Kondisi Ruang Siber Selama Pandemi Covid-19 dan Upaya Mengembangkan Kebijakan Publik di Indonesia

Cyberspace Conditions During the Covid-19 Pandemic and Efforts to Develop Public Policies In Indonesia

Irwansyah
Badan Siber dan Sandi Negara

Riant Nugroho
Rumah Reformasi Kebijakan

ABSTRAK

Artikel ini membahas tentang kondisi ruang siber selama pandemi Covid-19 dan upaya mengembangkan kebijakan publik di Indonesia. Tujuan penelitian ini adalah menelusuri secara kritis kondisi ruang siber selama pandemi Covid-19. Penelitian ini menggunakan metode PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-analyses*). Hasil penelitian menemukan target serangan, jenis serangan, dan respon beberapa negara terhadap kondisi ruang siber. Selama pandemi Covid-19, Indonesia telah mengeluarkan beberapa rilis atau kebijakan publiknya dalam mendeteksi, mencegah, mengedukasi, dan mengatasi beberapa insiden selama pandemi Covid-19. Untuk mengembangkan kebijakan publik yang unggul sebagai respon atas meningkatnya serangan siber selama pandemi direkomendasikan Indonesia perlu menetapkan strategi keamanan siber sebagai pondasi perumusan kebijakan publik, BSSN perlu mengoptimalkan *ways*-nya yaitu "memanfaatkan, mengembangkan, dan mengonsolidasikan unsur-unsur keamanan siber" kepada Lembaga yang memiliki kewenangan dalam 5 (lima) mandat keamanan siber nasional (*five mandates national cybersecurity*) sehingga dapat bersama-sama merespon serangan siber selama pandemi covid-19, serta BSSN perlu menentukan Jenis, model dan metode perumusan kebijakan publik secara tepat untuk mempermulus tersusunnya kebijakan dan mendapatkan dukungan dengan memperhatikan prinsip dasar kebijakan keamanan siber.

Kata Kunci : Covid-19, Kebijakan Publik, Keamanan Siber, Kebijakan Keamanan Siber

ABSTRACT

This article discusses the condition of cyberspace during the Covid-19 pandemic and efforts to develop public policies in Indonesia. The purpose of this study is to critically explore the condition of cyberspace during the Covid-19 pandemic. This study uses the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-analyses) method. The results of the study found the target of the attack, the type of attack, and the response of several countries to cyberspace conditions. During the Covid-19 pandemic, Indonesia has issued several releases or public policies in detecting, preventing, educating, and overcoming several incidents during the Covid-19 pandemic. In order to develop superior public policies in response to increasing cyberattacks during the pandemic, it is recommended that Indonesia needs to establish a cyber security strategy as the foundation for formulating public policies, BSSN needs to optimize its ways, namely "utilizing, developing, and consolidating cyber security elements" to institutions that has the authority in five national cybersecurity mandates so that they can jointly respond

to cyberattacks during the covid-19 pandemic, and the BSSN needs to determine the type, model and method of formulating public policies appropriately to facilitate the formulation of policies and gain support by observing the basic principles of cybersecurity policy

Keywords: *Covid-19, public policy, cybersecurity, cybersecurity policy*

A. Pendahuluan

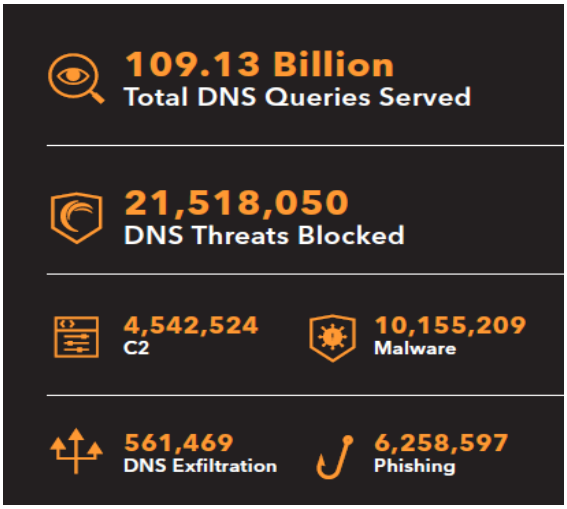
Penyebaran *corona virus infection desease* 2019 (Covid-19) yang begitu cepat dan luas memiliki dampak terhadap kehidupan sosial manusia. Pada bulan Desember 2019, *World Health Organization* (WHO) merilis bahwa Covid-19 yang xberasal dari Wuhan Tiongkok sebagai salah satu bencana pandemik global. Sebagai sebuah penyakit yang sangat menular, Kementerian Kesehatan (Kemenkes) memiliki kebijakan terhadap pencegahan penyebaran virus yang dikenal dengan 3M yaitu "mencuci tangan", "memakai masker" dan "menjaga jarak". Salah satu bentuk upaya "menjaga jarak" adalah membatasi adanya tatap muka/pertemuan dan menggantikan pertemuan yang pada awalnya dilakukan secara tatap muka dilakukan secara virtual (*online*). Kebijakan ini secara tidak langsung telah merubah interaksi sosial manusia baik di bidang pendidikan, ekonomi, agama dan seluruh aspek dimensi kehidupan manusia lainnya. Maka muncullah beberapa istilah dalam kehidupan sosial masyarakat seperti pembelajaran jarak jauh (*school from home*), bekerja dari rumah (*work from home*), seminar *online*, layanan kesehatan *online*, bahkan menjadi semakin maraknya belanja *online.*

Pandemi telah menyebabkan krisis pada multi sektor seperti ekonomi, sistem pendidikan, kemunduran sosial, agama dan budaya. Walaupun virus ini sangat berbahaya dan penyebarannya yang begitu cepat, manusia harus dapat beradapatasi dengan kondisi yang tidak normal tersebut agar dimensi kehidupan dapat berjalan. Bahkan adapatasi baru ini telah menjadi transformasi global seperti ditunjukkan pada

Tabel 1 di bawah (Weil & Murugesan, 2020). Pola adaptasi baru (*new normal*) dengan sistem *online* telah memberikan kemudahan pada aktivitas kehidupan manusia. Belajar dan bekerja secara *online* melalui *virtual conference* menjadi *new style* walaupun sebelumnya aktivitas ini telah dilakukan sebelum pandemi.

Sama halnya dengan belanja *online*. Sekarang orang lebih mudah mendapatkan kebutuhan pokoknya selama pandemi ini dengan berbelanja secara *online*. Bahkan beberapa aktivitas industri pun saat ini telah beralih kepada sistem *otomotisasi* robot yang dapat diakses dalam jarak jauh.

Gambar 1. Jumlah Serangan Siber Dunia 2020



Sumber : Akamai, 2021

Tabel 1. Transformasi Global Selama Pandemi Covid-19

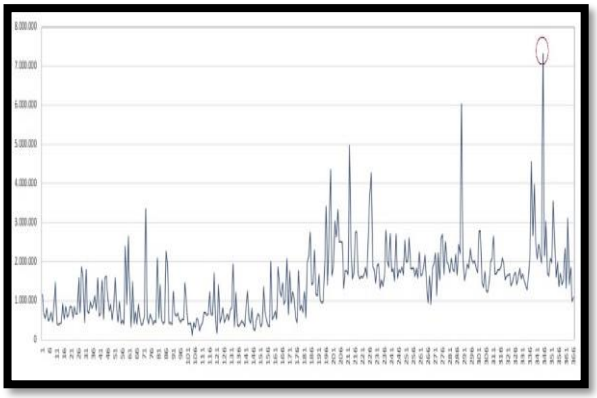
Sektor	Dampak Yang Ditimbulkan oleh Pandemi	Respon Pelaksanaan	Rekomendasi Teknologi yang berhubungan
Pendidikan	Penutupan institusi Pendidikan, pembatasan akses ke laboratorium	Pembelajaran virtual/jarak jauh	*Software video conference, lab virtual berbasis cloud*
Kesehatan	Rumah sakit penuh sehingga tidak dapat memenuhi kebutuhan	Pelacakan kontak, telehealth (konsultasi *online* dengan dokter), otomatisasi diagnosis, pengembangan vaksin, alokasi sumber daya berdasarkan tingkat emergensi pasien	*Aritifiial intelligence, Machine Learning, Cloud Computing*
Bisnis	Penutupan bisnis, pembatasan belanja eceran secara langsung	Penerapan social distancing, layanan *online*, bekerja dari rumah	*Chatbot, drone delivery, software meeting online, virtual office, remote access to work*
Industri	Penutupan bisnis, pembatasan belanja eceran secara langsung	Bekerja dari rumah, otomatisasi sistem, *remote operation*	Robot, otomatisasi, *3D-Printing*
Perdagangan	Penutupan toko dan hanya menyediakan layanan *online*	Belanja *online, home delivery*	Website, pembayaran *online*, pembayaran tanpa kontak langsung
Pemerintahan	Meningkatnya permintaan masyarakat untuk mendapatkan bantuan, pembatasan layanan pemerintahan	Layanan *online*	*Cloud, web*, aplikasi *meeting online*
Hiburan	Penutupan tempat hiburan	Penampilan hiburan secara *online*	Audio dan Video *streaming, virtual realitiy*
Kehidupan pribadi dan interaksi social	*Lockdown*	Kegiatan dalam ruangan	Telepon, *audio dan video chat, streaming, game online*
Keagamaan	Peneutupan tempat keagamaan	Beribadah dari rumah, ritual ibadah melalui *video conference*	Audio dan *video streaming, virtual reality*
Konferensi	*Virtual conference*	Presentasi dan diskusi secara *online*	*Video streaming, software virtual conference*

Sumber: Diolah dari Weil & Murugesan (2020)

Walaupun transformasi pola kehidupan *global* secara *online* telah memberikan kemudahan bagi kehidupan manusia, transformasi *online* dapat memunculkan risiko seperti pencurian data, penipuan belanja, kejahatan siber, kegagalan sistem akibat serangan *malware*, aktivitas mata-mata (*phishing*) bahkan gangguan dalam *video conference* (*zoom bombing*). Laporan Pusat Operasi Keamanan Siber Nasional (Pusopkamsinas) BSSN periode Januari-Desember 2020 mencatat selama pandemi Covid-19 terjadi peningkatan serangan siber di Indonesia menjadi 495,3 juta serangan dimana tren serangan berupa pencurian data melalui *malware* (Pusat Operasi Keamanan Siber Nasional, 2021). Anomali trafik tertinggi terjadi pada 10 Desember 2020 dengan jumlah mencapai 7.311.606 anomali.

