LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

MENINGKATKAN KAPASITAS *NATIONAL CYBERSECURITY AUTHORITY* (NCA) KERAJAAN ARAB SAUDI UNTUK MEMPERKUAT KEAMANAN DIGITAL NASIONAL

Oleh:

KHALIL IBRAHEEM SH. ALSHAIKHI
KOLONEL ARAB SAUDI, NRP.

KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)
PROGRAM PENDIDIKAN REGULER ANGKATAN LXV
LEMHANNAS RI
TAHUN 2023

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

KATA PENGANTAR

Assalamu alaikum Wr.Wb., salam sejahtera bagi kita semua.

Dengan memanjatkan puji syukur ke hadirat Tuhan Yang Maha Esa serta atas segala Rahmat dan karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Reguler Angkatan (PPRA) telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Ilmiah Perseorangab (Taskap) dengan judul: **"MENINGKATKAN KAPASITAS NATIONAL CYBERSECURITY AUTHORITY (NCA) KERAJAAN ARAB SAUDI UNTUK MEMPERKUAT KEAMANAN DIGITAL NASIONAL"**

Penentuan Tutor dan Judul Taskap ini didasarkan oleh Keputusan Gubernur Lembaga Ketahanan Nasional Indonesia Nomor: 69 Tahun Tahun 2023 tanggal 27 Maret 2023 tentang Penetapan Judul Taskap Peserta PPRA LXV Lemhannas RI untuk menulis Taskap dengan memilih judul yang telah ditentukan oleh Lemhannas RI.

Pada kesempatan ini, perkenankanlah penulis menyampaikan ucapan terimakasih kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPRA Angkatan LXV tahun 2023. Ucapan yang sama juga disampaikan kepada Pembimbing atau Tutor Taskap kami yaitu Bapak Marsekal Muda TNI (Purn) Surya Dharma,S.IP. serta semua pihak yang telah membantu serta membimbing Taskap ini sampai terselesaikan sesuai waktu dan ketentuan yang dikeluarkan oleh Lemhannas RI.

Penulis menyadari bahwa kualitas Taskap ini jauh dari kesempurnaan akademis, oleh karena itu dengan segala kerendahan hati mohon adanya masukan guna penyempurnaan naskah ini.

Besar harapan saya agar Taskap ini dapat bermanfaat sebagai sumbangan pemikiran penulis kepada Lemhannas RI, termasuk bagi siapa yang membutuhkannya.

Semoga Tuhan Yang Maha Esa senantiasa memberikan berkah dan bimbingan kepada kita semua dalam melaksanakan tugas dan pengabdian kepada negara dan bangsa Indonesia yang kita cintai dan kita banggakan.

Sekian dan terimakasih. Wassalamualaikum Wr.Wb.

Jakarta, 18 Juli 2023
Penulis

Khalil Ibraheem SH. Alshaikhi
Kolonel Arab Saudi, NRP.

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini:

   Nama : khalil Ibraheem SH. Alshaikhi

   Pangkat : Kolonel

   Jabatan : Direktur Strategis Departemen Penilaian

   Instansi : Angakatan Laut Arab Saudi

   Alamat : Arab Saudi

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) Angkatan ke-LVX tahun 2023 menyatakan dengan sebenarnya bahwa:

   a. Kertas Karya Ilmiah Perseorangan (Taskap) yang saya tulis adalah asli.
   b. Apabila ternyata Sebagian atau seluruhnya tulisan Taskap ini terbukti tidak asli atau plagiasi, maka saya bersedia dinyatakan tidak lulus Pendidikan.

2. Demikian pernyataan keaslian ini dibuat untuk dapat dioergunakan seperlunya.

Jakarta, 18 Juli 2023
Penulis Taskap

Khalil Ibraheem SH. Alshaikhi
Kolonel Arab Saudi, NRP.

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LEMBAR PERSETUJUAN TUTOR TASKAP

Yang bertanda tangan di bawah ini Tutor Taskap dari:

Nama : khalil Ibraheem SH. Alshaikhi

Peserta : Program Pendidikan Reguler Angkatan (PPRA)

Judul Taskap : Meningkatkan Kapasitas National Cybersecurity Authority (NCA) Kerajaan Arab Saudi Untuk Memperkuat Keamanan Digital Nasional

Taskap tersebut di atas telah ditulis "sesuai/~~tidak sesuai~~" dengan Petunjuk Teknis tentang Penulisan Ilmiah Peserta Pendidikan Lemhannas RI Tahun 2023 karena itu "layak/~~tidak layak~~" dan "disetujui/~~tidak disetujui~~" untuk diuji.

"coret yang tidak diperlukan"

Jakarta, 18 Juli 2023
Tutor Taskap

Surya Dharma.,S.IP
Marsekal Muda TNI (Purn)

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

DAFTAR ISI

Halaman

HALAMAN JUDUL…… I
KATA PENGANTAR…… Ii
PERNYATAAN KEASLIAN…… iv
LEMBAR PERSETUJUAN TUTOR…… v
DAFTAR ISI…… vi
TABEL…… viii
DAFTAR GAMBAR…… ix

BAB I PENDAHULUAN……
1. Latar Belakang…… 1
2. Rumusan Masalah…… 6
3. Maksud dan Tujuan…… 7
4. Ruang Lingkup dan Sistematika Penulisan…… 7
5. Metode dan Pendekatan…… 8
6. Pengertian…… 9

BAB II LANDASAN PEMIKIRAN……
7. Umum…… 12
8 Paradigma Nasional…… 12
9. Peraturan Perundang-undangan…… 15
10. Data dan Fakta…… 16
11. Kerangka Teoritis…… 21
12. Lingkungan Strategis…… 24

BAB III PEMBAHASAN……..

13. Umum…….. 33
14. Kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi saat ini……. 34
15. Visi Masa depan cyber security dan dampaknya terhadap keamanaan digital di Kerajaan Arab Saudi……. 44
16. Strategi meningkatkan kapastitas *National Cybersecurity Authority* (NCA)…….. 49

BAB IV PENUTUP……

17. Simpulan…….. 68
18. Rekomendasi…….. 70

DAFTAR PUSTAKA……

DAFTAR LAMPIRAN

1. Alur Pikir
2. Tabel
3. Daftar Gambar/Peta
4. Daftar Riwayat Hidup

TABEL

TABEL 1 Saudi Cybersecurity Market Forecast

TABEL 2 Global Cybersecurity Index 2019 Mena Regioal Results

TABEL 3 Prakiraan Pengeluaran Keamanan Cyber Perusahaan (Jutaan SAR)

TABEL 4 Perusahaan di Sektor yang Sangat Menjadi Sasaran Serangan Cyber

TABEL 6 Countries with the highest commitment to cyber security based on the Global Cybersecurity Index (GCI) in 2023

DAFTAR GAMBAR

GAMBAR 1. Saudi Arabia Hardest Hit by Ransomware

GAMBAR 2. 10 besar sektor industri yang ditargetkan pada kuartal pertama tahun 2020

GAMBAR 3. Cyber security

GAMBAR 4. Negara-negara terkena serangan cybercrime

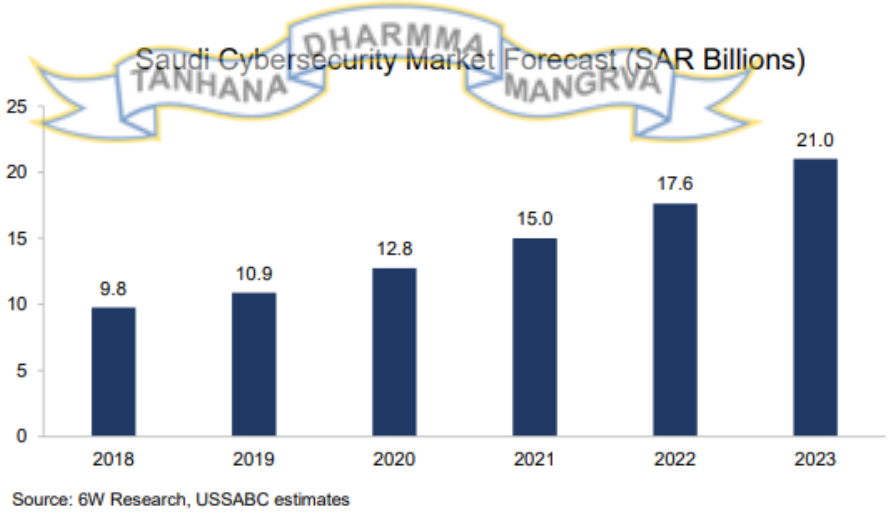
MENINGKATKAN KAPASITAS NATIONAL CYBERSECURITY AUTHORITY (NCA) KERAJAAN ARAB SAUDI UNTUK MEMPERKUAT KEAMANAN DIGITAL NASIONAL

BAB I

PENDAHULUAN

1. Latar Belakang

Lanskap keamanan dunia maya terus berkembang, dan bisnis harus tetap berada di depan ancaman terbaru untuk melindungi data dan jaringan mereka. Di Arab Saudi, pentingnya keamanan siber menjadi semakin jelas saat negara tersebut bergerak menuju Visi 2030. Agar Arab Saudi dapat mencapai tujuan ambisiusnya, infrastruktur digital yang kuat dan aman sangatlah penting. Serangan dunia maya dapat berdampak buruk pada pertahanan dan ekonomi kerajaan, jadi penting untuk berinvestasi dalam langkah-langkah keamanan dunia maya yang kuat. Anggaran 2020 Arab Saudi mengalokasikan SAR102 miliar ($27,2 miliar) untuk keamanan dan regional administrasi yang mencakup keamanan siber. Ukuran pasar keamanan siber Arab Saudi pada 2019 adalah SAR10,9 miliar ($2,9 miliar) dan pasar tersebut diharapkan tumbuh pada CAGR[1] 16,59 persen melalui 2023 menjadi sekitar SAR21 miliar ($5,6 miliar).



Secara global, industri keamanan siber diperkirakan akan mencapai

[1]CAGR adalah sebuah istilah yang sebenarnya tidak asing di kalangan investor atau penanam modal. Istilah ini sendiri merupakan singkatan dari *Compound Annual Growth Rate* atau tingkat pertumbuhan rerata tahunan pada periode atau jangka waktu tertentu

hampir $366,10 miliar pada tahun 2028, dan tren di Arab Saudi diperkirakan akan mengikuti pola ini. Pasar Keamanan Siber Arab Saudi diproyeksikan tumbuh pada CAGR 12,4% antara tahun 2020 dan 2026, dengan ukuran pasar mencapai SAR21 miliar ($5,6 miliar) pada akhir tahun 2023. Antara 2016 dan 2018, negara ini menempati posisi keenam secara global sebagai yang paling terpengaruh oleh serangan dunia maya. Pada tahun 2019, Arab Saudi dan UEA memiliki biaya rata-rata tertinggi kedua per pelanggaran data sebesar SAR22,4 juta ($5,97 juta), menurut laporan yang dikeluarkan oleh IBM. Pada tahun yang sama, kedua negara Teluk ini juga mengalami jumlah rekor pelanggaran rata-rata tertinggi 38.800 per insiden dibandingkan dengan rata-rata global 25.500 rekor per insiden.[2]

Sementara itu, serangan ransomware juga terus menjadi ancaman serius bagi organisasi Saudi. 88% organisasi di Arab Saudi telah melaporkan beberapa bentuk percobaan serangan ransomware, yang merupakan angka yang relatif tinggi dibandingkan dengan rata-rata global. Saat ini diperkirakan bisnis di Arab Saudi kehilangan sekitar $6,53 juta per serangan cyber semacam ini. Mempertimbangkan kemajuan teknologi yang pesat terlihat di Arab Saudi selama sepuluh tahun terakhir, angka-angka ini tidak mengherankan. Tanpa infrastruktur keamanan dunia maya yang tepat, bisnis akan rentan terhadap pelanggaran dan serangan data yang mahal.

Table 1: Global Cybersecurity Index 2019 MENA Regional Results

State	Score	Global Rank (2019)	Global Rank (2017)	Rank Change
Saudi Arabia	**0.881**	**13**	46	33
Oman	0.868	16	4	-12
Qatar	0.86	17	25	8
Egypt	0.842	23	14	-9
United Arab Emirates	0.807	33	47	14
Kuwait	0.6	67	139	72
Bahrain	0.585	68	65	-3

Source: ITU

Tidak ada yang menyangkal bahwa serangan dunia maya yang dihadapi komunitas internasional setiap hari dan dilakukan untuk tujuan spionase, sabotase, dan manipulasi telah menjadi lebih kompleks dari sebelumnya dalam beberapa tahun terakhir, karena berbagai jenis formasi elektronik dan

[2]http://ussaudi.org/wp-content/uploads/2020/01/Economic-Brief-Saudi-Cybersecurity-Leadership.pdf

banyak sektor industri, keuangan, dan ekonomi telah mengalami berbagai macam serangan siber dan ancaman elektronik. Metode-metode ini telah memanifestasikan dirinya dalam bentuk *ransomware*, virus berbahaya, manipulasi dan metode *phishing*, hingga ancaman ini menjadi begitu kompleks sehingga menjadi sulit untuk membatasi atau mengembangkan strategi yang ketat untuk menghadapinya sepenuhnya, terutama dengan banyaknya dan beragamnya bentuk dan sumbernya, serta perkembangannya yang cepat dan berkesinambungan.

Meningkatnya penggunaan teknologi di Arab Saudi mendorong permintaan yang berkelanjutan akan solusi keamanan siber. Saat keamanan dan ekonomi bergerak menuju transformasi digital, semakin banyak organisasi yang mengadopsi eCommerce dan platform online lainnya. Jumlah komponen yang dapat diakses dari jarak jauh juga bertambah di seluruh industri, memberikan titik kerentanan tambahan. Semua faktor ini berkontribusi pada peningkatan tingkat serangan dunia maya, yang berarti menegakkan langkah-langkah keamanan dunia maya yang efektif adalah satu-satunya jalan ke depan bagi kerajaan Arab Saudi. Risiko keamanan dunia maya telah meningkat secara dramatis karena bisnis tidak siap dan dengan cepat beralih untuk mengadopsi norma baru. Dengan akses tunggal, malware atau virus dapat masuk melalui VPN dan membahayakan seluruh jaringan organisasi. Untuk itu perlu mempertimbangkan mengadopsi strategi yang efektif untuk mengurangi risiko tersebut.

Serangan elektronik telah menjadi, tidak diragukan lagi, tajuk paling menonjol sebagai salah satu elemen pengaruh terpenting dalam aspek konflik internasional, setelah sebagian besar konflik antara kekuatan berpengaruh pindah ke Internet dan digital. Hal ini menyebabkan perubahan dalam hubungan dan pusat kekuasaan. Dan siapa pun yang memiliki mekanisme untuk menggunakan infrastruktur elektronik baru memiliki kemampuan untuk mencapai tujuannya, melindungi keamanan vitalnya, dan memengaruhi perilaku negara dan non-negara aktif lainnya melalui alat yang tidak melampaui komputer dan virus elektronik[3].

[3]Aladdin, Farhat (2019), Cyberspace: Shaping the Battlefield in the Twenty-First Century, (Journal of Legal and Political Science), Volume 10 (3), Desember 2019, hlm. 90

Pertumbuhan internet yang belum pernah terjadi sebelumnya telah menyebabkan peningkatan insiden serangan dunia maya yang biasanya mengakibatkan konsekuensi yang menyedihkan dan menghancurkan. Ekonomi modern, masyarakat, dan infrastruktur yang penting telah menjadi sangat bergantung pada platform digital. Ini telah meningkatkan ketergantungan pada informasi teknologi membuat serangan online semakin menarik bagi penyerang dan mungkin lebih berbahaya bagi masyarakat Bendovschi (2015). Dunia yang semakin didorong oleh data besar, jejaring sosial, transaksi online, informasi yang disimpan atau dikelola melalui internet dan proses otomatis dilakukan melalui penggunaan sistem IT, keamanan informasi dan privasi data secara permanen menghadapi resiko. Dengan pengembangan alat dan teknik baru, kejahatan dunia maya terjadi secara konsisten meningkat dalam hal jumlah serangan dan tingkat kerusakan yang ditimbulkan pada korbannya. Mengembangkan cara baru untuk mendapatkan akses tidak sah ke jaringan, program, dan data, penyerang bertujuan untuk berkompromi kerahasiaan, integritas dan ketersediaan informasi, membangun target mereka dari satu individu ke kecil atau perusahaan menengah dan bahkan raksasa bisnis. Setiap tahun tampaknya membawa lebih banyak serangan secara keseluruhan, tapi juga sejumlah besar serangan mengalahkan keamanan perusahaan yang sangat besar, sehingga mempengaruhi informasi keamanan, kelangsungan usaha dan kepercayaan pelanggan. Tren peningkatan tersebut telah mencapai puncak baru di tahun 2022, secara universal dikenal sebagai tahun serangan dunia maya, penulis percaya ini tidak akan menjadi puncaknya kecuali tindakan pencegahan dilakukan[4].

Seiring dengan kemajuan dan perkembangan dunia teknologi dan transformasi digital, tingkat penetrasi dan serangan siber semakin meningkat. Untuk mengikuti perkembangan ini, Arab Saudi berinteraksi dengan penyelarasan Visi 2030 yang telah menjadi salah satu tujuan Kerajaan untuk bergerak menuju transformasi digital dan pengembangan serta peningkatan

[4]Andreea, Bendovschi (2015), Cyber Attacks Trends, Patterns and Security Countermeasures 7th International Conference On Financial Criminology,Wadham College, United Kingdo..

infrastruktur. Karena pentingnya data ini dan menjaganya dari risiko dan ancaman dunia maya, negara membentuk *National Cybersecurity Authority* (NCA) sehingga otoritas tersebut menjadi otoritas yang kompeten di Kerajaan untuk keamanan siber sekaligus sebagai rujukan nasional untuk implementasi, mengembangkan, dan meningkatkan strategi keamanan dunia maya untuk melindungi kepentingan negara dan keamanan nasionalnya serta sektor, layanan, dan aktivitas pemerintah. Dengan menyediakan sistem keamanan yang kuat dan lingkungan yang aman untuk data dan operasi digital.

Pemerintah telah mengidentifikasi keamanan dunia maya sebagai prioritas strategis, dan bisnis berinvestasi dalam solusi baru untuk melindungi diri dari serangan. Otoritas Keamanan Siber Nasional (NCA) didirikan pada 2017 sebagai bagian dari Strategi Keamanan Siber Nasional Arab Saudi. Sejak didirikan, NCA telah menetapkan untuk menetapkan standar minimum keamanan dunia maya untuk lembaga nasional dan pemerintah yang berisiko terkena serangan dunia maya di dalam Kerajaan. Mereka telah menyediakan kebijakan dan kerangka kerja yang ekstensif untuk membantu organisasi-organisasi ini melindungi data dan jaringan mereka. Program Transformasi Digital Nasional juga melihat peningkatan pendanaan yang disalurkan untuk solusi keamanan siber. Program tersebut, yang bertujuan untuk memodernisasi ekonomi Saudi, menghasilkan investasi keamanan siber mencapai $425 juta pada tahun 2020.

Pemerintah Arab Saudi telah membentuk *National Cybersecurity Authority* (NCA) untuk menjadi entitas pemerintah yang bertanggung jawab atas keamanan siber di negara tersebut, dan berfungsi sebagai otoritas nasional dalam urusannya. NCA didirikan oleh Keputusan Raja yang menghubungkannya langsung dengan *Her Majesty* Raja Salman. NCA memiliki fungsi pengaturan dan operasional yang terkait dengan keamanan siber dan bekerja sama dengan entitas publik dan swasta untuk meningkatkan postur keamanan siber negara untuk melindungi kepentingan vitalnya, keamanan nasional, infrastruktur penting, sektor prioritas tinggi, dan layanan pemerintah dan kegiatan yang sejalan dengan Visi 2030.

