JURNAL KETAHANAN NASIONAL
Vol. 30, No. 2, Agustus 2024, Hal 222-242
DOI:http://dx.doi.org/ 10.22146/jkn.98563
ISSN:0853-9340(Print), ISSN:2527-9688(Online)
Online sejak 28 Desember 2015 di :http://jurnal.ugm.ac.id/JKN

VOLUME 30 No. 2, Agustus 2024 Halaman 222-242

Kemunculan Ancaman Siber Teknologi 5G dan Implikasinya terhadap Ketahanan Siber Indonesia

Chiara Vincha
Program Studi Hubungan Internasional
UPN Veteran Jakarta, Indonesia
email: chiaravincha19@gmail.com

Jati Satrio
Program Studi Hubungan Internasional
UPN Veteran Jakarta, Indonesia
email: jatisatrio@upnvj.ac.id

Dikirim: 24-7-2024, Direvisi: 4-9-2024, Diterima: 31-8-2024

ABSTRACT

One of the main trends in technological development is the emergence of the 5G technology internet network. This technology offers more powerful capabilities. Because of this, the Indonesian government is also committed to implementing the technology on a massive scale. The government, through the National Cyber and Crypto Agency (BSSN), has realized that 5G technology not only creates opportunities for national development but also presents new cyber threats to national cyber security.

This research aims to analyse the implications of the emergence of 5G technology for Indonesia's cyber resilience, where the author will use the dual-use security dilemma concept. This research uses exploratory qualitative method with interview and literature study as its data collection techniques. The interviews were held with the National Cyber and Crypto Agency (BSSN) employees from the Directorate of Cyber and Crypto Security Strategy and cyber security observers. The literature study method used internet sources, news, books, journals, articles, previous studies, and other scientific papers related to the topic. The data is presented using descriptive analysis method.

From the results, the author found that the dual-use security dilemma of 5G technology has encouraged the Indonesian government to develop a National Cyber Security Strategy that can maintain cyber resilience with the emergence of new cyber threats from this technology.

Keywords: 5G Technology, Cyber Threats, Dual-Use Security Dilemma, National Cyber Security Strategy

ABSTRAK

Salah satu tren utama perkembangan teknologi adalah kemunculan jaringan internet teknologi 5G. Teknologi ini menggadang kemampuan yang lebih mumpuni. Karena itu, pemerintah Indonesia turut berkomitmen untuk dapat mengimplementasikan teknologi secara masif. Pemerintah melalui Badan Siber dan Sandi Negara (BSSN), juga telah menyadari bahwa teknologi 5G tidak hanya akan memunculkan peluang bagi pembangunan nasional, tetapi juga menghadirkan ancaman siber baru bagi keamanan siber nasional.

Tujuan penelitian ini adalah untuk menganalisis implikasi dari kemunculan teknologi 5G terhadap ketahanan siber Indonesia; di mana penulis akan menganalisis pembahasan dengan menggunakan konsep dilema keamanan

penggunaan ganda *(dual-use security dilemma)*. Penelitian ini merupakan penelitian kualitatif eksploratif dengan teknik pengumpulan data melalui wawancara dan studi pustaka. Wawancara dilakukan kepada pegawai Badan Siber dan Sandi Negara (BSSN) dari Direktorat Strategi Keamanan Siber dan Sandi dan pengamat keamanan siber. Studi pustaka dilakukan melalui sumber internet, berita, buku-buku, jurnal, artikel, kajian-kajian terdahulu, serta berbagai karya tulis ilmiah lain yang bersangkutan dengan topik yang diangkat. Data-data penelitian lantas dianalisis dan dipaparkan menggunakan metode analisis deskriptif.

Dari hasil penelitian, penulis menemukan bahwa dilema keamanan penggunaan ganda dari teknologi 5G telah mendorong pemerintah Indonesia untuk mengembangkan Strategi Keamanan Siber Nasional yang mampu menjaga ketahanan siber dengan kemunculan ancaman siber baru oleh teknologi ini.

Kata Kunci: Teknologi 5G, Ancaman Siber, Dilema Keamanan Penggunaan Ganda, Strategi Keamanan Siber Nasional

PENGANTAR

Transformasi teknologi digital menjadi salah satu sarana pendukung utama dalam peningkatan pemenuhan kebutuhan manusia. Bentuk perkembangan teknologi digital yang tidak dapat dipisahkan dari kehidupan masyarakat modern pada masa ini seperti perkembangan dalam bidang Teknologi Informasi dan Komunikasi (TIK), contohnya kemunculan dan perkembangan jaringan internet. Perkembangan terbaru dari teknologi jaringan internet dengan kehadiran teknologi 5G menjanjikan konektivitas jaringan yang lebih cepat, latensi jaringan yang lebih rendah, kapasitas jaringan yang lebih besar, hingga kemampuan transformasi digital yang lebih besar (Oughton, dkk., 2021).

Pengembangan teknologi 5G bertujuan untuk mempermudah dan meningkatkan efektivitas pemenuhan kebutuhan manusia. Kemampuan teknologi 5G dalam mentransformasikan kehidupan masyarakat menjadikan pengembangan dan penyediaannya sebagai perlombaan bagi penyedia jasa internet dan negara-negara di dunia, termasuk Indonesia. Urgensi pengembangan teknologi 5G di Indonesia tercermin dalam pesan Presiden Joko Widodo mengenai perkembangan menuju Era Industri 4.0 yang memerlukan percepatan digitalisasi agar tidak tertinggal dari negara lain. Presiden Jokowi mendorong digitalisasi, terutama dalam produksi industri manufaktur yang berorientasi pada *Internet of Things* (IoT) (Kominfo, 2021c). Pernyataan ini mendukung pengembangan teknologi 5G karena kemampuannya dalam mendukung penggunaan IoT, yang memerlukan komunikasi berkelanjutan dengan kecepatan tinggi serta analisis data dan pengambilan keputusan cepat di dunia industri (Telenor IoT, 2023).

Pemerintah Indonesia juga berkomitmen mengembangkan infrastruktur digital, sebagaimana tercermin dalam peluncuran "Peta Jalan Making Indonesia 4.0" pada tahun 2018 dan penekanan pada urgensi digitalisasi melalui Sepuluh Program Prioritas Nasional yang melibatkan pembangunan infrastruktur digital. Selain itu, Rencana Strategis Kementerian Komunikasi dan Informatika 2020-2024 mendukung penyediaan infrastruktur TIK dan rencana implementasi teknologi 5G nasional untuk mempercepat digitalisasi (Kominfo, 2021a). Inisiatif dan program tersebut menunjukkan komitmen Pemerintah Indonesia dalam pengembangan teknologi jaringan 5G (Kominfo, 2021a).

Pengembangan teknologi 5G menjadi strategi pemerintah Indonesia untuk mendukung transformasi digital (Kominfo, 2021a; Kominfo, 2021b). Pemerintah dan operator telekomunikasi di Indonesia secara aktif berusaha mengadopsi teknologi 5G untuk

mengejar ketertinggalan dan meningkatkan daya saing bangsa, serta memanfaatkan berbagai peluang yang ditawarkan oleh teknologi ini (SDPPI Kominfo, 2023). Peluang tersebut mencakup kemudahan interaksi dan komunikasi, pengembangan ilmu pengetahuan, pembangunan smart cities, inovasi industri, pertumbuhan ekonomi, serta peningkatan efisiensi dan efektivitas (Wawancara, 2024).

Selain menawarkan berbagai peluang, teknologi 5G juga berpotensi menimbulkan sejumlah tantangan, termasuk dalam pembuatan regulasi, pendanaan, pembangunan infrastruktur, hingga ancaman siber yang akan menjadi fokus pembahasan dalam artikel ini. Ancaman dapat diartikan sebagai usaha dan tindakan, baik dari dalam maupun luar negeri, yang berpotensi untuk membahayakan keselamatan bangsa, kedaulatan negara, dan keutuhan wilayah negara. Sementara itu, ancaman siber merupakan potensial insiden siber yang dapat menyebabkan hasil yang tidak diinginkan, dan bahkan mengakibatkan kerusakan (Sudarmadi & Runturambi, 2019). Adapun dampak dari peningkatan kemampuan oleh teknologi 5G juga dapat menyebabkan ancaman siber yang lebih rumit dan besar bagi keamanan siber di Indonesia. Meski teknologi 5G belum sepenuhnya beroperasi secara nasional, pemerintah melalui Badan Siber dan Sandi Negara (BSSN) telah mengakui risiko peningkatan ancaman siber terkait implementasi teknologi ini, sebagaimana tertuang dalam Rencana Strategis BSSN Tahun 2020-2024.

Penerapan ekosistem teknologi jaringan nirkabel (5G) dengan kinerja yang menjanjikan kecepatan data tinggi, pengurangan latensi, penghematan energi, kapasitas sistem yang lebih tinggi, dan konektivitas perangkat secara masif akan menguraikan masalah keamanan siber yang baru ... mengadopsi teknologi informasi dan komunikasi (TIK) 5G juga berpotensi memunculkan ancaman siber dengan penggunaan untuk kegiatan kejahatan siber (Kominfo, 2021a).