Akamai pun mencatat adanya peningkatan serangan siber di dunia selama pandemi Covid-19 sebesar 109,13 milyar serangan dengan perharinya terdapat sekitar 299 juta serangan dimana mayoritas serangan berupa *malware* dan *phishing* (Akamai et al., 2021). Ini berarti meningkatnya *traffic* internet selama pandemi telah dimanfaatkan oleh pihak yang tidak bertanggungjawab untuk melakukan kejahatan di ruang siber.

Gambar 2. Anomali Trafik 2020 di Indonesia



Sumber : Pusopkamsinas, 2021

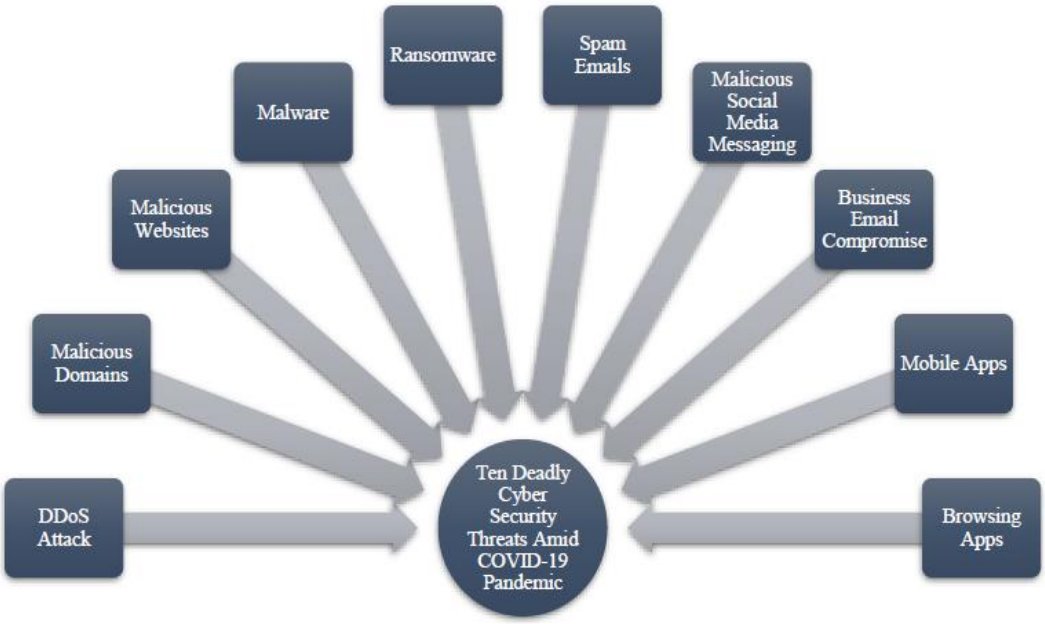
Walaupun data statistik serangan siber mengalami peningkatan, belum diketahui secara komprehensif dan terstruktur jenis serangan dan target serangan siber yang terjadi di Indonesia. Data serangan baru menggambarkan anomali terhadap jaringan dan sistem. Mengetahui target dan jenis serangan siber yang terjadi dapat menjadi landasan pokok bagi organisasi atau pemerintah dalam merespon secara cepat dan tepat terhadap kondisi tersebut.

Di samping itu, meningkatnya aktivitas kehidupan masyarakat di ruang siber memberikan tantangan bagi pemerintah untuk melindungi warga negaranya dari setiap ancaman dan kejahatan di ruang siber. Pada masa krisis ini masyarakat tidak hanya berhadapan dengan virus yang mematikan namun juga ancaman yang dapat hadir mengganggu aktivitas masyarakat di ruang siber. Selama pandemi covid-19 ini, Kan et.al (2020) dalam penelitiannya telah mencatat 10 jenis serangan siber menghancurkan selama pandemi ini dimana isu data pribadi menjadi hal yang sangat *hangat* pada masa pandemi ini (Khan et al., 2020).

Kejahatan dan serangan siber dapat memberikan dampak yang besar bagi kehidupan masyarakat selama pandemi ini terlebih aktivitas kehidupan manusia saat pandemi ini bertumpu pada aktivitas secara virtual/*online*. Terlebih jika serangan siber terjadi pada *industrial control system* infrastruktur vital (IV) yang dapat menimbulkan dampak yang sangat besar seperti kematian, krisis energi, krisis pangan, keracunan air, dan bencana lainnya.

Pada tahun 2007, Estonia mengalami krisis akibat serangan siber yang menyebabkan lumpuhnya fungsi layanan perbankan, pemerintahan, media massa, pendidikan, dan bahkan parlemen Estonia. Hal ini menjadi pelajaran berharga bagi dunia untuk memberikan perhatian penting kepada keamanan siber suatu negara. Pemerintah memiliki peran untuk menjamin keamanan bagi aktivitas warga negara di ruang siber, menegakkan hukum dari setiap kejahatan siber, dan mengedukasi masyarakat. Situasi meningkatnya interaksi manusia di ruang siber ditambah dengan meningkatnya ancaman dan kejahatan di ruang siber membutuhkan peran pemerintah untuk meresponnya. Hal ini dikarenakan serangan dan kejahatan siber dapat dianggap sebagai ancaman transnasional dan melewati batas-batas negara yang tidak dapat diselesaikan oleh setiap individu warga negara ataupun organisasi. Sehingga masyarakat membutuhkan kehadiran negara atau pemerintah untuk dapat meresponnya dengan segala kewenangan dan perangkat pemerintahan yang dimilikinya.

Gambar 3. 10 Jenis Serangan Siber



Sumber: Kan, et.al, 2020

Beberapa negara merespon hal itu dengan kebijakan publiknya berupa peringatan-peringatan, panduan, dan tindakan-tindakan dari serangan siber. Hanya pemerintahlah yang berwenang mengeluarkan kebijakan publik untuk mengurusi masyarakatnya. Keunggulan suatu masyarakat atau bangsa sangat ditentukan oleh kebijakan unggul yang dihasilkannya untuk menghebatkan masyarakatnya menuju cita-cita atau tujuan bangsa dan negara (Nugroho, 2020c). Peran Pemerintah akan menjadi efektif jika mampu memproduksi kebijakan berkualitas dan unggul tentang keamanan siber di masa pandemi ini. Kebijakan yang unggul adalah kebijakan yang dapat membuat masyarakat menjadi unggul (Nugroho, 2020).

Kebijakan yang membuat masyarakat dapat melewati masa krisis ini. Selama pandemi covid ini terdapat penelitian yang dilakukan oleh Well dan Murugesan (2020) tentang respon keamanan siber terhadap Covid-19 yang menyatakan bahwa kemampuan organisasi secara efektif merespon gangguan tidak hanya bergantung kepada efektifnya proses perencanaan tapi juga sebagaimana efektifnya persiapan, uji coba, dan training kepada stafnya untuk menghadapi hal tersebut yang sering diabaikan.

Persiapan, uji coba, dan training perlu diberikan oleh Pemerintah kepada organisasi agar dapat mengatasi gangguan yang disebabkan oleh serangan siber (Weil & Murugesan, 2020). NCSC dan CISA sebagai organisasi keamanan siber di Inggris dan Amerika telah mengeluarkan beberapa respon menghadapi ancaman siber selama pandemi Covid-19 yang telah dirangkum oleh Pranggono dan Arabo (2020) dalam menyikapi isu *phising* dan *malware* pada tools yang digunakan dalam WFH seperti *Zoom* dan sebagainya.

Indonesia telah memiliki instrumen kebijakan publik keamanan siber berupa kelembagaan yang memiliki fungsi dalam memproduksi, mengimplementasikan dan mengevaluasi kebijakan publik di bidang keamanan siber. Namun selama pandemi ini, belum terdokumentasi dan terstruktur kelembagaan ini merespon aktivitas serangan siber dalam wujud kebijakan publiknya sehingga pencegahan terjadinya serangan dan upaya merespon serta memulihkan dapat tertangani dengan baik. Karena dalam praktiknya, untuk meng-

hasilkan kebijakan publik sebagai upaya merespon situasi dan permasalahan diperlukan metode perumusan yang tepat dan cepat, terlebih dalam situasi krisis atau pandemi ini (Nugroho, 2020a).

Proses perumusan kebijakan publik yang tidak tepat dapat menimbulkan persoalan baru yang semestinya kebijakan publik yang dihasilkan dapat mengatasi kondisi dan situasi yang terjadi. Kebijakan publik kadang sering disalahartikan dan bahkan disalahgunakan (Nugroho, 2020). Menurut Nugroho, Kebijakan penanganan Covid-19 di Indonesia adalah tragedi keilmuan kebijakan publik. Hal ini dikarenakan tidak sesuainya isu kebijakan dengan cara mengatasinya. Menurutnya, Covid-19 adalah isu kebijakan level tiga, sementara cara mengatasi kebijakannya baru Level 1, bahkan mungkin kurang (Nugroho, 2020a).

Chigada dan Madzinga (2020) menyatakan bahwa pertumbuhan eksponensial serangan dan ancaman siber karena ekonomi global telah menaruh banyak perhatian pada pandemi Covid-19. Selama pandemi, perusahaan besar, industri perawatan kesehatan, dan lembaga pemerintah telah menjadi sasaran serangan dan ancaman siber. Mengetahui secara sistematis ancaman dan serangan siber pada beberapa organisasi dapat menjadi pelajaran bagi negara atau organisasi untuk menentukan respon yang tepat dan cepat (Chigada & Madzinga, 2020). Respon Negara merupakan kebijakan publik negara.

Beberapa penelitian yang telah dilakukan sebelumnya selama pandemi covid-19 terkait serangan siber dan beberapa respon yang telah dilakukan oleh beberapa negara, menggugah peneliti untuk melakukan penelitian terkait kondisi ruang siber selama pandemi covid-19 dan upaya untuk mengembangkan kebijakan publik yang unggul terkait keamanan siber di Indonesia yang akan peneliti jelaskan dalam penelitian ini. Dengan mengetahui kondisi ruang siber Indonesia secara kontekstual selama pandemi ini, Indonesia dapat merumuskan kebijakan publiknya berdasarkan bukti (*evidence-based policy*) sehingga kebijakan publik yang berkualitas dapat terwujud.