NCA *cybersecurity* sebagai perlindungan jaringan, sistem teknologi informasi, sistem teknologi operasional dan komponen perangkat keras dan perangkat lunaknya, layanan yang mereka sediakan, dan data yang dikandungnya, dari penetrasi, gangguan, modifikasi apa pun. masuk, menggunakan, atau mengeksploitasi. Konsep ini juga mencakup keamanan informasi, keamanan elektronik, keamanan digital, dan sejenisnya. Otoritas Keamanan Siber Nasional menjadi untuk melindungi kepentingan negara, melindungi keamanan Kerajaan, melindungi infrastruktur sensitif Kerajaan, dan meningkatkan keamanan sibernya. Tata kelola keamanan siber belum terintegrasi guna membentuk manajemen risiko siber yang efektif. Kemitraan dan kerja sama di bidang keamanan siber belum optimal. Pembangunan kapasitas manusia nasional belum maksimal dan industri keamanan siber di Kerajaan Arab Saudi belum berkembang, penulisan ini penting untuk dikaji lebih lanjut karena bersifat mendesak untuk diakselerasi, maka judul penulisan ini adalah "**Meningkatkan kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi untuk memperkuat keamanan digital nasional".**

2. Rumusan Masalah.

Dengan percepatan transformasi digital yang signifikan, tingkat serangan dunia maya dan risiko pelanggaran data telah meningkat, membuat Kerajaan lebih tertarik untuk menyediakan lingkungan yang aman untuk operasi data dan digital melalui sistem keamanan yang kuat. Di sinilah peran *National Cybersecurity Authority* dalam mengembangkan, menerapkan, dan mengawasi strategi. Strategi keamanan siber nasional dikembangkan untuk mencerminkan ambisi strategis Kerajaan dengan cara yang seimbang antara keamanan, kepercayaan, dan pertumbuhan. Itu dibuat untuk mencapai konsep ruang maya Arab Saudi yang aman dan andal yang memungkinkan pertumbuhan dan kemakmuran. Adapun yang menjadi rumusan masalah dalam penulisan ini adalah: **"Bagaimana Meningkatkan kapasitas National Cybersecurity Authority (NCA) Kerajaan Arab Saudi untuk memperkuat keamanan digital nasional?"**

Berdasarkan latar belakang dan rumusan masalah tersebut di atas, selanjutnya dapat diidentifikasi pertanyaan kajian sebagai berikut:

a. Bagaimana kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi saat ini?

b. Bagaimana permasalahaan yang dihadapi oleh *National Cybersecurity Authority* (NCA) dan dampaknya terhadap keamanaan digital di Kerajaan Arab Saudi?

c. Bagaimana rekomendasi kebijakan untuk meningkatkan kapastitas *National Cybersecurity Authority* (NCA) guna menguatkan keamanan digital di Kerajaan Arab Saudi?

3. Maksud dan Tujuan

a. **Maksud:** Penulisan taskap ini dimaksudkan untuk menggambarkan dan menganalisis permasalahan yang dihadapi oleh *National Cybersecurity Authority* (NCA) dan dampaknya terhadap keamanaan digital di Kerajaan Arab Saudi dan mencari solusi pemecahan masalah guna menguatkan keamanan digital di Kerajaan Arab Saudi.

b. **Tujuan**: Adapun tujuan dari penulisan taskap ini sebagai sumbang saran pemikiran yang bersifat membangun kepada para pemangku kebijakan untuk memecahkan permasalahan Meningkatkan kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi untuk memperkuat keamanan digital nasional.

4. Ruang Lingkup dan Sistematika

Ruang lingkup dalam penulisan Taskap ini dibatasi pada pembahasan mengenai permasalahan yang dihadapi dan dampaknya terhadap kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi yang berkembang saat ini, yang diprediksi akan mempengaruhi kekuatan keamanan digital nasional yang sudah berjalan sesuai harapan yang sudah ditetapkan, sehingga perlu akselarasi meningkatkan kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi berstandar regional bahkan internasional berdaya saing dengan negara-negara maju atau super power. Adapun ruang lingkup penulisan yang menjadi fokus meliputi aspek

capacity building, visi ke depan cyber security dan strategi meningkatkan kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi untuk memperkuat keamanan digital nasional.

Adapun penulisan taskap ini disusun dengan sistematika sebagai berikut:

1) **Bab I Pendahuluan**. Berisi latar belakang penulisan, perumusan masalah, maksud dan tujuan, ruang lingkup dan sistimatika, metoda dan pendekatan yang digunakan serta beberapa pengertian untuk memahami analisis dan pembahasan.
2) **Bab II Tinjuan Pustaka.** Terdiri dari dasar-dasar pemikiran dalam penulisan taskap berupa peraturan perundang-undangan yang masih berlaku. Disajikan pula data dan fakta terkait serta kerangka teoritis yang bersumber dari kajian pustaka maupun referensi ilmiah yang terkait dengan materi bahasan. Selanjutnya akan diuraikan pengaruh perkembangan lingkungan strategis berdasarkan faktor eksternal maupun internal yang berada pada tataran global, regional dan nasional.
3) **Bab III Pembahasan.** Meliputi tahapan analisis dan pembahasan setiap pokok-pokok bahasan dan pertanyaan penelitian terkait Meningkatkan kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi. Pembahasan berdasarkan teori yang ditetapkan. Hasil analisis ini nantinya akan dapat dirumuskan untuk menjawab pertanyaan kajian.
4) **Bab IV Penutup.** Berisi simpulan dari pembahasan dan rekomendasi kepada para *stakeholders* terkait dalam pengambilan keputusan kebijakan.

5. Metode dan Pendekatan

a. Metode. Metode yang digunakan dalam taskap ini menggunakan metode kualitatif/deskriptif, dengan Teknik pengumpulan data serta analisis penyajian data dan fakta menggunakan penelitian literatur (studi kepustakaan) dari data sekunder, yang akan dibahas sebagai kajian strategis dengan menggunakan analisis SWOT. Metode ini berperan

penting dalam mengurai permasalahan dan sekaligus memitigasi risiko secara multidimensioanal, untuk dapat menghasilkan kebijakan dan keputusan yang terbaik.

b. Pendekatan. Pendekatan yang digunakan dalam analisis data taskap bersifat holististik, komprehensif, dan integral dari perspektif kepentingan nasional dengan tinjauan pada aspek kesejahteraan dan keamanan dengan analisis multidisiplin, digunakan sesuai dengan kerangka teoritis yang digunakan.

6. Pengertian

a. Meningkatkan Kapasitas

Meningkatan kapasitas (atau pengembangan kapasitas, penguatan kapasitas) adalah peningkatan fasilitas (atau kemampuan) individu atau organisasi untuk menghasilkan, melakukan, atau menyebarkan.[5] Program Pembangunan Perserikatan Bangsa-Bangsa mendefinisikan dirinya dengan pengembangan kapasitas dalam arti bagaimana UNDP bekerja untuk memenuhi misinya.[6] *The Organisation for Economic Co-operation and Development 's-Development Assistance Committee*/ OECD-DAC mendefinisikan meningkatkan kapasitas sebagai berikut: Pengembangan kapasitas dipahami sebagai proses di mana orang, organisasi, dan masyarakat secara keseluruhan melepaskan, memperkuat, menciptakan, menyesuaikan, dan mempertahankan kapasitas dari waktu ke waktu. Kapasitas sendiri dipahami sebagai kemampuan orang, organisasi, dan masyarakat secara keseluruhan untuk mengelola urusan mereka dengan sukses.[7] Peningkatan kapasitas berarti mulai dari permukaan polos dan pembangunan struktur baru selangkah demi selangkah yang bukan merupakan cara kerjanya.

---

[5]Definisi Kapasitas. www.merriam-webster.com. Diakses tanggal 16 April 2023
[6]Peningkatan kapasitas aktivitas politik. Ensiklopedia Britannica. Diakses tanggal 16 April 2023
[7]UNDP (1998) Penilaian Dan Pengembangan Kapasitas Dalam Sistem dan Konteks Manajemen Strategis Kertas Penasihat Teknis No. 3 Divisi Pengembangan Manajemen dan Pemerintahan Biro Kebijakan Pembangunan Januari 1998

b. **National Cybersecurity Authority (NCA)**

Otoritas Keamanan Siber Nasional Saudi adalah entitas keamanan pemerintah yang berfokus terutama pada keamanan komputer di Kerajaan dan terhubung langsung dengan kantor Raja.[8] Organisasi tersebut didirikan melalui dekrit kerajaan yang dikeluarkan oleh Raja Salman bin Abdul Aziz Al Saud pada 31 Oktober 2017 yang didukung penuh oleh Putra Mahkota Muhammad bin Salman bin Abdul Aziz Al Saud.[9] Otoritas akan dikaitkan dengan Raja dan diciptakan untuk meningkatkan keamanan dunia maya negara, melindungi kepentingan vitalnya, keamanan nasional, dan infrastruktur sensitif.

c. **Memperkuat**

Menjadikan lebih kuat (dalam berbagai-bagai arti seperti memperkukuh, memperteguh, mempererat, mempersangat). Memperkuat memiliki arti dalam kelas verba atau kata kerja sehingga memperkuat dapat menyatakan suatu tindakan, keberadaan, pengalaman, atau pengertian dinamis lainnya.

d. **Keamanan Digital Nasional**

Cybersecurity national didefinisikan sebagai perlindungan sistem teknologi informasi dan jaringan serta sistem dan komponen teknologi operasi, termasuk perangkat keras dan perangkat lunak, bersama dengan layanan yang disediakan dan data yang termasuk di dalamnya, terhadap peretasan yang melanggar hukum : obstruksi, modifikasi, akses, penggunaan atau eksploitas.[10] Cybersecurity national adalah perlindungan sistem yang terhubung ke internet seperti perangkat keras, perangkat lunak, dan data dari ancaman dunia maya. Praktik ini digunakan oleh individu dan perusahaan untuk melindungi dari akses tidak sah ke pusat data dan sistem komputerisasi lainnya.[11] Cybersecurity juga berperan dalam mencegah serangan yang bertujuan

[8]Saudi Arabia sets up new commission to boost cybersecurity. Berita Arab . 02-11-2017. Diakses tanggal 16 April 2023
[9]King orders setting up of National Cyber Security Authority. Saudigazette . 01-11-2017. Diakses tanggal 16 April 2023
[10]https://nca.gov.sa/en/about. Diakses tanggal 16 April 2023
[11]https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. Diakses tanggal 16 April 2023

untuk menonaktifkan atau mengganggu operasi sistem atau perangkat. Keamanan dunia maya adalah praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan berbahaya. Ini juga dikenal sebagai keamanan teknologi informasi atau keamanan informasi elektronik. Istilah ini berlaku dalam berbagai konteks, mulai dari bisnis hingga komputasi seluler.[12]

[12]https://www.techtarget.com/searchsecurity/definition/cybersecurity. Diakses tanggal 16 April 2023

BAB II
LANDASAN PEMIKIRAN

7. Umum

Konsep keamanan telah berkembang dengan perkembangan masyarakat, hingga disebut keamanan nasional, dengan perkembangan informasi yang luar biasa dalam tiga puluh tahun terakhir, dan transformasi masyarakat untuk mengandalkan sistem informasi dan teknologi secara luas, banyak ancaman yang terkait dengan transformasi ini telah muncul, hal ini mengakibatkan munculnya istilah keamanan informasi sebagai jenis perang dan ancaman baru di mana informasi adalah target utama, senjata yang dapat digunakan, menjadi mudah bagi siapa pun, organisasi, atau negara untuk mengakses informasi tentang mereka di mana pun di dunia, menggunakan beberapa perangkat lunak dan perangkat tepat yang memungkinkan mereka menembus sistem informasi dan jaringan yang digunakan secara luas di seluruh dunia, dengan tujuan memperolehnya, mengubah isinya, atau menghindarinya. Perang informasi sipil dan militer merupakan konsep dunia maya muncul, sebagai informasi dan komunikasi teknologi menyebabkan revolusi di segala bidangnya, dan dalam kerangka kerja ini munculnya keamanan dunia maya, yang merupakan akibat tak terhindarkan dari ancaman dunia. Oleh karena itu, penulisan Taskap ini perlu mempertimbangkan beberapa landasan pemikiran yang berkaitan dengan paradigma nasional, aturan perundangan-undangan, data dan fakta, kajian teoritis serta perkembangan lingkungan strategis dalam memperkuat keamanan digital nasional.

8. Paradigma Nasional

a. **Islam Sebagai Landasan Idiil.** Menurut perspektif Islam, dalam QS Al-Kahfi ayat 90-98 terdapat dalam satu penggalan kisah yang menceritakan konsep keamanan pada masa Nabi Zulkarnaen AS dengan bangsa Ya'juj dan Ma'juj. Pada masa itu, Nabi Zulkarnaen AS diminta untuk membangun sebuah dinding yang tinggi dan tebal

sehingga tidak dapat ditembus oleh Ya'juj dan Ma'juj dan bertujuan untuk melindungi kaumnya dari kejahatan dan kerusakan yang dilakukan oleh mereka. Nabi Zulkarnaen AS kemudian memiliki ide untuk membangun sebuah dinding pertahanan yang terbuat dari bahan tembaga dan besi yang panas. Ternyata, konsep dinding tembaga dan besi panas tersebut diadopsi dalam keamanan teknologi modern yang disebut dengan dinding api (*firewall*) fungsi dari *firewall* yakni untuk menghalau akses dari pihak-pihak yang tidak dikehendaki dan tidak bertanggung jawab terhadap data atau komputer yang dimiliki oleh seseorang.[13]

b. **Dekrit Kerajaan Arab Saudi Tahun 1421H Sebagai Landasan Konstitusional.** Dekrit Kerajaan Arab Saudi No : a/90 Tanggal : 27/8/1412H. **Pasal 16** : Negara memiliki kewajiban untuk melindungi fasilitas negara dan baik warga negara maupun penduduk harus melindunginya. **Pasal 33** (Angkatan Bersenjata) Negara mendirikan dan memperlengkapi Angkatan Bersenjata untuk pertahanan agama Islam, Dua Tempat Suci, masyarakat, dan warga negara. **Pasal 34** (Layanan Militer) Pembelaan agama Islam, masyarakat, dan negara adalah kewajiban bagi setiap warga negara. Peraturan layanan militer diatur dalam undang-undang. **Pasal 62** Jika ada bahaya yang mengancam keselamatan Kerajaan atau keutuhan wilayahnya, atau keamanan rakyatnya dan kepentingannya, atau yang menghambat fungsi lembaga negara, Raja dapat mengambil tindakan segera untuk menghadapi bahaya ini dan jika Raja menganggap bahwa tindakan ini harus dilanjutkan, dia kemudian dapat menerapkan peraturan yang diperlukan untuk tujuan ini.[14]

c. **Visi Saudi 2030 Sebagai Landasan Visional.** Visi Saudi 2030 adalah mengembangkan sektor layanan umum seperti kesehatan, pendidikan, infrastruktur, rekreasi dan pariwisata. Visi 2030 memiliki tiga pilar utama. Pilar pertama adalah menjadikan Arab Saudi sebagai jantung dunia Arab

[13]https://recitequran.com/tafsir/en.ibn-kathir/18:98
[14]org/wiki/Basic_Law_of_Saudi_Arabia#Chapter_5_Rights_and_Duties

dan Islam. Kedua, determinasi sebagai kekuatan investasi global dan Ketiga, mengubah Arab Saudi sebagai perantara tiga benua yakni, Asia, Eropa dan Afrika. Program Pengembangan Kemampuan Manusia bertujuan untuk memastikan bahwa warga negara Saudi memiliki kemampuan yang dibutuhkan untuk bersaing secara global dengan menanamkan nilai-nilai dan mengembangkan keterampilan dasar dan masa depan, serta meningkatkan pengetahuan. Program ini berfokus pada pengembangan basis pendidikan yang kokoh bagi semua warga negara. Peningkatan keterampilan warga dengan memberikan kesempatan belajar seumur hidup, mendukung inovasi serta mengembangkan dan mengaktifkan kebijakan dan pendukung untuk memastikan daya saing Arab Saudi.[15] Program Transformasi Nasional bertujuan untuk mengembangkan infrastruktur yang diperlukan dan menciptakan lingkungan yang memungkinkan sektor publik, swasta, dan nirlaba mencapai Visi 2030. Ini akan dicapai dengan mencapai keunggulan operasional pemerintah, mendukung transformasi digital, memberdayakan sektor swasta, mengembangkan kemitraan ekonomi, dan mempromosikan pembangunan sosial, selain memastikan keberlanjutan sumber daya vital.

d. Ketahanan Nasional Sebagai Landasan Konsepsional. Keamanan dianggap sebagai kebutuhan manusia untuk individu, keluarga, masyarakat, dan negara.Tuhan Yang Maha Kuasa merujuk pada keamanan dalam firman-Nya: (Yang memberi mereka makan untuk melawan kelaparan dan membuat mereka aman dari ketakutan) Qur'an Quraisy : 4.[16] Konsep pertahanan nasional adalah untuk mencapai stabilitas di Kerajaan Arab Saudi dan untuk menekankan pertumbuhan dan perkembangannya. Prioritas keamanan nasional Saudi (1) Legitimasi, akidah Islam yang benar dan mapan, serta berhukum dengan hukum Tuhan Yang Maha Esa. (2) Keyakinan dan kebanggaan penuh atas realisasi, kemampuan dan kualifikasi warga negara Saudi. (3)

[15]https://www.vision2030.gov.sa/media/rc0b5oy1/saudi_vision203.pdf
[16]Abd al-Wahhab al-Kayyali and others, Arab National Security, referensi sebelumnya, hal 34

Kegigihan Kerajaan untuk mendukung tujuan adil bangsa Arab dan Islam, yang paling penting adalah perjuangan kedaulatan Kerajaan atas tanahnya, pengelolaan sumber dayanya, dan kemajuannya ke jajaran negara maju.[17]

9. Peraturan Perundang-undangan

a. Raja Salman bin Abdul Aziz Al Saud mengeluarkan dekrit kerajaan tertanggal 23 Juli 2018/10 Dhul Qada 1439 yang menekankan bahwa semua lembaga pemerintah harus meningkatkan keamanan dunia maya mereka untuk melindungi jaringan, sistem, dan data elektronik mereka, serta mematuhi kebijakan, kerangka kerja, standar, dan pedoman yang dikeluarkan oleh NCA.

b. Pada 6 Oktober 2018, NCA telah menerbitkan dokumen kontrol keamanan siber inti untuk standar minimum yang akan diterapkan di berbagai lembaga nasional guna mengurangi risiko ancaman siber. Selain menyebarkan berita ke sektor swasta, NCA juga mengatakan hal yang sama kepada departemen pemerintah bahwa mereka harus mematuhi kebijakan, kerangka kerja, kriteria, pedoman, dan peraturan yang dikeluarkan oleh otoritas terkait hal ini.[18]

c. Pada tanggal 5 Oktober 2020, NCA mengumumkan penerbitan Cloud Cybersecurity Controls, dengan tujuan memperkuat keandalan layanan cloud. Pengumuman tersebut datang bersamaan dengan banyak upaya NCA yang ada untuk melindungi bisnis dan komunitas dari ancaman keamanan dunia maya.

d. Undang-undang e-niaga 2020, yang mencakup ketentuan tentang perlindungan data. Undang-undang mewajibkan bisnis e-commerce untuk mengambil langkah-langkah untuk melindungi data pribadi konsumen dan menetapkan hukuman bagi perusahaan yang gagal melakukannya. Ini memastikan keandalan dan kepercayaan transaksi

[17]Muhammad Al Mashleh, The Concept of Cybersecurity. (Al-Baha: Universitas Al-Baha 2016 M), hal 22

[18]Saudi Arabia to Host Global Cybersecurity Forum in February. Saudigazette . 07-10-2018 . Diakses 16 April 2023

bisnis online sambil menjaga hak-hak konsumen dan melindungi pengguna online dari penipuan dan penipuan.

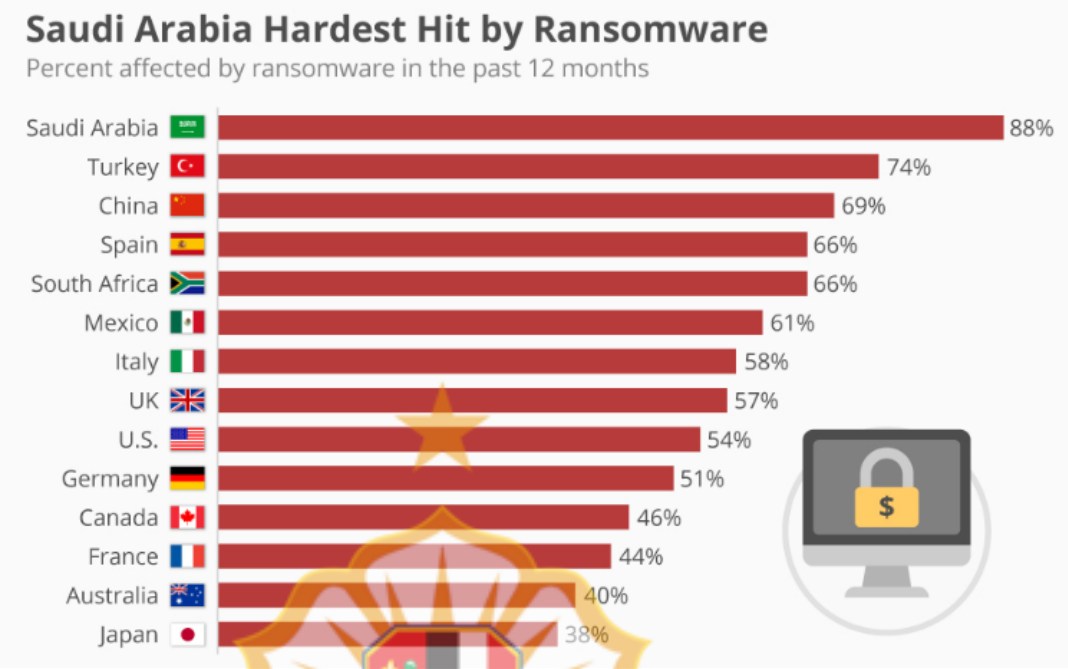
e. Undang-undang perlindungan data pribadi (PDPL) Maret 2022. Untuk memberikan perlindungan tambahan bagi data pribadi warga negara Saudi. Undang-undang mewajibkan organisasi untuk mengambil langkah-langkah untuk melindungi data pribadi penduduk Saudi, termasuk mendapatkan izin tertulis sebelum mengumpulkan, menggunakan, atau berbagi data pribadi. Pengontrol data akan diminta untuk mendaftar ke Saudi Data & Artificial Intelligence Authority (SDAIA) dan membayar biaya tahunan. Kegagalan untuk mematuhi undang-undang baru ini dapat dikenakan hukuman pidana termasuk penjara hingga dua tahun atau denda hingga SAR 3 juta.

f. Kerangka Regulasi Cloud Computing tahun 2020. Pemerintah Saudi merilis Cloud Computing Regulatory Framework (CCRF), yang menetapkan persyaratan bagi organisasi yang ingin menyediakan layanan cloud di negara tersebut. Penyedia Layanan Cloud (CSP) harus mendaftar ke Komisi Teknologi Informasi & Komunikasi (CITC) sebelum mereka dapat menyediakan layanan cloud di Arab Saudi. Jika terjadi jenis pelanggaran keamanan apa pun, CSP harus memberi tahu CITC dan semua pelanggan yang terpengaruh tentang layanan mereka, tanpa penundaan. Selain itu, CSP tidak diizinkan untuk membagikan, atau menggunakan data pelanggannya untuk tujuan apa pun, kecuali jika izin tegas diperoleh dari pelanggan.

