebut dapat dijelaskan sebagai berikut:

1. Kerja Sama (*Cooperation*)
   Security Assessment berperan pada indikator kerja sama antar instansi pemerintah. Hasil dari *Security Assessment* membuat BIN dan instansi pemerintah lainnya menjalin kerja sama di bidang keamanan siber. Sedangkan indikator lainnya seperti kerja sama bilateral, kerja sama multilateral, partisipasi pada forum internasional, dan kerja sama pemerintah dengan swasta tidak dapat dipengaruhi oleh *Security Assessment* karena *Security Assessment* dibatasi oleh Keputusan Kepala Badan Intelijen Negara Nomor 36 Tahun 2019 tentang Standar Pelayanan Badan Intelijen Negara, khususnya lampiran Standar Pelayanan *Security Assessment*, menyatakan bahwa hanya instansi pemerintah atau kementerian atau lembaga (K/L) yang dapat menyampaikan surat permohonan untuk melakukan *Security Assessment* pada K/L pemohon.
2. Organisasi
   Security Assessment merupakan salah satu upaya untuk memastikan tata kelola keamanan siber nasional sekaligus memastikan keamanan siber tetap berada pada posisi yang terbaik. Artinya, tata kelola siber mampu memberikan perlindungan terhadap serangan siber dan mampu mengelola risiko yang timbul jika terjadi serangan siber sehingga dampak yang ditimbulkan dapat diminimalisir. Dalam hal ini, serangan siber yang dimaksud adalah serangan siber yang menyasar pada instansi pemerintah. *Security Assessment* berkontribusi pada indikator metrik keamanan siber khususnya pada

audit keamanan siber dan alat serta tindakan lain untuk menilai atau mengevaluasi kinerja yang dihasilkan untuk perbaikan di masa mendatang. *Security Assessment* menghasilkan laporan mengenai sejauh mana sistem keamanan siber instansi pemerintah kemudian memberikan rekomendasi agar sistem tersebut mengalami penguatan atau tidak mudah menjadi korban serangan siber.

3. Teknis
   Security Assessment memberikan pelayanan berupa keamanan kepada kementerian atau lembaga pemerintah agar tidak menjadi sasaran serangan siber. Semakin banyak yang mendapat layanan *Security Assessment*, maka diharapkan semakin banyak kementerian/lembaga aman dari serangan siber. Secara khusus, *Security Assessment* berkotribusi pada indikator CERT sektoral tepatnya pada sektor intelijen, dalam hal ini terkait dengan sistem keamanan nasional sesuai dengan UU No. 11 Tahun 2017 yang menyatakan bahwa Intelijen Negara sebagai bagian dari sistem keamanan nasional yang merupakan lini pertama mampu melakukan deteksi dini dan peringatan dini terhadap berbagai bentuk dan sifat ancaman, baik yang potensial maupun aktual. Dalam UU tersebut juga ditegaskan bahwa BIN berkedudukan sebagai koordinator penyelenggara Intelijen Negara. Jadi BIN melalui *Security Assessment* melakukan deteksi dini dan peringatan dini terhadap ancaman siber.
4. Pengembangan Kapasitas
   Pilar ini tidak berkaitan langsung dengan *Security Assessment* karena pilar ini melibatkan negara secara umum dalam mengembangkan kapasitas keamanan siber. Pilar ini juga hanya bersifat memberikan pelayanan berupa jasa penilaian sistem keamanan siber instansi pemerintah sehingga tidak ada layanan yang memberikan insentif untuk mendorong penelitian dan pengembangan kapasitas SDM, teknologi atau keduanya.
5. Hukum
   Pilar ini diukur berdasarkan keberadaan lembaga hukum dan kerangka kerja yang berhubungan dengan keamanan siber dan kejahatan siber. *Security Assessment* merupakan layanan yang sifatnya teknis sedangkan pilar ini cenderung pada kebijakan atau aturan tentang keamanan siber baik berupa payung hukum maupun kebijakan penyelenggaraan pelatihan keamanan siber. Jadi, *Security Assessment* tidak berkaitan dengan indikator UU Kejahatan Siber, UU Keamanan Siber, dan indikator penyelenggaraan pelatihan keamanan siber bagi aktor hukum.