B. Tinjauan Literatur

Kebijakan Publik

Harold D. Laswell dan Abraham Kaplan (Suwitri, 2008) mendefinisikan kebijakan sebagai suatu program pencapaian tujuan, nilai-nilai dan praktik-praktik yang terarah. Pendapat lain, James E. Anderson mendefinisikan kebijakan sebagai serangkaian tindakan yang mempunyai tujuan tertentu yang diikuti dan dilaksanakan oleh seorang pelaku atau sekelompok pelaku guna memecahkan suatu masalah tertentu.

Seiring demi waktu kebijakan berkembang menjadi kebijakan publik. Hal ini dikarenakan objek dari kebijakan itu sendiri adalah ditujukan kepada orang atau sekelompok masyarakat. Thomas R. Dye mendefinisikan kebijakan publik sebagai pilihan pemerintah untuk melakukan atau tidak melakukan. Kebijakan publik adalah tentang apa yang pemerintah lakukan, mengapa melakukan itu dan apa bedanya jika itu dilakukan (Dye, 2017).

David Easton mendefinisikan kebijakan publik adalah pengalokasian nilai-nilai secara paksa (legal) kepada seluruh anggota masyarakat. Sedangkan James Anderson mendefiniskan kebijakan publik sebagai kebijakan yag dikembangkan oleh badan-badan dan pejabat-pejabat pemerintah.

Nugroho (2014) mendefinisikan kebijakan publik adalah keputusan yang dibuat oleh suatu negara sebagai strategi untuk merealisasikan tujuan dari negara yang bersangkutan. Beberapa definisi yang diungkapkan oleh pakar tentang kebijakan publik terungkap bahwa kebijakan publik hanya dapat ditetapkan pemerintah, pihak-pihak lain atau aktor

kebijakan publik yang dapat mempengaruhi kebijakan publik dalam batas kewenangannya masing-masing. Alasan pemerintah sebagai subjek kebijakan karena ada tiga kewenangan yang dimilikinya:

- Hanya pemerintah yang mempunyai kekuatan dan kemampuan untuk merealisasikan kebijakan publik secara universal kepada publik yang menjadi sasaran
- Hanya pemerintah yang mempunyai kekuatan dan kemampuan untuk melegitimasi atau mengesahkan kebijakan publik sehingga dapat diberlakukan secara universal kepada publik yang menjadi sasaran
- Hanya pemerintah yang mempunyai kekuatan dan kemampuan untuk melaksanakan kebijakan publik secara paksa kepada publik yang menjadi sasaran

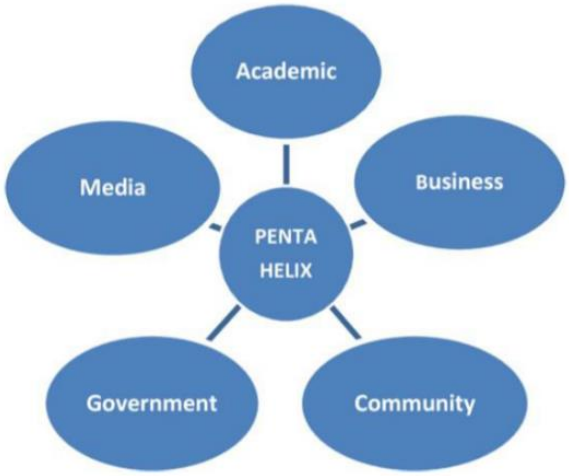
Untuk mengetahui kebijakan publik diimplementasikan, perlu diketahui jenis-jenis kebijakan publik. Secara generik kebijakan publik dapat diimplementasikan melalui empat hal (Nugroho, 2020b):

1. Peraturan formal, yaitu undang-undang (*act*), hukum (*law*), dan regulasi (*regulation*)
2. Konvensi, yaitu kebiasaan umum lembaga publik yang telah diterima bersama. Dapat ditumbuhkan dari proses manajemen organisasi public seperti upacara rutin, SOP tertulis atau tidak tertulis, atau ditumbuhkan dari aktor organisasi publik seperti pidato presiden setiap tanggal 17 agustus.
3. Pernyataan pejabat publik dalam forum publik, yaitu pejabat politik dan pejabat administratif yang telah mempunyai kewenangan politik disampaikan pada forum publik secara terbuka kepada para pemilik dan pemangku kepentingan terkait.
4. Perilaku pejabat publik, yatu dapat berupa perilaku perseorangan, kelompok atau perilaku keluarga.

Dalam penyusunan dan implementasi kebijakan publik, Pemerintah tidak dapat bekerja sendiri. Pemerintah membutuhkan partisipasi setiap masyarakat agar kebijakan publik yang dihasilkannya unggul. Partisipasi masyarakat dan unsur lainnya bersama pemerintah dalam perumusan dan implementasi kebijakan publik dikenal kolaborasi.

Saat ini telah dikenal kolaborasi Pentahelix yang merupakan pengembangan dari strategi *triple helix* dengan menambahkan elemen komunitas atau Lembaga nonprofit (Lindmark et al., 2009). Kolaborasi Pentahelix adalah referensi dalam mengembangkan sinergi antara Lembaga terkait dalam mendukung seoptimal mungkin untuk mencapai tujuan. Lembaga terkait tersebut meliputi Pemerintah, Pebisnis, Akademisi, Komunitas, dan Media.

Gambar 4. *Pentahelix Scheme*



Sumber: Koleksi pribadi

Melalui kolaborasi sinergis diharapkan terwujud suatu inovasi yang didukung oleh berbagai sumber daya yang saling berinteraksi secara sinergis. Akademisi adalah sumber pengetahuan. Mereka memiliki konsep, teori dalam mengembangkan bisnis untuk mendapatkan keunggulan kompetitif yang berkelanjutan. Komunitas adalah orang-orang yang memiliki minat yang sama dan relevan dengan bisnis yang dikembangkan. Peme-

rintah merupakan salah satu pemangku kepentingan yang memiliki regulasi dan tanggung jawab dalam mengembangkan bisnis. Pebisnis adalah suatu entitas yang memiliki aktivitas mengolah barang atau jasa menjadi bernilai. Sedangkan media adalah *stakeholder* yang memiliki lebih banyak informasi untuk mengembangkan bisnis dan berperan kuat dalam mempromosikan bisnis.

Kolaborasi pentahelix telah sukses dalam membangun sinergi diantara *stakeholder*. Dalam penelitian Muhyi et.al (2017) menyebutkan bahwa pada tahun pertama penelitiannya tentang pengembangan bisnis pariwisata di Bandung, peneliti menemukan tiga pihak kemitraan yang memiliki andil suatu keberhasailan kolaborasi, Namun setelah ditelusuri lebih jauh, peneliti menemukan pemangku kepentingan lain yang tidak bisa diabaikan yaitu akademisi dan media (Muhyi & Chan, 2017).

Pada saat pandemi Covid-19 ini, pemerintah mengalami ujian yang tidak hanya terkait Kesehatan dan ekonomi, akan tetapi ujian terkait kebijakan publiknya yang diharapkan dapat mengatasi permasalahan pandemi Covid-19 ini. Menurut Nugroho (2020), kebijakan penanganan Covid-19 di Indonesia adalah tragedi keilmuan kebijakan publik. Hal ini dikarenakan tidak sesuainya isu kebijakan dengan cara mengatasinya. Menurutnya, Covid-19 adalah isu kebijakan level tiga yaitu terkait isu bencana, sementara cara mengatasi kebijakannya baru level 1 (*think slow*), bahkan mungkin kurang. Ketika isu kebijakannya tentang isu bencana seperti penyakit infeksi, bencana maka cara mengatasinya harus cepat.

Untuk itu mengatasi isu kedaruratan dalam suatu negara, Nugroho merekomendasikan model kebijakan yang dapat diterapkan adalah: (1) *evidence base*, yaitu pendekatan berbasis *evidence* dalam hal ini adalah kebijakan disusun berdasarkan bukti atau fakta yang terjadi, dalam hal ini adalah isu kesehatan; (2) kolaboratif, perlu kebersamaan dan Kerjasama lintas Lembaga secara sinergi untuk mengatasinya; (3) tiga S: *Smart-Speed-Solidarity*, memerlukan Langkah yang cerdas, cepat, dan mengutamakan kemanusiaan; (4) mencermati risiko saat ini dan ke depan, baik makro dan mikro, sehingga perlu menggunakan prinsip GRC: *governance, risk, compliance* (Nugroho, 2020a).

Keamanan Siber

Istilah siber berasal dari kata *cyberspace* yang artinya ruang maya atau dunia maya. Ruang maya atau dunia maya terbentuk dari interaksi manusia melalui jaringan internet. Saat ini keamanan siber telah menjadi masalah kepentingan *global* terlebih di masa pandemi Covid-19. Hal ini dikarenakan perubahan kehidupan sosial dari interaksi manusia secara *online* (ruang siber) sering kali menemui kerawanan dan kejahatan. Kerawanan dan kejahatan yang muncul salah satunya menyangkut aspek keamanan informasi organisasi, pencurian data, beredarnya berita bohong, dan kerusakan lainnya. Sebagai upaya untuk mencegah, mendeteksi dan merespon kerawanan dibutukan keamanan siber.

Banyak literatur mendefinisikan keamanan siber secara berbeda-beda. *International Telecommunication Union* (ITU) mendefinisikan keamanan siber adalah kumpulan perangkat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan siber dan organisasi serta aset pengguna. Bayuk et.al (2012) mendefinisikan keamanan siber sebagai metode dengan menggunakan orang, proses dan teknologi untuk mencegah, mendeteksi, dan memulihkan dari kerusakan terhadap kerahasiaan, keutuhan, dan ketersediaan informasi di ruang siber (Bayuk, 2012).