10. Data dan Fakta

a. Pada tahun 2020, Arab Saudi mengalami lebih dari 22 juta serangan siber, yang merugikan ekonomi lebih dari $6 juta. Dalam sebuah survei oleh VMware, 88% profesional keamanan Arab Saudi melaporkan peningkatan serangan siber selama pandemi, karena meningkatnya jumlah karyawan yang bekerja dari rumah. Selama beberapa tahun terakhir, pemerintah telah mulai mengambil langkah-langkah untuk mengatasi kerentanan keamanan dunia maya yang sudah berlangsung lama di negara ini. Ransomware menyandera data perusahaan atau

menuntut pembayaran untuk mengambil informasi yang disusupi. Pihak keamanan menganggap serangan itu sebagai ancaman keamanan dunia maya teratas.



b. Perusahaan besar telah secara substansial meningkatkan investasi mereka dalam keamanan TI survei Gartner menunjukkan total pengeluaran kumulatif mencapai SAR7,4 miliar ($2 miliar) antara tahun 2018 dan 2023. Pengeluaran perusahaan tumbuh sekitar SAR911 juta ($242 juta) pada tahun 2018 menjadi SAR1,6 miliar ($415 juta) pada tahun 2023, CAGR sebesar 11,3 persen. Pengeluaran perusahaan adalah untuk layanan keamanan, peralatan keamanan jaringan, dan investasi infrastruktur. Pendekatan keamanan siber menuntut pergeseran dari memandang keamanan siber sebagai masalah teknologi melainkan pilar organisasi.

Prakiraan Pengeluaran Keamanan Cyber Perusahaan (Jutaan SAR)

Market	2018	2019	2020	2021	2022	2023	Total	CAGR
Application Security	23	26	26	30	34	38	176	10.8%
Cloud Security	4	4	8	15	23	34	86	55.2%
Consumer Security Software	86	94	101	109	116	124	630	7.5%
Data Security	26	30	41	53	64	75	289	23.4%
Identity Access Management	94	105	124	143	161	176	803	13.5%
Infrastructure Protection	98	113	131	150	173	195	859	14.9%
Integrated Risk Management	15	19	23	30	34	38	158	20.1%
Network Security Equipment	165	195	214	236	248	259	1,316	9.4%
Other Information Security Software	15	15	15	15	15	15	90	0.0%
Security Services	386	428	469	510	559	604	2,955	9.3%
Total	**911**	**1,028**	**1,151**	**1,290**	**1,425**	**1,556**	**7,361**	**11.3%**

Source: Gartner, USSABC

c. Identifikasi ukuran pasar potensial solusi keamanan siber, UKM Kerajaan**.** Menurut Otoritas Umum untuk Statistik (GAStat), UKM berjumlah 480.326 dari total 490.269 perusahaan di seluruh ritel, keuangan, pendidikan, dan perawatan kesehatan. UKM lainnya di sektor termasuk 2.411 perusahaan perawatan kesehatan (58 persen), 6.103 keuangan, perusahaan perkebunan, dan asuransi (87 persen), dan 6.074 perusahaan pendidikan (65,1 persen) di Arab Saudi. Bahwa 43 persen data melanggar target UKM, ini membawa total peluang pasar menjadi 480.326 perusahaan yang berisiko menjadi sasaran. Personel usaha kecil yang tidak mencukupi (74 persen) dan tidak memadai anggaran (55 persen) sebagai tantangan utama menjaga postur keamanan IT. 47 persen UKM menyatakan tidak memahami cara melindungi serangan siber. Kurangnya keahlian internal merupakan peluang bagi bisnis ini untuk berkolaborasi dengan keamanan terkelola penyedia layanan (MSSP).

Perusahaan di Sektor yang Sangat Menjadi Sasaran Serangan Cyber

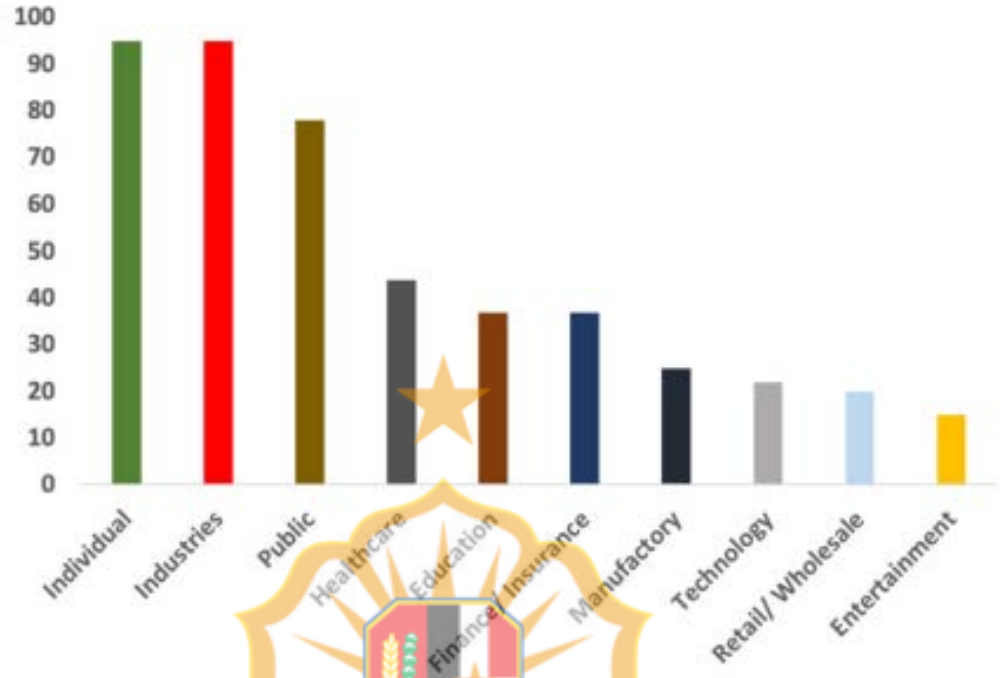
Sector	SMEs	Large Firms	Total
Retail	432,106	3,811	435,917
Finance, Real Estate, and Insurance	39,735	1,130	40,865
Education	6,074	3,253	9,327
Healthcare	2,411	1,749	4,160
Total	**480,326**	**9,943**	**490,269**

Source: GAStat

d. Untuk menekankan tingkat keparahan serangan malware, secara global, lebih dari 200.000 insiden malware terjadi setiap hari, termasuk ransomware, serangan phishing, dan pemindaian berbahaya, serangan somware meningkat 118% pada kuartal pertama 2019, menyebabkan kehilangan data yang parah dan implikasi keuangan. Membandingkan yang pertama hasil kuartal pada tahun 2020 dan 2019, statistik menunjukkan peningkatan 71% malware dan 689% di malware PowerShell. 10 sektor teratas yang ditargetkan pada kuarter pertama ter tahun 2020. Misalnya, serangan terhadap sektor individu meningkat 59% dibandingkan dengan kuartal yang sama tahun 2019. Serangan malware telah dampak yang serius terhadap perekonomian. Pada 2017, kejahatan dunia maya menelan biaya 600 miliar dolar di AS saja, dan

meningkat sekitar 50% pada tahun 2018, dan kerusakan finansial melebihi 1 triliun USD.[19]

10 besar sektor industri yang ditargetkan pada kuartal pertama tahun 2020[20]



e. National Cybersecurity Authority (NCA) didirikan pada tahun 2017 sebagai otoritas pusat untuk keamanan dunia maya di Arab Saudi. NCA bertanggung jawab untuk mengembangkan dan mengoordinasikan strategi keamanan dunia maya Kerajaan, serta mengawasi penerapan undang-undang dan peraturan baru. Pada tahun 2018, NCA merilis whitepaper yang menguraikan standar minimum untuk keamanan dunia maya yang harus dipatuhi oleh semua organisasi di Arab Saudi. Dokumen ini mencakup persyaratan untuk manajemen risiko, respons insiden, perlindungan data, dan lainnya. Itu diedarkan di antara organisasi swasta dan badan pemerintah, untuk meningkatkan kesadaran dan meningkatkan postur keamanan dunia maya di seluruh

[19]The Cost of Malicious Cyber Activity to the U.S. Economy, Online https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (February 2018), Accessed 19 April 2023

[20]B. Christiaan, D. Taylor, F. John, G. Steve, H. Tim, P. Tim, L. MarcRivero, R. Thomas, S.-M. Jessica, S. Raj, S. Ryan, McAfee Labs Threats Report, Online, https://www.mcafee.com/enterprise/en-us/threat-center/mcafeelabs/reports.html, July 2020. Accessed 19 April 2023.

negeri. Pada tahun 2019, NCA membentuk Tim Tanggap Darurat Komputer (CERT), yang bertanggung jawab untuk menanggapi insiden dunia maya dan memberikan dukungan teknis dan forensik. Dua tahun kemudian, Komisi Teknologi Komunikasi dan Informasi (CITC) Arab Saudi mengumumkan penerapan kerangka peraturan keamanan dunia maya yang bertujuan untuk meningkatkan tingkat keamanan penyedia layanan di sektor TI, komunikasi, dan layanan pos.

f. Pendapatan di pasar Cybersecurity diproyeksikan mencapai US$380,90 juta pada tahun 2023. Pasar terbesar dalam Cybersecurity adalah Cyber Solutions dengan volume pasar yang diproyeksikan sebesar US$201,90 juta pada tahun 2023. Pendapatan diharapkan menunjukkan tingkat pertumbuhan tahunan (CAGR 2023-2028) sebesar 8,49%, menghasilkan volume pasar sebesar US$572,60 juta pada tahun 2028. Pengeluaran rata-rata per Karyawan di pasar Cybersecurity diproyeksikan mencapai US$25,15 pada tahun 2023. Sebagai perbandingan global, sebagian besar pendapatan akan dihasilkan di Amerika Serikat (US$68.680,00 juta pada tahun 2023).

g. Keamanan dunia maya yang harus ditangani oleh setiap organisasi baik negara atau swasta untuk memastikan dan meningkatkan keberhasilan transformasi digital dari aktivitas operasional (proses otomatis, alat berbasis cloud, atau dukungan perangkat lunak). Didorong oleh meningkatnya kesadaran akan risiko dan ancaman data, pasar Cybersecurity global telah mengalami pertumbuhan yang kuat selama beberapa tahun terakhir dengan peningkatan pendapatan dari US$83 miliar pada tahun 2016 menjadi US$147 miliar pada tahun 2022. Adopsi cybersecurity diperkirakan akan tumbuh dengan meningkatnya penetrasi internet di antara negara berkembang dan maju. Sementara keamanan siber biasa diabaikan sebagai tugas departemen TI, kini hal itu semakin menjadi bagian dominan dari perencanaan strategis tingkat atas. Krisis COVID-19 menyebabkan banyak organisasi menghadapi lebih banyak serangan siber karena kerentanan keamanan pekerjaan jarak jauh serta peralihan ke lingkungan TI virtual, seperti infrastruktur, data, dan jaringan komputasi awan. Pasar diperkirakan terus menunjukkan pertumbuhan

yang kuat, dengan Amerika sebagai wilayah dominan di pasar ini. Cloud Security adalah subsegmen pasar yang berkembang paling cepat

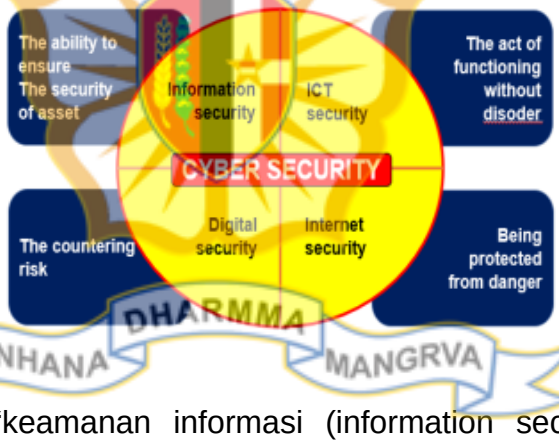
11. Kerangka Teoritis

a. **Teori Strategi Keamanan**. Pemahaman konsep keamanan pasca perang dingin tidak lagi sempit sebagai hubungan konflik atau kerjasama antar negara, tetapi juga berpusat pada keamanan untuk masyarakat, kemudian Arnold Wolfers mendefinisikan keamanan adalah, “security, in any objective sense, measures the absence of threats to acquired values and in a subjective sense, the absence of fear that such values will be at tacked”. Sementara itu, strategi menurut John P. Lovell diartikan sebagai serangkaian langkah-langkah atau keputusan-keputusan yang dirancang sebelumnya dalam situasi kompetititf dimana hasil akhirnya tidak semata-mata bersifat untung-untungan. Strategi adalah cara yang digunakan untuk mencapai suatu tujuan atau kepentingan dengan menggunakan power yang tersedia, termasuk juga kekuatan militer. Global cyber security menurut Arnold harus dibangun di atas lima bidang kerja: Kepastian Hukum (undang-undang cyber crime); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); capacity building dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman cyber crime terbaru); Kerjasama Internasional (termasuk di dalamnya kerjasama timbal balik dalam upaya mengatasi ancaman cyber).[21]

b. **Teori Cyber Security Concept.** Dalam keamanan nasional ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep “cyber security”. Karena cyber space merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi. Maka konsep cyber security tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi

[21]Wolfers, Arnold.“National Secuirty’ As an Ambigous Symbol.” dalam American Defense and Détente ed. Eugene J. Rosi. New York: Dodd, Mead, 1973.

ancaman terhadap keamanan nasional. Perkembangan teknologi informasi juga telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik tapi juga meluas ke dunia maya. Konsekuensinya, negara harus beradaptasi dengan perkembangan ini, konsep keamanan dunia maya sudah saatnya ditetapkan sebagai salah satu "wilayah" negara yang menjaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan cyber tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintah. Cyber security ditujukan pada isu keamanan informasi bagi pemerintahan, organisasi dan urusan individual yang dihubungkan dengan teknologi, dan secara khusus dengan teknologi internet. Cyber security tidak dapat diabstraksikan terlalu jauh dari wilayah aplikasinya dan lingkungan sosial-kultural.



Terminologi "keamanan informasi (information security)" dan cyber security adalah dua konsep berbeda. Dalam konteks tertentu ada kesamaan pemahaman jika dikaitkan dengan proteksi aset atau perlawanan terhadap spionase industri dan ekonomi, perlawanan terhadap terorisme atau kejahatan ekonomi, perlawanan terhadap konten-konten terlarang. Dalam konteks lain, dua konsep tadi memiliki perbedaan. Cyber security mencakup segala sesuatu berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental. Sedangkan keamanan informasi berhubungan dengan isu-isu yang lebih luas, seperti kedaulatan negara, keamanan nasional, proteksi atas

infrastruktur penting, keamanan aset-aset yang terlihat maupun yang tidak terlihat, dan proteksi data personal dan sebagainya.[22]

c. **Teori Manajemen Teknologi Informasi**. Ada 4 (empat) pondasi utama yang mendukung perkembangan teknologi informasi yaitu: perkembangan perangkat lunak (software) seperti sistem dan aplikasi dan perkembangan alat keras (hardware) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (content management), telecommunication and networking, perkembangan internet serta perdagangan online atau melalui internet. Sementara untuk pengorganisasian terkait dengan pengunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu: pertama, sistem informasi (information systems) dan kedua, kompetisi organisasi (organizational competition); ketiga, information systems (sistem informasi) dan organizational decision making (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan system informasi (organizational use of information systems).[23]

d. **Teori Cyber Attack**. Malware adalah setiap kode komputer yang dapat digunakan untuk mencuri data, melewati kontrol akses, serta menimbulkan bahaya terhadap atau merusak system. Dalam cyber attack, selain virus, terdapat beberapa jenis serangan malware antara lain: (1) Spyware yang melacak aktivitas, pengumpul penekanan tombol, dan pengambilan data, (2) Adware dirancang untuk menampilkan iklan namun juga ditemukan membawa spyware, (3) Bot yang dirancang otomatis melakukan tindakan tertentu secara online, (4) Ransomware yang mengenkripsi data di komputer dengan kunci yang tidak diketahui oleh pengguna.[24] Jenis-jenis malware inilah yang dimanfaatkan sehingga mempengaruhi karakteristik di ruang siber. Undang-Undang

---

[22]Ghernaouti, Solange. 2013. Cyber Power :Crime, Conflict and Security in Cyberspace. Lausanne: EPFL Press.

[23]O'Brien, J (1999). Sistem Informasi Manajemen – Mengelola Teknologi Informasi di Perusahaan Internetworked . Boston: Irwin McGraw-Hill. ISBN 0-07-112373-3.

[24]Koh, B. (t.t.): Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and
What to Do about It, HarperCollins Publishers, 2010, 290 pages 3

Anti-Cybercrime dikeluarkan melalui Keputusan Kerajaan di Arab Saudi pada tahun 2007. Undang-undang tersebut bertujuan untuk memerangi kejahatan dunia maya dengan mengidentifikasi kejahatan tersebut dan menentukan hukuman mereka untuk memastikan keamanan informasi, perlindungan hak yang berkaitan dengan penggunaan komputer dan jaringan informasi yang sah. Perlindungan kepentingan umum, moral dan perlindungan ekonomi nasional. Kejahatan dunia maya dihukum berat oleh Kementerian Dalam Negeri Saudi dan Komisi Teknologi Komunikasi dan Informasi dan hukuman dijatuhkan untuk pencurian identitas, pencemaran nama baik, pembajakan elektronik, pencurian email, dan aktivitas melanggar hukum lainnya.

12. Lingkungan Strategis

a. LIngkungan Strategis Global

Perekonomian global berada di persimpangan kritis dengan sejumlah tantangan dan krisis yang saling terkait yang berjalan secara paralel. Ketidakpastian perang Rusia melawan Ukraina terus berlangsung dan peran perang tersebut menciptakan ketidakstabilan global berarti bahwa masalah di sisi inflasi belum berakhir. Inflasi makanan dan bahan bakar akan tetap menjadi masalah ekonomi yang terus-menerus. Inflasi ritel yang lebih tinggi akan berdampak pada kepercayaan dan pengeluaran konsumen. Saat pemerintah memerangi inflasi dengan menaikkan suku bunga, penciptaan lapangan kerja baru akan melambat dan berdampak pada aktivitas dan pertumbuhan ekonomi. Dengan pertumbuhan yang lebih lambat dan inflasi yang tinggi, pasar negara maju tampaknya siap memasuki resesi. Ketakutan akan wabah COVID baru dan jalur pasca-pandemi China yang sudah tidak pasti menimbulkan risiko nyata bagi dunia yang mengalami kesulitan rantai pasokan dan gangguan manufaktur yang lebih akut tahun ini. Pasar keuangan yang bergejolak, meningkatnya ketegangan perdagangan, lingkungan peraturan yang lebih ketat, dan tekanan untuk mengarusutamakan perubahan iklim ke dalam keputusan ekonomi akan menambah kompleksitas tantangan yang dihadapi. Tahun 2023

diperkirakan akan menjadi tahun yang berat bagi sebagian besar pasar, investor, dan konsumen.

