E-ISSN : 2716-375X
P-ISSN : 2716-3768
JURNAL MANAJEMEN PENDIDIKAN DAN ILMU SOSIAL (JMPIS)
https://dinastirev.org/JMPIS dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jmpis.v5i4
Received: 31 Mei 2024, **Revised:** 12 Juni 2024, **Publish:** 13 Juni 2024

Budaya & Masyarakat Digital dalam Ketahanan Siber di Indonesia: Sebuah Adaptasi dari Pendekatan *Capacity Maturity Model* (CMM)

Arnold Hiras Simorangkir[1], Arthur Josias Simon Runturambi[2]
[1] Magister Kajian Ketahanan Nasional, Universitas Indonesia, Depok, Indonesia, hsimorangkir@gmail.com
[2] Program Ketahanan Nasional SKSG, Universitas Indonesia, Depok, Indonesia, simonrbi@yahoo.com

Corresponding Author: hsimorangkir@gmail.com

Abstract: *Indonesia has been ranked among the top in data leakage in the world in recent years, according to a study by the Dutch cybersecurity firm Surfshark. This paper discusses benchmarking Indonesia's cyber strategies and policies against best practices using Oxford University Capacity Maturity Model (CMM) Approach. In this paper, the author takes cultural and social dimensions from CMM to become the main attraction in this writing. This paper provides recommendations on the gap between the policy strategy and the CMM framework in achieving the ideal Maturity level. Maturity level is measured in 5 maturity levels start up, formative, established, strategic, dynamic. This study uses a qualitative method with literature study approach. Data collection involved through key informant interviews with cyber policy holders in Indonesia. CMM Approach to formulating recommendations on the ideal Cyber Resilience Roadmap next to be explained in the cultural and societal dimension of cyber resilience that is developing in Indonesia. This writing recommends that collaboration between the government and the private sector, which is structured and supported of good cyber governance, is very needed in maintaining and developing cybersecurity.*

Keyword: *Digital Culture, Cyber Security, Cyber Resilience, Capacity.*

Abstrak: Indonesia telah menduduki peringkat teratas dalam kebocoran data di dunia dalam beberapa tahun terakhir, menurut sebuah studi oleh perusahaan keamanan siber Belanda, Surfshark. Artikel ini membahas pembandingan strategi dan kebijakan siber Indonesia terhadap praktik terbaik dengan menggunakan pendekatan Oxford University *Capacity Maturity Model* (CMM). Dalam tulisan ini, penulis mengambil dimensi budaya dan sosial dari CMM menjadi daya tarik utama dalam tulisan ini. Makalah ini memberikan rekomendasi tentang kesenjangan antara strategi kebijakan dan kerangka kerja CMM dalam mencapai tingkat Kematangan yang ideal. Tingkat kematangan diukur dalam 5 tingkat kematangan mulai, formatif, mapan, strategis, dinamis. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi literatur. Pengumpulan data dilakukan melalui wawancara informan kunci dengan pemegang kebijakan siber di Indonesia. Pendekatan CMM untuk merumuskan

rekomendasi Peta Jalan Ketahanan Siber yang ideal selanjutnya dijelaskan dalam dimensi budaya dan kemasyarakatan ketahanan siber yang berkembang di Indonesia. Tulisan ini merekomendasikan bahwa kerja sama antara pemerintah dan swasta yang terstruktur dan didukung tata kelola siber yang baik sangat diperlukan dalam menjaga dan mengembangkan keamanan siber.

Kata Kunci: Budaya Digital, Keamanan Siber, Model Kematangan Kapasitas.

PENDAHULUAN

Indonesia tercatat sebagai salah satu negara dengan jumlah pengguna internet terbesar di dunia. Mengutip laporan *We Are Social* 2022, angka pengguna internet di tanah air mencapai sekitar 204,7 juta dengan tingkat penetrasi sebanyak 73,3 persen per Januari 2022. Angka ini naik sekitar 1,03 persen dibanding tahun sebelumnya (Annur, 2022). Sayangnya, angka pengguna internet yang makin banyak tiap tahunnya ini tidak dibarengi dengan tingkat keamanan siber yang mumpuni. Melansir data dari *National Cyber Security Index* (NCSI), skor keamanan siber Indonesia menempati peringkat 6 se-Asia Tenggara dan peringkat 83 dari total 160 negara di dunia. Nilai keamanan siber Indonesia hanya sebesar 38,96 dari 100 per Agustus 2022. Sementara, Malaysia menempati posisi nomor satu sebagai negara dengan indeks keamanan siber terbaik di Asia Tenggara yang mencapai skor 79,22 dan menduduki peringkat ke-19 secara global (Naurah, 2022). Adapun, NCSI mengukur indeks penilaian tersebut berdasarkan sejumlah indikator, misalnya terkait aturan hukum negara bersangkutan mengenai keamanan siber, ada atau tidaknya kerja sama pemerintah atau lembaga lain dalam keamanan siber, hingga rangkaian program yang terfokus pada keamanan siber (Daeng, et al., 2023).

Tingginya kasus kebocoran data internet di Indonesia secara global menjadikan Indonesia juga menempati urutan pertama sebagai negara dengan tingkat pembobolan data terbanyak se-Asean (Naurah, 2022). Kebocoran data di RI pada kuartal II/2022 bahkan mengalami kenaikan sebesar 143 persen dari kuartal I/2022 (*quarter to quarter*/qtq) (Dihni, 2022). Surfshark mencatat bahwa sejak tahun 2004, total kasus kebocoran data di tanah air sudah mencapai 120,9 juta. Sementara itu, akun yang mengalami kebocoran data pada kuartal II/2022 naik dua persen (qtq) secara global menjadi 459 akun dibobol per menitnya, dibanding kuartal sebelumnya sebanyak 450 akun per menit. Merujuk pada data, laporan dari akun yang mengalami kebocoran data di dunia sudah mencapai 74,9 juta kasus dari seluruh dunia pada kuartal II/2022. Angka ini meningkat dibandingkan kuartal sebelumnya (qtq) yang sebanyak 60,3 juta (Naurah, 2023).

Mencapai keamanan siber dan ketahanan di tingkat nasional merupakan tanggung jawab bersama dari semua pemangku kepentingan, yaitu pemerintah, sektor swasta, dan masyarakat sipil (BSSN, 2023). Tindakan terkoordinasi dan pendekatan multi *stakeholder* diperlukan untuk mengembangkan dan melaksanakan strategi dan rencana keamanan siber nasional (Rahmadiani, Mantovani, Hariz, Haryanto, & Aidad, 2019). Berbagai metodologi, pedoman, dan tempat untuk menentukan strategi keamanan siber nasional atau sektoral yang terstruktur dengan baik dan komprehensif disediakan oleh organisasi dunia seperti ITU, OECD, ENISA UE, OSCE, badan standardisasi, dan penelitian akademik. Sebagian besar dari mereka telah mendalilkan “ketahanan dunia maya” sebagai tujuan utama baru untuk meningkatkan ‘keamanan dunia maya’ (Ahmad, Putri, Styawan, Nugraha, & Magdalena, 2018). Strategi juga tercermin dalam peta jalan yang menguraikan langkah-langkah dan tujuan yang akan dicapai pada berbagai fase rencana peningkatan (Kementerian Pertahanan Republik Indonesia, 2014). Tantangannya adalah bagaimana mengevaluasi tingkat pencapaian, efisiensi, dan efektivitas langkah-langkah tersebut, dan secara lebih umum, bagaimana menilai keseluruhan tingkat kesiapan, kapasitas dan secara objektif mengevaluasi

kemampuan keamanan dan ketahanan di tingkat sektoral dan nasional (Priyono & Marnis, 2008). Ada juga kebutuhan akan metodologi terpadu untuk memantau kemajuan dan membandingkan status yang dicapai di antara organisasi, sektor, negara, dan masyarakat.

Selama beberapa dekade, pendekatan berdasarkan model maturitas telah digunakan secara luas di perusahaan IT dan sektor teknologi, serta pengadaan publik, dimulai dengan pertahanan, untuk menilai kesiapan dan kemampuan organisasi untuk memberikan produk dan layanan berkualitas tinggi sesuai kebutuhan. ruang lingkup, waktu dan anggaran (Carallo, et al., 2023). Di sisi lain, organisasi, komunitas, dan negara harus hidup dan mematuhi sejumlah peraturan, standar, dan persyaratan yang terus meningkat (Sekretariat Jenderal Komisi Yudisial Republik Indonesia, 2019). Untuk mengatasi semua itu dan belum memenuhi tujuan bisnis spesifik organisasi, model kematangan dan metode penilaian ternyata menjadi cara yang paling efisien dan efektif untuk organisasi yang lebih besar dan lebih kecil.