Istilah keamanan siber sering digunakan secara bergantian dengan istilah keamanan informasi. Namun kedua-nya memiliki tujuan yang berbeda. Keamanan

informasi memiliki tujuan untuk memastikan keberlangsungan bisnis dan meminimalisir bencana bisnis dengan membatasi dampak dari insiden keamanan. ISO/EIC 27002 (2005) mendefinisikan keamanan informasi sebagai upaya menjaga kerahasiaan, keutuhan dan ketersediaan informasi (ISO, 2005). Sedangkan Whitman dan Mattord (2009) dalam penelitiannya mendefinisikan keamanan informasi sebagai pelindungan informasi dan unsur-unsur pentingnya termasuk sistem dan perangkat keras yang menggunakan, menyimpan dan mentransmisikan informasi tersebut (Whitman ME, 2009).

Dari kedua definisi di atas, walaupun memiliki kemiripan, keamanan siber dan keamanan informasi adalah dua hal yang berbeda. Dalam sebuah penelitian perkembangan ruang siber dinyatakan bahwa Keamanan siber lebih luas dari pada keamanan informasi dan/atau keamanan TIK yang dicakupnya (Solms & Niekerk, 2013). Berdasarkan definisi-definisi di atas, upaya organisasi atau negara terhadap ancaman dan serangan yang muncul terhadap informasi dan ruang siber di negara atau organisasi melalui keamanan siber di masa pandemi ini adalah suatu kebijakan organisasi atau negara. Jadi, keamanan siber adalah wujud *policy* atau kebijakan terhadap organisasi atau negara untuk melindungi asset atau informasi organisasi atau negara.

Gambar 5. *Framework Core Cybersecurity*

Sumber: NIST, 2018

NIST telah merancang kerangka kerja keamanan siber yang merupakan pendekatan berbasis resiko untuk mengelola resiko keamanan siber yang terdiri dari tiga bagian yaitu *framework core, framework implementation* dan *framework profiles* (NIST, 2018). *Framework Core* adalah serangkaian aktivitas keamanan siber, hasil yang diinginkan, dan referensi yang berlaku umum bagi seluruh sektor infrasktur vital. *Framework* ini menyajikan standar, pedoman, dan praktik industri yang memungkinkan seluruh organisasi saling berinteraksi untuk mewujudkan keamanan siber. *Framework Core* terdiri dari lima fungsi yang berkaitan dan berkelanjutan yang meliputi *Identify*, *Protect*, *Detect*, *Respond*, *Recover.*

- *Identify* adalah mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, orang, aset, data dan kemampuan.
- *Protect* adalah mengembangkan dan menerapkan pelindungan yang tepat untuk memastikan keterlayanan.
- *Detect* adalah mengembangkan dan mengimplementasikan aktivitas yang tepat untuk mengidentifikasi terjadinya kejadian keamanan siber.
- *Respond* adalah mengembangkan dan mengimplementasikan aktifitas yang tepat untuk mengambil tindakan terkait insiden keamanan siber yang terdeteksi.
- *Recover* adalah mengembangkan dan mengimplemntasikan aktifitas yang sesuai untuk mempertahankan rencana ketahanan dan memulihkan kemampuan atau layanan yang terganggu akibat kejadian keamanan siber.

Penggunaan *framework* NIST dapat digunakan oleh organisasi atau negara untuk mengelola risiko keamanan siber pada organisasi atau negara yang akan dituangkan ke dalam kebijakan keamanan siber organisasi atau negara.

Kebijakan Keamanan Siber

Ruang siber telah menciptakan peningkatan produktifitas melalui melalui informasi yang terdistribusi secara efektif setiap saat. Meningkatnya arus informasi melalui ruang siber tanpa disadari akan menimbulkan kerawanan terhadap informasi dan di sinilah persyaratan keamanan amat diperlukan untuk menghindari adanya *loss* atau kerusakan terhadap informasi yang melewati ruang siber. Titik temu kebutuhan beraktivitas di ruang siber dengan persyaratan sebuah keamanan adalah kebijakan keamanan siber. Kebijakan keamanan siber disajikan sebagai sesuatu yang mengkodifikasi tujuan keamanan untuk mendukung konstituen, yang diharapkan dapat mengubah perilaku konstituen sesuai dengan kebijakan untuk menghasilkan keamanan siber (Bayuk, et.al., 2012).

Bayuk et.al menyatakan bahwa tujuan dari kebijakan keamanan siber adalah mengubah perilaku penggunanya untuk menciptakan kondisi keamanan siber melalui berbagai upaya terarah. Kebijakan keamanan siber berbeda dengan standar karena pada dasarnya standar mengikuti kebijakan keamanan siber atau standar harus sesuai dengan kebijakan keamanan siber. Kebijakan keamanan siber juga berarti dapat mengacu kepada hukum dan regulasi yang berkaitan distribusi informasi, pelindungan privasi informasi organisasi, pengendalian teknologi terhadap operasional komputer, dan variabel pembentuk perangkat elektro-nik (Gallaher, 2008).

Beberapa negara memiliki definisi tersendiri tentang kebijakan keamanan siber. US mendefinisikan kebijakan keamanan siber mencakup strategi, kebijakan, dan standar mengenai keamanan dan operasi di ruang siber, mencakup pengurangan ancaman, pengurangan kerentanan, pence-gahan, kerjasama internasional, tanggap insiden, ketahanan, dan kebijakan serta kegiatan pemulihan, termasuk operasi jaringan komputer, jaminan informasi, penegakan hukum, diplomasi, militer, dan misi intelijen yang berkaitan dengan keamanan dan stabilitas infrastruktur informasi dan komunikasi global (Hathaway, M, 2009).

Kebijakan keamanan siber diadopsi oleh kelembagaan pemerintah sesuai dengan domain tata Kelola yang sesuai. Pada dasarnya kebijakan keamanan siber suatu negara akan mencakup semua warga negara termasuk pelaku bisnis asing yang beroperasi di negara tersebut, Adapun kebijakan keamanan siber perusahaan hanya akan berlaku untuk staf atau yang bekerjasama dengan perusahaan atas perjanjian hukum. Hal ini dikarenakan tujuan keamanan negara dengan perusahaan tentu berbeda sehingga pernyataan kebijakan dan aktivitas yang diharapkan terkait dalam mendukung kebijakan pasti akan berbeda. Untuk itu domain kebijakan keamanan siber dapat terdiri dari:

a. Hukum dan Regulasi
b. Kebijakan organisasi
c. Operasional teknologi
d. Konfigurasi teknologi

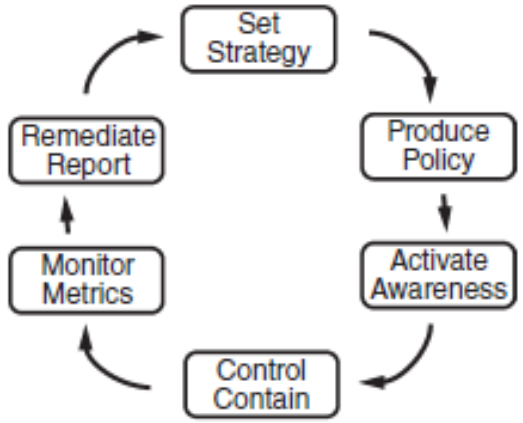
Kebijakan keamanan siber tidak statis dan harus sefleksibel ruang siber itu dirancang untuk melindungi dan mengelola. Seringkali, pemerintah tidak dapat beradaptasi dengan perubahan yang cepat dan cepat tertinggal dengan kebijakan publik lainnya sementara strategi serangan, sistem, dan pendidikan dan kesadaran manusia terus berkembang. Kebijakan keamanan siber diadopsi oleh Lembaga pemerintah sebagai metode untuk mencapai tujuan keamanan. Peran kebijakan adalah menyediakan dasar kerangka sebagai aturan agar perilaku yang diharapakan menjadi keamanan siber.

Walaupun beberapa perusahaan telah menggunakan standar internasional seperti NIST atau ISO, namun standar itu sendiri bukanlah kebijakan. Standar adalah *accepted best practice* yang berisi persyaratan dan panduan proses sesuai dengan rekomendasi pengawasan teknologi.

Kebijakan siber adalah salah satu bagian dari program keamanan organisasi

secara keseluruhan yang mencakup aturan dan mekanisme penegakan aturan (Amoros, 2010). Setiap badan pengatur yang menetapkan kebijakan juga harus menetapkan mekanisme pemantauan untuk menentukan apakah tujuan keamanan dipenuhi oleh kebijakan.

Gambar 6. Siklus Manajemen Keamanan Siber
Sumber: Bayuk et.al., 2012



Dalam Gambar 6 mengilustrasikan bahwa kebijakan mengalir dari strategi keamanan siber keseluruhan organisasi. Kebijakan diarahkan untuk dapat mengubah perilaku individu melalui kesadaran tentang pentingnya keamanan siber. Kebijakan juga harus berubah secara periodik (*periodally change)* sesuai dengan perubahan misi organisasi dan perubahan *threat* dan *vulnerability* yang berkembang. Menguatkan teori di atas, OECD (2012) menyatakan bahwa kebijakan keamanan siber yang baik dari sebuah organisasi menggambarkan tata kelola organisasi yang baik dan negara yang baik (Oecd, 2012).

C. Metode Penelitian

Penelitian ini menggunakan metode systematic review dengan menggunakan metode PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-analysis*). Alasan peneliti menggunakan metode ini adalah karena peneliti ingin mengetahui kondisi ruang siber selama pandemi covid-19 dan upaya respon yang telah dilakukan beberapa negara melalui tinjauan literatur secara sistematis. Peneliti fokus pada pertanyaan penelitian tentang kondisi ruang siber selama pandemi Covid-19 dan upaya respon yang telah dilakukan pada beberapa negara. Data diperoleh dengan mengidentifikasi semua studi yang relevan kemudian melakukan penilaian kritis terhadap penelitian dan analisis-analis yang jelas dari hasi studi yang memenuhi syarat. Pendekatan PRISMA dilakukan dengan mendefinisikan kriteria kelayakan, mendefinisikan sumber informasi, memilih literatur, mengumpulkan data, dan pemilihan item data.

Kriteria kelayakan dilakukan dengan menjadikan rujukan dari buku-buku, hasil riset dan kajian baik dalam bahasa Indonesia atau bahasa inggris. Artikel tersebut tentunya terkait dengan substansi keamanan siber, kebijakan publik, kebijakan keamanan siber, dan Covid-19 yang relevan dengan penelitian ini.