Artikel ini bertujuan untuk menganalisis permasalahan kemunculan ancaman siber dari pengembangan dan implementasi teknologi 5G di Indonesia, serta menilai ketahanan siber nasional dalam menghadapi permasalahan tersebut. Kemudian untuk menganalisis ketahanan siber, artikel ini menggunakan konsep dilema keamanan penggunaan ganda (*dual-use security dilemma*) oleh Amir Lupovici (2021). Dalam konsep ini, penggunaan teknologi 5G dipandang menimbulkan dilema keamanan karena dapat menjadi pedang bermata dua. Pada satu sisi, teknologi ini memberikan berbagai peluang bagi pembangunan nasional, tetapi pada sisi lain, teknologi ini juga memunculkan berbagai ancaman baru bagi ketahanan siber nasional. Dengan demikian, diperlukan pengembangan strategi keamanan siber yang meliputi kemunculan ancaman siber teknologi 5G untuk menjaga ketahanan siber nasional.

Artikel ini menggunakan metode kualitatif eksploratif. Metode ini berisi usaha-usaha untuk menemukan sesuatu yang relatif kurang dipelajari dan baru yang diangkat sebagai sebuah topik dalam penelitian (Swedberg, 2020). Mengingat teknologi 5G merupakan teknologi baru di Indonesia, pendekatan eksploratif tepat untuk digunakan. Data yang digunakan dalam penelitian ini terdiri dari data primer dan sekunder. Data primer diperoleh melalui teknik wawancara terhadap dua informan kunci dari pemerintah (pegawai Badan Siber dan Sandi Negara (BSSN) dari Direktorat Strategi Keamanan Siber dan Sandi) dan pengamat keamanan siber. Wawancara dilakukan pada bulan Februari 2024 serta bertujuan untuk

memperoleh informasi mengenai teknologi 5G dan pengaruh dari kehadiran teknologi tersebut di Indonesia sesuai dengan pedoman wawancara yang telah penulis susun. Data sekunder dikumpulkan melalui studi pustaka, yang mencakup sumber-sumber internet, berita, buku, jurnal, artikel, kajian terdahulu, serta berbagai karya tulis ilmiah lainnya yang relevan dengan topik penelitian ini. Data-data terkait lantas dianalisis menggunakan metode analisis deskriptif. Metode ini dilakukan dengan mendeskripsikan atau memberikan gambaran terhadap objek penelitian melalui data yang telah terkumpul sebagaimana adanya (Miles & Huberman, 1992).

PEMBAHASAN

Dinamika Implementasi Teknologi 5G di Indonesia

Dalam beberapa tahun terakhir, Indonesia telah memasuki era baru dalam kemajuan teknologi informasi. Hal ini terlihat dari berbagai upaya pemerintah dalam mengimplementasikan teknologi jaringan terbaru, yaitu teknologi Generasi Kelima atau 5G. Upaya-upaya ini mencerminkan komitmen pemerintah untuk mempercepat transformasi digital guna mencapai industri 4.0, di mana teknologi 5G diyakini dapat mendukung transformasi ini dengan lebih baik. Teknologi 5G mampu memberikan layanan yang lebih andal dalam proses pertukaran informasi dan komunikasi (Kominfo, 2021b).

Pengembangan teknologi 5G dimulai pada tahun 2012 oleh International Telecommunication Union (ITU) dan dilaksanakan bersama organisasi standarisasi seperti 3rd Generation Partnership Project (3GPP) dan Institute of Electrical and Electronics Engineers (IEEE). Implementasi jaringan 5G secara komersial mulai muncul di beberapa negara, termasuk Amerika Serikat, Tiongkok, Korea Selatan, Jepang, dan Inggris pada tahun 2019 (IME FTUI, 2023). Di Indonesia, perkembangan teknologi 5G diatur melalui Peraturan Menteri Komunikasi dan Informatika Nomor 2 Tahun 2021 tentang Rencana Strategis Kementerian Komunikasi dan Informatika Tahun 2020-2024. Peraturan ini menyebutkan bahwa lembaga pemerintah yang bertanggung jawab atas pengembangan teknologi 5G adalah Direktorat Jenderal Penyelenggaraan Pos dan Informatika dari Kementerian Komunikasi dan Informatika (Kominfo).

Gambar 1
Target Implementasi Teknologi 5G Pemerintah Indonesia

Target	*2021*	*2022*	*2023*	*2024*
Persiapan Implementasi 5G Nasional	*Roadmap* 5G Nasional	Regulasi Kebijakan Percepatan 5G	–	–
Jumlah lokasi yang terkoneksi 5G pada tahap awal implementasi	–	–	11 tempat, meliputi 6 ibu kota provinsi di Pulau Jawa dan 5 destinasi wisata super prioritas.	2 tempat, satu pada IKN dan satu pada kawasan industri manufaktur.
Infrastruktur 5G di Ibu Kota Negara (IKN)	Desain infrastruktur dan jaringan Telekomunikasi 5G untuk IKN.	*Memorandum of Understanding* antar-pemangku kepentingan dalam membangun infrastruktur dan jaringan telekomunikasi 5G di IKN.	75% Pembangunan jaringan telekomunikasi 5G di IKN.	100% Jaringan telekomunikasi 5G terbangun.

Sumber: Wawancara, 2024.

Gambar 1 menunjukkan linimasa pengembangan teknologi 5G di Indonesia. Secara komersial, teknologi 5G telah hadir di Indonesia sejak Mei 2021, yang diresmikan oleh Menteri Komunikasi dan Informatika saat itu, Johnny Gerard Plate. Peluncuran ini ditandai dengan penerbitan Surat Keterangan Laik Operasi (SKLO) kepada PT Telkomsel sebagai penyedia teknologi 5G pertama di Indonesia (Kominfo, 2021b).

Pemerintah Indonesia secara aktif mendorong implementasi teknologi 5G melalui beberapa strategi, yaitu pengembangan infrastruktur, kerja sama pengembangan teknologi, dan penerbitan peraturan. Strategi pertama, pengembangan infrastruktur, mencakup pembangunan dan pemerataan infrastruktur digital. Pemerintah mendorong pembangunan infrastruktur digital untuk menopang teknologi 5G, dengan pembangunan paling ambisius terlihat di Ibu Kota Nusantara (IKN) yang dirancang sebagai kota pintar berbasis teknologi 5G (Iradat, 2023). Selain itu, pemerintah berupaya memastikan pemerataan infrastruktur digital hingga ke pelosok dan desa di seluruh Indonesia.

Optimalisasi pemanfaatan sumber daya pendukung, seperti spektrum frekuensi radio, juga menjadi fokus pemerintah. Melalui Kominfo, pemerintah mendorong pelayanan 5G yang optimal dan sesuai dengan standar internasional, termasuk melalui pelelangan pita frekuensi radio, seperti pelelangan pita frekuensi 2,3 GHz pada awal 2021 yang menjadi basis jaringan teknologi 5G (Kominfo, 2021b). Selain itu, pemerintah meluncurkan program-program pendukung, seperti Program Analog Switch Off (ASO) pada tahun 2023, yang mempersiapkan spektrum frekuensi yang bersih untuk kebutuhan teknologi 5G (CNN Indonesia, 2022; Kominfo, 2023).

Pemerintah mendorong kerja sama pengembangan teknologi 5G dengan penyelenggara telekomunikasi, baik dari dalam maupun luar negeri, sebagai bagian dari strategi pengembangan teknologi. Contohnya, pemerintah telah mendukung lebih dari 12 kali uji coba teknologi oleh Telkomsel, termasuk uji coba pertama pada tahun 2017 di Jakarta melalui kolaborasi dengan Huawei, serta penyediaan pengalaman 5G pada Asian Games 2018 melalui Telkomsel 5G Experience Center di Stadion Utama Gelora Bung Karno. Pada tahun 2023, Telkomsel bekerja sama dengan Ericsson dan Qualcomm untuk menginisiasi Akses Nirkabel Tetap 5G menggunakan spektrum frekuensi 3,5 GHz dan 26 GHz. Beberapa uji coba teknologi 5G juga dilakukan bersama penyelenggara telekomunikasi luar negeri seperti Huawei dari Tiongkok, Ericsson dari Swedia, dan Qualcomm dari Amerika Serikat (Kominfo, 2021b; Nistanto, 2021).

Strategi terakhir pemerintah adalah pembuatan kebijakan terkait teknologi 5G, termasuk pemberian izin operasional. Pemerintah membuat kebijakan dengan memperhatikan sinergi antara aspek regulasi, spektrum frekuensi radio, model bisnis, infrastruktur, serta perangkat, ekosistem, dan talenta digital untuk menopang implementasi teknologi 5G secara maksimal (Kominfo, 2021d). Selain itu, pemerintah memberikan izin operasional agar penyedia jaringan dapat menghadirkan teknologi 5G di Indonesia. Contohnya, izin operasional jaringan 5G diberikan oleh Kominfo kepada Telkomsel, Indosat Ooredoo, XL Axiata, dan Smartfren pada tahun 2020, memungkinkan operator-operator seluler tersebut meluncurkan layanan di kota-kota seperti Jakarta, Surabaya, Makassar, Bandung, Denpasar, Balikpapan, Solo, Medan, dan Batam (Kominfo, 2021b).