Pasar global untuk Keamanan Internet diperkirakan mencapai US$57 Miliar pada tahun 2022, diproyeksikan mencapai ukuran yang direvisi sebesar US$98,5 Miliar pada tahun 2030, tumbuh pada CAGR sebesar 7,1% selama analisis periode 2022-2030. Diproyeksikan mencatat CAGR 6,9% dan mencapai US$49,6 Miliar pada akhir periode. Dengan mempertimbangkan pemulihan pascapandemi yang sedang berlangsung, pertumbuhan di segmen Perangkat Keras disesuaikan kembali ke CAGR 6,1% yang direvisi untuk periode 8 tahun ke depan. Pasar Keamanan Internet di AS diperkirakan mencapai US$17,2 Miliar pada tahun 2022. China, ekonomi terbesar kedua di dunia, diperkirakan akan mencapai ukuran pasar yang diproyeksikan sebesar US$17 Miliar pada tahun 2030, mengikuti CAGR sebesar 6,6% di atas periode analisis 2022 hingga 2030. Di antara pasar geografis penting lainnya adalah Jepang dan Kanada, masing-masing diperkirakan akan tumbuh masing-masing sebesar 6,6% dan 5,7% selama periode 2022-2030. Di Eropa, Jerman diperkirakan tumbuh sekitar 5,7% CAGR.[25]

Serangan keamanan siber terus meningkat sepanjang tahun 2020 dan 2021, tidak hanya dari segi vektor dan jumlah tetapi juga dalam hal dampaknya. Pandemi COVID-19 berdampak pada ancaman keamanan siber. Salah satu perkembangan yang lebih bertahan lama yang dihasilkan dari pandemi COVID-19 adalah pergeseran ke model kantor hybrid. Oleh karena itu, ancaman keamanan siber terkait pandemi dan eksploitasi menjadi arus utama. Peningkatan jumlah serangan dunia maya yang menargetkan organisasi dan perusahaan.[26]

b. Lingkungan Strategis Regional

Timur Tengah adalah salah satu wilayah favorit penyerang dunia maya. Ini telah meningkatkan kebutuhan akan keamanan siber di Timur

[25]https://www-researchandmarkets.internet-security-global-strategic-busines
[26]IBM – Cost of a Data Breach Report 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Tengah. Menurut perkiraan global oleh ResearchAndMarkets.com, ukuran pasar keamanan siber di Timur Tengah diperkirakan akan tumbuh dari $15,6 miliar pada tahun 2020 menjadi $29,9 miliar pada tahun 2025, dengan tingkat pertumbuhan tahunan gabungan (CAGR) sebesar 13,80%.[27] Perekonomian Timur Tengah yang berkembang pesat ditambah dengan digitalisasi yang cepat telah menarik perhatian penjahat dunia maya secara global. Studi oleh Ponemon Institute dan IBM Security, pelanggaran data mengakibatkan kerugian rata-rata $6,53 juta per organisasi di Timur Tengah, yang jauh lebih tinggi daripada kerugian rata-rata global sebesar $3,86 juta.[28] The National News melaporkan bahwa lebih dari 2,57 juta serangan phishing terdeteksi dari bulan April hingga Juni di seluruh Timur Tengah pada tahun 2020.[29] The Gulf News, UEA adalah negara yang paling banyak menjadi sasaran kejahatan dunia maya. Biaya serangan di negara ini diperkirakan mencapai $1,4 miliar per tahun.[30] Laporan oleh CNBC, UEA mengalami peningkatan serangan dunia maya sebesar 250% pada tahun 2020 yang ditandai dengan lebih seringnya insiden ransomware dan phishing.[31]

Di timur tengah, pelaku ancaman menargetkan industri dengan kepemilikan data pelanggan paling sensitif untuk keuntungan finansial maksimum. Perusahaan perawatan kesehatan mengeluarkan biaya per rekor tertinggi karena pelanggaran data, diikuti oleh sektor keuangan dan teknologi. Sebagian besar pelanggaran data dilakukan dengan memperoleh dan menggunakan kredensial pengguna yang sah untuk melakukan penipuan atau pencurian. 59% pelanggaran data dilakukan oleh aktor jahat, 24% karena gangguan sistem, dan 17% disebabkan oleh kesalahan manusia. Times of Oman , lebih dari 2,57 juta serangan phishing terdeteksi pada tahun 2020 di seluruh wilayah Timur Tengah, termasuk Mesir, UEA, Qatar, Arab Saudi, Kuwait, Oman, dan Bahrain.

[27]https://www-researchandmarkets.reports/middle-east-cybersecurity-market-with-covid-19
[28]https://www-albawaba- business/pr/2020-ibm-report-average-cost-data-breach-incident-middle-east-stands-653-million
[29]https://www-thenationalnews- business/money/uae-sees-more-than-600-000-phishing-attacks
[30]https://gulfnews-technology/cybercrime-cost-uae-dh514b-this-year. Diakses 18 April 2023
[31]https://www-cnbc-middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says Diakses 18 April 2023

Dengan baris subjek terkait COVID-19 yang meningkatkan kemungkinan terbukanya email jahat, Timur Tengah dilanda gelombang serangan phishing pada Q2 tahun 2020.[32] Menurut laporan yang diterbitkan oleh ENISA, Timur Tengah menyaksikan kebangkitan dan kesuksesan beberapa geng ransomware yang berkembang pesat seperti Maze, Sodinokibi, Egregor, dan Netwalker. Karena alasan ini, serangan ransomware yang ditargetkan telah menjadi salah satu masalah keamanan siber yang paling parah bagi perusahaan-perusahaan Timur Tengah.[33]

Di Timur Tengah, serangan Stuxnet terhadap fasilitas nuklir Iran pada 2009 dipicu serangan siber. Dengan serangan Stuxnet, negara-negara di seluruh dunia menemukan betapa rentannya infrastruktur terhadap serangan siber dan betapa dahsyatnya potensi dampaknya.[34] Akibatnya, Duqu, sebuah malware, digunakan di Iran dan Sudan pada tahun 2011 hingga mengumpulkan data dari beberapa target yang berpotensi digunakan dalam serangan siber di masa mendatang. Lain malware yang dikenal sebagai Flame, yang menggunakan desain yang sama dengan Stuxnet, menyerang minyak Iran dan perusahaan minyak nasional pada tahun 2012. Produsen gas alam cair terbesar kedua di Qatar, Ras Gas, sebuah perusahaan yang berbasis di Qatar, terinfeksi malware. Sekelompok hacktivists bernama "Parastoo" mulai menyerang sasaran publik Israel pada September 2012 dan September 2013 pada September 2012 untuk membantu program nuklir Iran. Pada tahun 2015 korban Duqu 2.0 ditemukan di banyak lokasi di Timur Tengah.[35]

c. LIngkungan Strategis Nasional

1) Gatra Geografi. Di Arab Saudi, keamanan dunia maya telah didiagnosis sebagai komponen penting yang berkontribusi terhadap keamanan di seluruh negara. Wilayah geografis ekstra

[32]https://timesofoman-com.business/oman-sees-more-than-190000-phishing-attacks Diakses 18 April 2023
[33]ENISA%20Threat%20Landscape%202021.pdf
[34]Baezner, M. (2018). Cyber and Information warfare in the Ukrainian conflict, 1, 1-56.
[35]Zetter, K. (2015). Kaspersky finds new nation-state attack-in its own network.

Arab Saudi menjadi terintegrasi ke dalam desa global, memerlukan proyek pemerintah tambahan yang bertujuan untuk menjembatani kesenjangan virtual dan mengatasi keamanan dunia maya. Salah satu inisiatif ini adalah pengembangan dan penerapan kebijakan keamanan siber Arab Saudi yang tepat.

2) **Gatra Demografi.** Pertumbuhan pesat dalam teknologi internet dan komunikasi (TIK) telah menghasilkan infrastruktur yang kuat dan akses luas ke internet, dengan 33,6 juta pengguna internet di Arab Saudi per Januari 2021, naik dari 28,9 juta pada tahun 2019. Pada Januari 2021, jumlah pelanggan seluler mencapai 39,5 juta atau setara dengan 112,7 persen populasi. Ini mewakili penurunan 1,2 persen dari Januari 2020. Arab Saudi adalah negara yang menarik bagi investor dan penjahat. Sebagai produsen minyak terbesar di dunia, populasi yang besar, lokasi geografis yang strategis, dan daya beli konsumen yang kuat. Penjahat dunia mayalah yang menaruh minat khusus di negara tersebut, mendorong pemerintah untuk meningkatkan keamanan digital nasional.

3) **Gatra Sumber Kekayaan Alam.** Peningkatan upaya pemerintah untuk mendiversifikasi sumber pendapatan dan mengurangi ketergantungan pada industri minyak yang sudah menjadi andalan utama sumber pendapatan negara, oleh karena itu ada peningkatan digitalisasi lembaga publik dan swasta, dan meningkatnya kekhawatiran tentang serangan dunia maya merupakan faktor utama yang mendorong permintaan keamanan dunia maya Arab Saudi.

4) **Gatra Idiologi**. Prioritas Arab Saudi adalah negara dan bangsa dan ketika identitas sektarian seperti syiah menjadi tidak sesuai dengan Visi 2030 kerajaan dan perkembangannya, maka kepentingan nasionalisme Saudi selalu didepankan, yang telah menyatukan negara. Kebijakan luar negeri Saudi First mengutamakan kepentingan negara dan bangsa dan berarti bangsa tidak lagi disandera oleh peristiwa politik dan ideologi regional.

5) **Gatra Politik**. Permintaan akan keamanan siber didorong oleh investasi kelas atas pemerintah dalam mengembangkan infrastruktur TI negara dan pemberlakuan peraturan pemerintah yang ketat yang menekankan perlunya solusi keamanan siber untuk data publik yang aman dan rahasia.

6) **Gatra Ekonomi**. Di KSA, Riyadh bermaksud untuk menarik investasi asing yang signifikan di tahun-tahun mendatang dengan mendirikan Zona Ekonomi Khusus. Riyadh juga telah menjadi launchpad 5G negara itu, dengan kota yang mengalami perluasan layanan 5G terbesar, menjadikan Riyadh sebagai penghasil permintaan utama untuk pasar keamanan siber Arab Saudi.

7) **Gatra Sosial Budaya**. Munculnya COVID-19 berkontribusi signifikan terhadap pertumbuhan Pasar Keamanan Siber Arab Saudi, karena organisasi memberi karyawan mereka pilihan untuk bekerja dari rumah untuk melindungi mereka dari infeksi. Karena peralihan ke platform jarak jauh digital, organisasi telah meningkatkan pengeluaran mereka untuk solusi keamanan siber tingkat lanjut untuk memastikan privasi dan keamanan data. Kemajuan teknologi yang pesat, adopsi teknologi canggih seperti IoT, kecerdasan buatan, dan penyebaran teknologi 5G diharapkan dapat menciptakan berbagai peluang pertumbuhan bagi industri.

8) **Gatra Pertahanan dan Keamanan**. Saudi Aramco (Saudi Arabian Oil Company) adalah perusahaan milik negara yang bertanggung jawab atas minyak eksplorasi, produksi, dan pemurnian. Nilai pasar Aramco diperkirakan hingga $10 triliun, menjadikannya organisasi paling bernilai di dunia. Ancaman terhadap Aramco dapat dimasukkan Keamanan nasional Arab Saudi dalam bahaya. Inti dari inisiatif ini adalah fokus pada teknologi, transformasi digital, dan pengembangan infrastruktur digital. Intinya, strategi itu sendiri tidak berurusan dengan masalah cyberspace atau cyberterrorism. Cybersecurity adalah garis pertahanan pertama untuk keamanan perangkat ini. Cybersecurity dikenal sebagai praktik pertahanan

dan perlindungan komputer, server, ponsel pintar, sistem elektronik, jaringan, dan data dari serangan berbahaya, dan kemampuan untuk mengambil informasi jika dikompromikan atau rusak

d. Peluang dan Kendala

1) Peluang

a) Pasar keamanan siber telah tumbuh secara eksponensial. Oleh karena itu, investasi di bidang ini oleh dana modal yang berani merupakan peluang penting secara lokal dan global, karena meningkatnya permintaan dan kebutuhan akan layanannya, karena telah tumbuh sebesar 20% selama 5 tahun terakhir. Hal ini juga diharapkan untuk dua kali lipat selama 5 tahun ke depan. Pada tahun 2019, investasi di pasar Amerika dari perusahaan keamanan CrowdStrike mencapai $7 miliar, yang merupakan bukti kuat bahwa sektor keamanan siber adalah salah satu sektor yang menjanjikan yang dapat tumbuh dan berkembang.

b) Ketika kita berbicara tentang memperkuat kemampuan dan pembelajaran serta memperoleh pengetahuan dan kesadaran yang diperlukan untuk mengimbangi transformasi digital, kita harus menyebutkan platform "Cybrary", yang merupakan salah satu platform paling populer dalam keamanan siber. Ini menyediakan kursus pelatihan dari masuk ke tingkat mahir. Ini adalah salah satu sumber pengetahuan dan pembelajaran jarak jauh terbaik.

c) Dalam keamanan siber, Arab Saudi telah membuat lompatan besar sehubungan dengan Visi Saudi 2030. Arab Saudi menempati peringkat ke-13 dari 175 negara dalam indeks keamanan siber global karena Kerajaan telah membentuk beberapa entitas yang bertanggung jawab untuk membuat peraturan dan undang-undang terkait keamanan siber; bertujuan untuk meningkatkan keamanan infrastruktur,

kepentingan vital dan keamanan nasional, serta membangun kemampuan lokal yang profesional.

d) Kerajaan juga baru-baru ini menjadi tuan rumah Forum Internasional tentang Cybersecurity untuk meningkatkan kemampuan sektor lokal dan bekerja untuk menemukan solusi dan produk baru untuk ancaman dan tantangan yang dihadapi dunia.

e) Sebagai indikasi pentingnya negara menempatkan keamanan siber, Riyadh menjadi tuan rumah Forum Keamanan Siber Global pertama pada Februari 2020. Acara tersebut mempertemukan 1.200 delegasi dan 100 pembicara, dan memberikan kesempatan untuk membahas tantangan, solusi, dan peran publik. dan sektor swasta dalam membangun masyarakat digital yang aman. Forum tersebut bertujuan untuk meningkatkan kerja sama guna memastikan keamanan siber kolektif dunia dan diselenggarakan di bawah naungan Raja Salman bin Abdulaziz Al Saud.

2) Kendala

a) Laporan World Economic Forum 2019 menyebutkan bahwa salah satu dari 3 risiko besar yang dihadapi masyarakat internasional dari individu atau lembaga adalah ancaman serangan siber. Apa yang kita saksikan hari ini adalah perkembangan teknis yang sangat besar saat kita memasuki era baru dengan revolusi Internet of Things (IoT). Revolusi ini akan sangat meningkatkan risiko keamanan siber. Menurut statistik global, rata-rata serangan dunia maya adalah 90 juta per tahun. Tidak terbatas pada kehilangan data dan peretasan, tetapi juga mencakup celah dalam sistem operasi, spyware, virus, analisis data yang dikirim, atau apa yang memengaruhi keamanan dan stabilitas kehidupan orang seperti pemerasan dan peniruan.

b) Keamanan Transparan adalah salah satu spesialisasi keamanan siber yang paling menjanjikan karena berbagai aspeknya dalam mengintegrasikan antarmuka pengguna (UI / UX) dengan keamanan siber dan perilaku psikologis. Tantangan saat ini bagi para spesialis dalam menyeimbangkan antara kemudahan penggunaan dan keamanan, selain kurangnya klasifikasi dan evaluasi perangkat dan aplikasi dalam hal tingkat keamanannya.

c) Fokus baru pada keamanan dunia maya mengikuti sejumlah insiden dalam beberapa tahun terakhir yang melihat kerentanan dunia maya dieksploitasi. Pada tahun 2018 Arab Saudi melaporkan bahwa lebih dari 160.000 serangan siber menyerang servernya setiap hari, menjadikan Kerajaan penerima serangan terbesar di Timur Tengah. Serangan besar termasuk yang terkait dengan malware Shamoon yang sangat merusak, yang melanda institusi besar seperti Saudi Aramco, Otoritas Umum Penerbangan Sipil dan Kementerian Tenaga Kerja antara 2012 dan 2017.

d) Munculnya komputasi awan juga membawa kebutuhan akan lapisan keamanan siber tambahan. Komputasi awan di Arab Saudi sangat diminati. Namun, semakin banyak data yang disimpan di cloud, semakin aman kebutuhan dunia maya Kerajaan saat ancaman dari pihak ketiga muncul.

e) Biaya pelanggaran data tinggi, dengan Arab Saudi menempati peringkat kedua dalam biaya pelanggaran data, menurut "Laporan Biaya Pelanggaran Data 2019" IBM, yang menganalisis pelanggaran dari 507 organisasi di 16 negara. Biaya rata-rata pelanggaran di Arab Saudi adalah $6 juta, di belakang AS, di mana biaya pelanggaran rata-rata $8,2 juta. Laporan tersebut menemukan bahwa Timur Tengah memiliki jumlah rata-rata rekor pelanggaran tertinggi, yaitu 38.300 per insiden, dibandingkan dengan rata-rata global 25.500.

BAB III
PEMBAHASAN

13. Umum

Tujuan utama membangun kapasitas *National Cybersecurity Authority* adalah untuk meningkatkan kemampuan untuk mengatasi ancaman yang disengaja dan tidak disengaja, respons dan pemulihan cepat sistem informasi, dan dengan demikian mengurangi dampak bahaya atau kerusakan akibat gangguan atau kerusakan teknologi informasi dan komunikasi atau karena penyalahgunaan teknologi informasi dan komunikasi dan membutuhkan perlindungan jaringan dan komputer, program dan data dari serangan, kerusakan, atau akses tidak sah, dan sebagai akibat dari pentingnya keamanan dunia maya dalam realitas masyarakat saat ini, banyak negara telah menjadikannya sebagai yang teratas prioritas, dalam referensi eksplisit berakhirnya perang konvensional yang menggunakan senjata berat, dan pengumuman dimulainya perang baru, yaitu perang dunia maya**.**

Pentingnya pendekatan masyarakat untuk membatasi eskalasi perang siber, bahwa kedaulatan dan keamanan negara kini bergantung pada kemampuannya untuk berperang di masa depan, dan karena itu negara-negara yang tidak memiliki teknologi maju dalam keamanan informasi dapat terkena dampak negatif dan sulit untuk tetap aman. Visi masa depan yang mempengaruhi keamanan nasional, seperti menuju perang pemusnahan yang komprehensif, mengubah keseimbangan kekuatan di dunia, dan masa depan keamanan nasional berkaitan dengan perkembangan teknik perang cyber**.**

Perang dunia maya menyebabkan lebih banyak perubahan daripada metode. Dan teknik dan taktik perang konvensional, karena mereka memengaruhi tingkat perang yang lebih tinggi, termasuk organisasi dan strategi militer, dan meningkatnya peran perang dunia maya memengaruhi teknologi serangan dan pertahanan di atas semua, karena senjata terkomputerisasi membutuhkan perlindungan terhadap serangan dunia maya pada saat ada kebutuhan untuk menghasilkan virus yang lebih efektif untuk merusak sistem komputer yang bermusuhan.

14. Kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi saat ini

Countries with the highest commitment to cyber security based on the Global Cybersecurity Index (GCI) in 2023

Characteristic	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	100	20	20	20	20	20
United Kingdom	99.54	20	19.54	20	20	20
Saudi Arabia	99.54	20	19.54	20	20	20
Estonia	99.48	20	20	20	19.48	20
Korea (Rep. of)	98.52	20	19.54	18.98	20	20
Singapore	98.52	20	19.54	18.98	20	20
Spain	98.52	20	19.54	18.98	20	20
Russian Federation	98.06	20	19.08	18.98	20	20

Arab Saudi secara aktif menangani kekurangan keterampilan TI dan keamanan siber melalui berbagai program. Pada 2019, Kerajaan melatih 751 karyawan di 113 perusahaan serta 288 siswa di protokol keamanan siber khusus. Beasiswa kepada 231 siswa di spesialisasi keamanan siber. Pada 2017, Pusat Sains dan Teknologi Raja Abdullah (KACST) mendirikan Saudi Research and Innovation Network (Maeen), keamanan informasi, dan menyelidiki serangan dunia maya. Pangeran Mohammed bin Salman College for Cybersecurity, Artificial Intelligence, dan Advanced Technologies mengembangkan sumber daya manusia nasional dalam kemampuan TI dan keamanan siber.

Pada tahun 2018, Keamanan Siber, Pemrograman, dan Drone (SAFCSP) didirikan untuk memacu inovasi teknologi dan memberikan pengembangan profesional kepada warga negara Saudi. Saudi Technology Development and Investment Company (TAQNIA), spesialisasi dalam TIK dan keamanan siber industri untuk perusahaan swasta. Program Badir mempromosikan kewirausahaan teknis dengan menawarkan pembiayaan dan inkubasi untuk startup di bidang keamanan dunia maya. Program Soft Landing startup internasional dan perusahaan baru di bidang teknologi untuk memfasilitasi akses ke pasar Saudi. Dalam benchmark Global Cybersecurity

Index ITU, Arab Saudi meningkat dari secara global pada tahun 2017 menjadi 13 pada tahun 2019, muncul sebagai pemimpin regional.