Mendefiniskan sumber informasi dilakukan dengan proses pencarian literatur pada *database online* melalui *Google Scholar* dan sumber elektronik lainnya. Dalam pemilihan literatur, penulis menentukan berdasarkan perpaduan kata kunci covid-19, keamanan siber, kebijakan keamanan siber, dan kebijakan publik. Eksplorasi dilakukan penulis dengan pemilihan judul, abstrak, dan kata kunci yang diperoleh dari hasil pencarian berdasarkan kelayakan.

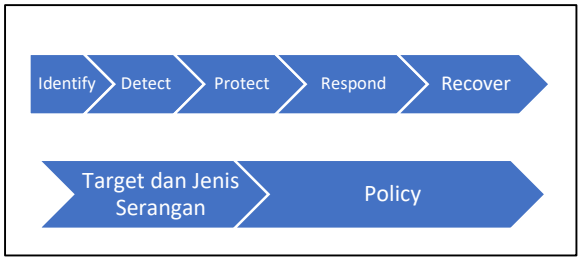
Dalam tahap pengumpulan data, penulis melakukannya secara manual melakukan ekstrasi berdasarkan tipe artikel, nama jurnal prosiding, tahun, topik, judul, kata kunci dan metode penelitian. Hingga dalam tahap akhir pemilihan item data yang didapatkan dari artikel-artikel terpilih. Studi terdahulu dari proses penyaringan yang terkait dengan penelitian ini terdapat 10 artikel terpilih yang terkait.

Berdasarkan tahap pendekatan tersebut peneliti menganalisis dengan mendeskripsikan kondisi ruang siber selama pandemi Covid-19 dari beberapa jurnal. Upaya mendeskripsikan kondisi ruang siber

ini merupakan bagian dari *Identify* dan *Detect* dalam *framework core cybersecurity* NIST.

Berdasarkan kajian literatur, peneliti menganalisis target serangan, jenis serangan dan relevansinya dengan respon yang telah diberikan pada beberapa negara. Peneliti merekonstruksi hasil review dan temuan tersebut untuk disistematiskan dalam pembahasan dari artikel ini yang dikaitkan dengan teori kebijakan publik. Berdasarkan teori kebijakan publik, peneliti merekomendasikan metode dan model dalam memproduksi kebijakan publik secara efektif dan efisien di Indonesia.

Gambar 7. Framework Analisis



D. Pembahasan

Dalam Analisis, peneliti menggunakan *Framework Core Cybersecurity* NIST yang meliputi *Identify, Detect, Protect, Respond, dan Recover*. *Identify dan Detect* dilakukan dengan mendeskripsikan kondisi ruang siber baik target atau jenis serangan selama pandemi Covid-19 yang menjadi trend di dunia dan membandingkannya dengan *tren* serangan siber yang ada di Indonesia.

Protect, Respond, dan Recover adalah upaya dilakukan terhadap target dan jenis serangan yang terjadi dalam bentuk policy (kebijakan). Peneliti membandingkan upaya yang telah dilakukan berdasarkan kajian literatur dengan upaya yang telah dilakukan di Indonesia dan menguraikan cara terbaik kebijakan keamanan siber disusun berdasarkan teori kebijakan publik.

Kondisi Ruang Siber Selama Pandemi Covid-19: Target Serangan Siber

Pandemi Covid-19 telah meningkatkan aktivitas manusia secara *online*. Hal ini diperkuat oleh data yang disajikan APJII bahwa selama pandemi terjadi peningkatan penggunaan internet di Indonesia mencapai 73,7% dari jumlah penduduk Indonesia.

Hal ini pula yang telah membawa perubahan fokus bagi para pelaku kejahatan siber dengan menargetkan kejahatannya pada pengguna akhir (*end user*). Hal ini dikarenakan sebagian sistem pengguna tidak memiliki pelindungan yang memadai untuk menghadapi dinamika baru serangan siber dan perubahan bisnis. Hal ini berdampak meningkatnya serangan siber dengan memanfaatkan momentum Covid-19 pada saat orang-orang memiliki kebutuhan untuk berinteraksi secara jarak jauh melalui *online*.

Dalam Laporan Pusopkamsinas tahun 2020 disampaikan bahwa selama pandemi Covid-19, sektor pemerintah menempati urutan pertama dalam melakukan aduan siber setelah sektor ekonomi digital dan sektor infrastruktur kritis nasional (Pusat Operasi Keamanan Siber Nasional, 2021). Pusopkamsinas tidak menyebutkan entitas mana yang menjadi target serangan. Target dikelompokkan berdasarkan pengklasifikasian stakeholder yaitu pemerintah, infrastruktur kritis nasional, dan ekonomi digital.

Beda halnya dengan Khan.et.al (2020), dalam penelitiannya terdapat tiga target serangan siber selama pandemi yaitu sistem kesehatan, layanan keuangan, dan fitur pemerintah dan media (Khan et al., 2020). Alasannya adalah ketiga entitas ini memiliki pengaruh yang sangat besar atau aktor yang berhubungan dengan pandemi Covid-19. Penyerang memanfaatkan pandemi ini untuk meraih keuntungan karena pandemi telah memberikan dampak kepada perekonomian negara.

Tabel 2. Target dan Motif Serangan Siber

No	Target	Motif
1.	Sistem Kesehatan	Layanan Kesehatan menjadi target serangan karena telah berkembangnya sistem e-healthcare khususnya pada masa pandemi ini. Serangan berupa malicious malware, DDoS
2.	Layanan Keuangan	Akibat pandemi, resesi keuangan terjadi yang menyebabkan industry keuangan rawan terhadap seranga siber seperti phishing, malware atau ransomware.
3.	Fitur Pemerintah dan Media	Akibat pandemi, pemerintah dan media diharapkan dapat memberikan informasi yang akurat dan cepat kepada publik, namun disisi lain penyerang dan hacker melakukan serangan siber pada fitur pemerintah dan media untuk menyebarkan berita bohong kepada masyarakat

Sumber: Hasil Pengolah Data

Chigada dan Madzinga (2020) memiliki pendapat yang sama dengan Khan dimana mereka menelaah data laporan keamanan siber dari Desember 2019 hingga Juni 2020 menemukan bahwa perusahaan besar, Industri Kesehatan, dan Lembaga Pemerintah menjadi target dari serangan dan ancaman siber selama pandemi (Chigada & Madzinga, 2020). Motif serangan berbeda-beda dengan memanfaatkan rasa khawatir, cemas, ketakutan pengguna, dan keingin-tahuan pengguna terhadap perkembangan Covid-19.

Pranggono dan Arabo (2020) menyatakan bahwa motif serangan siber selama pandemi Covid-19 didasari oleh motif komersial atau mengumpulkan informasi yang berhubungan dengan vaksin Covid-19. Serangan ini menyasar kepada Lembaga Kesehatan, perusahaan obat, dan lembaga penelitian dengan alasan masih banyak organisasi kesehatan yang tidak memiliki perhatian penting kepada aspek keamanan.

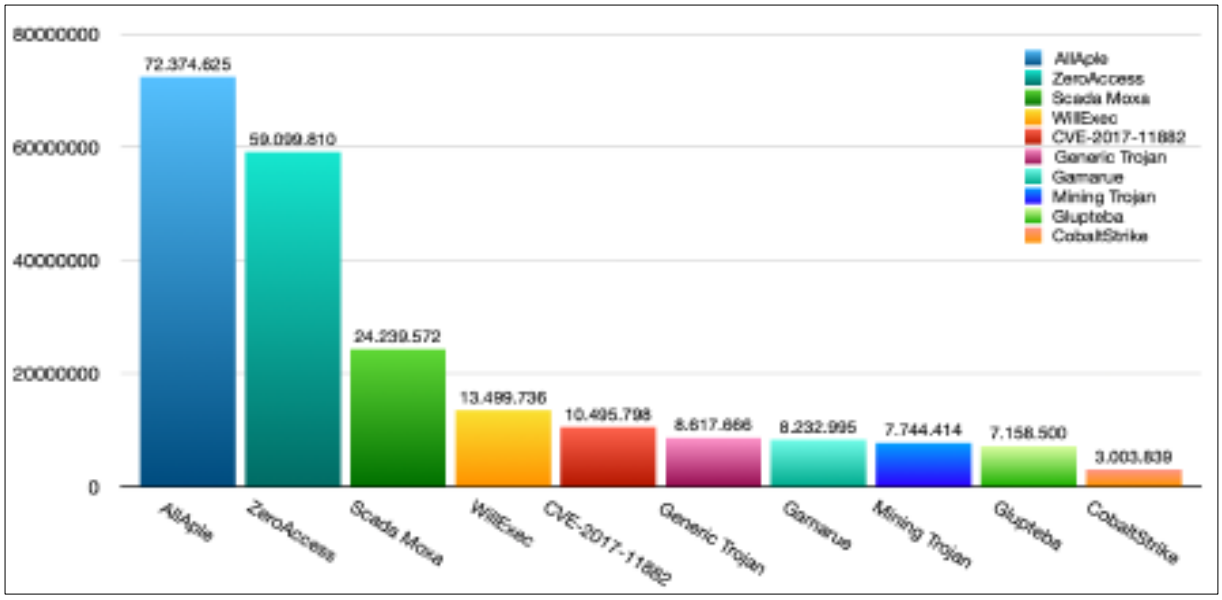
Berdasarkan telaah literatur, peneliti menyimpulkan selama pandemi covid-19, target serangan siber menyasar kepada sistem kesehatan, layanan keuangan/ finansial, dan pemerintahan. Motif didasari untuk mencari keuntungan.

Jenis Serangan Siber Selama Pandemi Covid-19

Atas dasar motif dan target serangan, pelaku menggunakan berbagai macam jenis serangan. Mereka melakukan penipuan melalui *social engineering* dimana penipu memanfaatkan faktor manusia seperti keputusasaan, kepanikan, ketakutan, dan ketidaktahuan untuk menyebarkan kode berbahaya yang menyamar sebagai informasi otentik terkait Covid-19.