METODE

Penelitian ini menggunakan bentuk analisis deskriptif dengan metodologi kualitatif guna menjelaskan sesuatu secara intuitif dan sistematis. Penelitian ini bersifat kualitatif, dimana peneliti kualitatif berusaha mencari arti, pemahaman, definisi tentang suatu fenomena, kejadian melalui keterlibatan langsung maupun tidak langsung dalam obyek yang diteliti. Penelitian kualitatif adalah cara yang memfokuskan untuk mendapatkan makna, definisi, konsep, karakteristik, dan sebagainya termasuk deskripsi mengenai fenomena tertentu yang memiliki sifat alami dan menyeluruh yang disajikan secara naratif (Sugiyono, 2019). Penelitian kualitatif merupakan mekanisme pencarian dan pengumpulan, termasuk analisis dan interpretasi secara komprehensif untuk menghasilkan pemahaman mengenai permasalahan yang menarik (Yusuf, 2017).

Penekanan analisis deskriptif digunakan dalam penelitian ini untuk menganalisis dan memberikan pemahaman. Jenis data dalam penelitian ini yaitu primer dan sekunder (Creswell, 1998). Di sisi lain, data sekunder dalam penelitian ini didapatkan melalui media *online* dan sumber-sumber lainnya, serta digunakan sebagai data pendukung yang memiliki keterkaitan terhadap masalah penelitian (Yin, 1989). Dengan penggunaan studi pustaka, peneliti akan menjabarkan dan menganalisis sesuai dengan data dan informasi yang dikumpulkan terkait penelitian ini. Pengumpulan data juga dilakukan melalui wawancara informan kunci dengan pemegang kebijakan siber di Indonesia.

HASIL DAN PEMBAHASAN

Peran Negara dalam Ruang Siber

Memaknai perkembangan teknologi dalam suatu negara tidak mungkin tanpa mengaitkannya dengan peranan negara di dalamnya. Untuk itu, perlu memaknai negara sebagai salah satu bagian dari elemen yang terdapat di dalam politik, selain kekuasaan, pengambilan keputusan, kebijakan, dan pembagian alokasi sumber daya. Representasi kekuasaan yang terdapat dalam suatu negara demokrasi dipegang oleh pemerintah berdaulat yang mendapatkan mandat dari rakyat yang memiliki pokok tujuannya, yaitu untuk meningkatkan kesejahteraan rakyat. Adanya perkembangan teknologi berdampak besar terhadap cara-cara pemerintah menjalankan roda pemerintahan, memberikan pelayanan publik, dan memberikan kepastian hukum yang lebih baik kepada rakyatnya dengan memanfaatkan segala bentuk teknologi baru dalam ruang siber (Tambun, Damayanti, Sari, & Darmawan, 2023).

Terkait hal tersebut perlu terlebih dahulu kita memahami konsep mengenai negara. Harold J.Laski dalam Syaiful Bakhri (2018) berpandangan bahwa negara memiliki kewenangan yang secara sah dapat memaksa individu-individu atau kelompok-kelompok yang menjadi bagiannya. Negara juga bisa disebut sebagai suatu masyarakat atau kelompok manusia yang hidup, bekerja sama, dan terintegrasi untuk mewujudkan keinginan bersama.

Dalam sebuah negara, cara masyarakat hidup harus ditaati bersama dan diawasi oleh negara karena memiliki kewenangan mengikat dan dapat memaksa (Bakhri, 2018). Keamanan siber dapat dipahami sebagai sebuah konsep, teknologi, pedoman, kebijakan, pelatihan, praktek, jaminan, dan tindakan keamanan yang berguna untuk melindungi organisasi, aset, dan lingkungan siber pengguna. Dalam sebuah keamanan lingkungan siber terdapat perangkat yang dihubungkan dengan infrastruktur, aplikasi, komputasi, layanan, sistem telekomunikasi dan informasi yang termasuk dalam organisasi dan aset pengguna. Dengan demikian, memelihara dan memastikan aset pengguna dan organisasi aman terhadap ancaman atau risiko keamanan yang mungkin muncul di ranah siber, adalah salah satu fungsi dari keamanan siber (Ardiyanti, 2014). Peran negara dan pemerintah merupakan hal yang tidak dapat dibedakan. Kita juga bisa memahami bahwa di ranah siber peran pemerintah sebagai representasi kekuasaan yang menyatakan bahwa negara hadir di dalam ruang siber untuk mengatur kehidupan warganya dalam rangka mencapai tujuan bersama untuk menyejahterakan kehidupan rakyat terbukti sangat besar.

Berkaitan dengan peran negara dalam ruang siber dalam konteks nasional, maka perlu disusun suatu regulasi yang jelas dan detail sebagai pedoman bagi warga negara dalam beraktivitas di dalam ruang siber, juga untuk menjamin kedaulatan negara maupun warga negaranya dari data-data yang berkaitan dengan dirinya. Untuk mengawasi aktivitas warga negara dalam semangat yang demokratis, kritis, tetapi tetap tidak kebablasan, diperlukan regulasi hukum yang dikeluarkan oleh negara yang berfungsi sebagai rambu-rambu. Terkait perlunya disusun dasar hukum yang jelas sebagai pedoman aktivitas warga di ruang siber, menurut Boele-Woelki dalam Nudirman Munir (2017), dibutuhkan peran dan keterlibatan pemerintah secara langsung untuk membuat regulasi di ruang siber, utamanya untuk menyelesaikan masalah (hukum atau non-hukum) yang bisa timbul. Tom Maddox dalam Munir sejalan dengan Boele-Woelki, perbedaannya hanya pada fungsi pengendalian saja (Munir, 2017). Kelemahan dunia siber di Indonesia disebabkan karena minimnya pengaturan terkait siber yang berakibat pada timbulnya kerancuan di tengah anggota masyarakat. Dunia siber yang melewati batas-batas negara, batas wilayah kepemilikan, hingga batasan pribadi yang berakibat timbulnya konflik juga sengketa yang terjadi di tengah anggota masyarakat (Munir, 2017).

Dalam konteks Indonesia, pada tahun 2017 Presiden Jokowi membentuk Badan Siber dan Sandi Negara atau biasa disingkat BSSN. Pembentukan BSSN yang merepresentasikan hadirnya negara dalam pengelolaan ruang siber nasional memilki peranan yang penting untuk mengoptimalkan koordinasi juga kerjasama lembaga-lembaga lainnya selaku *stakeholder* dalam ranah siber di Indonesia. *Stakeholder* lainnya terkait ruang siber nasional yaitu: TNI/ Kementerian Pertahanan (terkait pertahanan siber), Polri (terkait kejahatan siber), Kementerian Luar Negeri (diplomasi siber), dan kementerian/lembaga lainnya yang terkait dengan tupoksi di bidang siber. Dalam perjalanannya, BSSN sebetulnya telah menjalankan pembinaan terkait *cyber security community*. Terkait fungsi dari proteksi ini ada pada Deputi II bidang proteksi yang memiliki tugas dalam bidang tata kelola keamanan informasi (Chotimah, 2019). Hal ini tidak terlepas dari sebagian besar unit kerja BSSN sebelumnya berasal dari Lembaga sandi Negara (Lemsaneg). Lemsaneg sudah didirikan sejak lama, bahkan sejak era Soekarno dengan bentuk jawatan sandi. Tupoksi Lemsaneg terkait dengan persandian yang memiliki fokus pada keamanan informasi. Dalam hal ini fungsi keamanan informasi memiliki kedekatan substansial dengan keamanan siber yang menjadi tupoksi dari BSSN saat ini.

Menurut mantan Kepala BSSN, Djoko Setiadi, BSSN mampu mendeteksi ancaman siber yang terjadi sepanjang 2018. Dengan kemampuan deteksi ini diharapkan agar semua pihak bisa memahami pergeseran perilaku serangan siber. Terkait kemampuan tersebut, BSSN telah mendeteksi jumlah serangan sepanjang Januari hingga Oktober 2018, sebanyak 207.9 juta serangan. Serangan paling banyak adalah melalui virus *trojan*. Selain itu, sebanyak

36 juta aktivitas *malware* juga menyerang situs-situs penting di Indonesia. Kasus peretasan *hacker* di Indonesia belum lama ini juga terjadi yang menghadirkan nama "Bjorka" menjadi perhatian publik. Selain kasus "Bjorka" terdapat beberapa kasus-kasus lain yang meresahkan publik khususnya terkait permasalahan perlindungan data pribadi. Pada Bulan Mei Tahun 2021, BPJS Kesehatan juga mengalami peretasan yang menyebabkan kebocoran data sejumlah besar Warga Negara Indonesia. Termasuk juga beberapa kementerian/lembaga yang diretas oleh *hacker* yang menyebabkan kebocoran data, terutama data-data pribadi pegawai instansi tersebut, dan data-data lainnya. Sedangkan pada Tahun 2022, menurut data BSSN di Indonesia telah terjadi lebih dari 700 juta serangan siber. Serangan siber ini didominasi oleh *malware* maupun *ransomware* yang memiliki motif menginginkan sejumlah tebusan. Sedangkan sebelumnya pada Tahun 2021, data BSSN menyampaikan bahwa di Indonesia terjadi 1,6 Miliar serangan siber yang didominasi kategori *malware* (Gustiani, 2023). Dalam hal ini, jumlah data serangan siber di Indonesia dapat merepresentasikan bahwa keamanan siber merupakan hal yang fundamental dalam kehidupan berbangsa dan bernegara.