Kerajaan Arab Saudi telah menempati posisi kedua dalam Indeks Keamanan Siber global dalam Buku Tahunan Daya Saing Dunia (WCY) untuk tahun 2023 oleh International Institute for Management Development (IIMD). Arab Saudi juga menempati peringkat ke-17 secara keseluruhan pada tahun 2023 melonjak tujuh peringkat dari tahun 2022 dalam peringkat daya saing keseluruhan. Dengan Arab Saudi sering menempati peringkat di antara ekonomi teratas di dunia untuk keamanan siber, pengakuan terbaru oleh IIMD adalah bukti upaya entitas seperti National Cybersecurity Authority (NCA), salah satu pendukung keamanan nasional utama Arab Saudi. Arab Saudi telah mengukuhkan posisi kepemimpinannya melalui beberapa inisiatif untuk membangun ekosistem keamanan siber yang sehat dan berkelanjutan di Kerajaan.[36]

a. Transisi dari pencegahan nuklir ke pencegahan dunia maya.

Tidak ada strategi yang dapat mencegah semua aktivitas berbahaya di dunia maya, pencegahan dunia maya tidak secara otomatis gagal jika terjadi serangan. Maka harus fokus pada efek perilaku musuh, apakah itu akibat dari satu serangan dunia maya berskala besar atau lebih dari satu. Strategi dunia maya seharusnya tidak hanya berfokus pada pertahanan dan pencegahan, tetapi juga memengaruhi tren perilaku dan teknologi pertahanan dunia maya. Kesesuaian antara sarana yang digunakan untuk mencapai tujuan itu sendiri, lebih fokus pada kualitas operasi siber, baik ofensif maupun defensif. Transisi konsep penangkalan tradisional ke penangkalan siber melalui *National Cybersecurity Authority* guna menghindari kerusakan di dunia maya.

b. Pencegahan dan pencegahan dengan pembalasan.

Konsekuensi perang dunia maya penulis menerapkan teori cyber attack sesuai Undang-Undang Anti-Cybercrime tahun 2007, dua elemen harus ada: menghalangi dan mencegah serangan dunia maya, dan pencegahan dengan mengancam serangan dunia maya. Sebagaimana

[36]https://www.saudi-expatriates.com/2023/06/saudiarabia-ranks-second-in-world-in-cybersecurity-index.html diakses 2 Jun 2023

dituangkan dalam Undang-Undang Anti-Kejahatan Siber berkontribusi untuk mengurangi kejadian Kejahatan Siber : Ancaman hukuman penjara tidak lebih dari 10 tahun dan denda tidak lebih dari SR5 juta, membuat dan menerbitkan situs web untuk organisasi teroris di Internet, menghasut, membantu, setuju dengan kejahatan Cyber Crime.

1) **Penangkalan dengan pelarangan.** Pentingnya sistem pertahanan yang baik terbukti, yang membuat peluang keberhasilan setiap serangan minimal, meskipun tindakan defensif dan ofensif.
2) **Penangkalan dengan pembalasan.** Jenis penangkalan ini mencakup dua jenis lain: penangkalan dengan perlawanan dan penangkalan dengan keteguhan, dan ketabahan di sini berarti kemampuan untuk mengembalikan sesuatu ke bentuk aslinya sebelum penyerangan terjadi.

c. Orientasi terhadap tindakan defensif

Fondasi menjaga keamanan nasional dalam menghadapi perang dunia maya adalah mengamankan struktur informasi di lembaga-lembaga vital dan bergerak menuju sistem pertahanan sebagai berikut:

1) **Pembentukan badan dan lembaga yang peduli dengan keamanan siber**. (a) Menyusun rencana strategis nasional terkait keamanan siber. (c) mengelola perang dunia maya dan konflik elektronik yang pecah antar negara. (e) Meluncurkan inisiatif pendidikan dan kampanye kesadaran keamanan siber.
2) **Pentingnya membangun perlindungan pribadi yang kuat**. Membangun infrastruktur informasi nasional multi segi dan multi.
3) **Mengantisipasi risiko dan mencari cara untuk menghadapinya**. Menerapkan program komprehensif di tingkat lembaga dan lembaga negara yang bekerja untuk melatih para insinyur untuk mengusir peretasan dan pembajakan elektronik.
4) **Berinovasi berarti canggih baru untuk mengurangi risiko perang cyber**. Pengelolaan informasi dengan mendukung keamanan nasional memerlukan pemahaman dan visi baru tentang metode dan alat untuk pertukaran informasi antara pihak-pihak masyarakat dan satu sama lain secara internal dan eksternal.

5) **Mengembangkan dan memutakhirkan sarana perlindungan**. Peraturan perundang-undangan yang terintegrasi di bidang teknologi informasi.

6) **Mengamankan media penyimpanan**. Media penyimpanan eksternal atau yang disebut penyimpanan jaringan.

d. Orientasi terhadap tindakan ofensif

Serangan seringkali lebih baik daripada pertahanan, terutama jika ada sumber yang dikonfirmasi yang mengkonfirmasi bahwa serangan ini sama saja dengan perang preventif atau pencegahan. Landasan teori Cyber security ditujukan pada isu keamanan informasi bagi pemerintahan, organisasi dan individual dengan teknologi internet

1) **Membangun tentara modern**. Membangun pasukan modern yang mampu menghadapi tantangan masa depan dan bertujuan untuk melakukan spionase, serangan elektronik, dan perang informasi, persentase anggaran yang dialokasikan untuk keamanan dunia maya, yaitu sekitar (1,5) miliar setiap tahun.

2) **Peran pencegahan langsung**. Dengan jaringan yang mudah ditembus oleh peretas, serangan dunia maya dapat menimbulkan konsekuensi strategis yang parah, menghabiskan sumber daya yang tersedia, dan memerlukan keahlian unik. membutuhkan perpaduan sarana siber dan non-siber, mempertahankan keunggulan strategisnya melalui fleksibilitas dan pertahanan.

3) **Penggunaan teknologi elektronik dan kecerdasan buatan**. Pola perilaku yang mencurigakan dapat dideteksi lebih awal, serta merespons dengan segera dan tegas sebelum serangan dapat terbentuk sepenuhnya. Implementasi keamanan yang terfragmentasi. Keamanan terintegrasi diperlukan di masa depan, Sistem kecerdasan buatan menaungi banyak tugas kasar. Sistem keamanan dunia maya harus memiliki perencanaan dan strategi tingkat tinggi, operasi, mendeteksi, dan merespons peristiwa keamanan secara mandiri secara langsung.

e. Berorientasi pada komunitas internasional untuk mengurangi eskalasi perang siber.

Eskalasi perang dunia maya sangat mempengaruhi keamanan nasional dan ekonomi global dan dapat menciptakan konflik baru yang lebih berbahaya dan lebih kompleks. Peran masyarakat internasional menjadi salah satu peran yang paling menonjol untuk membatasi eskalasi perang dunia maya. Teori Global cyber security menurut Arnold harus dibangun : kepastian hukum; struktur organisasi. Capacity building Kerjasama Internasional upaya mengatasi ancaman cyber

1) **Aliansi dan kerja tim untuk mencapai dunia maya yang aman**. Negara secara kolektif dengan membentuk aliansi, mengadakan konferensi dan rumah keahlian, serta bertukar pengalaman dan informasi menjadi pencegah untuk melakukan kejahatan dunia maya, negara Arab telah menyetujui seperangkat undang-undang memerangi terorisme dunia maya, dan berada di garis depan negara-negara Arab terkemuka di bidang keamanan dunia maya (Arab Saudi, Uni Emirat Arab, Oman, Aljazair).

Negara-negara terkena serangan cybercrime

2) **Perjanjian regional dan internasional untuk keamanan siber**.

a) Negara-negara Persemakmuran, terutama setelah tahun (2002 M), memberlakukan beberapa teks hukum dan legislatif

untuk menghadapi ancaman dunia maya, dan yang paling menonjol dari teks-teks ini adalah Hukum Bukti Digital.

b) Komunitas Ekonomi Afrika Barat telah dimulai; Terutama setelah tahun (2009 M) dengan menghadirkan serangkaian rekomendasi untuk mengelola dan mengatasi konflik dunia maya, dan rekomendasi ini dianggap sebagai kerangka hukum dan legislatif yang dipatuhi oleh Negara Anggota.

c) Konvensi Arab tetang Pemberantasan Cybercrime telah disepakati; Untuk menjaga keselamatan publik, keamanan dan stabilitas di dunia Arab.

d) Perjanjian Budapest diselesaikan pada tahun 2001. Perjanjian Eropa tentang keamanan siber, dan perlu dicatat bahwa perjanjian ini merupakan pionir dalam hal kerjasama antar negara.Perjanjian ini mulai berlaku setelah tahun (2004 M).

e) Di tingkat internasional, Perserikatan Bangsa-Bangsa telah mengeluarkan serangkaian keputusan penting yang akan mencapai keamanan dunia maya, mengamankan dan melindungi sistem informasi, serta mendidik masyarakat internasional tentang keseriusan ancaman dunia maya. Keputusan tahun (1990 M) tentang Undang-Undang Tindak Pidana Informasi.

f) Keputusan tahun 2001 M untuk membentuk Kelompok Ahli Pemerintahan.

g) Keputusan tahun 2003 M tentang mencapai keamanan dunia maya dan menghadapi ancaman dan kejahatan dunia maya.

h) Keputusan tahun 2010 M dengan keamanan dunia maya, yang menekankan perlunya negara-negara untuk mencari kesesuaian kerangka hukum dan kemampuan dalam memerangi perang dunia maya.

3) **Mengaktifkan hukum internasional di bidang keamanan dunia maya**. Cybercrime adalah hal baru jenis kejahatan khusus dalam hal karakteristiknya melintasi batas-batas wilayah dan geografis, dampak destruktifnya terhadap berbagai institusi ekonomi dan

sosial militer dan sipil, dan terhadap berbagai organisasi pemerintah dan swasta, dalam hal ancamannya terhadap keamanan internasional secara umum, yang menekankan pentingnya masa depan cybersecurity, Perjanjian bilateral dan multipel untuk ekstradisi penjahat adalah salah satu metode terpenting untuk memerangi kejahatan ini yang didukung oleh hukum internasional untuk mengatasi fitur lintas batas. Sesuai teori konsep cyber security tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional.

4) **Kerjasama internasional antar lembaga kepolisian.** Kerjasama antara semua negara untuk memberantas kejahatan lintas batas, mengembangkan prosedur umum layanan kepolisian di semua negara. berkoordinasi dengan lembaga polisi antar negara. Membentuk penghubung antara lembaga kepolisian di seluruh dunia. Kerja sama komunikasi antar lembaga kepolisian. Kerja sama lapangan Polisi internasional/INTERPOL. Mencari database Internet dengan ahli internasional dan laboratorium internasional di tingkat global, Kerja sama operasional administrasi bandar udara, bea cukai, penjaga perbatasan, intelijen atau pasukan khusus polisi. Kerja sama memerangi serangan dunia maya dengan Polisi Internet Internasional. Pusat Pelaporan Penipuan Elektronik.

5) **Kerjasama peradilan internasional.** Kerjasama Peradilan Internasional menyeimbangkan kekhususan negara dalam menjalankan otoritas kriminalnya di wilayahnya dan haknya.. Kedaulatan internasional setiap negara memiliki hak untuk menerapkan hukuman di wilayahnya. Penerapan hukum pidana memerlukan prosedur pidana pada kerjasama yudisial. pelanggaran batas internasional kejahatan dunia maya membutuhkan kerja sama polisi dan yudisial untuk dapat mengadili dan menghukum para pelaku kejahatan ini..

6) **Perencanaan strategis untuk menjaga keamanan siber.** Keamanan siber memerlukan kesiapan yang komprehensif di tingkat dimensi militer dan politik.

a) Perencanaan untuk mengatasi risiko serangan dunia maya. (1) Keganasan serangan informasi. (2) Kapasitas destruktif serangan (3) Perang asimetris Aktor non-negara dapat berpartisipasi dalam serangan ini dan perang asimetris berskala besar. (4) Konflik dunia maya.

b) Perencanaan untuk meningkatkan kemampuan tempur militer dengan teknologi informasi dan komunikasi sebagai senjata, Penggunaan operasi dunia maya dapat mencapai keunggulan dalam lingkup perang informasi, meningkatkan kemampuan tradisional dari kekuatan keras, dengan meluncurkan operasi ofensif dan defensif bersamaan dengan intervensi bersenjata.

c) Pilar Dunia Maya. Kredibilitas pertahanan, mempertahankan sistem informasi dan menghalangi setiap upaya untuk menembusnya. Keinginan untuk membalas dendam Konflik nuklir. Kemampuan untuk membalas. Balas dendam seringkali membutuhkan kehancuran yang lebih berbahaya.

Pentingnya menjaga keamanan nasional akibat eskalasi perang dunia maya dengan melindungi institusi vital negara sebab ini memerlukan penerapan strategi defensif dan ofensif di samping kekuatan diplomasi negara serta bekerja sama dengan komunitas internasional untuk mengurangi perang siber, ada indikasi kelompok teroris mengembangkan kemampuan dunia maya, yang mengancam infrastruktur informasi negara.

f. Upaya Arab Saudi untuk meningkatkan kemampuan *National Cybersecurity Authority*.

Dengan akselerasi transformasi digital yang luar biasa, tingkat serangan dunia maya dan risiko pelanggaran data telah meningkat, membuat Kerajaan lebih tertarik dalam menyediakan lingkungan yang aman untuk operasi data dan digital melalui sistem keamanan yang solid.

1) **Program dan inisiatif nasional**. Kerajaan Arab Saudi bekerja untuk membangun dan meluncurkan prakarsa pendidikan dan pelatihan khusus untuk membantu kualifikasi dan membangun

kompetensi nasional yang menonjol Program dan prakarsa nasional yang diluncurkan oleh Pemerintah Kerajaan Arab Saudi meliputi:

a) **Pusat Panduan Keamanan Siber**. Pusat Penasihat Keamanan Siber Nasional diluncurkan untuk meningkatkan kesadaran keamanan siber, menghindari risiko siber dan mengurangi dampaknya, memberi peringatan kerentanan dan paling berbahaya, meluncurkan kampanye dan program kesadaran, dan bekerja sama dengan pusat penasihat lainnya.

b) **Federasi Saudi Keamanan Siber**. Federasi Saudi untuk Keamanan Siber di bawah Komite Olimpiade Saudi guna kemampuan profesional keamanan siber, pengembangan perangkat lunak, dan drone. Menyediakan kegiatan dan program meningkatkan kesadaran masyarakat keamanan siber, pemrograman, dan drone, mendukung dan mendorong generasi muda untuk menjadi profesional di bidang ini.

c) **Akademi Keamanan Siber Nasional.** Bekerja sama dengan Dana Pengembangan Sumber Daya Manusia guna meningkatkan kemampuan digital nasional di berbagai bidang teknologi modern untuk mengimbangi kebutuhan transformasi digital.

d) **Komisi Komunikasi dan Informatika.** Komisi Teknologi Komunikasi dan Informasi, dengan mengatur keamanan dunia maya di Kerajaan. (1) Melindungi kepentingan umum dan kepentingan pengguna. (2) Menjaga kerahasiaan komunikasi dan keamanan informasi, sesuai dengan standar kualitas dan keamanan tertinggi. (3) Meningkatkan tingkat kematangan keamanan dunia maya di Kerajaan pada umumnya, dan khususnya di sektor komunikasi, teknologi informasi, dan pos.

e) **Otoritas Nasional untuk Keamanan Siber**. Otoritas Keamanan Siber Nasional di Kerajaan Arab Saudi telah mengembangkan kontrol dasar untuk keamanan siber,

mempelajari persyaratan nasional terkait undang-undang, peraturan dan keputusan.

f) **inisiatif Haseen**. Meningkatkan keamanan dunia maya di tingkat nasional dan peduli dengan perlindungan email dari spoofing dan penggunaan yang tidak sah. (1) Untuk mengetahui tingkat penerapan inisiatif Haseen entitas. (2) membuat rekaman nama domain. (3) Survei catatan nama domain. (4) Mendidik otoritas nasional tentang pentingnya mengaktifkan otentikasi nama domain dan metode penerapannya. Portal Nasional untuk Layanan Keamanan Siber (HASEEN) untuk mengembangkan dan mengelola layanan siber, mendukung mekanisme komunikasi untuk penerima manfaat nasional, meningkatkan tingkat keamanan siber di Kerajaan, mengatur anggaran keamanan siber nasional dan pengembangan konten lokal di sektor TIK. HASEEN dikembangkan platform berbagi informasi, manajemen kepatuhan, memeriksa file dan tautan, dan otentikasi email.

2) **Berinvestasi di pasar keamanan cyber**. Pangsa pasar keamanan siber Saudi meningkat pada 2023 menjadi lebih dari 21 miliar riyal sebagai sektor yang paling menonjol, dan investasi di bidang ini berada di sektor energi sebesar 4,6 miliar riyal.

3) **Mempersiapkan kader manusia secara teknis.** Meningkatkan keamanan siber di Kerajaan Arab Saudi, NEOM melakukan pelatihan bidang keamanan siber bekerjasama dengan mitra lokal seperti National Authority for Cybersecurity, Universitas Pangeran Muqrin bin Abdulaziz, dan Universitas Tabuk. Mengembangkan program pelatihan dan pendidikan keamanan siber di NEOM dan Tabuk.

4) **Legislasi hukum di bidang keamanan siber**. Pada September 2021, Arab Saudi mengumumkan undang-undang perlindungan data pertamanya. UU Perlindungan Data Pribadi (PDPL) melalui Keputusan Kerajaan M/19 tanggal 2/9/1443H dengan No.98

tanggal 7/2/1443H 14 September 2021. PDPL mengatur pengumpulan, penanganan, pengungkapan dan penggunaan data pribadi dan termasuk kewajiban tata kelola dan transparansi. PDPL berlaku pada 23 Maret 2022. Pada 21 Maret 2023, beberapa amandemen ini disahkan oleh Dewan Menteri Saudi.

15. Visi Masa depan cyber security dan dampaknya terhadap keamanaan digital di Kerajaan Arab Saudi

a. Menuju perang pemusnahan yang komprehensif

1) **Pentingnya membangun perlindungan pribadi yang kuat**. Secara perencanaan dan administratif salah bagi negara mana pun untuk secara aktif membangun infrastruktur informasi nasional multi segi dan multi-level dengan cara ini dan kemudian tidak mengembangkan kebijakan atau strategi nasional untuk melindungi infrastruktur ini dan menjaga keamanannya dan keamanan data dan informasi yang beredar di dalamnya, menyerahkannya pada tindakan spontan, inisiatif individu, proyek, dan rencana parsial berlebihan yang terjadi di sana-sini tanpa kebijakan atau strategi yang jelas. Melanjutkan pembangunan infrastruktur informasi nasional yang sangat besar tanpa strategi keamanan yang komprehensif dan memadai merupakan cacat serius dalam proses pengembangan informasi, dan berdampak negatif terhadap keamanan nasional..

2) **Mengantisipasi risiko dan mencari cara untuk menghadapinya**. Bahaya perang dunia maya kini telah meningkat ke tingkat yang mengancam keamanan nasional secara keseluruhan, sarana konfrontasi dan perlindungan harus dibayangi oleh sistem keamanan nasional, karena bahaya dan ancaman itu salah jika bersifat komprehensif dan mungkin terkoordinasi. dan kadang-kadang direncanakan, maka cara dan sarana untuk menghadapinya menjadi parsial, spontan, tanpa perencanaan dan kurangnya koordinasi dan rasionalitas.

3) **Berinovasi berarti canggih baru untuk mengurangi risiko perang cyber**. Pengelolaan informasi yang beredar dalam infrastruktur informasi nasional dengan cara yang mendukung keamanan nasional memerlukan pemahaman dan visi baru tentang metode, metode dan alat untuk pertukaran informasi antara pihak-pihak masyarakat dan satu sama lain secara internal, serta pendekatan, alat dan metode. Mengelola dan bertukar informasi antara mereka dan pihak eksternal, seperti mitra dalam politik, perdagangan, bisnis, pendidikan, dan penelitian ilmiah Industrialisasi, dan ini merupakan masalah penting dan kompleks pada saat yang sama, dan tidak benar untuk menyerahkannya kepada yurisprudensi individu, lembaga dan ahli.