Pusopkamsinas melaporkan bahwa selama pandemi jenis serangan yang terjadi di Indonesia adalah *phising*, *ransomware*, dan kebocoran data. *Malware Allaple* dan *ZeroAccess* menempati urutan pertama dan kedua dalam top ten anomali.

Gambar 10. Top 10 Anomali Tahun 2020



Sumber: Laporan Pusopkamsinas, 2021

Dalam Penelitian yang dilakukan oleh Okereafor dan Adeliye disebutkan pada tahun 2020 terdapat trend enam jenis serangan yang terjadi selama pandemi covid-19 di dunia antara lain: *Spear phishing dan email spam, malware, website highjack, website cloning, cyber espionage,* dan *cyber bullying* (Okereafor & Adelaiye, 2020). Karena lingkup serangan siber tidak dibatasi batas negara, dapat dimungkinkan jenis serangan yang sama terdapat juga di Indonesia. Namun upaya meresponnya disesuaikan dengan kondisi Indonesia.

Tabel 3. Jenis Serangan Siber Popular Selama Pandemi Covid-19

No	Jenis serangan	Dampak
1.	**Spear phishing dan email spam** Email yang tidak diminta dan menipu yang meniru merek terkenal dan tokoh terkenal, dengan maksud untuk mengekstrak informasi rahasia atau menyebarkan malware lainnya	• Kebocoran data • Perubahan data • Kehilangan data • Pelanggaran privasi • Sistem Crash • Pencurian identititas • Kehilangan reputasi • Kehilangan pendapatan • Gangguan layanan • Inefisiensi operasional • Denda • Pengungkapan publik • Litigasi • Skandal dan kematian
2.	**Malware** Kode perangkat lunak yang berbahaya dan mengganggu yang menyebabkan kerusakan dan hasil yang tidak diinginkan pada komputer atau aset digital korban termasuk akses tidak sah dan perubahan data ilegal. Misalnya. ransomware, virus komputer, adware, spyware, worm, trojan, dll.	
3.	**Website highjack** Pengambilalihan situs web dengan memperoleh kendali administratif penuh atas seluruh konten situs web dengan maksud memposting konten yang menyinggung dan propaganda ideologi	• Permintaan tebusan • Konten rusak • Deep fakes • Berita palsu • Skandal • Image smearing • Gangguan layanan • Gangguan pekerjaan • Kehilangan reputasi
4.	**Website Cloning** Duplikasi secara ilegal situs web korban dengan tujuan menipu pengguna dengan mengalihkan permintaan web sah mereka ke situs web kloning untuk mendapatkan informasi rahasia untuk mencari keuntungan	
5.	**Cyber espionage** Penggunaan teknik *online* untuk memata-matai perilaku digital atau transaksi *online* seseorang atau organisasi perusahaan melalui rekayasa sosial, spyware, shoulder surfing, cyber stalking, man-in-the-middle, brute-force, keylogging, atau metode lain	• Pencurian identitas • Pelanggaran privasi • Image smearing
6.	**Cyber bullying** Penggunaan aset digital untuk kejahatan dengan melecehkan atau menyebarkan kebohongan dan konten yang menyinggung terhadap individu, kelompok, atau organisasi perusahaan, dengan bersembunyi di bawah anonimitas platform *online*, blog, dan forum.	• Skandal • Gangguan individu • Gangguan layanan • Kehilangan reputasi • Libel • Ujaran kebencian

Sumber: Hasil Pengolahan Data

Respon terhadap Serangan Siber

Akibat meningkatnya serangan siber, organisasi berperan memberikan respon terhadap hal dan dampak yang akan atau telah terjadi dan menggunakan sumber-dayanya untuk mencegah insiden. Hal ini dikarenakan setiap insiden berpotensi menimbulkan dampak yang luas kepada organisasi bahkan negara. Pada tabel di bawah ini Okereafor dan Adelaiye (2020) menjelaskan beberapa upaya penanggulang-an dan pencegahan dari setiap jenis serangan siber.

Pada Tabel 4 upaya respon dan pencegahan dapat melalui respon operasio-nal teknis, *policy* (kebijakan), dan *training* (pelatihan) (Okereafor & Adelaiye, 2020). Di samping beberapa upaya pada Tabel 4, terdapat beberapa rekomendasi yang dirangkum dari NCSC dan CISA yang dapat dilakukan oleh organisasi (Pranggono & Arabo, 2020):

1) Berikan Pendidikan kepada pengguna pentingnya keamanan siber. Hal ini dapat dilakukan melalui training kesadaran keamanan siber (*cyber-security awareness*)
2) Gunakan *Virtual Private Network* terhadap aktivitas anggota organisasi yang menyangkut data/informasi terbatas organisasi
3) Gunakan dan aktifkan *Multifactor Authentication* sebagai otentikasi ganda dalam sebuah sistem

4) Pastikan semua perangkat lunak atau aplikasi diupdate secara berkala
5) Pastikan semua anti *malware* terupdate secara berkala
6) Implementasikan kebijakan sistem *online* pada perusahaan secara ketat
7) Lakukan segmentasi dan separasi/ pemisahan pada beberapa sistem
8) Implementasikan keamanan fisik secara ketat pada lingkungan kantor untuk mencegah adanya penyusupan atau akses fisik ilegal

Tabel 4. Upaya Penanggulangan dan Pencegahan serangan siber

No	Jenis serangan	Upaya Penanggulangan dan Pencegahan
1.	Spear phishing dan email spam	• Intrusion detection • Intrusion prevention • Antivirus • Kesadaran keamanan siber • Pelatihan tentang keamanan • Endpoint protection • Perimeter protection • Firewalling • Proper encryption • Steganografi • Machine learning • Anomali detection
2.	Malware	
3.	Website highjack	• Proper encryption • Sound Password ethics • Otentikasi bimoterik • Oktentikasi multifactor • Steganografi • Honeypot
4.	Website Cloning	• Publik disclaimer • Corporate damage control • Kesadaran keamanan siber
5.	Cyber espionage	• Counter espionage • Anti espionage • Perangkat monitoring jaringan • Otentikasi biometric • Sound Password ethics • Kesadaran keamanan siber • Antivirus • Onine ethics • Intrusion detection • Firewalling
6.	Cyber bullying	• Publik disclaimer • Soundpassword ethics • Kesadaran keamanan siber • *Online* ethics

Sumber: Okereafor & Adelaiye, 2020

Lain halnya dengan *Deloite Global Technologi* sebagai perusahaan konsultan internasional merekomendasikan strategi keberlangsungan Deloite sebagai skenario menghadapi isu perubahan guncangan organisasi akibat pandemi dengan merekomendasikan tiga strategi:

1) Strategi penanggulangan, dapat dilakukan melalui:
   - Mereview *business continuity* (BC)/ *disaster recovery plans* (DRP);
   - Membangun fungsi manajemen krisis
   - Mengembangkan rencana komunikasi
2) Pengelolaan Personil (Kesehatan dan keselamatan), dapat dilakukan melalui:
   - Menegakkan Tindakan pencegahan dan merevisi kebijakan cuti;
   - Mereview atau mengubah kebijakan *work from home*;
   - Merencanakan absensi
3) Keberlangsungan operasi, dapat dilakukan melalui:
   - Merasionalisasi proyek dan portofo-lio teknologi;

- Melengkapi koneksi, keamanan infrastruktur untuk *traffic* baru dan pola penggunaan beberapa negara dan organisasi dalam menghadapi ancaman dan serangan siber menandakan pentingnya sebuah negara memberikan respon terhadap berbagai ancaman yang mengganggu masyarakatnya terlebih dalam situasi krisis ini sebagai wujud pelindungan negara terhadap masyarakatnya.

Respon Indonesia tentang Kebijakan Keamanan Siber di Masa Pandemi

Indonesia belum memiliki Undang-Undang (*act*) yang mengatur khusus tentang keamanan siber. Walaupun demikian, hal-hal pelindungan penyelenggaraan sistem elektronik telah diatur dalam UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). UU ITE dilandasi salah satunya bahwa "pemerintah mendukung pengembangan teknologi informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai agama dan sosial budaya masyarakat Indonesia" (Undang-Undang Republik Indonesia, 2008). UU ITE mengatur tentang penyelenggaraan sistem elektronik yang didalamnya mengatur tentang kewajiban penyelenggara sistem elektronik dan perbuatan yang dilarang yang berkaitan dengan transaksi elektronik.

Undang-Undang ITE dapat dikatakan sebagai kebijakan publik formal dan model kebijakan prosedural terkait keamanan siber Indonesia. Kebijakan publik formal karena UU merupakan instrumen kebijakan publik yang dibuat secara formal atau legal. Sedangkan model kebijakan prosedural karena kebijakan ini dibuat berdasarkan aturan resmi dari negara. UU ITE mengatur penyelenggaraan informasi dan transaksi elektronik dan selayaknya UU ini dapat diimplementasikan dalam kondisi apapun di Indonesia khususnya saat krisis.

Selain peraturan perundang-undangan, Indonesia telah memiliki Lembaga yang memiliki kewenangan di bidang keamanan siber yaitu Badan Siber dan Sandi Negara (BSSN). Dalam model kebijakan publik, BSSN merupakan model kebijakan publik institutional terkait keamanan siber. Pemerintah melalui BSSN sah membuat kebijakan publik, karena fungsi tersebut bersifat universal dan memang Pemerintahlah yang dapat memonopoli fungsi pemaksaan (koersi) dalam kehidupan bersama (Dye, 2011). Pemerintah atau Negara menginstitusionalkan kebijakan publiknya melalui pembentukan BSSN dilatarbelakangi oleh adanya suatu cita-cita meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional.

Hal ini mengisyaratkan kebijakan publik pemerintah didasari oleh nilai luhur tujuan nasional yaitu melindungi segenap bangsa Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial. Tugas BSSN adalah melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber.

Pandemi Covid-19 telah merubah multi dimensi kehidupan manusia dari interaksi secara tatap muka menjadi interaksi secara *online* (jarak jauh). Hal ini tentunya meningkatkan interaksi masyarakat melalui jaringan internet. Merespon isu kerawanan, ancaman dan serangan siber di Indonesia, BSSN mengeluarkan beberapa kebijakan pernyataan publik kepada masyarakat untuk mengantisipasi ancaman dan kerawanan siber. Beberapa kebijakan tersebut disajikan dalam Tabel 5.