Model Kedewasaan dan Masyarakat Digital

Asal dan Jenis Kematangan Model

Konsep model kedewasaan untuk industri perangkat lunak/TIK pada awalnya disponsori oleh militer AS yang ingin mengembangkan metode untuk secara objektif mengevaluasi kapabilitas dan kematangan proses subkontraktor perangkat lunak/TIK. Karena berbagai teknologi, standar, ukuran dan kapasitas pemasok yang berbeda, ada kebutuhan untuk menilai secara objektif secara terpadu tingkat keandalan, kepercayaan, dan risiko terkait kualitas perangkat lunak/layanan TIK. Model kedewasaan memberikan transisi terukur juga antara level yang berbeda (atau langkah, tahapan). Mereka memungkinkan untuk membandingkan organisasi dengan "tingkat kematangan" mereka dan memberikan pendekatan terstruktur dan diprioritaskan untuk rencana perbaikan.

Model kematangan dapat dikelompokkan menjadi tiga jenis (Sharkov, 2020):

1. *Progression Maturity Models*, sering diilustrasikan dengan *'journey'*, merepresentasikan perkembangan atau penskalaan sederhana dari atribut, karakteristik, indikator, pola di mana pergerakan naik tingkat kematangan menunjukkan perkembangan kematangan atribut. Level menggambarkan "status yang lebih tinggi" berikutnya dari pencapaian, kemajuan, atau 'langkah' dalam evolusi dan memberikan peta jalan transformatif yang jelas. Namun dalam praktiknya, mereka tidak mengukur kematangan proses maupun kapabilitas;
2. *Capability Maturity Models* (CMMs): dimensi yang dievaluasi mewakili kemampuan organisasi di sekitar serangkaian karakteristik, indikator, atau pola, yang sering dinyatakan sebagai 'praktik'. Biasanya disebut sebagai "model proses". Level tipikal model CMM diberi nama di sekitar kematangan proses, misalnya:
3. ad-hoc → dikelola → ditentukan → dikelola secara kuantitatif → dioptimalkan
4. *Hybrid Maturity Models* menggabungkan karakteristik model progresif dengan atribut kapabilitas dari model maturitas kapabilitas dan mencerminkan transisi antar level yang terkait dengan maturitas kapabilitas sementara secara arsitektural menggunakan atribut, indikator, dan pola model progresi. Mereka relatif mudah digunakan dan dipahami, terutama dalam domain materi pelajaran tertentu.

Model kematangan, terlepas dari jenisnya, memiliki struktur serupa yang memastikan hubungan yang harmonis antara tujuan, praktik terbaik, dan penilaian, dan juga memfasilitasi definisi peta jalan peningkatan antara kemampuan saat ini dan target dalam konteks tujuan bisnis, standar, dan karakteristik khusus domain. Struktur tipikal meliputi (Sharkov, 2020)::

1. Tingkat kematangan: menunjukkan keadaan transisi (juga langkah); dalam pendekatan *hybrid* mereka juga dapat dipetakan ke "tingkat kemampuan";

2. Domain model: kelompok atribut dan aktivitas ke dalam area, biasanya disebut sebagai "area proses";
3. Atribut: isi inti model, dikelompokkan berdasarkan domain dan level, berdasarkan praktik, resep, pengetahuan, standar;
4. Metode penilaian: penilaian secara terpadu yang menghasilkan penilaian yang sebanding dan bermakna (lebih dari sekadar kotak centang). Kegunaan utamanya adalah untuk mengevaluasi kepatuhan terhadap model secara objektif, memberikan indikator yang terukur untuk pencapaian dan kemajuan, daripada membandingkan organisasi. Penilaian bisa formal (ahli) dan informal (termasuk penilaian diri);
5. Rencana peningkatan (peta jalan): metode penilaian memberikan evaluasi keadaan saat ini, analisis kesenjangan terhadap tingkat target, identifikasi ruang lingkup dan prioritas peningkatan, perencanaan peningkatan, dan memverifikasi hasil (mencapai tingkat selanjutnya atau mempertahankan tingkat saat ini).

Pengenalan dan penggunaan awal model kematangan berada di industri perangkat lunak/TI. Setelah penggunaan pertama model kematangan bertahap oleh Richard L. Nolan pada tahun 1973, dan karya berikutnya dari Watts Humphrey, awalnya di IBM dan setelah tahun 1986 di Institut Rekayasa Perangkat Lunak (SEI), Universitas Carnegie Mellon (CMU), Departemen AS of Defense meminta kerangka maturitas proses yang diformalkan dari SEI untuk dapat mengevaluasi kontraktor perangkat lunak. Pada awal 1990-an, SEI memperkenalkan *Capability Maturity Model* (CMM) formal dengan lima tingkat kematangan. Selanjutnya, pada tahun 2002, model yang jauh lebih komprehensif dan terintegrasi, *Capability Maturity Models Integration* (CMMI) diterbitkan, dengan versi paling populer 1.3 tahun 2010. Ini berlaku untuk rekayasa perangkat lunak, rekayasa sistem, akuisisi perangkat lunak dan sistem, dan pengiriman layanan sebagai konstelasi yang berbeda dengan inti yang sama. CMMI selanjutnya dikelola oleh CMMI Institute (*spin-off* dari CMU), yang diakuisisi pada tahun 2016 oleh ISACA. Versi baru 2.0 dirilis pada tahun 2018. Lima tingkat kematangan yang ditentukan oleh CMMI untuk mencerminkan kematangan proses yang telah ditetapkan dan dilembagakan adalah:

Awal -> Dikelola -> Ditetapkan -> Dikelola secara kuantitatif -> Mengoptimalkan

Sejak saat itu, model kematangan kapabilitas telah diperkenalkan secara luas dalam domain seperti infrastruktur TIK, semua jenis rekayasa perangkat lunak, manajemen layanan, manajemen proses bisnis, manufaktur, teknik sipil, dan keamanan siber. Institut CMMI menerbitkan pada tahun 2018 "*CMMI Cyber Maturity Platform*" untuk mengatasi penilaian ketahanan dunia maya.

Model Kematangan Kemampuan untuk Keamanan Siber dan Ketahanan Siber

Selama dekade terakhir, beberapa kerangka keamanan siber dan ketahanan telah diusulkan. Sebuah studi baru-baru ini mengidentifikasi lebih dari 25 kegiatan penelitian di 36 industri berbeda yang berusaha mencapai kejelasan yang lebih baik tentang ruang lingkup, karakteristik, sinergi, dan kesenjangan yang akan memfasilitasi kemajuan penelitian ilmiah di bidang ini (Fischer-Hübner, et al., 2021). Pemetaan teknis tahun 2017 yang membandingkan model kematangan yang digunakan di berbagai sektor, termasuk pendidikan dan kesadaran, menjadi sumber lain untuk survei kami. Studi ini mengklasifikasikan kerangka kerja sebagai strategis atau operasional, berdasarkan hierarki pengaruh keputusannya, berdasarkan serangan yang ditangani, melalui metode yang digunakan dan area implementasi. Sebagai latihan untuk menentukan popularitas istilah tersebut, kami melakukan penelusuran sederhana di *Google Scholar*, yang menghasilkan lebih dari 10.000 hasil untuk "model kedewasaan keamanan siber", dan sekitar 12.000 hasil untuk "penilaian kedewasaan ketahanan siber". Untuk survei kami, kami memilih beberapa kerangka kerja yang diidentifikasi dalam penelitian sebelumnya dan menambahkan pekerjaan yang lebih baru, karena kami bertujuan mengidentifikasi penerapan di tingkat yang lebih tinggi dari organisasi

(seperti sektor, komunitas, negara), kesamaan hasil penilaian, dan kemungkinan untuk aplikasi interdisipliner, lintas sektoral dan lintas batas.

Model Kematangan Kapasitas Keamanan Siber untuk Negara (CMM-GCSCC)

CMM-GCSCC adalah kerangka kerja metodis yang dirancang untuk meninjau kematangan kapasitas keamanan siber suatu negara. Ini dikembangkan oleh Pusat Kapasitas Keamanan Siber Global (GCSCC) melalui latihan kolaboratif global yang diluncurkan pada tahun 2014. Untuk masing-masing dari lima dimensinya sebagaimana ditunjukkan pada Tabel 1, model memberikan faktor (total 24 untuk versi ini) yang menentukan kriteria untuk menunjukkan kapasitas keamanan siber masing-masing. Sebagian besar faktor diperiksa dari beberapa sudut pandang, dan terdiri dari serangkaian indikator dalam lima tahap kematangan untuk setiap dimensi, yang diberi nama sebagai berikut: start-up; formatif; didirikan; strategis; dinamis.