Konsep Dilema Keamanan Penggunaan Ganda (Dual-Use Security Dilemma)

Amir Lupovici (2021) mengembangkan konsep dilema keamanan penggunaan ganda *(dual-use security dilemma)* yang menggabungkan dua konsep: penggunaan ganda *(dual-use)* dan dilema keamanan *(security dilemma)*. Penggunaan ganda merujuk pada penggunaan barang-barang yang memiliki fungsi ganda, baik untuk kebutuhan militer maupun sipil (Atlas & Dando, 2006; Lin, 2016). Barang-barang ini dapat mencakup penelitian, artefak, dan teknologi (Forge, 2010). Konsep ini mengasumsikan bahwa barang-barang militer dapat diciptakan melalui industri komersial, dan sebaliknya, barang-barang militer dapat digunakan untuk kebutuhan komersial atau sipil (Afshar & Khorasani, 2020). Dengan demikian, penggunaan ganda dari suatu teknologi berarti teknologi tersebut memiliki kemampuan untuk ditransformasikan dari fungsi asli untuk keperluan militer maupun sipil.

Sementara itu, dilema keamanan mengacu pada situasi di mana tindakan sekuritisasi oleh satu aktor untuk mempersiapkan diri menghadapi ancaman dari aktor lain justru menimbulkan ketidakamanan. Tindakan sekuritisasi ini didasarkan pada pandangan bahwa ancaman dari suatu aktor melegitimasi tindakan luar biasa untuk menanggapi atau memenangkan tantangan dari aktor lain. Namun, tindakan sekuritisasi ini juga dapat memprovokasi aktor lain untuk melakukan tindakan sekuritisasi serupa, yang kemudian memicu spiral tindakan balas-membalas, sehingga menimbulkan dilema keamanan (Lupovici, 2021). Konsep dilema keamanan penggunaan ganda mengacu pada fenomena penggunaan ganda dari suatu barang yang memunculkan dan meningkatkan dilema keamanan (Lupovici, 2021). Ketika diterapkan dalam teknologi, Konsep ini dapat diartikan sebagai sebuah kondisi dilema keamanan yang terjadi karena suatu aktor tidak dapat memastikan penggunaan ganda teknologi oleh aktor lain, entah itu bagi tujuan defensif atau ofensif; atau bagi tujuan sipil atau militer.

Lupovici (2021) menggambarkan ketidakpastian penggunaan teknologi oleh suatu aktor sebagai faktor yang dapat memperluas dilema keamanan bagi aktor lain. Kekhawatiran ini berubah seiring perkembangan teknologi, dengan contoh konkret termasuk teknologi nuklir dan teknologi robot.

Pertama, teknologi nuklir. Sebelum dan selama Perang Dunia II, penelitian tentang atom dan nuklir berfokus pada tujuan militer, terutama pengembangan senjata, seperti yang terlihat dalam Proyek Manhattan oleh Amerika Serikat, yang menghasilkan bom atom dan mengakhiri Perang Dunia II dengan peledakan di Hiroshima dan Nagasaki pada tahun 1945 (Khan Academy, 2018; Etania & Indriawati, 2023). Pasca Perang Dunia II, penelitian beralih ke penerapan teknologi nuklir yang damai, seperti pembangkit listrik tenaga nuklir dan berbagai aplikasi sipil lainnya, termasuk ilmiah, medis, dan industri (None, 1985). Namun, program teknologi nuklir masih menciptakan dilema keamanan karena kerahasiaan dan ketidakpastian yang menyertainya, baik karena keterbatasan pengumpulan intelijen dan pengawasan, maupun kemungkinan penggunaan penipuan atau disinformasi mengenai kemampuan teknologi nuklir suatu negara (Kahan, 1975; Douglass, 1981).

Kedua, teknologi robot. Robot modern pertama kali diciptakan oleh George Devol

pada awal 1950-an dengan "Unimate" atau "Universal Automation" untuk industri. Pada tahun 1958, Charles Rosen dari Stanford Research Institute memimpin pengembangan robot "Shakey," yang lebih canggih dan dirancang untuk aplikasi industri khusus (Pa, n.d.). Robot awalnya diciptakan untuk kebutuhan industri atau penggunaan sipil, namun kini mencakup ranah militer dan peperangan. Misalnya, Kendaraan Udara Tak Berawak (UAV) "Predator" milik Angkatan Udara Amerika Serikat yang memiliki tingkat otonomi dan dapat mengambil keputusan sendiri (Afshar & Khorasani, 2020). Penggunaan ganda robot ini menciptakan dilema keamanan. Di satu sisi, robot memiliki kelebihan praktis dibandingkan tentara, seperti ketahanan terhadap kelelahan dan risiko kematian di medan perang. Namun, di sisi lain, penggunaan robot dalam peperangan menimbulkan kekhawatiran tentang kemungkinan malfungsi atau peretasan oleh aktor lawan atau penjahat siber, yang dapat menimbulkan bahaya bagi militer dan sipil (Afshar & Khorasani, 2020).

Terakhir, teknologi di ruang siber telah menjadi kebutuhan penting untuk kelancaran sistem informasi dan komunikasi global saat ini (Riebe & Reuter, 2019). Melalui perkembangan teknologi di ruang siber menggunakan sistem komputer dan internet, kemampuan seseorang dalam membagikan dan memperoleh informasi menjadi semakin mudah (Davies, 2021). Namun, terdapat ancaman siber yang menghantui setiap penggunaan teknologi terkait ruang siber. Kompleksitas yang muncul dalam ruang siber memungkinkan aktor non-negara terlibat dalam proses sekuritisasi teknologi tersebut, memunculkan risiko penyalahgunaan oleh aktor seperti penjahat dan teroris. Dengan kata lain, kemudahan ini telah memunculkan ancaman baru di ranah siber, menimbulkan dilema keamanan bagi pengguna teknologi itu sendiri (Afshar & Khorasani, 2020).

Berdasarkan penjelasan, dapat disimpulkan bahwa konsep dilema keamanan penggunaan ganda dapat menjelaskan dilema keamanan yang timbul dari penggunaan ganda teknologi, termasuk teknologi 5G. Penggunaan teknologi 5G tidak hanya menawarkan peluang, tetapi juga berpotensi memunculkan ancaman siber. Implementasi teknologi 5G yang masif, seperti yang direncanakan oleh pemerintah Indonesia, dapat menimbulkan kekhawatiran baru bagi keamanan nasional, terutama dalam hal keamanan siber (Kominfo, 2021). Oleh karena itu, penting bagi pemerintah dan penyedia layanan untuk mempertimbangkan potensi risiko ini dalam upaya menjaga keamanan siber nasional.

Teknologi 5G Sebagai Dilema Keamanan Penggunaan Ganda (Dual Use Security Dilemma)

Perkembangan teknologi berlangsung dengan cepat dan dinamis. Sebagai hasilnya, kekhawatiran aktor terhadap ketidakpastian yang terkait dengan penggunaan ganda teknologi berkembang seiring waktu. Salah satu aspek teknologi yang fundamental dalam kehidupan saat ini adalah teknologi informasi dan komunikasi, dengan teknologi 5G menjadi perkembangan terbaru dalam jaringan internet. Seperti yang telah dibahas, berbagai kelebihan teknologi 5G telah mendorong negara-negara untuk bersaing dalam mengadopsi teknologi ini. Namun demikian, penggunaan teknologi 5G oleh suatu aktor dapat digunakan baik untuk tujuan sipil maupun militer, serta untuk kepentingan defensif atau ofensif oleh aktor lain. Dengan demikian, teknologi

ini memberikan peluang baru sekaligus menimbulkan ancaman siber bagi pengguna, termasuk bagi Indonesia yang berkomitmen untuk mengadopsi teknologi 5G secara luas.

Selanjutnya, beberapa aspek terkait dengan teknologi 5G yang dapat memberikan peluang dan menimbulkan ancaman siber tergantung pada penggunaannya seperti: Pertama, teknologi 5G memfasilitasi interaksi dan komunikasi yang lebih cepat, memungkinkan masyarakat untuk menggunakan media sosial dengan lebih efisien tanpa batasan waktu dan tempat. Namun, kecepatan ini juga memberikan kesempatan bagi penjahat siber untuk melancarkan serangan DDoS terhadap platform media sosial, mengganggu fungsi interaksi dan komunikasi. Kedua, teknologi 5G mendorong inovasi industri dengan mendukung pengembangan *Internet of Things* (IoT), yang memungkinkan operasi industri menjadi lebih otomatis dan produktif. Namun, keberadaan teknologi ini juga meningkatkan risiko terhadap serangan siber, seperti serangan *malware* yang dapat mempengaruhi keamanan data pribadi yang disimpan oleh industri (IBM, 2022).

Akhirnya, penggunaan teknologi 5G sebagai pedang bermata dua ini berhubungan erat dengan konsep dilema keamanan penggunaan ganda oleh Amir Lupovici (2021). Pada satu sisi, penggunaan teknologi ini mampu memberikan berbagai peluang bagi pembangunan nasional. Tetapi pada sisi lain, penggunaan teknologi ini juga mampu memunculkan berbagai ancaman bagi baru keamanan siber nasional.

Dilema Keamanan Penggunaan Ganda (Dual-Use Security Dilemma) Teknologi 5G dengan Kondisi Keamanan Siber Indonesia

Pengimplementasian teknologi 5G di Indonesia, yang direncanakan untuk diadopsi secara masif, menciptakan sebuah dilema keamanan yang terlihat dari dua aspek. Aspek pertama berhubungan dengan ancaman yang muncul dari teknologi 5G dan keamanan siber. Aspek kedua terkait perhatian pemerintah Indonesia terhadap keamanan siber.