Tabel 5. Rilis BSSN

Substansi Kebijakan	Respon Serangan
Antisipasi Fake News dan Malware : Peta Palsu sebaran Covid-19 yang terdapat malware AZORult	Website Highjack, Website Cloning
Panduan Keamanan Work From Home	Spear phising&email spam, malware, website highjack, website cloning, cyber espionage, cyber bullying
Imbauan adanya Spyware Massad Clipper and Stealer	Spear phising&email spam, malware
Imbauan Bahaya Ransomware Berkedok Informasi Covid-19	Spear phising&email spam, malware
Imbauan Kepada Penyelenggara sistem elektronik untuk antisipasi terjadi insiden siber	Spear phising&email spam, malware, website highjack, website cloning, cyber espionage
Imbauan Phishing dan Hoaks Informasi Covid-19	Spear phising&email spam, malware, website cloning, cyber espionage,
Imbauan Waspada Covidlock Malware	Spear phising&email spam, malware
Imbauan Jangan Asal Klik sembarang tautan	Spear phising&email spam, malware, website highjack, website cloning, cyber espionage, cyber bullying
Imbauan Keamanan Waspada Corona Virus APPS	Spear phising&email spam, malware
Tips Aman lindungi Aplikasi Video Conference	cyber espionage
Panduan Keamanan Pemanfaatan Aplikasi Video Conference	cyber espionage
Buku Putih Mitigasi Insiden Siber Saat Pandemi Covid-19	Spear phising&email spam, malware, website highjack, website cloning, cyber espionage
Peringatan Corona Virus Malware	Spear phising&email spam, malware
Tanda Tangan Elektronik Mendukung WFH	cyber espionage
Digitalisasi Perkantoran	cyber espionage
Tips Aman belanja online sambil rebahan	Spear phising&email spam, malware, website highjack, website cloning, cyber espionage, cyber bullying
Imbauan security alert SMS WORM Corona Safety Mask.apk	Spear phising&email spam, malware

Sumber: Hasil Olah data Rekapitulasi Rilis BSSN selama tahun 2020

Respon BSSN dengan rilis tersebut menandakan bahwa Pemerintah atau Negara hadir untuk melindungi segenap bangsa Indonesia dari setiap ancaman dan kejahatan siber pada masa pandemi Covid-19. Rilis BSSN adalah kebijakan publik pemerintah di bidang keamanan siber sebagai bentuk respon terhadap ancaman dan serangan siber di Indonesia belum melibatkan partisipasi aktif elemen terkait dalam menyikapi ancaman dan serangan siber. Sehingga belum mendapatkan dukungan beberapa pihak terkait agar rilis ini dikampanyekan dan diimplementasikan secara massif untuk mengantisipasi ancaman.

Dalam tugas yang diemban BSSN, Pemerintah pun sebenarnya sudah mengatur strategi yang perlu dilaksanakan oleh BSSN yaitu dengan "*memanfaatkan, mengembang-kan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber*". Kalimat tugas BSSN dalam Perpres 53/2017 bukanlah sekedar kata-kata formal namum memuat strategi yang memang sudah diatur oleh Pemerintah. Strategi adalah cara (*ways*) BSSN untuk mencapai tujuan. Strategi BSSN ini selayaknya dapat menjadi panduan bagi BSSN dalam merumuskan kebijakan publiknya di bidang keamanan siber sebagaimana tertuang dalam *cybersecurity management cycle* Bayuk (2007) bahwa "*Cyber security policy articulates the strategy for cyber security goal achievement and provides its constituents with direction for the appropriate use of cyber security measures*".

Mengembangan Kebijakan yang Unggul di Masa Pandemi Covid-19 di Indonesia

Bayuk (2007) telah menjelaskan dalam *cybersecurity management cycle*

bahwa untuk menyusun kebijakan keamanan siber, organisasi terlebih dahulu menetapkan strategi atau dengan kata lain kebijakan keamanan siber adalah strategi mencapai tujuan keamanan siber dan memberikan arahan kepada konstituennya untuk menggunakannya secara tepat atas langkah-langkah keamanan siber.

Respon negara menghadap krisis yang disebabkan oleh pandemi harus cepat, efektif dan efisien. Respon negara pada dasarnya tergantung pada bagaimana negara merumuskan kebijakan publiknya yang unggul sehingga Indonesia dapat melewati masa pandemi ini dengan baik. *Ways* BSSN "*memanfaatkan, mengembangkan, dan mengonsolidasikan unsur-unsur keamanan siber"* perlu dioptimalkan dengan cara sebagai berikut:

1) *Memanfaatkan unsur-unsur keamanan siber*, caranya adalah dalam merumuskan dan melaksanakan kebijakan publiknya, BSSN mengoptimalkan pihak yang terkait dalam merumuskan kebijakan publiknya sesuai domain yang menjadi tanggung jawabnya dan mengarahkan serta mengoordinasikan pihak terkait untuk mengimplementasikan kebijakan publik BSSN. Unsur terkait keamanan siber sebagaimana dalam NCSFM NATO tentang 5 (lima) mandat keamanan siber nasional, adalah lembaga yang memiliki kewenangan dalam 5 (lima) mandat keamanan siber nasional meliputi (Klimburg, 2012):
   - *military cyber*,
   - *counter cybercrime*,
   - *intelligence and counter intelligence*,
   - *critical infrastructure protection and national crisis management*, dan
   - *cyber diplomacy and internet governance*.
2) *Mengembangkan unsur-unsur keamanan siber*, caranya adalah dalam merumuskan dan melaksanakan kebijakan publiknya, BSSN dapat meningkatkan kapabiltas dan kapasitas pihak terkait agar bersama BSSN dapat mengimplementasikan kebijakan publik,
3) *Mengonsolidasikan unsur-unsur keamanan siber*, caranya adalah dalam merumuskan dan melaksanakan kebijakan publiknya, BSSN dapat berkolaborasi dengan unsur terkait dalam mengimplementasikan kebijakan publiknya. Kolaborasi Pentahelix dapat menjadi suatu strategi kolaborasi sinergis yang diharapkan dapat mewujudkan suatu inovasi yang didukung oleh berbagai sumber daya yang saling berinteraksi secara sinergis

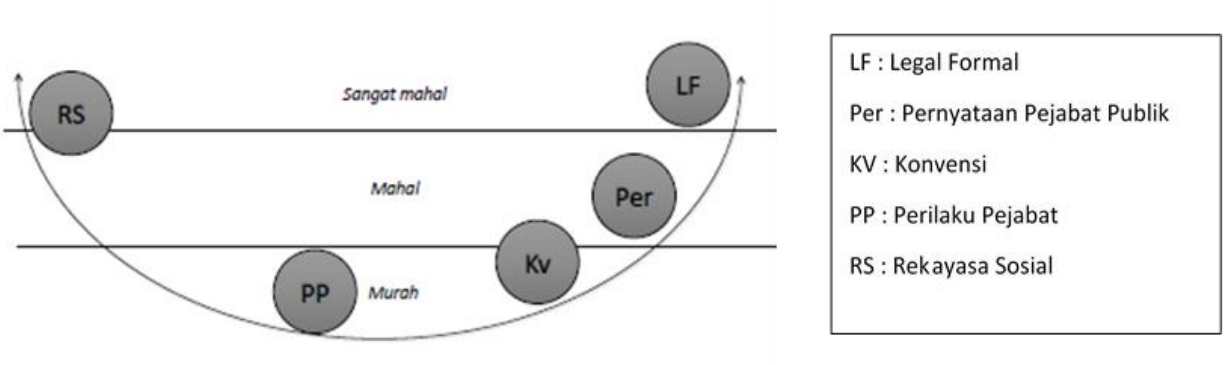
Dengan *ways* yang telah dimilikinya, prinsip kebijakan keamanan siber yang dapat menjadi dasar bagi BSSN adalah:

1. Kebijakan berbasis resiko dan proporsional
   Kebijakan yang diproduksi oleh pemerintah dapat menjawab resiko yang dihadapi masyarakat selama pandemi Covid-19. Tren resiko keamanan siber yang saat ini dihadapi beberapa negara dapat menjadi bahan bagi pemerintah untuk Menyusun kebijakan berbasis resiko. Kebijakan yang disusun juga harus dapat menjawab isu yang saat ini terjadi dan didasarkan pada pemahaman menyeluruh tentang ancaman, kerentanan, dan konsekuensi potensial yang dihadapi negara. Pemerintah harus mengembangkan kerangka kerja dan sistem yang proporsional dan dirancang khusus untuk mengatasi ancaman, kerentanan, dan konsekuensi potensial akibat pandemi Covid-19. Resiko sangat dinamis dan senantiasa berubah. Sehingga kebijakan dengan mempertimbangkan kerangka kerja berbasis risiko yang proporsional yang memungkinkan organisasi untuk berinovasi dan dapat mengadopsi teknologi baru sehingga negara dapat terhindar dari resiko keamanan siber yang tidak perlu.
2. Kebijakan yang berfokus pada hasil
   Kebijakan memiliki fokus kepada keadaan akhir yang diinginkan daripada menentukan cara untuk mencapainya serta senantiasa mengukur kemajuan dari implementasi kebijakan yang

dilakukan. Kebijakan yang diproduksi mampu menjawab tantangan masyarakat menghadapi ancaman dan serangan siber di masa pandemi sekaligus *enabler* utama aktivitas masyarakat di ruang siber.