CMM-GCSCC adalah salah satu alat penilaian paling populer yang berlaku untuk negara dan wilayah, yang digunakan oleh organisasi internasional seperti ITU, Organisasi Negara-Negara Amerika (OAS), Bank Dunia, Pusat Keamanan Siber Oseania, Pusat Kapasitas Keamanan Siber untuk Afrika Selatan, RAND Corporation, dll. Telah digunakan di lebih dari 80 negara dengan lebih dari 110 penilaian dan dua studi regional oleh OAS. Banyak profil negara tersedia untuk umum dan tingkat yang dicapai dapat ditinjau, bersama dengan perbaikan yang disarankan. Versi baru direncanakan untuk diterbitkan pada paruh kedua tahun 2020. Perlu dicatat bahwa 'kapasitas' tidak setara dengan 'kemampuan', dan modelnya kurang formal daripada penilaian kematangan, meskipun dimensi dan faktor mungkin cocok.

Tabel 1. Model Kematangan Kapasitas Keamanan Siber untuk Negara (CMM dari GCSCC).

Dimensi	Faktor-faktor
Kebijakan dan Strategi Keamanan Siber	Strategi Keamanan Siber Nasional; Tanggapan Insiden; Perlindungan Infrastruktur Kritis (CI); Manajemen Krisis; Pertahanan dunia maya; Redundansi Komunikasi
Budaya dan Masyarakat Cyber	Pola Pikir Keamanan Siber; Kepercayaan dan Keyakinan di Internet; Pemahaman Pengguna tentang Perlindungan Informasi Pribadi Online; Mekanisme Pelaporan; Media dan Media Sosial
Pendidikan, Pelatihan, dan Keterampilan Cybersecurity	Peningkatan Kesadaran; Kerangka Pendidikan; Kerangka Pelatihan Profesional
Kerangka Hukum dan Regulasi	Kerangka Hukum; Sistem keadilan kriminal; Kerangka Kerja Sama Formal dan Informal untuk Memerangi Cybercrime
Standar, Organisasi, dan Teknologi	Kepatuhan terhadap Standar; Ketahanan Infrastruktur Internet; Kualitas Perangkat Lunak; Kontrol Keamanan Teknis; Kontrol Kriptografi; Pasar Keamanan Siber; Pengungkapan yang Bertanggung Jawab

Indeks dan Kematangan *Cybersecurity*

Dengan meningkatnya minat dan ambisi negara-negara untuk mempercepat program perbaikan dan mempromosikan prestasi mereka secara internasional, instrumen evaluasi dan pemeringkatan status negara lainnya adalah indeks internasional/global. Ada banyak indeks yang telah dibuat selama beberapa dekade di berbagai bidang seperti pengembangan masyarakat informasi, kesiapan digital, konektivitas internet, literasi komputer, dll. ITU menerbitkan “Indeks keamanan siber” pada tahun 2017 dengan indeks keamanan siber internasional paling populer. Penulis akan mengomentari tiga di antaranya dengan fokus pada penilaian negara.

Global Cybersecurity Index (GCI) sebagai kerangka penilaian berdasarkan *Global Cybersecurity Agenda* (GCA) dari ITU. GCI mengukur komitmen negara terhadap keamanan siber di tingkat global. Penilaian tersebut mengukur tingkat pembangunan atau keterlibatan

suatu negara melalui survei *online* berbasis pertanyaan yang disusun berdasarkan lima pilar—Langkah Hukum, Langkah Teknis, Langkah Organisasi, Peningkatan Kapasitas, dan Kerja Sama—menggunakan 25 indikator dan sub-indikator tambahan, lalu menghitung sebuah skor keseluruhan (Cloramidine & Badaruddin, 2023). Sejak survei pertama di tahun 2013, GCI mempromosikan inisiatif keamanan siber melalui perbandingan. Edisi ketiga GCI (tahun 2018), yang mencakup lebih dari 193 negara dan menghasilkan tiga laporan regional, menunjukkan peningkatan yang signifikan dalam keamanan siber di seluruh dunia, karena semakin banyak negara yang memiliki strategi keamanan siber, rencana nasional, tim respons, dan undang-undang khusus. Namun, kesenjangan yang signifikan antar daerah masih diamati.

National Cybersecurity Index (NCSI) mengukur kesiapan negara untuk mencegah ancaman dunia maya dan mengelola insiden, kejahatan, dan krisis dunia maya dalam skala besar. Akademi e-Governance Estonia mengembangkannya bekerja sama dengan Kementerian Luar Negeri Estonia. Indeks tersebut menekankan pada aspek publik keamanan siber nasional yang dilaksanakan oleh pemerintah pusat. Indeks tersebut memiliki 12 indikator utama dengan sub-indikator yang dibagi menjadi tiga kelompok: *General Cyber Security, Baseline Cyber Security, Incident* dan *Crisis Management*. Indikatornya terkait dengan masyarakat informasi dan masalah keamanan dunia maya seperti identitas elektronik, tanda tangan digital, dan keberadaan lingkungan yang aman untuk layanan elektronik. NCSI menyediakan materi bukti yang tersedia untuk umum dan alat untuk membangun kapasitas keamanan siber nasional. Peringkat negara dibandingkan dengan GCI (ITU), ICT *Development Index*, dan *Networked Readiness Index* (Wirght, Digitales, Ralby, & Karisma, 2018).

Cyber Readiness Index 2.0 (CRI 2.0) melakukan evaluasi kematangan dunia maya suatu negara serta komitmen keseluruhannya terhadap masalah dunia maya, mendefinisikan arti "siap dunia maya" sambil mengusulkan cetak biru yang dapat ditindaklanjuti untuk diikuti. Indeks tersebut menggunakan seperangkat tujuh indikator: strategi nasional, respons insiden, kejahatan elektronik dan penegakan hukum, berbagi informasi, investasi dalam R&D, diplomasi dan perdagangan, pertahanan, dan respons krisis. Seratus dua puluh lima negara dipelajari, dan metodologinya didasarkan pada pilar yang sama dengan Agenda Keamanan Siber Global ITU. Setiap negara diberi skor, sedangkan penambahan kemampuan militer melampaui yang dicakup oleh ITU GCI. Namun, CRI 2.0 tidak menawarkan peringkat apa pun terlepas dari mekanisme penilaiannya (Demchak, Kerben, McArdle, & Spidalieri, 2015).

Meskipun ini dan indeks lain yang dikenal (Indeks Keamanan Siber Kaspersky, Kematangan Siber di Wilayah Asia-Pasifik, dll.) Cukup populer dan mudah untuk dipromosikan di negara-negara, penggunaannya sebagai indikator penilaian kematangan dunia maya diragukan. Area dan indikator terlihat serupa dengan model maturitas, tetapi tidak memiliki ketelitian dan perincian dari tingkat maturitas dan penilaiannya. Tidak ada tingkatan, dan rencana perbaikan tidak dapat diprioritaskan dan disusun dengan tahapan dan target yang jelas. Peringkat yang lebih tinggi dalam indeks bisa menjadi indikator keberhasilan, tetapi kemungkinan besar tidak akan ditetapkan sebagai target. Skor berbasis pertanyaan sangat bergantung pada keterlibatan dan motivasi badan lokal untuk memberikan bukti.

Fokus pada Kematangan dalam Strategi Keamanan Siber Nasional

Fokus pada kematangan keamanan siber sudah dimasukkan, dan penilaian kematangan direkomendasikan di sebagian besar manual dan pedoman yang diperbarui untuk pengembangan strategi keamanan siber nasional. Dalam Panduan Praktik Baik Strategi Keamanan Siber Nasional (NCSS) ENISA (diperbarui tahun 2016), ada dua referensi untuk kematangan dan penilaian selama siklus hidup pengembangan dan implementasi strategi.

Untuk menetapkan langkah-langkah keamanan dasar, beberapa aspek kompleks harus dipertimbangkan: tingkat kematangan yang berbeda di antara para pemangku kepentingan, perbedaan kapasitas operasional setiap organisasi, dan perbedaan standar yang ada di setiap sektor penting. Di antara tindakan yang direkomendasikan adalah "Membuat alat penilaian diri kedewasaan dan mendorong pemangku kepentingan untuk menggunakannya." Menurut Rekomendasi 9: "Tingkatkan kemampuan sektor publik dan swasta," setelah persyaratan dasar ditetapkan, kemampuan yang ada perlu dievaluasi untuk mengidentifikasi kesenjangan dan penyimpangan. Untuk mengembangkan rencana peningkatan dan menilai hasil, pemerintah disarankan untuk "secara aktif mendukung pembangunan kapasitas dengan menerbitkan standar nasional, merancang model kematangan kemampuan keamanan siber, mempromosikan dan mendorong pertukaran pengetahuan….."