Dalam melihat bagaimana ancaman teknologi 5G mempengaruhi keamanan siber, maka dinamika yang terjadi di level internasional dapat menjadi contoh. Salah satu perkembangan penting dalam konsep keamanan adalah keamanan siber, yang mencakup ancaman non-militer seperti serangan siber. Dengan berkembangnya teknologi 5G, isu keamanan siber menjadi perhatian serius. Sebagai contoh, Amerika Serikat menganggap pengadaan teknologi 5G sebagai risiko. Perangkat 5G dari Huawei, penyedia teknologi 5G global, dianggap memungkinkan pemerintah Cina mengumpulkan informasi sensitif (Frieden, 2020 dalam Lupovici, 2021). Akibatnya, Amerika Serikat mendeklarasikan "darurat nasional" karena potensi eksploitasi kerentanan teknologi 5G oleh Cina yang dianggap sebagai ancaman terhadap keamanan nasional (Gedung Putih, 2019). Amerika Serikat melarang penggunaan teknologi 5G dari Huawei dan menerapkan sanksi terhadap perusahaan tersebut karena pelanggaran hak kekayaan intelektual. Tindakan ini memicu Cina untuk meningkatkan ketahanan, otonomi, dan kemandirian, sehingga Huawei mencari pemasok alternatif dan mengembangkan teknologi pengganti. Cina juga mengancam sanksi terhadap perusahaan yang memboikot produk Cina, menyebabkan Amerika Serikat menghadapi ancaman ekonomi karena kehilangan potensi pendapatan (Creemers, 2020 dalam Lupovici, 2021). Respon saling balas antara Amerika Serikat dan Cina

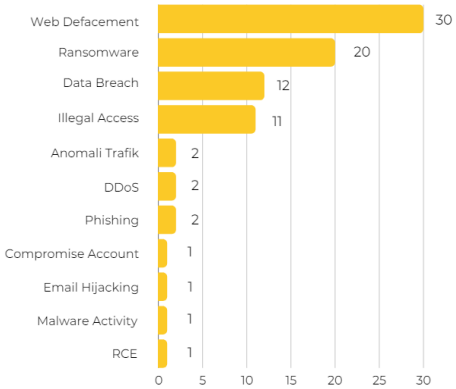
ini menciptakan dilema keamanan yang berkelanjutan.

Dalam konteks Indonesia, implementasi teknologi 5G berada di bawah tanggung jawab Direktorat Jenderal Penyelenggaraan Pos dan Informatika, Kementerian Komunikasi dan Informatika (Kominfo). Penyedia teknologi 5G di Indonesia, seperti Telkomsel, bekerja sama dengan pihak asing, termasuk Huawei. Kerja sama ini dapat menimbulkan dilema keamanan terkait keamanan siber nasional. Di satu sisi, kekhawatiran tentang risiko pengumpulan informasi sensitif oleh Huawei adalah wajar, mengingat hubungan perusahaan tersebut dengan pemerintah Cina (Frieden, 2020 dalam Lupovici, 2021; Savitri, 2021). Di sisi lain, menolak Huawei sebagai pemasok sulit dilakukan karena keterbatasan perusahaan nasional dan keterlibatan Huawei yang sudah mendalam dalam pengimplementasian teknologi 5G di Indonesia.

Konsep keamanan siber mendapat perhatian serius dari pemerintah Indonesia, yang mengakui bahwa perkembangan teknologi tidak hanya membawa peluang tetapi juga tantangan baru berupa ancaman siber. Buku Putih Pertahanan Indonesia Tahun 2015 mencatat bahwa teknologi informasi dan komunikasi dapat digunakan untuk kesejahteraan, namun juga memiliki potensi dampak keamanan (Buku Putih, 2015). Terkait dampak keamanan dari serangan siber, National Cyber Security Index (NCSI) 2023 menempatkan Indonesia pada peringkat ke-49 dari 176 Negara (Anggana, 2024). Namun demikian, jika diperingkatkan dengan 20 negara dengan ekonomi terbesar di dunia, maka Indonesia menduduki peringkat terakhir pada tahun 2022 (MIT Technology Review, 2023)

Apabila kita melihat insiden serangan siber yang terjadi di Indonesia, maka Gambar 2. memperlihatkan tingkatan jenis serangan siber yang paling sering terjadi di Indonesia pada tahun 2023, dan juga sektor-sektor yang paling sering terdampak dari serangan. Dari Gambar 2., dapat dilihat beberapa jenis serangan yang paling sering terjadi adalah *web defacement, ransomware* (salah satu jenis *malware*), dan kebocoran data *(data breach)*. Sementara itu, sektor yang paling sering terdampak dari serangan terutama adalah sektor pemerintahan. Dari sini, hasil klasifikasi masih sangat signifikan dengan kondisi

Gambar 2
Klasifikasi Serangan Siber dan Sektor Terdampak di Indonesia



Sektor	Jumlah
Adm. Pemerintahan	59
ESDM	6
Kesehatan	5
Keuangan	5
Lainnya	4
Transportasi	3
TIK	1

Sumber: Lanskap Keamanan Siber Indonesia BSSN, 2023a.

kerentanan keamanan siber di Indonesia saat ini. Hal ini karena, pada pertengahan 2024 saja, pemerintah Indonesia telah mengalami serangan siber yang mengkhawatirkan. Di mana Pusat Data Nasional Sementara (PDSN) sebagai bagian dari program besar pemerintah Indonesia, Pusat Data Nasional (PDN), telah mengalami serangan *ransomware*. Serangan *ransomware* menggunakan Lock Bit 3.0 varian Brain Cipher, dan diketahui telah dimulai pada 17 Juni 2024. Lebih lanjut, serangan *ransomware* dilaporkan telah menyebabkan berbagai gangguan pada layanan pemerintah pusat dan daerah; serta telah mengakibatkan data-data PDN yang terenkripsi atau terkunci dan tak dapat dipulihkan (Hardiansyah, 2024).

Hal yang menjadi perhatian adalah mengenai ketidakmampuan pemerintah Indonesia dalam menangani serangan *ransomware* ini. Terlepas dari kerja sama penanganan yang dilakukan bersama antara BSSN, Kominfo, dan Kepolisian, pemerintah Indonesia telah gagal untuk memulihkan kembali data-data PDN yang terdampak (Sutrisna & Prabowo, 2024). Ketidakmampuan pemerintah dalam menangani serangan *ransomware* ini menyoroti kekurangan sistem keamanan siber nasional, seperti keterbatasan sumber daya manusia, infrastruktur yang ketinggalan, dan penanganan reaktif terhadap insiden keamanan siber (Savitri, 2024).

Implementasi teknologi 5G dapat meningkatkan kesejahteraan dan taraf hidup, namun juga membawa risiko ancaman siber (BSSN, 2022). Contoh serangan siber di negara-negara tetangga menunjukkan bahwa teknologi 5G dapat meningkatkan risiko ancaman siber, seperti peningkatan serangan DDoS dan *malware* di Malaysia (Law, 2023; Blackman, 2023; Raj, 2023). Mengingat kekurangan sistem keamanan siber nasional Indonesia, implementasi teknologi 5G sebagai perkembangan TIK dapat memunculkan dilema keamanan baru. Oleh karena itu, diperlukan strategi keamanan siber nasional baru yang mencakup kebutuhan dalam menjaga ketahanan siber dengan kemunculan ancaman siber dari teknologi 5G di Indonesia (Chotimah, Iswardhana, dan Pratiwi, 2019).

Ketahanan Siber Indonesia dalam Menghadapi Dilema Keamanan Penggunaan Ganda dari Kehadiran Teknologi 5G

Ketahanan nasional merupakan kondisi dinamis suatu bangsa dalam membentuk kekuatan nasional sehingga mampu menghadapi ancaman, tantangan, hambatan, serta gangguan (Suryohadiprojo, 1997). Sementara ketahanan nasional untuk menghadapi ancaman dari ranah siber lantas dapat dikatakan sebagai ketahanan siber nasional. Pemerintah Indonesia turut bertanggung jawab untuk menjaga ketahanan siber nasional dari ancaman siber. Ketika membahas mengenai tanggung jawab ketahanan siber, salah satu aspek penting yang terdapat di dalamnya adalah tanggung jawab keamanan siber nasional itu sendiri (Suryohadiprojo, 1997). Peraturan Presiden Nomor 53 Tahun 2017 dan perubahan Nomor 133 Tahun 2017 telah menetapkan Badan Siber dan Sandi Negara (BSSN) sebagai titik fokus dalam keamanan siber nasional. BSSN memiliki peran utama untuk mempersiapkan, mengamankan, dan menjaga keamanan siber di Indonesia secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan memantapkan seluruh unsur yang terkait dengan keamanan siber nasional. Adapun demikian, permasalahan ketahanan siber dalam ancaman siber dari kehadiran teknologi

5G di Indonesia juga akan menjadi tanggung jawab BSSN.