3. Kebijakan yang memiliki prioritas
   Dalam keamanan siber, tidak semua ancaman sama. Kebijakan keamanan siber harus mengadopsi pendekatan bertahap terhadap aspek kritis yaitu dengan dengan memprioritaskan risiko terhadap infrastruktur kritis. Dalam pandemi Covid-19 ini, sektor Kesehatan merupakan infrastruktur kritis yang perlu mendapatkan perhatian penting.
4. Kebijakan yang praktis dan realistis.
   Kebijakan keamanan siber tidak akan bernilai jika diterapkan pada organisasi yang tidak semestinya dan tidak memiliki otoritas terhadap keamanan siber. Dalam implementasinya kebijakan ini harus melibatkan pihak yang berkepentingan khususnya kolabarosasi pentahelix agar kebijakan dapat dipraktikkan dan realistis
5. Kebijakan yang mengindahkan privasi, kebebasan warga negara dan supremasi hukum.
   Dalam menegakkan kebijakan ruang siber tidak boleh mengorbankan privasi, kebebasan sipil, dan supremasi hukum. Misalnya, kewenangan luas bagi pemerintah dan penegak hukum untuk mengakses data privasi tanpa mengikuti proses yang sesuai dapat merusak reputasi negara untuk supremasi hukum dan pada akhirnya dapat melemahkan kepercayaan organisasi untuk menyimpan data mereka di dalam negara tersebut. Untuk itu diperlukan pendekatan yang seimbang dengan menghormati prinsip-prinsip dasar ini.
6. Kebijakan yang mendunia atau relevan dengan kehidupan global
   Ancaman siber bersifat luas dan lintas negara. Sehingga dibutuhkan pendekatan nasional yang mengintegrasikan dengan standar internasional dengan tujuan agar terdapat keharmonisan dengan beberapa negara dalam menghadapi ancaman tersebut.

Gambar 6. Jenis Kebijakan Berdasarkan Biaya



Sumber: Nugroho, 2020

Prinsip dasar dalam kebijakan keamanan siber ini dapat menjadi acuan bagi negara dalam memproduksi kebijakan publik keamanan siber. Adapun strategi agar kebijakan ini dapat tersusun dan terimpelemtasikan dengan baik sehingga bangsa dapat melewati krisis pandemi ini adalah:

1. Menentukan jenis-jenis kebijakan publik yang akan diproduksi. Dalam pandemi ini kebijakan publik yang dibuat adalah kebijakan yang dapat menyelesaikan masalah krisis pandemi ini yang berkaitan ruang siber.

   Konvensi, pernyataan pejabat publik, dan perilaku pejabat publik dapat menjadi alternatif kebijakan publik yang

mudah dibuat dibandingkan kebijakan publik berupa legal/formal dan rekayasa sosial yang membutuhkan waktu dan biaya yang relative mahal.

2. Menentukan metode perumusan kebijakan publik. Pada masa pandemi Covid-19 ini, Respon pemerintah haruslah cepat. Karena metode perumusan kebijakan publik dengan model rasional tidak dapat dijalankan seutuhnya sehingga dikatakan memerlukan suatu kebijakan publik khusus yaitu kebijakan yang dibuat dalam kondisi sangat darurat dan cakupan akibatnya sangat luas. Isu yang dihadapi saat ini adalah terkait wabah sehingga kebijakan dapat dibuat oleh Pemerintah dengan melibatkan unsur terkait seperti pimpinan Lembaga legislatif, pakar, tokoh masyarakat. Waktu hingga pengesahan keputusan kurang dari 48 jam.
3. Karena masalah pandemi covid-19 adalah masalah kedaruratan, maka kebijakan keamaan siber di saat covid-19 dapat dinilai sebagai masa darurat yang terlihat dari meningkatnya serangan siber selama pandemi covid-19 ini.

Untuk itu model kebijakan di masa darurat didasarkan kepada aspek: (1) *evidence base*, yaitu pendekatan berbasis *evidence* dalam hal ini adalah kebijakan keamanan siber disusun berdasarkan bukti atau fakta yang terjadi, dalam hal ini adalah isu kerawanan dan serangan siber selama pandemi covid-19; (2) kolaboratif, perlu kebersamaan dan Kerjasama lintas organisasi yang berkepentingan terhadap keamanan siber di Indonesia secara sinergi untuk mengatasinya; (3) tiga S: *Smart- Speed- Solidarity*, memerlukan Langkah yang cerdas, cepat, dan mengutamakan kemanusiaan; (4) mencermati risiko saat ini dan ke depan, baik makro dan mikro, sehingga perlu menggunakan prinsip GRC: *governance, risk, compliance.*

E. Kesimpulan

Pandemi Covid-19 telah menyebabkan perubahan interaksi sosial manusia secara *online* sehingga meningkatnya aktivitas manusia di ruang siber. Hal ini memicu meningkatnya serangan siber selama pandemi dengan target serangan sistem kesehatan, layanan keuangan, dan pemerintah. Jenis serangan berbeda-beda dengan memanfaatkan faktor manusia seperti keputusasaan, kepanikan, ketakutan, dan ketidaktahuan tentang pandemi Covid-19. Pemerintah memiliki peran merespon hal ini dengan kebijakan keamanan siber sebagai strategi keamanan di ruang siber selama pandemi dengan memberikan arahan kepada pengguna untuk menggunakannya secara tepat sesuai prosedur keamanan siber.

Indonesia sudah memiliki kebijakan publik institusional dalam wadah BSSN yang merupakan wakil pemerintah yang sah merumuskan kebijakan publik di bidang keamanan siber. Selama pandemi covid-19 BSSN telah memproduksi beberapa kebijakan publiknya dalam bentuk rilis sebagai respon terhadap ancaman dan serangan siber yang terjadi selama pandemi. Namun rilis BSSN belum melibatkan pihak terkait baik dalam perumusan dan implementasinya. Untuk mengembangkan kebijakan publik unggul sebagai respon atas meningkatnya serangan siber selama pandemi direkomendasikan sebagai berikut:

1. Dalam *cybersecurity management cycle*, menetapkan stategi menjadi hal pertama bagi BSSN sebagai pondasi dasar merumuskan kebijakan publik.
2. Untuk mengefektifikan dan mengefisienkan perumusan kebijakan publiknya, BSSN dapat mengoptimalkan *ways* nya yaitu “memanfaatkan, mengembangkan, dan mengonsolidasikan unsur-unsur keamanan siber” kepada Lembaga yang memiliki kewenangan dalam 5 (lima) mandat keamanan siber nasional sehingga da-

pat bersama-sama merespon serangan siber selama pandemi Covid-19.

3. Jenis, model dan metode perumusan kebijakan publik selama pandemi perlu ditentukan untuk mempermulus tersusunnya kebijakan dan mendapatkan dukungan dengan memperhatikan prinsip dasar kebijakan keamanan siber.

Daftar Pustaka

Buku

Amoros, E. (2010). *Cyber Attacks*. Butterworth-Heinemann.

Bayuk. (2012). *Cyber Security Policy Guidebook*. John Wiley&Sons.

Dye, T. R. (2017). *Understanding Public Policy* (15th ed.). Person Education.

Gallaher, L. (2008). *Cyber Security, Economic Strategies dan Publik Policy Alternatives*. Edward Elgar

Hathaway, M, et. a. (2009). *Cyberspace Policy Review, assuring a trusted and Resillient Information, and Communication Infrastructure*. US Executive Branch.

Klimburg, A. (2012). *National Cyber Security Framework Manula*. NATO CCD COE Publication.

Nugroho, R. (2014). *Public Policy : Teori, Manajemen, Dinamika, Analisis, Konvergensi dan Kimia kebijakan* (5th ed.). Elex Media Komputindo.

Nugroho, R. (2020a). *Kebijakan Anti Pandemi Global: Kasus Covid 19* (1st ed.). Yayasan Rumah Reformasi Kebijakan.

Nugroho, R. (2020b). *Model-Model Perumusan Kebijakan Publik* (1st ed.). Yayasan Rumah Reformasi Kebijakan.

Nugroho, R. (2020c). *Perumusan Kebijakan Dalam Praktik* (1st ed.). Yayasan Rumah Reformasi Kebijakan.

Suwitri, S. (2008). Konsep Dasar Kebijakan Publik MODUL 1. In *Analisis Kebijakan Publik* (1st ed., Issue 2). Badan Penerbit Universitas Diponegoro. https://doi.org/http://dx.doi.org/10.1016/j.atmosenv.2007.12.054

Whitman ME, M. H. (2009). *Principles of Information Security* (3rd ed.). Thompson Course Technology.

Jurnal

Chigada, J., & Madzinga, R. (2020). Cyberattacks and threats during COVID-19 : A systematic literature review Coronavirus Disease-2019. *South African Journal of Information Management*, 1–11.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. *TechRxiv Powered by IEEE*, *May*, 1–6. https://www.techrxiv.org/articles/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792

Muhyi, H. A., & Chan, A. (2017). The Penta Helix Collaboration Model in Developing Centers of Flagship Industry in Bandung City. *Review of Integrative Business and Economics Research*, *6*(1), 412–417. http://buscompress.com/journal-home.html

Okereafor, K., & Adelaiye, O. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. *International Journal of Recent Engineering Research and Development (IJRERD) Www.Ijrerd.Com ||*, *05*(July), 61–72. www.ijrerd.com

Pranggono, B., & Arabo, A. (2020). COVID -19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), 1–6. https://doi.org/10.1002/itl2.247

Solms, R. Von, & Niekerk, J. Van. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Weil, T., & Murugesan, S. (2020). IT Risk and Resilience-Cybersecurity Response to COVID-19. *IT Professional*, *22*(3), 4–10. https://doi.org/10.1109/MITP.2020.2988330

Dokumen

Akamai, McKeay, M., Ragan, S., Goedde, A., & Tuttle, C. (2021). Adapting to the Unpredictable. In *State of the Internet* (Vol. 7, Issue 1). https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-research-adapting-to-the-unpredictable-report-2021.pdf

ISO. (2005). *ISO/IEC: 27002 Code of Practice for Information Security Management*. ISO.

NIST. (2018). Framework for improving critical infrastructure cybersecurity. In *Proceedings of the Annual ISA Analysis Division Symposium* (Vol. 535).

OECD. (2012). Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy. In *Organisation for Economic Co-operation and Development*. https://doi.org/http://dx.doi.org/10.1787/5k8zq92vdgtl-en

Pusat Operasi Keamanan Siber Nasional. (2021). Laporan Tahunan Hasil Monitoring Keamanan Siber 2020. In *Buletin Jendela Data dan Informasi Kesehatan*.

Undang-Undang Republik Indonesia. (2008). *UU RI Nomor 11 Tahun 2018 Tentang ITE*.

Thesis

Lindmark, A., Sturesson, E., & Nilsson-Roos, M. (2009). *Difficulties of collaboration for innovation - A study in the Öresund region* [Lund University]. http://lup.lub.lu.se/student-papers/record/1437850