Namun demikian, tinjauan singkat terhadap strategi keamanan siber nasional (tercantum di situs web ENISA) menunjukkan bahwa kata "kedewasaan" hampir tidak disebutkan, dan "tingkat kematangan" atau model tidak dirujuk. Pengamatan ini mungkin tidak lengkap, karena masalah ini mungkin dibahas dalam rencana dan peta jalan. Beberapa penyebutan model kedewasaan dan kedewasaan dunia maya adalah:

1. Strategi Inggris Raya yang diadopsi pada tahun 2016 menyatakan bahwa tingkat dukungan Pemerintah Inggris Raya untuk setiap sektor ditentukan "dengan mempertimbangkan kematangan sibernya". *Cyber Assessment Framework* (CAF) oleh NCSC diperkenalkan untuk memandu organisasi dari layanan yang sangat penting;
2. Dalam Strategi Keamanan Siber Estonia ketiga (2019), "tingkat kematangan yang teruji" dianggap sebagai salah satu kekuatan utama Estonia. Berbagai bidang kemampuan dan jenis kematangan indikator didefinisikan, dengan penjelasan rinci tentang tingkat 'awal' dan 'target', tujuan yang jelas dan bidang kegiatan (yang memang menjadikannya contoh yang baik dari strategi yang dapat ditindaklanjuti), tetapi tidak ada penjabaran lebih lanjut tentang pengenalan "model kedewasaan dunia maya" atau penilaian akhirnya tercakup;
3. Strategi Keamanan Siber Lituania (2018) ditetapkan sebagai target pertamanya "untuk memperkuat keamanan siber di negara tersebut dan untuk mengembangkan kemampuan pertahanan siber";
4. Strategi Finlandia (diperbarui pada tahun 2019) merekomendasikan agar "setiap cabang administrasi membuat penilaian risiko dan analisis kematangannya...," yang dikembangkan lebih lanjut dalam Program Implementasi, di mana Sekretariat Komite Keamanan akan "melakukan penelitian proyek untuk membuat model dan instrumentasi maturitas yang diperbarui untuk tujuan memantau status keamanan dunia maya Finlandia dan pencapaian tujuan… Model maturitas dan instrumen akan digunakan untuk memberikan laporan reguler tentang status…"

Strategi dan Kebijakan Siber Indonesia Dengan Menggunakan Pendekatan Oxford University Capacity Maturity Model (CMM).

Dalam penelitian ini terdapat empat aspek teori yang dibahas, yaitu *Culture, Cyber Culture, Cyber Resilience* dan *Capacity Maturity Model* (CMM). Dalam praktiknya di Indonesia, berikut adalah gambaran umum mengenai keempat aspek tersebut:

1. *Culture* (Budaya)

Aspek budaya memiliki peran penting dalam praktik keamanan siber di Indonesia. Kultur keamanan siber sedang berkembang dan semakin diakui sebagai prioritas nasional. Pemerintah, sektor swasta, dan masyarakat secara bertahap menyadari pentingnya keamanan siber dalam menghadapi ancaman yang terus berkembang. Peningkatan kesadaran keamanan siber terjadi melalui kampanye kesadaran publik, pelatihan, seminar, dan konferensi. Meskipun masih ada tantangan, seperti rendahnya tingkat kesadaran dan kurangnya literasi digital di beberapa segmen masyarakat, kesadaran akan keamanan siber terus meningkat di Indonesia.

2. *Cyber Culture* (Budaya Siber):

Indonesia memiliki budaya siber yang berkembang pesat dengan penggunaan yang luas dari internet dan media sosial. Aktivitas online, seperti berbagi informasi, berinteraksi dengan platform media sosial, dan perdagangan elektronik, semakin meluas. Namun, sebagai bagian dari budaya siber, juga ada tantangan dalam hal keamanan siber, seperti penyebaran hoaks, serangan siber, dan kejahatan siber lainnya. Pemerintah dan lembaga terkait berupaya meningkatkan literasi digital dan kesadaran akan ancaman siber di kalangan masyarakat untuk mempromosikan budaya siber yang lebih aman.

3. *Cyber Resilience* (Ketahanan Siber):

Ketahanan siber menjadi fokus penting dalam praktik keamanan siber di Indonesia. Pemerintah dan lembaga terkait telah mengembangkan rencana dan kebijakan ketahanan siber untuk menghadapi dan merespons ancaman dan serangan siber. Langkah-langkah yang diambil termasuk peningkatan keamanan infrastruktur kritis, pengembangan kebijakan dan standar keamanan, peningkatan kapabilitas tanggap insiden, dan kerjasama dengan sektor swasta dan internasional. Meskipun masih ada ruang untuk peningkatan lebih lanjut, Indonesia terus berupaya membangun ketahanan siber yang lebih kuat untuk melindungi infrastruktur dan sistem informasi kritis.

4. *Capacity Maturity Model* (Model Kematangan Kapabilitas):

Model Kematangan Kapabilitas (*Capacity Maturity Model*) merupakan kerangka kerja yang digunakan untuk mengevaluasi tingkat kematangan organisasi dalam praktik keamanan siber. Upaya telah dilakukan untuk meningkatkan kapabilitas keamanan siber melalui peningkatan kebijakan, pengembangan standar dan pedoman, pelatihan dan sertifikasi, serta kerja sama dengan mitra internasional.

Pendekatan *Oxford University Capacity Maturity Model* (CMM) adalah kerangka kerja yang dapat digunakan untuk mengevaluasi dan meningkatkan kapabilitas keamanan siber suatu organisasi. Dalam konteks penerapan strategi dan kebijakan siber di Indonesia, berikut adalah beberapa cara dimana CMM dapat digunakan:

1. Evaluasi Kematangan: CMM dapat digunakan untuk mengevaluasi tingkat kematangan strategi dan kebijakan siber di Indonesia. Dengan menganalisis berbagai aspek seperti visi strategis, kebijakan dan peraturan, struktur organisasi, kapabilitas keamanan, dan pengukuran kinerja, CMM dapat membantu dalam menentukan tingkat kematangan saat ini.
2. Identifikasi Kelemahan: CMM membantu dalam mengidentifikasi kelemahan atau kekurangan dalam strategi dan kebijakan siber yang ada. Dengan menganalisis setiap tahap kematangan, CMM dapat mengidentifikasi area di mana Indonesia mungkin belum mencapai tingkat kematangan yang diharapkan. Hal ini dapat membantu pihak berwenang dalam merumuskan langkah-langkah perbaikan yang tepat.
3. Pengembangan *Roadmap*: Berdasarkan penilaian CMM, pihak berwenang dapat mengembangkan *roadmap* atau rencana tindakan untuk meningkatkan strategi dan kebijakan siber di Indonesia. *Roadmap* ini dapat mencakup langkah-langkah konkret yang harus diambil untuk mencapai tingkat kematangan yang lebih tinggi. CMM dapat membantu dalam menentukan urutan prioritas dan menyusun strategi implementasi yang efektif.
4. *Benchmarking* dengan Praktik Terbaik: CMM dapat digunakan sebagai tolok ukur untuk membandingkan strategi dan kebijakan siber Indonesia dengan praktik terbaik di tingkat internasional. Dengan membandingkan diri dengan organisasi atau negara-negara lain yang telah mencapai tingkat kematangan yang lebih tinggi, Indonesia dapat mengidentifikasi peluang perbaikan dan mengadopsi praktik terbaik yang relevan.
5. Peningkatan Kesadaran: Penerapan CMM dapat meningkatkan kesadaran akan pentingnya strategi dan kebijakan siber yang matang di Indonesia. Dengan melibatkan pemangku kepentingan dan menyampaikan hasil evaluasi CMM, pihak berwenang dapat membangun

pemahaman yang lebih baik tentang tantangan dan kebutuhan keamanan siber, serta mendorong partisipasi aktif dalam upaya perbaikan.

Penerapan CMM dalam strategi dan kebijakan siber di Indonesia dapat membantu pihak berwenang dalam mengidentifikasi kelemahan, merumuskan langkah-langkah perbaikan yang tepat, dan meningkatkan kapabilitas keamanan siber secara keseluruhan. Penting untuk melibatkan pemangku kepentingan yang relevan dan mempertimbangkan konteks nasional dalam menerapkan pendekatan CMM ini.