BSSN melandasi peranan penyelenggaraan keamanan siber nasional pada Peraturan Presiden Nomor 47 Tahun 2023. Peraturan ini menegaskan pentingnya mempersiapkan strategi keamanan siber untuk mewujudkan keamanan siber nasional (Perpres Nomor 47 Tahun 2023). Strategi merupakan alat yang disusun oleh suatu organisasi untuk mencapai tujuan atau keunggulan bersaing dengan melihat faktor eksternal dan internal. Identifikasi faktor internal yang dilakukan dalam pembentukan strategi yaitu dengan merumuskan keunggulan dan kelemahan yang berasal dari dalam organisasi. Sementara itu, identifikasi faktor eksternal yaitu dengan merumuskan peluang dan ancaman yang berasal dari luar organisasi (Sudarmadi & Runturambi, 2019).

Strategi nasional BSSN disusun selaras dengan nilai dasar internal dalam kehidupan berbangsa dan bernegara Indonesia: Kedaulatan, Kemandirian, Keamanan, Kebersamaan, dan Adaptif. Secara khusus, pembentukan Strategi Keamanan Siber Nasional Indonesia oleh BSSN mengacu pada takaran internasional berupa 5 (lima) Pilar the Global Cybersecurity Index (GCI) 2017, di mana survei ini dirilis oleh International Telecommunication Union (ITU) dan ditujukan untuk mengukur komitmen negara anggota terhadap peningkatan kesadaran dan membangun kapasitas keamanan siber pada level nasional, regional maupun internasional. Strategi keamanan siber sesuai 5 (lima) pilar GCI 2017 sebagai berikut:

Tabel 1 menggambarkan 5 (lima) pilar aspek yang terdapat dalam Strategi Keamanan Siber Nasional BSSN. Kelima aspek tersebut adalah aspek hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama (Sudarmadi & Runturambi,

Tabel 1
Aspek dan Indikator dari Strategi Keamanan Siber Nasional BSSN

No	Aspek	Indikator
1.	Aspek Hukum	Keberadaan UU Kejahatan Siber; UU Keamanan Siber; dan Penyelenggaraan pelatihan keamanan siber bagi aktor hukum.
2.	Aspek Teknis	Keberadaan Cyber Emergency Response Team (CERT) baik secara nasional, pemerintah, dan sektoral; Standar keamanan siber bagi organisasi; Standar dan sertifikasi bagi profesional di bidang keamanan siber; dan Perlindungan dalam jaringan.
3.	Aspek Organisasi	Keberadaan strategi keamanan siber nasional; Organisasi yang bertanggung jawab dalam bidang keamanan siber; dan Matrik pengukuran perkembangan keamanan siber.
4.	Aspek Pengembangan Kapasitas	Keberadaan organisasi standarisasi; Dokumen praktik terbaik sehubungan dengan keamanan siber; Program penelitian dan pengembangan; Kampanye kesadaran publik; Kursus pelatihan profesional; Program pendidikan dan kurikulum akademik skala nasional dalam keamanan siber; Mekanisme insentif yang diberikan dalam bidang keamanan siber; dan Industri keamanan siber dalam negeri.
5.	Aspek Kerja Sama	Kerja sama bilateral; Kerja sama multilateral; Partisipasi pada forum internasional; Kerja sama pemerintah dengan swasta; dan Kerja sama antar instansi pemerintah.

Sumber: Penulis, 2024.

2019). Sehubungan dengan ini, penulis akan menganalisis ketahanan siber Indonesia dalam menghadapi dilema keamanan penggunaan ganda teknologi 5G melalui indikator aspek Strategi Keamanan Siber Nasional BSSN di atas. Analisis ini akan melihat berbagai bentuk pelaksanaan aspek yang telah dilakukan oleh pemerintah Indonesia, serta dilanjutkan dengan pemberian rekomendasi langkah-langkah spesifik yang dapat diadopsi dalam menghadapi ancaman siber dengan kehadiran teknologi 5G.

Pelaksanaan Aspek Hukum dalam Teknologi 5G

Pada Aspek Hukum, pemerintah Indonesia memiliki daftar regulasi terkait teknologi informasi dan teknologi telekomunikasi. Sehubungan dengan teknologi 5G, keberadaan undang-undang terkait kejahatan dan keamanan siber dilakukan oleh pemerintah Indonesia melalui keberadaan paling tidak 8 (delapan) aturan terdahulu yang secara umum mengakomodasi implementasi teknologi ini. Beberapa peraturan sebagai berikut: UU No. 36 Tahun 1999 tentang Telekomunikasi, UU No. 11 Tahun 2008 sebagaimana telah diubah oleh UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), UU No. 11 Tahun 2020 tentang Cipta Kerja, PP No. 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi, PP No. 53 Tahun 2000 tentang Penggunaan Spektrum Frekuensi Radio dan Orbit Satelit, PP No. 46 Tahun 2021 tentang Pos, Telekomunikasi, dan Penyiaran (PP Postelsiar), UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), dan Peraturan Menteri Kominfo sebagai aturan pelaksanaan.

Sementara itu, penyelenggaraan pelatihan keamanan siber dilakukan oleh pemerintah Indonesia secara rutin dan berkala, yang mana pelatihan sekarang juga meliputi teknologi 5G. Dalam hal ini, BSSN melakukan pelatihan pengembangan kapasitas dalam rangka mengatasi ancaman siber dengan kehadiran teknologi 5G. Pelatihan sendiri kerap kali dilaksanakan bersama dengan pemangku kepentingan nasional, dan bahkan internasional. Sebagai contoh, BSSN mengadakan pelatihan keamanan siber bertajuk *"5G Security Training and NESAS Best Practices Discussion"* bersama dengan Perusahaan Huawei di Huawei ASEAN Academy Engineering Institute pada tahun 2021 (BSSN, 2021b).

Pelaksanaan Aspek Teknis dalam Teknologi 5G

Aspek Teknis diukur berdasarkan keberadaan institusi teknis dan kerangka kerja yang berhubungan dengan keamanan siber. Dalam kaitannya dengan teknologi 5G, keberadaan CERT dilakukan oleh pemerintah Indonesia melalui Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 2 tahun 2021 mengenai Rencana Strategis Kementerian Komunikasi dengan menetapkan Badan Siber dan Sandi Negara (BSSN) sebagai lembaga CERT untuk turut bertanggung jawab dalam menjaga keamanan siber nasional terkait dengan kehadiran teknologi 5G (Wawancara, 2024). Dalam hal ini, BSSN berperan aktif dalam mengatasi ancaman siber dan menjaga keamanan siber nasional di dalam implementasi teknologi 5G di Indonesia.

Pemerintah Indonesia mengatur standar keamanan siber melalui penguatan tiga pilar arsitektur keamanan siber. Ketiga pilar arsitektur keamanan siber tersebut adalah proses *(process)* (berupa pengembangan

kebijakan, mekanisme, tata kelola, regulasi), sumber daya manusia *(people)* (berupa pemberian literasi, pelatihan, seminar, atau bentuk peningkatan kapasitas lain), dan teknologi *(technology)* (berupa pelaksanaan riset bersama, penumbuhkembangan industri, dan lain-lain) untuk menghadapi peningkatan ancaman siber. Ketiga pilar ini didorong melalui penetapan standar seperti identifikasi, analisa, maupun koordinasi standar keamanan siber sesuai pada instansi yang terkait.

Pemerintah Indonesia telah melakukan beberapa upaya terkait pembentukan standar keamanan siber. Pemerintah Indonesia membentuk Matrik Rencana Aksi Nasional Keamanan Siber (RAN KS) sebagai turunan dari Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (SKSN dan MKS), di mana matrik ini menjadi pedoman bagi penetapan standar keamanan siber di Indonesia. Selanjutnya, pemerintah juga mengeluarkan Peraturan Direktur Jenderal BSSN terkait Standar Teknis Perangkat Telekomunikasi 5G. Terakhir, pemerintah juga menetapkan Peta Okupasi Nasional Bidang Keamanan Siber (2019) oleh Kepala BSSN melalui Keputusan Kepala BSSN Nomor 563.1 Tahun 2016. Peta ini berfokus pada teknologi 5G serta dilengkapi dengan deskripsi, tugas, dan ketersediaan standar nasional (SKKNI/ SKKI/SKK) dalam pengembangan kapasitas keamanan siber dengan kehadiran teknologi 5G (Wawancara, 2024).

Pemerintah Indonesia menetapkan standar dan sertifikasi bagi profesional di bidang keamanan siber melalui pembentukan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Bidang Komunikasi dan Informasi sebagai tindak lanjut Peta Okupasi Nasional Bidang Keamanan Siber (2019) sebagai berikut: SKKNI *Security Operation Center* (2020); SKKNI Bidang Audit Keamanan Informasi; SKKNI Bidang Uji Keamanan Siber; SKKNI Bidang Kriptografi (2022); SKKNI Bidang *Secure SDLC* (2023); SKKNI Bidang *Malware Analyst* (2024); dan berbagai SKKNI lain terkait Keamanan Siber. Di mana dengan berbagai standar ini, pemerintah Indonesia mengharapkan peningkatan kemampuan keamanan siber untuk mendukung perkembangan teknologi 5G, sekaligus untuk mempersiapkan diri dari ancaman siber karena perkembangan itu sendiri (BSSN, 2021a; BSSN, 2023b).

Indikator terakhir terkait aspek teknis berkaitan dengan perlindungan terhadap kejahatan dan keamanan siber bagi pengguna, dan karena itu berhubungan erat dengan Aspek Hukum. Dalam hal ini, berbagai peraturan pendukung terkait Kejahatan dan Keamanan Siber lantas menjadi landasan untuk menjaga keamanan siber nasional, termasuk dengan kehadiran teknologi 5G.