4) **Mengembangkan prosedur keamanan jaringan**. Menempatkan prosedur untuk melindungi dan memastikan keamanan jaringan melalui pemeriksaan terus menerus terhadap sistem ini dan menyediakan perangkat khusus untuk pengujian, dan sistem operasi yang digunakan dan bertanggung jawab untuk mengelola komputer harus memiliki efisiensi dan kemampuan tinggi untuk mendeteksi intrusi ke dalam jaringan.

b. Mengubah keseimbangan kekuatan di dunia

Sumber kekhawatirannya adalah untuk menutup celah yang mengakibatkan kebocoran rahasia negara yang mencengangkan, pencurian kekayaan intelektual, campur tangan asing melalui dunia maya dalam politik, dan buruknya kinerja keamanan dunia maya untuk banyak sektor ekonomi dan masyarakat. Masa depan yang mengharuskan kita mempersenjatai diri dengan iman, pengetahuan, dan sains, bekerja menghadapi banyak tantangan. Tingkat Baik di sektor publik dan swasta, maupun di tingkat militer, tetapi juga di tingkat pribadi, menggunakan teknologi informasi dan komunikasi secara lokal dan global. Membuat kebijakan dan strategi nasional untuk melindungi infrastruktur nasional untuk komunikasi dan informatika, Mengembangkan teknologinya dan mempersiapkan diri dengan baik

untuk dunia maya, menerapkan perlindungan kemampuan Patriotisme dan menjaga kesejahteraan dan keamanan warga negara dengan melindungi infrastruktur informatika dan komunikasi nasional dari bahaya penyalahgunaan teknologi ini oleh musuh, orang yang iri atau jahat.

c. Masa depan keamanan nasional dalam perkembangan teknik perang siber

Visi Kerajaan Arab Saudi dianggap sebagai salah satu visi global paling menonjol yang mengadopsi pengembangan sistem teknis alat dan sarana perang, sebagaimana visi Kerajaan Arab Saudi (2030) diarahkan. Menuju keamanan dunia maya dan menjadi panutan, terutama dalam teknologi, karena didasarkan pada aspek transformasi digital dan kemajuan teknis dan teknologi, mendukung keamanan siber dengan seperangkat kebijakan dan rencana strategis, terutama dalam fase transisi ke dunia maya, sebagai akibat dari Strategi Nasional Keamanan Siber :

1) **Visi strategis nasional untuk keamanan siber**. Otoritas Keamanan Siber Nasional sangat ingin mencapai visinya (ruang siber yang aman dan andal yang memiliki kemampuan untuk mencapai pertumbuhan dan kemakmuran sehingga Kerajaan dapat mencapai ambisi dan aspirasinya untuk melindungi infrastruktur dan sistem teknologi serta teknologi modern, dan meningkatkan kepercayaan otoritas nasional dan investor di dunia maya Saudi, tujuan yang diwakili secara terintegrasi tata kelola keamanan siber di tingkat nasional, pengelolaan risiko siber yang efektif, perlindungan ruang siber, penguatan kemampuan teknis nasional dalam pertahanan terhadap ancaman siber, penguatan kemitraan dan kerja sama di bidang ini:
   a) Bekerja pada proyek pengembalian tinggi .
   b) Mengerjakan program untuk mendukung otoritas nasional.
   c) Bekerja untuk mengimplementasikan sejumlah inisiatif nasional .Otoritas Cybersecurity untuk menerjemahkan strategi nasional ini ke dalam tindakan kelembagaan secara

terintegrasi dengan otoritas terkait, untuk mencapai dunia maya Saudi yang aman dan andal.

2) **Tema strategi nasional keamanan siber**. Menjaga keamanan nasional berlangsung, sebagai berikut:

a) Integrasi. Mencapai integrasi berbagai elemen dan komponen sistem keamanan siber, dan sumbu ini mencakup tiga elemen, yaitu: (a) Peraturan dan kebijakan..(b) Mengukur efektivitas strategi nasional. (c) Tata kelola dan manajemen keamanan siber . melaksanakan operasi.

b) Organisasi. Bertujuan untuk menjelaskan infrastruktur kritis dan menghadapi ancaman dunia maya, dan sumbu ini mencakup dua elemen utama sebagai berikut: (a) Mengelola risiko dan ancaman dunia maya. (b) Standar dan pengawasan nasional. Mengembangkan kerangka referensi yang berisi seperangkat kontrol dan standar nasional yang diperlukan untuk mencapai keamanan dunia maya.

c) Penekanan. Berputar di sekitar gagasan perlindungan ruang angkasa dunia maya. (1) Kesadaran keamanan dunia maya. Meluncurkan kampanye kesadaran pendidikan dan pelatihan; (2) Identitas digital nasional. Memperkuat dan angkat derajat keandalan identitas digital di dalam luar angkasa dunia maya. (3) koding nasional Buat sistem enkripsi Informasi, termasuk pengembangan dan evaluasi sistem, algoritme, dan standar enkripsi nasional yang sangat efisien .

d) Pertahanan. (a) Mengidentifikasi, menganalisis, dan memantau ancaman dan isiko Risiko dunia maya yang menghalangi keamanan. (b) Mengidentifikasi setiap celah yang dapat dimanfaatkan untuk menghadapi ancaman dunia maya. (c) Pemantauan, koordinasi dan promosi tingkat diluar jangkauan keamanan dan menentukan kualitasnya ancaman Cyber dan klasifikasinya. (d) Responnya untuk kecelakaan Dan tes Rencananya .(e) Kelangsungan dan pemulihan bisnis dengan ketergantungan rencana untuk keadaan darurat , dan

tes cokelat infrastruktur peka dan layanan Teknis dan teknologi vitalitas dan kesiapan masa depan .

e) Kerjasama. Untuk membangun hubungan partisipatif dan berbagi informasi.

f) Konstruksi. (a) Penelitian dan pengembangan industri keamanan siber. Merangsang melakukan lebih banyak penelitian dan studi terkait keamana. (b) Membangun kapasitas nasional melalui persiapan dan rehabilitasi sumber daya kemanusiaan nasional spesialis (c) Infrastruktur keamanan, dengan cara mengembangkan dan kontrol untuk evaluasi dan pengujian.

3) **Tujuan Strategi Nasional Keamanan Siber**.

a) Tata kelola terpadu keamanan siber di tingkat nasional dari Oke jaminan skor Banyak tugas koordinasi dan integrasi dan pekerjaan institusi berkaitan dengan pencapaian keamanan cyber

b) Pengelolaan ancaman dunia maya yang efektif di tingkat nasional Dengan mengidentifikasi mekanisme terbaik, mengikuti prosedur perlindungan dan pertahanan, dan mengidentifikasi cara untuk melaporkan insiden dunia maya .

c) Perlindungan dunia maya. Dengan kontrol Inklusif dan standar Nasional, sekaligus meningkatkan derajat pemahaman dan kesadaran anggota masyarakat tentang keamanan siber.

d) Meningkatkan kemampuan teknis pertahanan nasional terhadap ancaman siber bantuan dan pengembangan rajin untuk potensi Nasional di dalam Pertahanan melawan serangan dunia maya,

e) Memperkuat kemitraan dan kerjasama di bidang keamanan siber . temuan Kemitraan patriotisme Dan universal efektif, Dan penuh Dengan sarana dan teknologi modern dan canggih untuk berbagi praktik data dan informasi.

f) Menyiapkan dan mengkualifikasikan kader insan nasional serta mengembangkan industri keamanan siber dan itu

menginisialisasi dasar kuat dari Sumber daya manusia yang berkualitas di dalam ini. Bidang Informasi dan Komunikasi Strategi ini berupaya melindungi infrastruktur informasi dan komunikasi serta membangun masyarakat yang mampu .

16. Strategi meningkatkan kapastitas *National Cybersecurity Authority* (NCA

a. Tata Kelola

Struktur tata kelola *National Cybersecurity Authority* termasuk semua entitas dengan tanggung jawab dan wewenang untuk memajukan digital dan mengurangi risiko ketidakamanan siber. Usaha tersebut harus dengan jelas menyatakan tujuan dan hasil, mengidentifikasi peran dan tanggung jawab pemangku kepentingan, mengidentifikasi dan memberdayakan otoritas kompeten yang bertanggung jawab atas pelaksanaan usaha, berkomitmen memasukkan tujuan spesifik, terukur, dapat dicapai, berbasis hasil dan waktu dalam rencana implementasi; dan mengenali kebutuhan untuk melakukan sumber daya (kemauan politik, pendanaan, waktu, dan orang) untuk mencapai hasil yang diinginkan.

1) **Memastikan tingkat dukungan tertinggi.** Tata kelola harus memiliki dukungan formal dari tingkat pemerintahan tertinggi, meningkatkan sumber daya yang memadai dan koordinasi. Ekosistem nasional yang bergantung pada sistem digital dan prioritas nasional. Kodifikasi kerangka hukum domestik untuk mendapatkan relevansi dan prioritas nasional.

2) **Menguatkan *National Cybersecurity Authority* yang kompeten.** *National Cybersecurity Authority* dengan otoritas kompeten nasional khusus tanggung jawab otoritasnya. Kewenangan tertinggi memberikan arahan, mengoordinasikan tindakan, dan memantau implementasi kebijakan. Melaporkan kemajuan dan hasil programnya. Mengklarifikasi peran, tanggung jawab, proses, hak keputusan, dan tugas implementasi program. Mengawasi pelaksanaan usaha dan menetapkan target kinerja untuk berbagai kementerian atau departemen pemerintah, lembaga, atau individu

yang bertanggung jawab. Memastikan bahwa otoritas nasional yang kompeten memiliki kemampuan untuk melibatkan dan mengarahkan pemangku kepentingan yang relevan, undang-undang tambahan yang mengamanatkan entitas pemerintah untuk melaporkan kembali kepada otoritas kompeten nasional. Menggunakan indikator kinerja utama dalam menilai kemajuan.

3) **Menjamin kerja sama intra-pemerintah.** Komitmen, koordinasi, dan kerja sama intra-pemerintah merupakan fungsi inti dari lembaga-lembaga pemerintah tersebut, yang diperlukan untuk memastikan bahwa mekanisme tata kelola (standar, peraturan, insentif) dan sumber daya menghasilkan hasil kebijakan yang diinginkan. Memiliki otoritas kompeten *National Cybersecurity Authority* tingkat tinggi yang mapan. Memastikan kementerian dan lembaga pemerintah mengetahui kewenangan, misi, dan tugas masing-masing. Komitmen mendukung kebijakan yang konsisten dari waktu ke waktu dalam pertemuan berkala dan pembentukan gugus tugas intra-pemerintah untuk mengatasi masalah tertentu.

4) **Menjamin kerjasama antar sektor.** *National Cybersecurity Authority* pemahamanan dalam mencapai ekosistem yang lebih aman, selamat, dan tangguh. Mengartikulasikan melibatkan para pemangku kepentingan yang berbeda ini dan menentukan peran dan tanggung jawabnya. *Men*selaraskan dengan prioritas nasional lainnya, seperti memastikan konektivitas terjangkau, tersedia, dan inklusif; memajukan perlindungan data dan privasi; memperkuat ketahanan infrastruktur dan ketersediaan layanan; menjelajahi teknologi baru seperti AI, blockchain, komputasi kuantum.

5) **Alokasikan anggaran dan sumber daya khusus.** Alokasi sumber daya khusus dan tepat untuk implementasi, pemeliharaan, dan revisinya. Pendanaan yang cukup, konsisten, dan berkelanjutan memberikan fondasi untuk postur keamanan siber nasional yang efektif. Komitmen dan kepemimpinan politik, yang didukung oleh kemitraan terpercaya. Mempertimbangkan pembentukan anggaran

pusat untuk keamanan siber tata kelola *National Cybersecurity Authority*.

6) **Mengembangkan rencana implementasi.** Mengidentifikasi entitas akuntabel yang bertanggung jawab untuk setiap tugas dan tujuan, sumber daya yang diperlukan dalam jangka pendek, jangka menengah, jangka panjang, proses yang akan digunakan, dan hasil yang diharapkan.

b. Manajemen risiko dalam *National Cybersecurity Authority*

Dalam menangani keamanan siber melalui manajemen risiko. Sebagaimana diatur dalam Prinsip Manajemen Risiko dan Ketahanan, pendekatan manajemen risiko harus diadopsi, karena risiko dunia maya tidak dapat sepenuhnya dihilangkan. Dalam hal menilai risiko, pendekatan harus berfokus pada identifikasi antar-ketergantungan dan juga mempertimbangkan risiko yang timbul dari ketergantungan lintas batas negara.

1) **Melakukan penilaian ancaman dunia maya** dan menyelaraskan kebijakan dengan lanskap ancaman dunia maya yang terus berkembang. Mengevaluasi lingkungan ancaman dunia maya yang terus berkembang serta dampak dan konsekuensi potensial pada infrastruktur penting dan layanan penting. Mengidentifikasi infrastruktur dan layanan kritis domestik. Menginformasikan dan membantu menyelaraskan kebijakan manajemen risiko dunia maya dengan rencana manajemen krisis negara. Ini juga dapat membantu memanfaatkan kemampuan/kapasitas, orang, pendanaan, dan strategi untuk memperkuat keseluruhan postur keamanan siber Bangsa.

2) Tentukan pendekatan manajemen risiko. Menetapkan pendekatan yang koheren untuk manajemen risiko yang harus diikuti oleh semua entitas pemerintah dan operator infrastruktur penting yang diidentifikasi di dalam negeri. Membangun penilaian ancaman dunia maya dan mengembangkan daftar risiko nasional. Pengawasan pemerintah terhadap risiko dan pendekatan yang

diambil untuk mengelolanya. Mengembangkan metode penentuan prioritas berdasarkan perhitungan kemungkinan menyadari risiko dan dampaknya. Penentuan tanggung jawab entitas utama di setiap sektor terkait penilaian, penerimaan, dan penanganan risiko keamanan siber tingkat nasional.

3) **Identifikasi metodologi umum untuk mengelola risiko keamanan siber.** Mengidentifikasi metodologi umum untuk mengelola risiko keamanan siber. Efisiensi dan konsistensi di seluruh organisasi dan memfasilitasi pertukaran informasi ancaman dan risiko di seluruh sistem yang saling bergantung. Metodologi standar internasional harus diutamakan karena dapat mengurangi biaya dan menghasilkan interaksi yang lebih baik dengan sektor swasta. Metodologi harus mencakup program sertifikasi untuk membantu menilai dan akhirnya meningkatkan kepatuhan.

4) **Mengembangkan profil risiko keamanan siber sektoral.** Menyerukan penggunaan profil risiko sektoral untuk keamanan siber. Profil risiko sektoral merupakan analisis kuantitatif terhadap jenis ancaman yang dihadapi. Penggunaan profil risiko sektoral memberikan dasar untuk penilaian risiko yang lebih spesifik untuk masing-masing organisasi, memperkenalkan koherensi di dalam dan di semua sektor secara nasional, dan mengurangi sumber daya yang diperlukan untuk penilaian risiko organisasi.

5) **Menetapkan Strategi keamanan siber.** Mendorong pembentukan kebijakan keamanan siber untuk entitas nasional yang kritis, antara lain, seperti otoritas pemerintah dan operator infrastruktur penting. Pengembangan menentukan program berbagi informasi, mengoordinasikan pengungkapan kerentanan, menetapkan standar perawatan minimum, garis dasar keamanan, program sertifikasi untuk kepatuhan, dan mengamanatkan pelaporan insiden keamanan siber kepada otoritas yang berwenang. Pendekatan terkoordinasi di tingkat nasional dapat menghasilkan manajemen keamanan siber yang lebih efisien dan efektif guna

menyelaraskan praktik dan memfasilitasi koordinasi dan interoperabilitas.

c. Kesiapsiagaan dan ketahanan

1) **Menetapkan kemampuan respons insiden dunia maya.** Pembentukan kemampuan respons insiden nasional yang tepat untuk mengatasi tantangan keamanan siber operasional. Pembentukan Tim Tanggap Darurat Komputer (CERT), Tim Tanggap Insiden Keamanan Komputer (CSIRT), atau Tim Tanggap Insiden Komputer (CIRT) dengan tanggung jawab nasional. Meskipun bentuk organisasi tertentu dari CERT/CSIRT/CIRT nasional, pemerintah, sektoral. Tim khusus dan berdedikasi ini harus menyediakan satu set, fungsi proaktif dan reaktif, serta layanan preventif dan pendidikan. Layanan CERT/CSIRT/CIRT respons dan koordinasi insiden dunia maya, manajemen kerentanan, kesadaran situasional, transfer pengetahuan, dan berbagi informasi ancaman dan intelijen. Pembentukan PSIRT (Product Security Incident Response Teams) oleh sektor swasta untuk meningkatkan kemampuan menangani kerentanan produk TIK. Mengembangkan mekanisme kerja sama dan prosedur komunikasi antara tim tanggap insiden nasional dan sektoral serta dengan mitra internasional.
2) **Menyusun rencana darurat untuk manajemen krisis keamanan siber dan pemulihan bencana.** Pengembangan rencana darurat nasional untuk keadaan darurat dan krisis keamanan siber. Rencana khusus untuk infrastruktur informasi penting. Memberikan gambaran tentang mekanisme respon insiden nasional; serta menyoroti insiden keamanan siber dikategorikan dan ditingkatkan, berdasarkan dampaknya terhadap aset dan layanan penting.
3) **Mempromosikan berbagi informasi.** Pembentukan mekanisme berbagi informasi untuk memungkinkan pertukaran informasi intelijen dan ancaman yang dapat ditindaklanjuti antara dan di antara sektor publik dan swasta. Program berbagi informasi formal

dan informal dapat membantu mendorong koordinasi yang efektif dan komunikasi yang konsisten, akurat, dan tepat selama respons insiden dan kegiatan pemulihan; memfasilitasi pembagian informasi ancaman dan intelijen dengan cepat di antara pihak-pihak yang terkena dampak dan pemangku kepentingan lainnya; membantu meningkatkan pemahaman tentang bagaimana dan sektor mana yang menjadi sasaran; menyebarluaskan informasi tentang metode yang dapat digunakan untuk mempertahankan dan mengurangi kerusakan pada aset yang terkena dampak.

4) **Melakukan latihan keamanan siber.** Mendorong organisasi dan koordinasi keamanan siber domestik dan internasional serta latihan tanggap insiden. Simulasi atau latihan waktu nyata dan menargetkan audiens teknis dan non-teknis. Latihan keamanan siber dan mekanisme perencanaan krisis lainnya, memverifikasi kemampuan operasional CERT/CSIRT/CIRT untuk merespons insiden keamanan siber dan gangguan layanan di bawah tekanan, dan membantu memahami ketergantungan lintas sektor. Memperkuat kapasitas respons insiden dunia maya antar negara, memahami ketergantungan lintas batas, membangun kepercayaan dan kepercayaan antar negara, dan meningkatkan tingkat ketahanan dan kesiapan internasional secara keseluruhan.

5) **Menetapkan penilaian dampak atau keparahan insiden keamanan siber.** Mendorong pembentukan mekanisme penilaian dampak atau tingkat keparahan untuk menilai dan mengevaluasi insiden keamanan siber berdasarkan dampaknya terhadap aset, layanan, infrastruktur, dan orang-orang penting. Penilaian berbagai pemangku kepentingan secara terbuka, inklusif, dan transparan dan diintegrasikan ke dalam pemulihan bencana nasional dan rencana darurat.

d. Infrastruktur Kritis dan layanan penting

Menyelidiki praktik baik dengan melindungi Infrastruktur Kritis (CI) dan Infrastruktur Informasi Kritis (CII), dan memperkuat ketahanannya.

1) **Menetapkan pendekatan manajemen risiko untuk mengidentifikasi dan melindungi infrastruktur penting dan layanan penting.** Pentingnya melindungi CI dan CII dari risiko terkait dunia maya dan menyusun pendekatan manajemen risiko yang komprehensif sesuai dengan Prinsip Manajemen Risiko dan Ketahanan. Strategi harus menyertakan atau disertai dengan daftar CI dan/atau CII tertentu dan korelasinya, yang dapat ditinjau dan diperbarui secara berkala sesuai kebutuhan. Menerapkan kriteria sektoral atau fungsional, seperti ketergantungan dan saling ketergantungan dengan infrastruktur lain, layanan, dan cakupan dampak, dan relevansi infrastruktur untuk mempertahankan layanan minimum. Memanfaatkan praktik terbaik yang ada, memungkinkan industri dalam negeri untuk berintegrasi dengan rantai pasokan TIK global, dan menghindari masalah interoperabilitas CI/CII lintas batas negara, pendekatan manajemen risiko.
2) **Mengadopsi model tata kelola dengan tanggung jawab yang jelas.** Menggambarkan struktur tata kelola, peran, dan tanggung jawab berbagai pemangku kepentingan untuk perlindungan CI dan CII. Program perlindungan CI yang efektif dan efisien mensyaratkan pemangku kepentingan memiliki peran dan tanggung jawab yang jelas dan menetapkan mekanisme koordinasi untuk mengelola masalah yang sedang berlangsung. CI dan CII seringkali tidak dimiliki atau dikendalikan oleh pemerintah, dan upaya perlindungan CI dan CII umumnya melebihi kemampuan dan mandat dari satu lembaga tunggal dalam pemerintahan. Komite antarlembaga membantu dalam upaya melindungi infrastruktur penting.
3) **Menentukan baseline keamanan siber minimum.** Mengusulkan pengembangan kerangka kerja legislatif dan peraturan baru yang menguraikan antara lain garis dasar keamanan siber minimum untuk operator CI dan CII. Baseline keamanan prioritas manajemen risiko tingkat tinggi serta praktik keamanan siber yang lebih spesifik, seperti mengidentifikasi risiko siber dan membangun struktur tata

kelola manajemen risiko; melindungi data dan sistem melalui protokol manajemen akses dan tindakan lainnya; memantau lingkungan digital dan mendeteksi potensi anomali atau peristiwa; dan menanggapi dan pulih dari insiden. Standar dan praktik terbaik yang diakui secara internasional. Fokus pada hasil untuk memastikan ketangkasan yang lebih besar dari waktu ke waktu karena lanskap risiko dan teknologi terus berkembang pesat. Pembentukan lingkungan nasional CI dan CII yang tangguh, dan mempersiapkan pemangku kepentingan untuk merespons, memitigasi, dan memulihkan dari potensi insiden keamanan siber.