Dalam tulisan ini terdapat empat aspek teori yang dibahas, yaitu *Culture, Cyber Culture, Cyber Resilience* dan *Capacity Maturity Model*. Menurut pendapat Letjen Purn Hinsa Siburian selaku Kepala Badan Siber dan Sandi Negara Republik Indonesia, bahwa dalam mewujudkan ekosistem keamanan siber Indonesia, BSSN terus berupaya melaksanakan empat aspek tersebut melalui :

1. Terkait *Culture* atau Budaya : Seperti diketahui bahwa Indonesia terdiri dari beragam budaya yang ada di masyarakat. Tentunya budaya masyarakat juga dapat dipengaruhi sebagai dampak dari penggunaan ruang siber. Hal ini karena serangan siber dapat berdampak pada perubahan budaya akibat adanya perubahan pola pikir yang ada di masyarakat karena adanya arus informasi yang masuk.
2. *Cyber Culture* : Budaya siber merupakan hal yang sangat penting dalam penguatan keamanan siber. Salah satu upaya dalam meningkatkan budaya siber adalah dengan melakukan peningkatan keamanan siber. BSSN terus melakukan literasi keamanan siber dan program peningkatan kapasitas SDM melalui kegiatan Pendidikan dan pelatihan di bidang keamanan siber dan sandi baik bagi masyarakat maupun bagi pengelola sistem elektronik.
3. *Cyber Resillience* : Sebagai upaya mewujudkan ketahanan siber BSSN terus mendorong adanya payung hukum yang mengatur terkait keamanan siber. Salah satunya dengan terbitnya Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV). Hal ini sebagai upaya untuk melindungi Sistem Elektronik dalam menunjang sektor strategis, dari terjadi gangguan, kerusakan, dan/ atau kehancuran pada infrastruktur dimaksud berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional. Selain itu, BSSN juga sedang menyusun Peraturan Presiden tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber yang dimana sudah diajukan kepada Bapak Presiden untuk pengesahan. Payung hukum inilah sebagai upaya mewujudkan ketahanan siber nasional dengan sinergi pemangku kepentingan yaitu Pemerintah, Pelaku Usaha, Akademisi dan Komunitas/Masyarakat. Ketahanan siber sangat terkait dengan bagaimana upaya penanganan insiden yang baik sehingga diperlukan kesiapan penggunaan sumber daya dalam menghadapi serangan siber yang semakin meningkat. Saat ini BSSN terus mengembangkan jumlah CSIRT (*Computer Security Incident Response Team*) baik bagi sektor pemerintah dan swasta sehingga tercipta ketahanan siber yang lebih baik. Ketahanan siber sangat dipengaruhi oleh budaya keamanan siber, intelijen siber, keamanan siber, kebijakan siber, hukum siber dan pengaruh siber.
4. *Capacity Maturity Model* : Saat ini dalam menilai keamanan siber secara nasional, BSSN menggunakan pengukuran yang dikeluarkan oleh ITU yakni menggunakan *Global Cybersecurity Index* (GCI). Pada tahun 2020 Indonesia menempati ranking 24 dari 194 negara. Sedangkan untuk melihat kematangan keamanan siber pada Penyelenggara Sistem Elektronik (PSE) telah dilakukan menggunakan CSM (*Cyber Security Maturity*).

Mengenai penggunaan *Capacity Maturity Model* (CMM) yang dikeluarkan oleh Oxford saat ini belum diterapkan, namun BSSN sedang menyusun mekanisme pengukuran kematangan keamanan siber nasional yang berdasarkan pendekatan risiko, dimana menggunakan parameter yang ada pada CMM. Mengingat CMM adalah salah satu hasil penelitian yang memiliki basis argumentasi yang relevan, tentu CMM dapat digunakan untuk

penerapan strategi dan kebijakan siber di Indonesia. Namun demikian CMM bukan satu satunya yang dapat dirujuk. Dalam hal penyusunan strategi keamanan siber nasional itu sendiri, BSSN merujuk *framework* yang lebih besar, yaitu panduan ITU yang lebih luas. Panduan ITU mempertimbangkan 7 (tujuh) fokus area, yaitu Tata Kelola, Manajemen Risiko, Ketahanan dan Kesiapsiagaan, Infrastruktur Informasi Vital, Pengembangan Kapasitas dan Kapabilitas, Legislasi dan Regulasi, Kerja Sama Internasional, dan Kriptografi. Kriptografi adalah fokus area tambahan yang dipertimbangkan oleh BSSN dalam mencapai kedaulatan siber di masa depan nanti. Saat ini Strategi Keamanan Siber telah selesai disusun dan menunggu pengesahan oleh Presiden.

Dalam tulisan ini, penulis mengambil dimensi budaya dan sosial dari CMM menjadi daya tarik utama dalam tulisan ini. Akan tetapi, Oxford University *Capacity Maturity Model* (CMM) tidak secara khusus mengeksplorasi dimensi budaya dan sosial. CMM lebih fokus pada aspek-aspek seperti visi strategis, kebijakan dan peraturan, struktur organisasi, kapabilitas keamanan, dan pengukuran kinerja dalam konteks keamanan siber. Dimensi budaya dan sosial yang disebutkan lebih relevan dengan analisis budaya organisasi atau evaluasi budaya keamanan siber yang dapat dilakukan terpisah atau sebagai tambahan dari CMM (Creese, Dutton, & Esteve-González, 2021). Untuk menggali dimensi budaya dan sosial yang lebih mendalam, beberapa kerangka kerja lain dapat digunakan, seperti:

1. Kerangka Kerja Keamanan Siber Berbasis Budaya (*Culture-Based Cybersecurity Framework*): Kerangka kerja ini fokus pada pengaruh budaya organisasi terhadap keamanan siber. Ini melibatkan pemahaman tentang norma, nilai, sikap, dan perilaku yang ada di organisasi dan bagaimana faktor-faktor tersebut mempengaruhi keberhasilan keamanan siber.
2. Kerangka Kerja Keamanan Siber Berbasis Masyarakat (*Community-Based Cybersecurity Framework*): Kerangka kerja ini mempertimbangkan faktor-faktor sosial dalam keamanan siber, termasuk partisipasi masyarakat, kesadaran publik, pendidikan, dan upaya kolaboratif dalam menghadapi ancaman siber.
3. Kerangka Kerja Keamanan Siber Berbasis Insan (*Human-Centric Cybersecurity Framework*): Kerangka kerja ini menekankan peran individu dan kelompok dalam keamanan siber. Hal ini mencakup pemahaman tentang perilaku manusia, kesadaran individu, keterampilan, dan pengaruh faktor psikologis dalam menghadapi ancaman siber.

Penggunaan kerangka kerja seperti yang disebutkan di atas dapat membantu dalam menganalisis dimensi budaya dan sosial yang berkontribusi pada keamanan siber. Namun, perlu dicatat bahwa konteks budaya dan sosial di Indonesia dapat berbeda dengan konteks di negara lain, dan oleh karena itu, pendekatan ini harus disesuaikan dengan kebutuhan dan karakteristik unik Indonesia. Menurut pendapat Letjen Purn Hinsa Siburian selaku Kepala Badan Siber dan Sandi Negara Republik Indonesia, bahwa untuk mendapatkan hasil yang komprehensif. Idealnya seluruh dimensi pada CMM menjadi tolak ukur dalam melakukan peningkatan kapasitas keamanan siber. CMM meyakini bahwa keamanan *cyber* terdiri dari lima dimensi, yang bersama-sama membentuk keluasan kapasitas nasional yang dibutuhkan sebuah negara agar efektif dalam menyediakan keamanan *cyber* antara lain :

1. Mengembangkan kebijakan dan strategi keamanan *cyber*.
2. Membina budaya keamanan *cyber* yang bertanggung jawab di masyarakat.
3. Membangun pengetahuan dan kapasitas di bidang keamanan *cyber*.
4. Membuat kerangka kerja hukum dan peraturan yang efektif.
5. Kontrol risiko melalui standar dan teknologi

Namun demikian untuk penelitian dalam hal keamanan siber secara sosial, dimensi budaya dan sosial sudah cukup untuk mewakili. Seperti diketahui bahwa keamanan siber tidak hanya berkaitan dengan aspek teknis terkait ilmu komputer, jaringan komunikasi, perangkat keras dan perangkat lunak. Namun keamanan siber juga berkaitan dengan aspek sosial, yakni bagaimana menciptakan stabilitas keamanan nasional dari upaya-upaya

disintegrasi bangsa akibat disinformasi, penyebaran berita palsu, ujaran kebencian dan propaganda asing. Sebuah Peta Jalan Ketahanan Siber yang ideal berdasarkan dimensi budaya dan sosial dapat mencakup langkah-langkah berikut:

1. Kesadaran dan Pendidikan: Membangun kesadaran yang kuat tentang keamanan siber dan mengedukasi masyarakat tentang ancaman yang ada serta langkah-langkah yang dapat diambil untuk melindungi diri mereka. Ini dapat melibatkan kampanye kesadaran publik, pelatihan keamanan siber, dan integrasi literasi digital ke dalam kurikulum pendidikan.
2. Kolaborasi dan Kemitraan: Mendorong kolaborasi antara pemerintah, sektor swasta, lembaga akademik, dan masyarakat sipil untuk membangun ekosistem keamanan siber yang kuat. Ini termasuk pertukaran informasi, koordinasi respons terhadap ancaman, dan pengembangan kerja sama yang saling menguntungkan.
3. Etika dan Kesadaran Hukum: Memperkuat pemahaman tentang etika digital dan hukum terkait keamanan siber. Ini mencakup peningkatan pemahaman tentang tanggung jawab dalam penggunaan teknologi, privasi, perlindungan data, dan konsekuensi hukum terkait dengan pelanggaran keamanan siber.
4. Pemberdayaan Masyarakat: Mendorong partisipasi aktif masyarakat dalam keamanan siber dengan memberikan alat dan pengetahuan yang diperlukan. Ini meliputi pengembangan mekanisme pelaporan ancaman siber, pelibatan masyarakat dalam kegiatan mitigasi dan respons, serta penguatan kapasitas individu dan kelompok dalam menghadapi ancaman siber.
5. Penghargaan dan Pengakuan: Mendorong penghargaan dan pengakuan terhadap praktik keamanan siber yang baik. Ini dapat melibatkan penghargaan bagi organisasi dan individu yang menunjukkan komitmen terhadap keamanan siber dan praktik yang efektif.
6. Kebijakan dan Regulasi: Meningkatkan kebijakan dan regulasi terkait keamanan siber yang mencerminkan nilai budaya dan sosial masyarakat Indonesia. Kebijakan harus mengakomodasi keunikan budaya dan nilai lokal, serta melindungi privasi dan kebebasan individu.
7. Pendekatan Komprehensif: Membangun pendekatan keamanan siber yang holistik, melibatkan seluruh lapisan masyarakat dan sektor. Hal ini termasuk melibatkan tokoh-tokoh masyarakat, pemangku kepentingan, lembaga pendidikan, dan sektor swasta dalam merumuskan kebijakan dan praktik yang efektif.
8. Penelitian dan Inovasi: Mendorong penelitian dan inovasi dalam keamanan siber dengan melibatkan universitas, lembaga riset, dan sektor industri. Ini dapat membantu mengembangkan solusi baru, memperbarui pengetahuan tentang ancaman siber terkini, dan meningkatkan kapabilitas teknologi di bidang keamanan siber.

Menurut pendapat Letjen Purn Hinsa Siburian selaku Kepala Badan Siber dan Sandi Negara Republik Indonesia, bahwa dalam menyusun *roadmap* ketahanan siber yang ideal dari dimensi budaya dan sosial, terdapat beberapa langkah yang dapat dipertimbangkan. Berikut adalah beberapa poin yang relevan:

1. Kesadaran dan Pendidikan: Meningkatkan kesadaran tentang keamanan siber di antara individu-individu dan masyarakat secara umum. Kampanye kesadaran, pelatihan, dan program pendidikan tentang ancaman keamanan siber dan langkah-langkah yang dapat diambil untuk melindungi diri sendiri dan informasi pribadi menjadi langkah awal yang penting.
2. Pemahaman Risiko: Mendorong pemahaman yang lebih baik tentang risiko yang terkait dengan keamanan siber dan dampaknya pada individu dan masyarakat. Mengkomunikasikan secara jelas tentang ancaman dan kerentanan yang ada, serta memberikan informasi tentang tindakan pencegahan yang dapat diambil, dapat membantu membangun pemahaman yang lebih luas dan mendalam.
3. Partisipasi Masyarakat: Mendorong partisipasi aktif masyarakat dalam upaya keamanan siber. Ini dapat melibatkan kampanye partisipasi publik, penggunaan kelompok advokasi,

dan pemberdayaan masyarakat untuk melaporkan kejadian yang mencurigakan atau berbagi informasi terkait keamanan siber.
4. Pengaturan dan Kebijakan: Membangun kerangka kerja regulasi dan kebijakan yang mendorong praktik keamanan siber yang baik di tingkat masyarakat. Ini melibatkan upaya kolaboratif antara pemerintah, sektor swasta, dan masyarakat sipil untuk mengembangkan regulasi yang efektif, mempromosikan standar keamanan, dan mengawasi kepatuhan.
5. Etika dan Privasi: Mempromosikan penggunaan teknologi dengan etika dan memperhatikan privasi individu. Mengedepankan perlindungan data pribadi dan mempertimbangkan implikasi etis dari penggunaan teknologi dapat membangun kepercayaan masyarakat terhadap upaya keamanan siber.
6. Kolaborasi dan Kemitraan: Membangun hubungan kolaboratif antara pemerintah, sektor swasta, lembaga akademik, dan organisasi masyarakat sipil untuk berbagi informasi, pengetahuan, dan sumber daya dalam menghadapi ancaman keamanan siber.
7. Tanggung Jawab Bersama: Mendorong tanggung jawab bersama dalam menjaga keamanan siber. Menyebarkan pesan bahwa keamanan siber adalah tanggung jawab bersama dan bahwa setiap individu dan organisasi memiliki peran dalam melindungi diri mereka sendiri dan berkontribusi pada keamanan secara keseluruhan.

Dengan *roadmap* yang mencakup langkah-langkah seperti di atas, diharapkan dapat terbentuk budaya dan sosial yang sadar dan tanggap terhadap keamanan siber, sehingga meningkatkan ketahanan siber secara menyeluruh. Peta Jalan Ketahanan Siber yang ideal berdasarkan dimensi budaya dan sosial harus mengintegrasikan aspek budaya dan sosial dengan kerangka kerja keamanan siber yang lebih luas. Penting untuk melibatkan pemangku kepentingan yang relevan, termasuk pemerintah, sektor swasta, masyarakat sipil, dan akademisi, dalam merumuskan dan melaksanakan peta jalan ini. Untuk menjaga dan mengembangkan keamanan siber di Indonesia, berikut adalah beberapa langkah konkret yang dapat dilakukan:

1. Pembangunan Kebijakan dan Hukum: Menguatkan kerangka kebijakan dan hukum terkait keamanan siber di Indonesia. Ini meliputi pengembangan undang-undang, peraturan, dan kebijakan yang mengatur aspek keamanan siber, perlindungan data pribadi, kejahatan siber, dan kerja sama internasional dalam penanganan ancaman siber.
2. Kesadaran dan Pendidikan: Melakukan kampanye kesadaran publik yang meluas tentang keamanan siber. Hal ini mencakup pendidikan dan pelatihan untuk masyarakat, baik dalam lingkup pendidikan formal maupun nonformal, serta pelatihan khusus bagi pekerja di sektor teknologi informasi dan komunikasi. Peningkatan literasi digital dan pemahaman tentang risiko keamanan siber juga perlu ditingkatkan.
3. Perlindungan Infrastruktur Kritis: Meningkatkan keamanan infrastruktur kritis seperti sistem telekomunikasi, sistem keuangan, sistem kelistrikan, dan sektor kesehatan. Ini mencakup penerapan standar keamanan yang ketat, pengujian keamanan secara teratur, dan memastikan kerja sama antara pemerintah dan sektor swasta dalam mengatasi risiko keamanan siber.
4. Pengembangan Kapabilitas: Meningkatkan kapabilitas dalam mendeteksi, mencegah, dan merespons serangan siber. Ini melibatkan pelatihan dan pengembangan sumber daya manusia dalam bidang keamanan siber, peningkatan keahlian teknis, serta pendirian pusat keamanan siber yang berfokus pada pemantauan dan tanggap terhadap ancaman.
5. Kerja sama dan Kemitraan: Meningkatkan kerja sama antara sektor publik, swasta, dan akademik dalam mengatasi ancaman siber. Ini meliputi pertukaran informasi dan intelijen, berbagi praktik terbaik, kolaborasi dalam penelitian dan pengembangan, serta kerja sama internasional dalam menghadapi ancaman siber yang bersifat lintas batas.
6. Audit Keamanan: Melakukan audit keamanan secara berkala untuk mengevaluasi tingkat keamanan sistem informasi dan infrastruktur yang ada. Audit ini akan membantu mengidentifikasi kelemahan dan celah keamanan yang perlu diperbaiki.

7. Tanggapan Terhadap Insiden: Membangun dan meningkatkan kemampuan tanggap insiden untuk merespons serangan siber dengan cepat dan efektif. Hal ini melibatkan perencanaan, latihan, dan koordinasi antara lembaga penegak hukum, regulator, dan sektor swasta dalam menangani insiden keamanan siber.
8. Penelitian dan Inovasi: Mendorong penelitian dan inovasi dalam bidang keamanan siber. Ini termasuk pengembangan teknologi baru, analisis ancaman, dan pengembangan solusi keamanan yang inovatif.