KESIMPULAN DAN SARAN

Kesimpulan

Optimalisasi *Security Assessment* dapat dilakukan dengan cara menerapkan kontra intelijen siber dan mengoptimalkan publikasi layanan tersebut. Namun, optimalisasi tersebut harus memperhatikan aturan-aturan tentang kerahasiaan intelijen yang diatur dalam UU Nomor 17 Tahun 2011 tentang Intelijen Negara. Dengan adanya optimalisasi *Security Assessment*, maka akan mempengaruhi penilaian pilar teknis, kerja sama, dan organisasi pada survei *Global Cybersecurity Index* sehingga diharapkan peringkat Indonesia akan meningkat pada survei yang dilakukan selanjutnya.

Saran

Peneliti selanjutnya dapat melengkapi data-data layanan *Security Assessment* BIN dengan melakukan wawancara terhadap narasumber yang berasal dari BIN, misalnya Juru Bicara atau Deputi Komunikasi dan Informasi BIN. Kemudian membandingkan peran layanan tersebut terhadap hasil-hasil survei GCI sebelumnya. Saran lain yaitu peneliti selanjutnya meneliti tentang inovasi dalam *Security Assessment* agar dapat berkontribusi pada pilar pengembangan kapasitas dan pilar hukum.

DAFTAR PUSTAKA

Alfarizi, Moh Khory dan Erwin (Ed.). (2021). *Kaspersky: Serangan Siber di Indonesia Meningkat pada Kuartal I 2021*. Tempo. Diakses dari https://tekno.tempo.co/read/1470760/kaspersky-serangan-siber-di-indonesia-meningkat-pada-kuartal-i-2021.

BSSN. (2019). Laporan Tahunan Gov-CSIRT BSSN 2019. Diakses dari https://cloud.bssn.go.id/s/SwZYPYfqdGGb48S#pdfviewer.

Deputi Siber Badan Intelijen Badan Intelijen Negara. (2020). Diakses dari https://secassiber.bin.go.id/index.php.

Deputi Siber Badan Intelijen Badan Intelijen Negara. (2020). Diakses dari http://secassiber.bin.go.id/Hasil_Survei.

Djoyonegoro, Ngasiman. (2017). *Intelijen di Era Digital: Prospek dan Tantangan Membangun Ketahanan Nasional*. Jakarta: CMB Press.

ITU. (2020). Global Cybersecurity Index 2020. International Telecommunication Unit.

Kemp, Simon. (2021). *Digital 2021: Indonesia.* Diakses dari https://datareportal.com/reports/digital-2021-indonesia.

Keputusan Kepala Badan Intelijen Negara Nomor 36 Tahun 2019 tentang Standar Pelayanan Badan Intelijen Negara. Diakses dari https://www.bin.go.id/PelayananPublik/Standar_Pelayanan.

Kliwantoro, D. Dj., (2021). Kebocoran Data Pribadi Gegara Server Aplikasi Lama Tidak Di-"Takedown". Antaranews, Diakses dari https://m.antaranews.com/amp/berita/2366182/kebocoran-data-pribadi-gegara-server-aplikasi-lama-tak-di-takedown.

Lubbi, Khiliyatul. (2020). Paparan Laporan Hasil IT Security Assessment (ITSA) oleh Badan Siber dan Sandi Negara (BSSN). Dinas Komunikasi dan Informatika Kabupaten Pekalongan. Diakses dari https://dinkominfo.pekalongankab.go.id/index.php/publikasi/berita/224-paparan-laporan-hasil-it-security-assessment-itsa-oleh-badan-siber-dan-sandi-negara-bssn.

Peraturan Menteri Negara Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 15 tahun 2014 tentang Pedoman Standar Pelayanan.

Pusparisa, Yosepha & Muhammad Ahsan Ridhoi (Ed.). (2020). *Tren Serangan Siber Meningkat Selama Pandemi Covid-19*. Katadata. Diakses dari https://databoks.katadata.co.id/datapublish/2020/11/20/tren-serangan-siber-meningkat-selama-pandemi-covid-19.

Undang-Undang (UU) Nomor 17 Tahun 2011 tentang Intelijen Negara.