4) **Memanfaatkan berbagai pengungkit pasar.** Strategi ini mempertimbangkan berbagai kebijakan untuk memastikan bahwa semua organisasi dan individu memang diberi insentif untuk memenuhi tanggung jawab keamanan siber masing-masing. Mengidentifikasi kesenjangan antara apa yang dapat dan harus didorong oleh pasar dan apa yang dibutuhkan oleh lingkungan risiko merupakan langkah penting untuk menentukan kapan dan bagaimana memanfaatkan kisaran insentif dan disinsentif yang tersedia untuk meningkatkan keamanan. Mendorong penerapan standar dan praktik keamanan siber di seluruh CI dan CII.

5) **Membangun kemitraan publik-swasta.** Mendorong terciptanya kemitraan publik-swasta formal untuk meningkatkan keamanan CI dan CII. Membangun kemitraan yang berkelanjutan mensyaratkan bahwa semua pemangku kepentingan yang berpartisipasi memiliki pemahaman yang jelas tentang tujuan kemitraan dan manfaat keamanan bersama yang berasal dari kerja sama. Mengembangkan garis dasar keamanan siber lintas sektor dan khusus sektor, membangun struktur koordinasi yang efektif serta proses dan protokol berbagi informasi, membangun kepercayaan, mengidentifikasi dan bertukar ide, pendekatan, dan praktik terbaik untuk meningkatkan keamanan, serta meningkatkan koordinasi internasional.

e. Peningkatan kemampuan dan kapasitas serta peningkatan kesadaran

Tantangan yang berkaitan dengan memajukan pembangunan kapasitas keamanan siber (baik manusia maupun kelembagaan) dan peningkatan kesadaran di antara para pemangku kepentingan, termasuk entitas pemerintah, warga negara, bisnis, dan organisasi lainnya yang sangat penting untuk memungkinkan digital. Praktik baik meliputi koordinasi kegiatan peningkatan kapasitas, pembentukan kurikulum khusus keamanan siber dan program peningkatan kesadaran, perluasan skema pelatihan dan program pengembangan tenaga kerja, adopsi skema sertifikasi internasional, dan promosi inovasi serta penelitian dan pengembangan (R&D) cluster.

1) **Merencanakan secara strategis peningkatan kemampuan dan kapasitas serta peningkatan kesadaran.** Menetapkan peran dan tanggung jawab yang jelas kepada entitas yang bertugas mengkoordinasikan kegiatan peningkatan kapasitas dan peningkatan kesadaran di tingkat nasional untuk memastikan sumber daya disederhanakan, upaya tidak diduplikasi, dan akuntabilitas ditetapkan. Bertanggung jawab untuk memantau implementasi dan mengevaluasi hasil dari kegiatan tersebut, serta merekomendasikan perubahan. Kapabilitas keamanan siber dan peningkatan kapasitas serta peningkatan kesadaran harus berbasis bukti dan direncanakan secara strategis. Penilaian mendetail tentang lanskap keamanan siber nasional dan inisiatif pembangunan kapasitas saat ini harus memandu identifikasi kesenjangan yang ada dalam kebutuhan kapasitas, keterampilan, dan kesadaran serta menginformasikan solusi berwawasan ke depan. Alokasi anggaran, jadwal, dan metrik untuk memantau kemajuan dari setiap tindakan yang direncanakan tersebut.
2) **Mengembangkan kurikulum keamanan siber.** Memfasilitasi pengembangan atau perluasan kurikulum sekolah khusus yang ditujukan untuk mempercepat pengembangan dan kesadaran keterampilan cybersecurity di seluruh sistem pendidikan formal.

Kurikulum harus bersifat inter/multi-disiplin dan mencakup tidak hanya teknis tetapi juga keterampilan dan topik cybersecurity non-teknis, seperti literasi digital, kebijakan publik, hukum, tata kelola, ekonomi, manajemen risiko, etika, ilmu sosial, dan hubungan internasional. Mengintegrasikan kursus keamanan siber di semua ilmu komputer dan program TI di pendidikan tinggi, dan menciptakan gelar dan magang keamanan siber khusus. Bekerja lintas departemen dan dengan mitra akademis lainnya untuk mengoptimalkan sumber daya dan upaya saat mengembangkan atau memperbarui program. Menetapkan berbagai skema insentif, seperti beasiswa untuk program pendidikan swasta dan hibah untuk magang yang relevan.

3) **Merangsang pengembangan kapasitas dan pelatihan tenaga kerja.** Pengembangan skema pelatihan keamanan siber dan pengembangan keterampilan bagi para ahli dan non-ahli baik di sektor publik maupun swasta. Upaya tersebut dapat mencakup penyediaan pelatihan eksekutif dan operasional, magang dan magang formal, dan sertifikasi profesional keamanan nasional dan internasional. Pelatihan khusus untuk aktor tingkat nasional yang terlibat dalam kebijakan dalam dan luar negeri, termasuk regulator dan legislator. Pelatihan manajemen risiko dunia maya, dan dengan latihan praktis di dalam dan di antara entitas pemerintah dan pemangku kepentingan lainnya seperti latihan dan simulasi. Mengembangkan jalur karier keamanan siber yang berdedikasi dan jaringan karyawan masa depan yang efektif, khususnya untuk sektor publik, dan mempromosikan insentif untuk meningkatkan pasokan profesional keamanan siber yang berkualitas dan membantu mempertahankan bakat. Kemitraan dengan akademisi, sektor swasta, dan masyarakat sipil. Pendekatan seimbang gender yang memotivasi, mendorong, dan memfasilitasi lebih banyak keterlibatan perempuan di semua upaya yang ditujukan untuk pengembangan dan pelatihan keterampilan, memastikan inklusivitas di masa depan.

4) **Menerapkan program peningkatan kesadaran keamanan siber yang terkoordinasi.** Berkolaborasi dengan pemangku kepentingan terkait untuk mengembangkan dan menerapkan program kesadaran keamanan siber yang berfokus pada penyebaran informasi tentang risiko dan ancaman keamanan siber, serta tentang praktik terbaik untuk melawannya. Kampanye peningkatan kesadaran yang ditujukan untuk masyarakat umum, anak-anak, tantangan digital, program pendidikan yang berfokus pada konsumen, dan inisiatif peningkatan kesadaran antara lain, yang ditargetkan pada eksekutif di seluruh sektor publik dan swasta. Program kesadaran harus menyertakan KPI dan metrik yang relevan untuk mengukur dampak dan efektivitas.

5) **Mendorong inovasi dan R&D keamanan siber.** Menumbuhkan lingkungan yang merangsang penelitian dasar dan terapan dalam keamanan siber lintas sektor dan berbagai kelompok pemangku kepentingan. Penelitian nasional mendukung tujuan Strategi Keamanan Siber Nasional; mengembangkan program R&D yang berfokus pada keamanan dunia maya di organisasi riset publik; pengembangan yang efektif dan penyebaran temuan baru, teknologi dasar, teknik, proses, dan alat. Pengembangan pasar layanan keamanan siber lokal yang efisien dan memadai. Menjalin hubungan dengan komunitas riset internasional di bidang ilmiah yang berkaitan dengan keamanan dunia maya, seperti ilmu komputer, teknik elektro, matematika terapan dan kriptografi. Mekanisme insentif yang tersedia dari hibah, pengadaan, kredit pajak, kompetisi, dan inisiatif lain yang mendorong pengembangan solusi, produk, dan layanan keamanan siber yang inovatif.

6) **Menyesuaikan program untuk sektor dan kelompok rentan.** Peningkatan kapasitas dan kemampuan keamanan siber serta peningkatan kesadaran. Kelompok yang sangat berisiko atau yang perlu diberdayakan untuk melindungi diri mereka sendiri, seperti usaha kecil dan menengah (UKM), organisasi berbasis

masyarakat, masyarakat kurang terlayani, dan/atau masyarakat berpenghasilan rendah.

f. Perundang-undangan dan regulasi

Pengembangan kerangka hukum dan peraturan untuk melindungi masyarakat dari kejahatan dunia maya dan mempromosikan lingkungan dunia maya yang aman dan terjamin, sesuai dengan Prinsip Inklusivitas, Hak Asasi Manusia Mendasar, dan Lingkungan Kepercayaan. Adopsi undang-undang yang mendefinisikan apa yang merupakan aktivitas dunia maya ilegal, serta alat prosedural yang diperlukan untuk menyelidiki dan mengadili kejahatan ini di tingkat nasional dan untuk bekerja sama lintas batas; pembentukan mekanisme kepatuhan; pembangunan kapasitas untuk menegakkan kerangka kerja; pelembagaan entitas kritis; dan kerja sama internasional untuk memerangi kejahatan dunia maya. Kerangka kerja harus mengakui dan konsisten dengan kewajiban negara di bawah internasional, Keamanan dunia maya, kejahatan dunia maya, dan perlindungan data pribadi adalah konsep yang saling terkait.

1) Menetapkan kerangka hukum domestik untuk keamanan siber. Pengembangan kerangka hukum keamanan siber dan perlindungan data domestik, yang mengacu pada tindakan yang relevan dengan pencegahan, pemantauan, dan penanganan insiden terkait dunia maya, dan tindakan lain apa pun yang harus dilakukan oleh entitas publik dan swasta untuk mendorong keamanan dan tangguh dunia maya nasional. Menetapkan, memperbarui, dan mereformasi kerangka hukum untuk keamanan dunia maya, termasuk namun tidak terbatas pada: aturan keamanan informasi dan penerapannya pada keamanan sistem informasi; identifikasi infrastruktur informasi kritis nasional; pembentukan badan nasional dan sektoral yang menangani aspek keamanan siber; sertifikasi organisasi, proses, produk, dan kebijakan keamanan siber; aturan keamanan nasional/negara yang berlaku untuk keamanan dunia maya; dan hal-hal lain yang relevan.

2) **Menetapkan kerangka hukum domestik tentang kejahatan dunia maya dan bukti elektronik.** Pengembangan kerangka hukum domestik yang dengan jelas mendefinisikan apa yang dimaksud dengan kejahatan dunia maya dan tindak pidana terkait, dan yang memberikan kekuatan prosedural yang memadai untuk penyelidikan dan penuntutan yang efektif, serta putusan kasus terkait berdasarkan bukti elektronik yang dapat diterima. Undang-undang kejahatan dunia maya, yang dapat dicapai dengan memberlakukan undang-undang baru yang spesifik atau mengubah undang-undang yang sudah ada. Undang-undang ini harus menentukan: tindak pidana substantif; sarana prosedural untuk mengumpulkan bukti elektronik; dan alat untuk kerja sama internasional yang cepat dan efektif dalam kasus-kasus seperti itu. Undang-undang kejahatan dunia maya lintas batas yang jelas dan dapat ditegakkan, negara menyelaraskan kerangka hukum domestik mereka dengan instrumen hukum internasional dan regional yang ada mengenai masalah ini. Memberikan panduan untuk aspek operasional investigasi dan penuntutan kejahatan dunia maya. Mengidentifikasi kesenjangan dan otoritas yang tumpang tindih, serta mengklarifikasi dan memprioritaskan bidang-bidang yang membutuhkan modernisasi (misalnya undang-undang yang ada seperti undang-undang telekomunikasi lama).

3) **Mengakui dan melindungi hak asasi manusia dan kebebasan.** Pengembangan kerangka hukum domestik tentang keamanan dunia maya, kejahatan dunia maya, dan bidang terkait lainnya yang menghormati dan melindungi hak asasi manusia. Dalam melakukannya, perbedaan konteks antara cybersecurity (aspek teknis keamanan) dan cybercrime (respons peradilan pidana) harus disorot dan dipertimbangkan dengan baik. Perhatian khusus pada masalah hukum terkait teknologi yang dapat memengaruhi tingkat keamanan dunia maya dan berdampak pada hak asasi manusia (enkripsi, pengungkapan kerentanan anonimitas, peretasan etis, dan lain-lain). Pendekatan yang konsisten dengan hak asasi

manusia individu. Melindungi hak proses hukum yang penting yang berlaku dalam penyelidikan dan penuntutan pidana, serta hak privasi dan perlindungan data pribadi, dan kebebasan berekspresi, sesuai dengan Prinsip Hak Asasi Manusia Mendasar dan Kepercayaan. Memastikan bahwa hak-hak mereka yang menjadi korban atau berisiko dari insiden dunia maya dan kejahatan dunia maya dipertimbangkan dan dilindungi secara memadai.

4) **Menciptakan mekanisme kepatuhan.** Pembentukan mekanisme kepatuhan domestik (baik penegakan maupun insentif). Mekanisme ini harus ditetapkan untuk mencegah, memerangi, dan mengurangi tindakan yang ditujukan terhadap kerahasiaan, integritas, dan ketersediaan sistem dan infrastruktur TIK, dan mengancam data komputer.

5) **Mempromosikan pembangunan kapasitas untuk penegakan hukum.** Pengembangan kapasitas penegakan hukum dunia maya, termasuk pelatihan dan pendidikan untuk berbagai pemangku kepentingan yang terlibat dalam memerangi kejahatan dunia maya (misalnya, hakim, jaksa, pengacara, pejabat penegak hukum, spesialis forensik, penyelidik keuangan, dan lain-lain). Penegakan hukum harus menerima pelatihan khusus untuk menafsirkan dan menerapkan undang-undang kejahatan dunia maya domestik; untuk secara efektif mendeteksi, mencegah, menyelidiki, dan menuntut pelanggaran kejahatan dunia maya dengan tetap menghormati hak asasi manusia; dan berkolaborasi secara efektif dengan industri dan entitas penegak hukum internasional (misalnya, INTERPOL, Europol) untuk mengatasi kejahatan dunia maya dan meningkatkan keamanan dunia maya. Pelatihan dan pendidikan tersebut harus berkelanjutan dan mencakup semua profesional peradilan pidana dan keamanan yang relevan, dan harus terus diperbarui dengan tantangan dan ancaman terkait dunia maya saat ini.

6) **Menetapkan proses antar organisasi.** Mengidentifikasi dan mengakui mandat lembaga domestik dengan otoritas utama untuk

memastikan kepatuhan terhadap undang-undang kejahatan dunia maya (terutama otoritas peradilan pidana dan layanan forensik), pencegahan dan tanggapan terhadap insiden dunia maya yang meningkat ke tingkat nasional (termasuk perlindungan). infrastruktur informasi penting), dan mereka yang bertanggung jawab untuk memastikan bahwa semua persyaratan kejahatan dunia maya internasional dipenuhi (misalnya, memastikan bahwa undang-undang nasional mematuhi kewajiban perjanjian internasional) dan lintas garis yudisial (misalnya, kerja sama lintas batas).

7) **Mendukung kerja sama internasional untuk memerangi ancaman dunia maya dan kejahatan dunia maya.** Komitmen untuk melindungi masyarakat dari kejahatan dunia maya secara global, melalui ratifikasi, perjanjian kejahatan dunia maya internasional atau perjanjian yang setara untuk memerangi kejahatan dunia maya, dan melalui promosi mekanisme koordinasi untuk menangani kejahatan dunia maya internasional. Menyelaraskan undang-undang nasional dengan kewajiban perjanjian internasional dan perjanjian bilateral, misalnya dengan membangun bantuan hukum timbal balik, memungkinkan penyelidikan dan penuntutan lintas batas, penanganan bukti digital, dan ekstradisi. Membangun mekanisme informal yang memungkinkan kerja sama terpercaya dan pertukaran informasi, intelijen, dan dukungan teknis lintas batas antara pelaku keamanan siber baik di sektor publik maupun swasta. Kerja sama penegakan hukum internasional memainkan peran penting dalam memerangi kejahatan dunia maya melalui pertukaran informasi, investigasi lintas batas, operasi, dan penangkapan. INTERPOL menyediakan sistem komunikasi polisi global yang aman bagi negara-negara untuk memfasilitasi permintaan antar polisi dan permintaan bantuan hukum timbal balik formal dari satu otoritas pusat ke otoritas pusat lainnya. Meningkatkan interoperabilitas lintas yurisdiksi dan memastikan tindakan polisi bersama yang tepat

waktu dan terkoordinasi. Organisasi lain seperti AFRIPOL, AMERIPOL, ASEANAPOL, GCCPOL, ECOPOL, dan Europol juga mendorong kerja sama penegakan hukum di tingkat regional.

g. Kerja sama internasional

Strategi dalam hal keterlibatan keamanan siber eksternal dari negara tertentu, baik di tingkat regional maupun internasional. Dengan digitalisasi yang berdampak pada semua bidang hubungan internasional, seperti hak asasi manusia; pembangunan ekonomi dan sosial; negosiasi perdagangan; hubungan perdagangan; kontrol senjata; penggunaan teknologi baru dan mengganggu; keamanan rantai pasokan; dan keamanan, stabilitas, perdamaian, dan resolusi konflik, cybersecurity telah menjadi bagian integral dari kebijakan luar negeri suatu negara. Diskusi internasional dan bekerja sama dengan pemangku kepentingan nasional dan internasional, serta masyarakat sipil, industri, dan organisasi non-pemerintah. Keterlibatan internasional dengan pemangku kepentingan publik dan swasta adalah kunci untuk memfasilitasi dialog yang konstruktif, mengembangkan mekanisme kepercayaan dan kerja sama, menemukan solusi yang dapat diterima bersama dan mengatasi tantangan bersama, serta menciptakan pemahaman global tentang pentingnya keamanan dan ketahanan dunia maya. Kerja sama regional dan internasional harus dibina selaras dengan tatanan politik, sosial, budaya, dan ekonomi negara.

1) **Mengakui keamanan dunia maya sebagai komponen kebijakan luar negeri dan menyelaraskan upaya domestik dan internasional.** Komitmen terhadap kerja sama internasional dalam keamanan siber dan mengakui masalah siber sebagai komponen integral dari kebijakan luar negeri negara di semua bidang yang relevan, termasuk stabilitas siber internasional dan negosiasi. Mengartikulasikan area fokus pemerintah dan menunjukkan tujuan jangka panjang untuk kerjasama internasional, termasuk pemangku kepentingan mana (misalnya, publik, swasta, regional, global) yang akan dilibatkan. Dukungan untuk pembentukan norma

keamanan dunia maya internasional dan langkah-langkah pembangunan kepercayaan, komitmen terhadap pembangunan kapasitas keamanan dunia maya, partisipasi dalam pengembangan standar keamanan dunia maya internasional, serta bergabung dengan proses regional dan internasional. Konsistensi antara agenda kebijakan domestik dan luar negeri negara tersebut dengan menyelaraskan kerangka hukum dan kebijakan nasionalnya dengan komitmen internasionalnya, dan menyelaraskan pendekatan keamanan siber nasionalnya dengan upaya internasionalnya. Harmonisasi antara entitas pemerintah yang berbeda (misalnya, kepala negara dan kabinet, Kementerian Luar Negeri, Kementerian TIK, Kementerian Perindustrian dan Perdagangan, Kementerian Kehakiman, Kementerian Pertahanan, dll.).

2) **Terlibat dalam diskusi internasional dan berkomitmen untuk implementasi.** Forum internasional spesifik dan mekanisme kerja sama yang ingin diikuti atau dikerjakan oleh negara untuk terlibat secara efektif secara internasional dalam isu-isu terkait dunia maya. Ini dapat mencakup organisasi regional atau global, badan standardisasi, diskusi antar pemerintah atau multipihak, aliansi sektor publik dan/atau swasta, serta mekanisme kerjasama dan kolaborasi tradisional yang memiliki komponen dunia maya atau digital. Komitmen negara terhadap penerapan hukum internasional, termasuk Piagam Perserikatan Bangsa-Bangsa dan hukum hak asasi manusia internasional. Komitmen nasional untuk bergabung dan menerapkan instrumen regional dan internasional yang ada untuk memerangi kejahatan dunia maya dan ancaman dunia maya lainnya (misalnya, Konvensi Budapest tentang Kejahatan Dunia Maya Dewan Eropa, Konvensi Uni Afrika tentang Keamanan Dunia Maya, Konvensi Arab tentang Memerangi Pelanggaran Teknologi Informasi, Petunjuk ECOWAS tentang memerangi kejahatan dunia maya, dll.). Mengakui bahwa banyak perjanjian perdagangan internasional juga memiliki komponen digital atau dunia maya

(misalnya, Pengaturan Wassenaar mengatur teknologi penggunaan ganda, komitmen negara untuk memajukan norma sukarela perilaku negara yang bertanggung jawab di dunia maya dan di dunia maya. Penggunaan teknologi informasi dan komunikasi (OEWG), Organisasi Keamanan dan Kerjasama di Eropa (OSCE) tentang langkah-langkah membangun kepercayaan dan norma-norma internasional yang berlaku di dunia maya, pekerjaan Subkelompok Kejahatan Teknologi Tinggi Grup G7, serta inisiatif regional dan upaya multipihak lainnya. Memprioritaskan upaya keterlibatan internasional, mengalokasikan sumber daya yang memadai (personil dan uang), komitmen terhadap penerapan norma-norma perilaku sukarela Negara yang disepakati di dunia maya seperti yang diusulkan oleh kelompok ahli Pemerintahan PBB tentang Perkembangan Bidang Informasi dan Telekomunikasi dalam Konteks Keamanan Internasional, Memajukan perilaku Negara yang bertanggung jawab di dunia maya dalam konteks keamanan internasional, yang menyelesaikan tugasnya.