Langkah-langkah ini harus didukung oleh komitmen kuat dari pemerintah, kerja sama antara pemangku kepentingan yang relevan, dan alokasi sumber daya yang memadai. Peningkatan keamanan siber adalah upaya yang berkelanjutan dan membutuhkan kerja sama lintas sektor dan lintas negara untuk menghadapi ancaman yang terus berkembang.

KESIMPULAN

Strategi dan kebijakan siber Indonesia, meliputi 1) Kebijakan Nasional Keamanan Siber (*National Cybersecurity Policy*): Pada tahun 2017, Indonesia mengeluarkan Kebijakan Nasional Keamanan Siber yang bertujuan untuk melindungi infrastruktur kritis dan data penting negara, mengatasi ancaman siber, dan meningkatkan kapabilitas keamanan siber di Indonesia. 2) Pembentukan Badan Siber dan Sandi Negara (BSSN): BSSN adalah lembaga pusat yang bertanggung jawab atas kebijakan dan koordinasi keamanan siber di Indonesia. BSSN bekerja untuk melindungi infrastruktur kritis, menyusun kebijakan keamanan siber, dan meningkatkan kapabilitas nasional dalam menghadapi ancaman siber. 3) Kerja sama Internasional: Indonesia telah melakukan kerja sama dengan negara-negara lain, termasuk kerja sama dengan negara-negara ASEAN dan Australia, untuk meningkatkan keamanan siber dan pertukaran informasi tentang ancaman siber. Kerja sama ini membantu dalam memperoleh wawasan dan pengalaman dari praktik terbaik di tingkat global. 4) Kesadaran dan Pendidikan: Pemerintah Indonesia juga telah mengadakan kampanye untuk meningkatkan kesadaran masyarakat dan pendidikan tentang keamanan siber. Ini termasuk program-program kesadaran siber untuk masyarakat umum, pelatihan keamanan siber untuk profesional IT, dan pengembangan kurikulum yang terkait dengan keamanan siber di perguruan tinggi.

Pendekatan Oxford University *Capacity Maturity Model* (CMM) dapat digunakan untuk mengevaluasi tingkat kematangan strategi dan kebijakan siber Indonesia dengan memperhatikan aspek budaya dan sosial. Juga direkomendasikan kerja sama antara pemerintah dan swasta yang terstruktur dan didukung tata kelola siber yang baik sangat diperlukan dalam menjaga dan mengembangkan keamanan siber.

REFERENSI

Ahmad, D., Putri, D. A., Styawan, H., Nugraha, L. K., & Magdalena, M. (2018). *Kebijakan Cybersecurity Dalam Perspektif Multistakeholder.* Jakarta: Global Partners Digital.

Annur, C. M. (2022, Maret 23). *Ada 204,7 Juta Pengguna Internet di Indonesia Awal 2022*. Diambil kembali dari databoks.katadata.co.id: https://databoks.katadata.co.id/datapublish/2022/03/23/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022#:~:text=Indonesia%20merupakan%20salah%20satu%20negara,%2C03%25%20dibandingkan%20tahun%20sebelumnya.

Ardiyanti, Handrini. 2014. "Cyber Security dan Tantangan Pengembangannya di Indonesia" .*Jurnal Politica* 5, No 1.

Bakhri, Syaiful. 2018. *Ilmu Negara: Dalam Pergumulan Filsafat, Sejarah dan Negara Hukum.* Depok: Rajawali Pers, 2018.

BSSN. (2023). *Lanskap Keamanan Siber Indonesia.* Jakarta: BSSN.

Carallo, A., Crespino, A. M., Vecchio, V. D., Gervasi, M., Lazoi, M., & Marra, M. (2023). Evaluating maturity level of big data management and analytics in industrial companies. *Technological Forecasting and Social Change, 196*.

Cloramidine, F., & Badaruddin, M. (2023). MENGUKUR KEAMANAN SIBER INDONESIA MELALUI INDIKATOR PILAR KERJASAMA DALAM GLOBAL CYBERSECURITY INDEX (GCI). *Populis : Jurnal Sosial dan Humaniora, 8*(1), 57-73.

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and Ubiquitous Computin*, 941-955.

Creswell, J. W. (1998). *Qualitative Inquiry And Research Design: Choosing Among Five Traditions.* London: SAGE Publications.

Daeng, Y., Levin, J., Karolina, Prayudha, M. R., Ramadhani, N. P., Noverto, . . . Virgio. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. *INNOVATIVE: Journal Of Social Science Research, 3*(6), 1135-1145.

Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). *Cyber Readiness Index 2.0 A Plan For Cyber Readiness: A Baseline And An Index.* Arlington: Potomac Institute for Policy Studies.

Chotimah, Hidayat Chusnul. 2019. "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara, *Jurnal Politica* 10, No. 2.

Dihni, V. A. (2022, Agustus 9). *Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022*. Diambil kembali dari databoks.katadata.co.id: https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocoran-data-di-indonesia-melonjak-143-pada-kuartal-ii-2022#:~:text=Ada%201%2C04%20juta%20akun%20yang%20mengalami%20kebocoran%20data,to%20quarter%20%2Fqtq%29%20yang%20sebanyak%20430%2C1%20ribu.

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., . . . Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications, 61*.

Gustiani, Witri. "Terjadi 1,6 Miliar Serangan Siber Sepanjang 2021, Bagaimana dengan 2022 dan Kemunculan Bjorka?" Pikiran Rakyat, 27 September 2022, diakses 28 September 2022, https://www.pikiran-rakyat.com/nasional/pr-015583077/terjadi16-miliar-serangan-siber-sepanjang-2021-bagaimanadengan-2022-dan-kemunculan-bjorka

Kementerian Pertahanan Republik Indonesia. (2014). *Pedoman Pertahanan Siber*. Jakarta: Kementerian Pertahanan Republik Indonesia.

Munir, Nudirman. 2017. *Pengantar Hukum Siber di Indonesia*. Depok: Rajawali Pers.

Naurah, N. (2022, Juni 23). *Membandingkan Indeks Keamanan Siber Indonesia dengan Negara ASEAN*. Diambil kembali dari goodstats.id: https://goodstats.id/article/indeks-keamanan-siber-indonesia-jauh-lebih-buruk-dari-malaysia-ini-grafiknya-GQkGl

Naurah, N. (2022, November 21). *Meninjau Tingkat Kasus Kebocoran Data Global, Apakah RI Aman?* Diambil kembali dari goodstats.id: https://goodstats.id/article/meninjau-tingkat-kasus-kebocoran-data-global-apakah-ri-aman-gsBoq

Naurah, N. (2023, Juni 2). *Serangan Ransomware Makin Marak, Bagaimana Kondisi Keamanan Siber di Indonesia?* Diambil kembali dari goodstats.id: https://goodstats.id/article/serangan-ransomware-makin-marak-bagaimana-kondisi-keamanan-siber-di-indonesia-f9QwO

Priyono, & Marnis. (2008). *Manajemen Sumber Daya Manusia.* Sidoarjo: Zifatama Publisher.

Rahmadiani, A., Mantovani, A. P., Hariz, S. U., Haryanto, J., & Aidad, F. F. (2019). *Strategi Keamanan Siber Indonesia: Rekomendari Rencana Aksi dan Implementasi.* Yogyakarta: Fakultas Ilmu Sosial dan Ilmu Politik Universitas Gajah Mada

Sekretariat Jenderal Komisi Yudisial Republik Indonesia. (2019). *Memperkuat Peradaban Hukum dan Ketatanegaraan Indonesia.* Jakarta: Sekretariat Jenderal Komisi Yudisial Republik Indonesia..

Sharkov, George. 2020. Assessing the Maturity of National Cybersecurity and Resilience. *Connections: The Quarterly Journal*, ISSN 1812-1098, e-ISSN 1812-2973

Sugiyono. (2019). *Metode Penelitian Kuantitatif, Kualitatif dan R&D.* Bandung: Alfabeta.

Tambun, A. P., Damayanti, N., Sari, K. Y., & Darmawan, I. (2023). Pengaruh Perkembangan Teknologi Sebagai Bentuk Perubahan Sosial dalam Pelayanan Data Kependudukan (E-Ktp) di Indonesia Upaya Penerapan Prinsip Good Governance. *JISPENDIORA: Jurnal Ilmu Sosial, Pendidikan Dan Humaniora, 2*(2), 203-218.

Wirght, C., Digitales, D., Ralby, I., & Karisma, F. (2018). *National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions.* Global Partners Digital.

Yin, R. K. (1989). *Case Study Research Design and Methods.* Washington: COSMOS Corporation.

Yusuf, A Muri. 2017. *Metode Penelitian: Kuantitatif, Kualitatif & Penelitian Gabungan*. Jakarta: Kencana.