Pelaksanaan Aspek Organisasi dalam Teknologi 5G

Aspek Organisasi bagi keamanan siber di Indonesia diukur berdasarkan keberadaan lembaga koordinasi kebijakan dan strategi untuk pengembangan keamanan siber di tingkat nasional. Indikator pertama dilakukan oleh pemerintah Indonesia melalui pengembangan strategi keamanan siber nasional baru yang membahas aspek implementasi teknologi 5G sendiri. Strategi ini ditetapkan dalam Renstra Kemen Kominfo Tahun 2020-2024. Renstra terdiri dari penyusunan *road map,* penyediaan alokasi pita frekuensi, penyusun kebijakan dan regulasi penyelenggaraan, pengembangan ekosistem dan perangkat penunjang, serta fasilitasi dan pendampingan penggelaran

infrastruktur teknologi 5G. Kemudian daripada itu, aspek keamanan siber dari teknologi ini juga mulai mendapat perhatian. Dalam hal ini, BSSN mengakui bahwa implementasi teknologi 5G juga berpotensi memunculkan ancaman siber seperti tertulis pada Rencana Strategis BSSN Tahun 2020-2024.

Indikator kedua dilakukan oleh pemerintah Indonesia dengan kembali membahas Peraturan Pemerintah (PP) Nomor 2 tahun 2021 mengenai Rencana Strategis Kementerian Komunikasi menetapkan yang BSSN untuk turut bertanggung jawab dalam menjaga keamanan siber nasional terkait dengan kehadiran teknologi 5G.

Indikator ketiga dilakukan oleh pemerintah Indonesia melalui Matrik Rencana Aksi Nasional Keamanan Siber (RAN KS) BSSN sebagai turunan dari Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (SKSN dan MKS) (BSSN, 2023b). Matrik ini menjadi pedoman dalam penyusunan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) di bidang Keamanan Siber dan Sandi, Standar Nasional Indonesia (SNI) di bidang Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi, dan berbagai skema penilaian kesesuaian teknologi keamanan siber dan sandi di Indonesia. Dalam hal ini, walau Matrik RAN KS tidak terkait secara spesifik membahas keamanan siber teknologi 5G, matrik ini mendorong pemenuhan 3 (tiga) Pilar Arsitektur yang dapat menjadi landasan untuk menghadapi ancaman siber dari implementasi teknologi tersebut (Olsson, 2021). Ketiga pilar sebagai berikut: Proses *(process)*, Sumber Daya Manusia *(people)*, dan Teknologi *(technology)*. Selain daripada itu, BSSN juga mengambil langkah lanjutan terkait melalui penetapan Peta Okupasi Nasional Bidang Keamanan Siber (2019). Peta okupasi dibentuk dengan fokus implementasi, penggunaan, serta ancaman siber yang muncul dari teknologi 5G. Peta okupasi lantas ditindaklanjuti dengan deskripsi, tugas, dan ketersediaan standar (seperti SKKNI/SKKI/SKK) untuk dapat dimanfaatkan oleh pemangku kepentingan untuk pengembangan kapasitas (seperti penyediaan SDM, peningkatan kompetensi, sertifikasi kompetensi, Alih Teknologi dan Alih Keahlian, hingga peningkatan budaya kesadaran keamanan informasi) yang menjadi semakin penting dengan implementasi teknologi 5G.

Pelaksanaan Aspek Pengembangan Kapasitas dalam Teknologi 5G

Aspek Pengembangan Kapasitas diukur berdasarkan keberadaan penelitian dan pengembangan; program pendidikan dan pelatihan; serta profesional bersertifikat dan lembaga sektor publik yang mendukung pengembangan kapasitas keamanan siber.

Indikator pertama dan kedua dihubungkan dengan teknologi 5G, dalam berbagai usaha yang dilakukan oleh BSSN. Dalam hal ini, BSSN mengembangkan berbagai standar dan pedoman yang bertujuan untuk menangani ancaman siber dan mempersiapkan keamanan siber dengan kehadiran teknologi 5G. Sebagai contoh, penetapan Peta Okupasi Nasional Keamanan Siber yang berfokus pada teknologi 5G; serta ditindaklanjuti dengan pembentukan standar nasional oleh sebagai pedoman pengembangan kapasitas, mulai dari penyediaan SDM, peningkatan kompetensi, sertifikasi kompetensi, Alih Teknologi dan Alih Keahlian, dan peningkatan budaya kesadaran keamanan informasi dengan kehadiran teknologi 5G.

Sementara itu, indikator ketiga sampai kedelapan dihubungkan dengan teknologi 5G, dalam salah satu tema 8 (delapan) Fokus

Area pada Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (SKSN dan MKS). Tema ini adalah Fokus Area 6 terkait Peningkatan Kapabilitas, Kapasitas, dan Kualitas yang mencakup enam tindakan sebagai berikut:

- Pengembangan kurikulum berkaitan dengan Keamanan Siber pada pendidikan anak usia dini, pendidikan dasar, pendidikan menengah, dan pendidikan tinggi (Indikator 6 & 7);
- Pengembangan dan penerapan program keterampilan dan pelatihan sumber daya manusia (Indikator 3 & 5);
- Pengembangan dan penerapan program peningkatan kesadaran Keamanan Siber yang terkoordinasi dan berkesinambungan (Indikator 4);
- Penguatan kapasitas teknologi Keamanan Siber (Indikator 3, 7 & 8);
- Peningkatan riset, pengembangan, dan inovasi ilmu pengetahuan dan teknologi di bidang Keamanan Siber (Indikator 3 & 8); dan
- Pengembangan program yang khusus untuk sektor dan kelompok rentan sesuai dengan kebutuhan (Indikator 6 & 7).

Pelaksanaan Aspek Kerja Sama dalam Teknologi 5G

Aspek Kerja Sama diukur berdasarkan keberadaan kemitraan, kerangka kerja kooperatif, dan jaringan berbagi informasi.

Indikator pertama sampai kelima dihubungkan dengan teknologi 5G, dalam berbagai bentuk kerja sama oleh pemerintah, terutama BSSN, dengan berbagai aktor dan pemangku kepentingan keamanan siber yang lain, baik secara nasional maupun internasional. Beberapa contoh kerja sama sebagai berikut:

- Indonesia menandatangani perjanjian bilateral Memorandum of Understanding (MoU) di bidang keamanan siber dengan berbagai negara. Seperti penandatanganan MoU dengan Belanda pada tahun 2023. Penandatangan ini dilakukan oleh Kepala BSSN, Hinsa Siburian, dengan Menteri Perdagangan Luar Negeri dan Kerjasama Pembangunan Belanda, Hanke Bruins Slot (BSSN, 2023c);
- ID-SIRTII/CC, yang bekerja di bawah Pusat Operasi Keamanan Siber Nasional BSSN, tergabung ke dalam Forum of Incident Response and Security Teams (FIRST) yang menyatukan berbagai tim respon insiden keamanan komputer global sebagai usaha untuk meningkatkan keamanan siber nasional;
- BSSN mengadakan pelatihan bertajuk *"5G Security Training and NESAS Best Practices Discussion"* untuk meningkatkan kemampuan keamanan siber dalam penggunaan teknologi 5G dengan Huawei Indonesia di Huawei ASEAN Academy Engineering Institute pada tahun 2021 (BSSN, 2021b);
- Politeknik Siber dan Sandi Negara (Poltek SSN) BSSN berkolaborasi dengan akademisi dari Institut Teknologi Del untuk melakukan tinjauan strategis keamanan siber menuju 5G pada tahun 2021; dan
- Politeknik Siber dan Sandi Negara (Poltek SSN) BSSN mengadakan Focus Group Discussion (FGD) yang diikuti oleh unsur pemerintah, akademisi, penyedia perangkat telekomunikasi, dan juga penyedia jaringan telekomunikasi mengenai Penyusunan Rekomendasi Kebijakan Keamanan pada Teknologi Telekomunikasi terkait Teknologi 5G pada tahun 2022 (BSSN, 2022).

Dalam hal ini, kerja sama ditujukan mempersiapkan dan mengatasi ancaman siber, termasuk dari teknologi 5G. Selain itu, kerja sama juga dilakukan untuk membangun kapabilitas dalam keamanan siber pada 3 (tiga) pilar arsitektur keamanan siber yang penting dalam implementasi teknologi 5G: Proses *(process)*, Sumber Daya Manusia *(people)*, dan Teknologi *(technology)*.

Analisis Ketahanan Siber Indonesia dalam Menghadapi Dilema Keamanan Penggunaan Ganda dari Kehadiran Teknologi 5G

Setelah meninjau pelaksanaan strategi keamanan siber yang mencakup lima pilar utama (hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama) yang diusulkan oleh Badan Siber dan Sandi Negara (BSSN), pemerintah Indonesia perlu mengadopsi langkah-langkah spesifik untuk menghadapi ancaman siber yang muncul dengan kehadiran teknologi 5G. Pada aspek hukum, pemerintah harus merancang undang-undang terpusat yang menangani keamanan dan ketahanan siber nasional, mengingat undang-undang yang ada seperti UU ITE dan UU PDP masih tersebar. Pada aspek teknis, diperlukan skema keamanan siber 5G yang kuat, termasuk sertifikasi, pengujian, deteksi, dan respons ancaman, serta praktik kesadaran keamanan siber yang baik. Dalam aspek organisasi, penting untuk mengembangkan roadmap keamanan siber yang terukur untuk implementasi teknologi 5G, melengkapi *roadmap* teknologi yang sudah ada.