3) **Mempromosikan kerja sama formal dan informal di dunia maya.** Mekanisme kerja sama internasional operasional (baik sektor publik maupun swasta) yang ingin dilakukan oleh kerajaan Arab Saudi. Upaya internasional formal dan informal untuk memajukan kerja sama dalam pengembangan kebijakan dan legislatif, penegakan hukum (misalnya, INTERPOL, EUROPOL, WIPO), berbagi informasi dan ancaman. Mendukung kerja sama yang lebih baik dan pertukaran informasi yang tepat waktu dan dapat ditindaklanjuti antara otoritas terkait tentang potensi ancaman dan kerentanan serta koordinasi dalam mekanisme pertahanan dan tanggapan. Pertukaran informasi lintas batas dengan organisasi sektor swasta dan industri yang berurusan dengan ancaman keamanan siber (perusahaan anti-virus, komunitas intelijen ancaman, penyedia media sosial global, dan

aktor terkait lainnya) juga harus dianggap sebagai komponen penting dari upaya kerja sama internasional.

4) **Mempromosikan pembangunan kapasitas untuk kerja sama internasional.** Mengembangkan kompetensi dan keterampilan tambahan yang berfokus pada masalah dunia maya dan meningkatkan kapasitas keseluruhannya untuk menangani berbagai masalah dunia maya yang terus meningkat, termasuk stabilitas dunia maya internasional, perlindungan data, dan privasi, perdagangan, kontrol senjata, penggunaan teknologi baru, keamanan pasokan, dan hal-hal digital lainnya. Pengembangan dan penggunaan kompetensi dan keterampilan yang berfokus pada isu dunia maya (diplomasi dunia maya dan negosiasi). Pengembangan struktur organisasi khusus dan pembentukan beberapa kantor khusus atau personel terlatih. Peningkatan kerja sama penegakan hukum dan peradilan, hukum internasional publik yang berlaku, norma sukarela dari perilaku Negara yang bertanggung jawab, dll. Peningkatan kapasitas internasional untuk mendukung upaya tersebut (misalnya, GLACY, Global Forum Keahlian Cyber (GFCE), INTERPOL, dll.). Upaya peningkatan kapasitas penegakan hukum dapat membantu lembaga penegak hukum lokal dan nasional meningkatkan keterampilan, pengetahuan, dan kemampuan teknis mereka untuk memanfaatkan alat dan sistem berteknologi tinggi untuk pencegahan, deteksi, investigasi, dan penuntutan kejahatan dunia maya lintas batas. Penegakan hukum untuk tetap mengikuti tren kejahatan dunia maya dan lanskap ancaman yang terus berkembang untuk tetap berada di depan kejahatan. Mempertimbangkan inisiatif keamanan siber regional dan internasional yang ada dan mendorong harmonisasi dan keselarasan. Memanfaatkan praktik baik yang ada, serta berkontribusi terhadap kohesi dan konvergensi pendekatan keamanan siber. Pembelajaran sejawat dan transfer pengetahuan dan keterampilan keamanan siber dengan mitra internasional.

BAB IV

PENUTUP

18. Simpulan

Membangun kapasitas otoritas keamanan siber nasional membutuhkan infrastruktur pendukung keamanan siber yang serius. Ancaman siber yang multidimensi membuat penanganannya tidak hanya menjadi tanggung jawab Kapasitas *National Cybersecurity Authority* (NCA) Kerajaan Arab Saudi saat ini belum optimal melampaui tingkat I dunia yaitu Amerika, oleh karena itu perlu standar internasional pada transisi dari pencegahan nuklir ke pencegahan dunia maya, pencegahan dengan pembalasan. Penangkalan dengan pelarangan dan Penangkalan dengan pembalasan. Orientasi terhadap tindakan *defensif*: seperti Pembentukan badan dan lembaga yang peduli dengan keamanan siber. Pentingnya membangun perlindungan pribadi yang kuat. Mengantisipasi risiko dan mencari cara untuk menghadapinya. Berinovasi berarti canggih baru untuk mengurangi risiko perang *cyber*. Mengembangkan dan memutakhirkan sarana perlindungan. Mengamankan media penyimpanan. Tindakan Orientasi terhadap tindakan *ofensif* Membangun tentara modern. Peran pencegahan langsung. Penggunaan teknologi elektronik dan kecerdasan buatan. Berorientasi pada komunitas internasional untuk mengurangi eskalasi perang siber terdiri aliansi dan kerja tim untuk mencapai dunia maya yang aman, Perjanjian regional dan internasional untuk keamanan siber, Mengaktifkan hukum internasional di bidang keamanan dunia maya. Kerjasama internasional antar lembaga kepolisian. Kerjasama peradilan internasional. Perencanaan strategis untuk menjaga keamanan siber. Untuk itu Upaya Arab Saudi untuk meningkatkan kemampuan *National Cybersecurity Authority*. Program dan inisiatif nasional. Berinvestasi di pasar keamanan *cyber*. Mempersiapkan kader manusia secara teknis. Legislasi hukum di bidang keamanan siber yang kuat.

Visi masa depan *cyber security* dan dampaknya terhadap keamanaan digital di Kerajaan Arab Saudi adalah menuju perang pemusnahan yang komprehensif. Pentingnya membangun perlindungan pribadi yang kuat. Mengantisipasi risiko dan mencari cara untuk menghadapinya. Berinovasi berarti canggih baru untuk mengurangi risiko perang *cyber*. Mengembangkan prosedur keamanan jaringan.

Mengubah keseimbangan kekuatan di dunia. Masa depan keamanan nasional dalam perkembangan teknik perang siber. Visi strategis nasional untuk keamanan siber. Tema strategi nasional keamanan siber dan tujuan strategi nasional keamanan siber.

Strategi meningkatkan kapastitas *National Cybersecurity Authority* (NCA yaitu meningkatkan tata kelola. Memastikan tingkat dukungan tertinggi. Menguatkan *National Cybersecurity Authority* yang kompeten. Menjamin kerja sama intra-pemerintah. Menjamin kerjasama antar sektor. Alokasikan anggaran dan sumber daya khusus. Mengembangkan rencana implementasi. Manajemen risiko dalam *National Cybersecurity Authority*. Kesiapsiagaan dan ketahanan terdiri dari menetapkan kemampuan respons insiden dunia maya. Menyusun rencana darurat untuk manajemen krisis keamanan siber dan pemulihan bencana. Mempromosikan berbagi informasi. Melakukan latihan keamanan siber. Menetapkan penilaian dampak atau keparahan insiden keamanan siber. Infrastruktur Kritis dan layanan penting. Menetapkan pendekatan manajemen risiko untuk mengidentifikasi dan melindungi infrastruktur penting dan layanan penting. Mengadopsi model tata kelola dengan tanggung jawab yang jelas. Menentukan baseline keamanan siber minimum. Memanfaatkan berbagai pengungkit pasar. Membangun kemitraan publik-swasta dan Peningkatan kemampuan dan kapasitas serta peningkatan kesadaran dengan Perundang-undangan dan regulasi serta kerja sama internasional.

19. Rekomendasi

a. Gubernur Otorita *Saudi Data and Artificial Intelligence Authority* perlu memiliki dan membangun kemitraan di bidang siber di tingkat regional dan internasional serta Gubernur Otorita *National Cybersecurity Authority* untuk mempercepat kemajuan teknis, teknologi dan informasi serta pesatnya perkembangan di bidang dunia maya, bahaya dunia maya, dan tidak ada negara yang dapat mencapai keamanan dunia maya sendirian, tetapi membutuhkan tindakan kolektif, regional atau global. Dunia maya telah menciptakan peluang baru bagi para pelaku, dan berkontribusi pada munculnya jenis kejahatan baru, yaitu kejahatan dunia maya, yang direpresentasikan dalam operasi yang kompleks dan

mempengaruhi negara di semua bidangnya, yang meningkatkan pentingnya mencapai keamanan dunia maya. Cyber crime sebagai ancaman keamanan lintas batas baru yang mengandalkan teknik teknologi modern untuk melakukan operasi kejahatan.

b. Menteri Pertahanan Arab Saudi agar memiliki kemampuan dunia maya defensif dan ofensif sebab perang dunia maya berkembang pesat menjadi faktor penentu dalam konflik atau konflik internasional, dan kemenangan di dalamnya akan menjadi sekutu bagi mereka yang yang mencapai keamanan dunia maya untuk mereka. Ketergantungan suatu negara pada satu sistem merupakan ancaman strategis bagi negara jika terkena ancaman siber, apalagi jika sistem tersebut melekat pada infrastruktur utama negara. Banyak negara cenderung meningkatkan kemampuan dunia maya mereka dalam keamanan dunia maya, dan juga bekerja untuk mengamankan infrastruktur mereka dengan menggunakan sistem perlindungan tercanggih, mencapai tingkat keunggulan teknologi tertinggi, dan menyusun strategi dan kebijakan keamanan dunia maya.

c. Menteri Teknologi Informatika perlu menggunakan teknik kecerdasan buatan sebagai salah satu cara modern yang paling penting untuk mencapai keamanan dunia maya. Cyberpower harus dimasukkan sebagai salah satu kemampuan Kerajaan untuk mengukur sejauh mana kekuatan dan kemampuannya untuk melindungi dunia maya dan infrastrukturnya serta informasi penting yang dikandungnya. Institusi pemerintah dan swasta harus mengikuti perkembangan dan mengeluarkan mekanisme implementasi untuk strategi nasional keamanan siber Saudi .

d. Menteri Pertahanan agar memanfaatkan dan mengaktifkan jaringan dan sistem elektronik, dan transformasi digital untuk mengimbangi dunia dengan anggaran untuk mencapai keamanan siber tanpa mempengaruhi satu sama lain.

e. Panglima Dewan Keamanan Nasional Arab Saudi agar mengembangkan pelatihan di lembaga pendidikan militer dan keamanan dan termasuk keamanan siber dalam rencana mereka telah menjadi salah satu dasar yang diberikan kepada perwira dan individu dalam kursus wajib dan

perguruan tinggi militer dan keamanan, dan mengadakan kursus khusus dalam keamanan siber. Kader-kader bangsa yang bekerja di bidang elektronik diserahi amanah untuk mencapai keamanan siber, sehingga harus berkualitas dan bidang tersebut dibuka di universitas dan perguruan tinggi dalam disiplin ilmu yang tepat di bidang keamanan siber untuk studi pascasarjana dan doktor, dan dikirim dengan beasiswa. ke universitas dengan preseden di bidang siber, karena hanya kader nasional Saudi yang berkualitas yang dapat mencapai keamanan Kerajaan.

f. Gubernur Otorita *National Cybersecurity Authority* agar mengaktualisasikan adopsi pusat penelitian yang berkaitan dengan penelitian di bidang cyber muncul. Pentingnya pusat penelitian sebagai anak sungai utama untuk semua bidang, dan di sini pentingnya menarik kader nasional terkemuka di bidang elektronik dan membuka jalan bagi mereka untuk berinovasi di bidang kecerdasan buatan untuk mencapai perisai keamanan siber dan memiliki mekanisme siber yang unik

DAFTAR PUSTAKA

Andi Widjajanto, (2022). *Ketahanan Nasional di Era Digital.* Bahan Paparan Gubernur pada rapat Arsitektur Digital Indonesia, di Ruang Nusantara III, tanggal 25 Mei 2022.

———————— , (2022). *Tranformasi Lemhannas RI: Ketahanan Nasional Era 5.0. "Geo V".* Gubernur Lemhannas RI. Disampaikan pada Orasi Ilmiah Hut Ke-57 Lemhannas RI, pada tanggal 19 Mei 2022. Jakarta.

Asril Hamzah Tanjung, (2019). *Optimalisasi regulasi penyebaran informasi di masyarakat.* Wakil Ketua Komisi I DPR RI. Disampaikan dalam FGD Lemhannas RI, pada tanggal 28 Februari 2019.

Alexander Haryanto, (2023). *Apa Itu Buzzer Politik? Arti, Strategi, Sejarah dan Pola Rekrutmen*, dalam https://tirto.id/gaaE. Diakse pada tanggal 7 Februari 2023.

Budiman Tanuredjo. (2023). *Politik Lato-lato.* Catatan Politik dan Hukum. Kompas. Jakarta: PT Kompas Media Nusantara, Edisi Sabtu, 21 Januari 2023.

Christiany Juditha (2019), *Buzzer Di Media Sosial Pada Pilkada Dan Pemilu Indonesia.* Prosiding Seminar Nasional Komunikasi dan Informasi #3 Tahun 2019:199-212. Balai Pengembangan SDM dan Penelitian Komunikasi dan Informatika Manado, Kementerian Komunikasi dan Informasi RI.

Fauzi Syarif (2017), *Pemanfaatan Media Sosial Dalam Proses Pembentukan Opini Publik* (Analisa Wacana Twittwer Sby). Jurnal Komunikasi, 3 September 2017: 2579-329.

Haryatmoko, (2018). *Hantu Kebenaran Era "Posth Truth.* Jakarta: Penerbit PT Kompas Media Nusantara, Edisi Jumat, 21 Desember 2018, yang digelar oleh Fakultas Komunikasi Universitas Taruma Negara pada tanggal 15 November 2018.

———————— (2014). *Etika Politik dan Kekuasaan*. Jakarta: Penerbit PT. Kompas Media Nusantara.

Heru Puji Winarso, (2005). *Sosiologi Komunikasi Massa.* Jakarta: PT. Prestasi Pustaka Notonagoro, (1984), *Pancasila Dasar Filsafat Negara*. Jakarta: PT. Bina Aksara, Cetakan ke-6.

James A.F., Stoner (2023). *Management Jilid I dan II Edisi II* dalam https://lemhannas.go.id/publik/ media/ catalog/0010-121500000011680 /swf/4387/files/basic-html/page4.html. Diakses pada tanggal 7 Februari 2023.

Kietzman, Jan H, Kristoper Hermkent, et.al (2011), *Social Media?Get Serious! Undersatanding the Fuction* Building Block os Social Media" Businness Horizon 54(3):241-51. doi:10.1016/ j.bushor.2011.01.00

Kompas, (2019). "*Habis Debat, Terbitlah Adu Tagar"*. Edisi Jumat, 19 Februari 2019.

_____ (2023), *"Kegaduhan yang Tidak Perlu".* Tajuk Rencana, Kompas, 4 Maret 2023.

Monavia Ayu Rizaty (2023*)," Pengguna Internet di Indonesia Sentuh 212 Juta Pada 2023*". Diakses dalam https://dataindonesia.id/Digital/detail/pengguna-internet-di-indonesia-sentuh-212-juta-pada-2023. Diakses pada tanggal 4 Maret 2023.

Samantha Bradshaw, dan, Philip N. Howard. (2019). *The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation*. University of Oxford. Diakses pada tanggal 7Februari 2023.

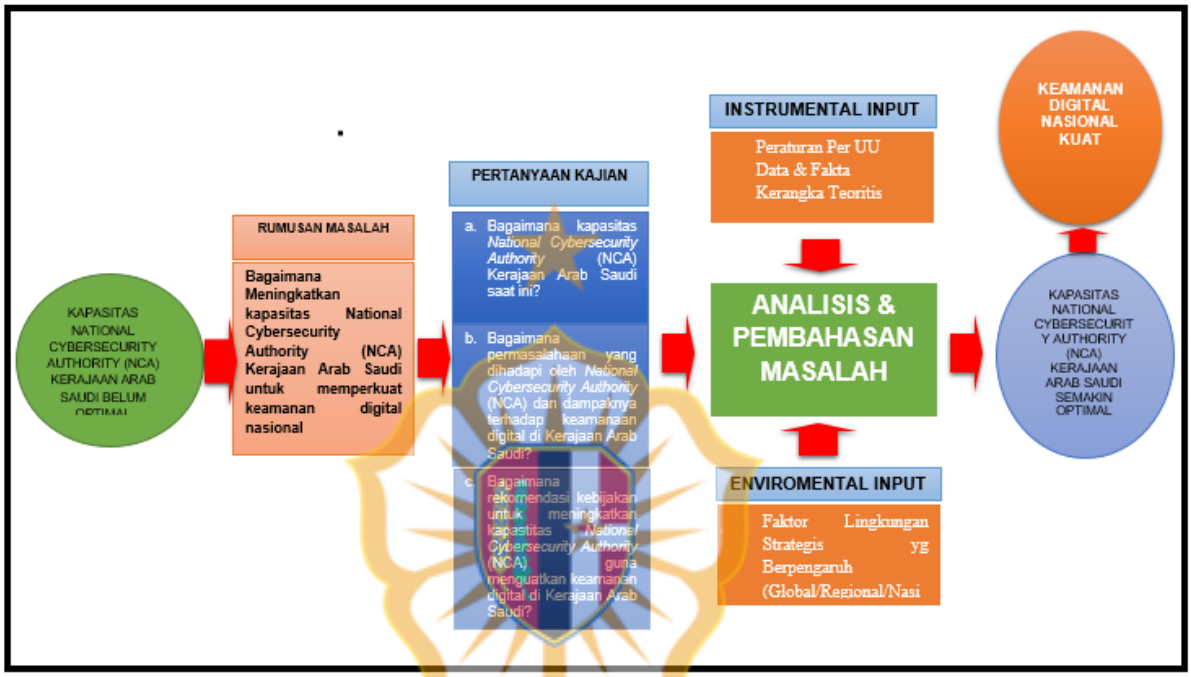
Siti Zuhro, (2019). *Menjaga Stabilitas Ketahanan Nasional Pasca Pemilu 2019*. Peneliti Utama LIPI. Disampaikan dalam acara *Round Table Discussion* (RTD) yang dilaksanakan pada tanggal 30 April 2019 di Lemhannas RI.

Suharso Monoarfa (2023). *Percepatan Transformasi Digital Pemerintah.* Menteri Perencanaan Pembangunan Nasional/ Kepala Badan Perencanaan Pembangunan Nasional. *Disampaikan pada Rapat Percepatan Penerapan Sistem Elektronik/Digitalisasi Birokrasi yang diselenggarakan Kementerian Koordinator Bidang Maritim dan Investasi* Jumat, 23 Desember 2022

Van Dijk, (2013), dalam I. Snellen and W.Van de Donk, *Publik Administration in The Information*. Amsterdam: IOS-Press.

ALUR PIKIR

"MENINGKATKAN KAPASITAS NATIONAL CYBERSECURITY AUTHORITY (NCA) KERAJAAN ARAB SAUD UNTUK MEMPERKUAT KEAMANAN DIGITAL NASIONAL"



DAFTAR RIWAYAT HIDUP

Kolonel Staf / Khalil Ibrahim Alshaikhi

Informasi pribadi

Nama: Khalil Ibrahim Alshaikhi
Jabatan : Direktur Strategis Departemen Penilaian
Pangkat: Staf Kolonel
Cabang: Angkatan Laut

Profil profesional

Perwira Angkatan Laut ahli dengan pengalaman lebih dari 25 tahun dalam kepemimpinan Militer, perencanaan Strategis, operasi dan pelatihan dengan karir merencanakan dan melaksanakan banyak operasi militer.

Edukasi akademik

- Sarjana Ilmu Kelautan Militer, Akademi Angkatan Laut Raja Fahad, 1998
- Magister Ilmu Militer, Sekolah Staf dan Komando Saudi, 2013.

Kursus pelatihan

Mencapai banyak kursus di antara yang paling penting adalah sebagai berikut:

- Kursus Sekolah Perwira.
- Kursus Artileri untuk Perwira.
- Kursus komunikasi untuk siswa.
- Kursus instruktur bahasa Inggris untuk siswa.
- Kursus operasi lanjutan.
- Kursus Persiapan Pemimpin
- Kursus manajemen pelatihan.

Pengalaman profesional

- Petugas Pelatihan di Kapal Raja HM, Armada Barat.
- Petugas Pelatihan di kapal perang, Armada Barat.

- Perwira Artileri di Kapal Raja HM, Armada Barat.
- Petugas instruktur persenjataan di Fleet Training Center, Armada Barat.
- Perwira Operasi, Armada Barat.
- Kepala Departemen Operasi di Kapal Raja HM, Armada Barat.
- Perwira Analis Informasi, Bagian Intelijen, Markas Besar Komando Angkatan Laut
- Manajer seksi Alat Bantu Latihan, Bagian Latihan, Markas Besar Komando Angkatan Laut
- Perwira Pelaksana, Komando Pasukan Gabungan.
- Direktur Departemen Kajian Strategis, Perencanaan Strategis TNI Otoritas.

Medali dan Penghargaan

Saya adalah penerima banyak medali dan penghargaan, terutama sebagai berikut:

- Medali Raja Faisal tingkat ketiga
- Medali Perisai Selatan
- Penghargaan Centenary
- Penghargaan Guru
- Penghargaan Penguasaan
- Medali Administrasi Militer