Selain itu, dalam aspek pengembangan kapasitas, pemerataan infrastruktur digital harus dimaksimalkan, terutama di daerah pedesaan, dan kualitas serta kesadaran siber sumber daya manusia akan risiko ancaman siber harus ditingkatkan untuk memastikan semua pemangku kepentingan dapat memanfaatkan teknologi 5G dengan aman (Putranti, Amaliyah, & Windiani, 2019). Pada aspek kerja sama, penting untuk memperkuat kolaborasi antar pemangku kepentingan untuk membangun ekosistem keamanan siber yang baik serta meningkatkan kesadaran dan literasi keamanan siber, guna menghadapi ancaman yang timbul dari implementasi teknologi 5G. Dengan langkah-langkah ini, Indonesia dapat lebih siap menghadapi risiko dan memanfaatkan peluang yang ditawarkan oleh teknologi 5G.

Berbagai langkah di atas dibutuhkan untuk dapat mempersiapkan keamanan siber nasional, terlebih dengan implementasi teknologi 5G di Indonesia. Pemerintah sendiri, melalui Badan Siber dan Sandi Negara (BSSN), beranggapan bahwa ketahanan siber nasional masih rentan dan membutuhkan peningkatan (Wawancara, 2024). Hal ini dapat dilihat dari frekuensi serangan siber yang masih tinggi. Pertama, melalui kehadiran ancaman dari negara lain. Serangan siber seperti *spyware* dan *espionage* sudah menjadi permasalahan serius di Indonesia (Lanskap Keamanan Siber Indonesia, 2023a). Sehubungan dengan kerja sama pengembangan teknologi 5G nasional bersama dengan Huawei, tentu kekhawatiran akan eksploitasi kerentanan dan pengumpulan informasi sensitif seperti yang ditakutkan oleh pemerintah Amerika Serikat tidak janggal untuk muncul di Indonesia (Gedung Putih, 2019). Kedua, melalui kehadiran ancaman dari aktor non-negara. Serangan siber seperti *ransomware, web defacement,* kebocoran data, dan lain-lain dari aktor non-negara masih sering sekali terjadi. Bahkan, serangan siber paling sering mempengaruhi infrastruktur penting milik pemerintah (Lanskap Keamanan

Siber Indonesia, 2023a). Sebagai contoh, serangan siber *ransomware* di Pusat Data Nasional Sementara (PDSN) seperti yang sudah dipaparkan. Sehubungan dengan potensi ancaman siber dari teknologi 5G, tentu kerentanan dan ketidakmampuan pemerintah Indonesia dalam menjaga keamanan siber nasional seperti terlihat pada kasus *ransomware* PDN perlu diperhatikan dan ditangani.

SIMPULAN

Artikel ini membahas mengenai implikasi dari implementasi teknologi 5G terhadap ketahanan siber Indonesia. Dalam penelitian, dapat ditarik simpulan sebagai berikut.

Pertama, penggunaan teknologi 5G dapat menghasilkan dilema keamanan bagi Indonesia. Hal ini karena penggunaan teknologi tersebut tidak hanya dapat memberikan peluang bagi pembangunan nasional, tetapi juga dapat memunculkan ancaman siber baru yang berdampak bagi ketahanan siber Indonesia.

Kedua, Pemerintah Indonesia melalui Badan Siber dan Sandi Nasional (BSSN) telah menerapkan strategi keamanan siber untuk menjaga ketahanan siber dengan mengacu kepada 5 (lima) Pilar the Global Cybersecurity Index (GCI) 2017 oleh International Telecommunication Union (ITU). Kelima pilar meliputi aspek hukum, aspek teknis, aspek organisasi, aspek pengembangan kapasitas, dan aspek kerja sama. BSSN sendiri telah mendorong pengembangan strategi keamanan siber terkait teknologi 5G. Adapun demikian, pemerintah Indonesia dapat dikatakan telah menyadari perlunya pengembangan strategi keamanan siber untuk menghadapi ancaman siber dengan kehadiran teknologi 5G di Indonesia.

Ketiga, penulis melihat bahwa strategi keamanan siber nasional masih memerlukan pengembangan lebih lanjut. Pengembangan ini perlu mencakup beberapa hal seperti: pembuatan peraturan dan pedoman, penguatan dan peningkatan kinerja organisasi, pembangunan infrastruktur, peningkatan kemampuan sumber daya, hingga pelaksanaan kerja sama keamanan siber yang memenuhi kebutuhan akan kemunculan ancaman siber dari teknologi 5G di seluruh Indonesia.

DAFTAR PUSTAKA

Afshar, B., & Khorasani, K. (2020, Oktober). *DUAL USE TECHNOLOGY.* https://www.concordia.ca/content/dam/ginacody/research/spnet/Documents/BriefingNotes/EmergingTech-MilitaryApp/BN-19-Emerging-technology-and-military-application-Oct2020.pdf

Anggana, N. D. (2024, Februari 2). *Data Jumlah Serangan Cyber di Indonesia Tahun 2023*. Widya Security. https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/

Badan Siber dan Sandi Negara. (2021a, Oktober 26). *BSSN Selenggarakan Prakonvensi Rancangan Standar Kompetensi Kerja Nasional Indonesia RSKKNI-1 Bidang Audit Keamanan Informasi*. Badan Siber dan Sandi Negara. https://www.bssn.go.id/bssn-selenggarakan-prakonvensi-rancangan-standar-kompetensi-kerja-nasional-indonesia-rskkni-1-bidang-audit-keamanan-informasi/

Badan Siber dan Sandi Negara. (2021b, November 2). *BSSN berkolaborasi dengan Huawei Indonesia Gelar Pelatihan Standar Cybersecurity 5G Dukung Kesiapan Kebijakan Keamanan Ekosistem Digital*. Badan Siber dan Sandi Negara. https://www.bssn.go.id/

bssn-berkolaborasi-dengan-huawei-indonesia-gelar-pelatihan-standar-cybersecurity-5g-dukung-kesiapan-kebijakan-keamanan-ekosistem-digital/

Badan Siber dan Sandi Negara. (2022, Agustus 24). *FGD BSSN Rekomendasikan Identifikasi Kepentingan Nasional, Pemetaan Peran dan Tanggung Jawab, serta Literasi Publik dalam Pemanfaatan Teknologi 5G Indonesia*. Badan Siber dan Sandi Negara. https://www.bssn.go.id/fgd-bssn-rekomendasikan-identifikasi-kepentingan-nasional-pemetaan-peran-dan-tanggung-jawab-serta-literasi-publik-dalam-pemanfaatan-teknologi-5g-indonesia/

Badan Siber dan Sandi Negara. (2023a, Desember 6). Lanskap Keamanan Siber 2023. Jakarta; BSSN - ID-SIRTII/CC.

Badan Siber dan Sandi Negara. (2023b, Oktober 11). *Pembahasan rencana aksi Nasional Keamanan Siber Sebagai Turunan Perpres nomor 47 Tahun 2023*. Badan Siber dan Sandi Negara. https://www.bssn.go.id/pembahasan-rencana-aksi-nasional-keamanan-siber-sebagai-turunan-perpres-nomor-47-tahun-2023/

Badan Siber dan Sandi Negara. (2023c, November 1). *Satu Dekade Kemitraan Komprehensif, RI dan Belanda Tingkatkan Kerja Sama di Bidang Keamanan Siber*. Badan Siber dan Sandi Negara. https://www.bssn.go.id/satu-dekade-kemitraan-komprehensif-ri-dan-belanda-tingkatkan-kerja-sama-di-bidang-keamanan-siber/

Blackman, J. (2023, Juni 7). *DDoS attacks using IOT bots have jumped five-fold in 12 months, says report*. RCR Wireless News. https://www.rcrwireless.com/20230607/internet-of-things-4/ddos-attacks-using-iot-bots-have-jumped-five-fold-in-12-months-says-report.

Chotimah, Hidayat Chusnul, Muhammad Ridha Iswardhana, dan Tiffany Setyo Pratiwi. (2019). Penerapan Military Confidence Building Measures Dalam Menjaga Ketahanan Nasional Indonesia Di Ruang Siber. *Jurnal Ketahanan Nasional*, *25*(3), 16-25. https://doi.org/10.22146/jkn.50344

CNN Indonesia. (2022, November 6). *Viral TV analog Dimatikan Demi 5G, Kominfo Beri Penjelasan*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20221106043115-213-870039/ viral-tv-analog-dimatikan-demi-5g-kominfo-beri-penjelasan

Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In D. Broeders, & B. van den Berg (Eds.), *Governing cyberspace. Behavior, power and diplomacy.*

Davies, V. (2021, Oktober 4). *The history of Cybersecurity*. Cyber Magazine. https://cybermagazine.com/cyber-security/history-cybersecurity

Douglass, J. D. (1981). Soviet disinformation. *Strategic Review,* (9), 16-25.

Etania, R. B. & Indriawati, T. (2023, Oktober 6). *Manhattan Project, Awal Diciptakannya Bom Atom*. Kompas. https://www.kompas.com/stori/read/2023/10/06/202055979/manhattan-project-awal-diciptakannya-bom-atom?page=all

Forge, J. (2010). A note on the definition of "dual use". *Science and Engineering Ethics, 16*(1), 111–118. https://doi.org/10.1007/s11948-009-9159-9

Gedung Putih. (2019, Mei 15). *Executive Order on Securing the Information*

and Communications Technology and Services Supply Chain. The White House. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

Hardiansyah, Z. (2024, Juli 10). *Kronologi Serangan ransomware Ke Pdn Dan Penanganannya Yang Tak Kunjung Usai*. KOMPAS.com. https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai#google_vignette

IBM. (2022, April 14). *What is malware?*. IBM. https://www.ibm.com/topics/malware#:~:text=Increasingly%2C%20malware%20attacks%20target%20businesses,sums%20of%20money%20from%20them.

IME FTUI. (2023, September 11). *Perkembangan 5g Saat Ini di Indonesia*. Ikatan Mahasiswa Elektro UI. https://ime.eng.ui.ac.id/perkembangan-5g-saat-ini-di-indonesia/

Iradat, D. (2023, November 9). *Menkominfo Tegaskan Jaringan internet di IKN harus 5G*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20231109192412-213-1022207/menkominfo-tegaskan- jaringan-internet-di-ikn-harus-5g

Kementerian Pertahanan. (2015, November 20). BUKU PUTIH PERTAHANAN INDONESIA 2015. Jakarta; Kementerian Pertahanan Republik Indonesia.

Khan Academy. (2018, Agustus 30). *The Atomic Bomb & The Manhattan Project (article)*. Khan Academy. https://www.khanacademy.org/humanities/us-history/rise-to-world-power/us-wwii/a/the-manhattan-project-and-the-atomic-bomb#:~:text=Overview,in%20the%20Second%20World%20War.

Kominfo. (2021a). *Rencana Strategis 2020-2024*. Kementerian Komunikasi dan Informatika.

Kominfo. (2021b, Mei 31). *Jaringan 5G Resmi Beroperasi, Transformasi Digital Melesat*. Kementerian Komunikasi dan Informatika. https://www.kominfo.go.id/content/detail/34812/jaringan-5g-resmi-beroperasi-transformasi-digital-melesat/0/artikel

Kominfo. (2021c, Mei 24). *Pemerintah Dorong pemanfaatan 5G untuk industri dalam negeri*. Kementerian Komunikasi dan Informatika. https://www.kominfo.go.id/content/detail/35312/pemerintah-dorong-pemanfaatan-5g-untuk-industri-dalam-negeri/0/berita

Kominfo. (2021d, April 7). *Dukungan Tata Kelola 5G yang Komprehensif, Menteri Johnny Paparkan 5 Aspek Kebijakan*. Kementerian Komunikasi dan Informatika. https://www.kominfo.go.id/content/detail/33740/siaran-pers-no114hmkominfo042021-tentang-dukungan-tata-kelola-5g-yang-komprehensif-menteri-johnny-paparkan-5-aspek-kebijakan/0/siaran_pers

Kominfo. (2023, September 21). *ASO Tuntas, Pemerintah Dorong Pemanfaatan Teknologi 5G*. Kementerian Komunikasi dan Informatika. https://www.kominfo.go.id/content/detail/51744/siaran-pers-no-320hmkominfo092023-tentang-aso-tuntas-pemerintah-dorong-pemanfaatan-teknologi-5g/0/siaran_pers

Law, M. (2023, September 27). *Global events driving rise in ddos attacks, says netscout*. Cyber Magazine. https://cybermagazine.com/articles/global-

events-driving-increase-in-ddos-attacks

Lin, H. (2016). Governance of Information Technology and Cyber Weapons. In E. D. Harris (Ed.), *Governance of Dual use Technologies: Theorie and Practice*. American Academy of Arts & Sciences.

Lin, H. (2016). Governance of information technology and cyber weapons. In E. D. Harris (Ed.). *Governance of dual-use technologies: Theory and practice.* American Academy of Arts and Sciences

Lupovici, A. (2021). The dual-use security dilemma and the social construction of insecurity. *Contemporary Security Policy*, *42*(3), 257–285. https://doi.org/10.1080/13523260.2020.1866845

Miles, M. B. & Huberman, M. (1992). *Analisis Data Kualitatif*. Jakarta: Penerbit Universitas Indonesia.

MIT Technology Review. (2023, September 15). *The Cyber Defense Index 2022/23*. MIT Technology Review. https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/

Nistanto, R. K. (2021, Mei 29). *Perjalanan 5g di Indonesia, Dari Uji Coba, Lelang Frekuensi, Hingga Komersil Halaman all*. KOMPAS.com. https://tekno.kompas.com/read/2021/05/29/19210047/perjalanan-5g-di-indonesia-dari-uji-coba-lelang-frekuensi-hingga-komersil?page=all

None, N. (1985). *The history of nuclear energy*. U.S. Dept. of Energy. https://www.energy.gov/ne/articles/history-nuclear-energy

Olsson, J., Shorov, A., Abdelrazek, L., & Whitefield, J. (2021, Mei 12). 5G ZERO TRUST. ERICSSON.

Oughton, E. J., Lehr, W., Katsaros, K., Selinis, I., Bubley, D., & Kusuma, J. (2021). Revisiting Wireless Internet Connectivity: 5G vs Wi-Fi 6. *Telecommunications Policy*, *45*(5), 102127. https://doi.org/10.1016/j.telpol.2021.102127

Pa, W. (n.d.). *Robotics: A Brief History*. Stanford. https://cs.stanford.edu/people/eroberts/courses/soco/projects/1998-99/robotics/history.html

Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

Putranti, Ika Riswanti, Anita Amaliyah, dan Reni Windiani. (2020). Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah. *Jurnal Ketahanan Nasional*, *26*(3), 359-379. https://doi.org/10.22146/jkn.57322

Raj, A. (2023, September 14). *Cybersecurity in Malaysia sees significant improvements in 2023*. Tech Wire Asia. https://techwireasia.com/09/2023/businesses-in-malaysia-increase-cybersecurity-budget-allocation-in-2023/

Riebe, T., & Reuter, C. (2019). Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In *Information Technology for Peace and Security* (pp. 165–183). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4_8

Savitri, D. (2024, Juli 3). *PPI Dunia usulkan 6 solusi Konkret Soal ransomware Pusat Data nasional*. detikedu. https://www.detik.com/edu/edutainment/d-7420462/ppi-dunia-usulkan-6-solusi-konkret-soal-ransomware-pusat-data-nasional

Savitri, P. I. (2021, Agustus 12). *Akademisi: Jaringan 5G merupakan Tantangan Bagi keamanan nasional*. Antara

News. https://www.antaranews.com/berita/2323094/akademisi-jaringan-5g-merupakan-tantangan-bagi-keamanan-nasional

SDPPI Kominfo. (2023, Juli 28). *Implementasi 5g Beri Layanan Berkualitas di Masa Depan: Seputar SDPPI*. Direktorat Jenderal Sumber Daya dan Perangkat Pos dan Informatika. https://www.postel.go.id/berita-implementasi-5g-beri-layanan-berkualitas-di-masa-depan-27-6003

Singh, M. (2022, Desember 23). *5G could pose a huge cybersecurity risk: Ruchir Shukla, MD, Safehouse Tech*. The Times of India. https://timesofindia.indiatimes.com/gadgets-news/5g-could-pose-a-huge-cybersecurity-risk-ruchir-shukla-md-safehouse-tech/articleshow/96435263.cms

Sudarmadi, D.A. & Runturambi, A.J.S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157–178.

Suryohadiprojo, S. (1997). Ketahanan Nasional Indonesia. *Jurnal Ketahanan Nasional, 2*(1), 13-31. https://doi.org/10.22146/jkn.19163

Sutrisna, T., & Prabowo, D. (2024, Juni 26). *Pemerintah Akui Tak Bisa Pulihkan data Kementerian/lembaga Terdampak Peretasan PDN*. Kompas. https://nasional.kompas.com/read/2024/06/26/18375561/pemerintah-akui-tak-bisa-pulihkan-data-kementerian-lembaga-terdampak

Swedberg, R. (2020). Exploratory Research. *The Production of Knowledge, 2*(2), 17-41.

Telenor IoT. (2023, November 8). *What is 5G technology and what does 5G mean for IOT?*. Telenor IoT. https://iot.telenor.com/technologies/connectivity/5g/#:~:text=5G%20is%20well%2Dpositioned%20to,needs%20of%20the%20use%20case.

Telkomsel. (2021, Mei 25). *Perjalanan Telkomsel Mempersiapkan Kehadiran 5G di Indonesia*. Telkomsel. https://www.telkomsel.com/about-us/blogs/perjalanan-telkomsel-mempersiapkan-kehadiran-5g-di-indonesia

Telkomsel. (2023, Maret 2). *Telkomsel, Ericsson, dan Qualcomm Perkuat Kolaborasi dalam Pengembangan Peta Jalan Teknologi Fixed Wireless Access Berbasis 5G*. Telkomsel. https://www.telkomsel.com/about-us/news/telkomsel-ericsson-dan-qualcomm-perkuat-kolaborasi-dalam-pengembangan-peta-jalan