

HASIL PENELITIAN DAN PEMBAHASAN

Penelitian ini dilaksanakan dengan menggunakan *Soft System Methodology (SSM)* sebagai metodologi utama. Sebagaimana disampaikan dalam bab terdahulu, melalui pelaksanaan langkah demi langkah dalam metodologi ini akan dijawab keseluruhan enam pertanyaan utama penelitian. Setiap tahapan *SSM* berkaitan dan berkontribusi menjawab keenam pertanyaan penelitian yang ada. Berikut adalah peta pemetaannya.

Tabel 4. 1 Pemetaan Relasi Pertanyaan Penelitian terhadap Proses SSM

Tahap	Proses SSM	Relasi Pertanyaan Penelitian
1	Menggambarkan Kompleksitas Permasalahan	1. Seperti apakah potensi ancaman siber terhadap sistem pertahanan negara saat ini dan di masa mendatang?
2	Mengidentifikasi Permasalahan secara Komprehensif	2. Dampak apakah yang membahayakan pertahanan negara apabila serangan siber tersebut benar-benar terjadi? 3. Bagaimana tingkat kerawanan siber Indonesia dalam sektor pertahanan? 4. Seperti apakah kebijakan pertahanan siber nasional yang dimiliki Indonesia saat ini? Bagaimana tingkat efektivitas kebijakan pertahanan siber pada sektor pertahanan yang diterapkan di Indonesia sekarang?
3	Mengidentifikasi Akar Permasalahan	1. Seperti apakah ekosistem pertahanan dan kedaulatan siber yang holistik dan komprehensif? Seperti apakah model
4	Mengembangkan Model Konseptual	kebijakan pertahanan dan kedaulatan siber nasional yang ideal dalam sebuah

negara?

5 Menganalisis Gap Kondisi Ideal dan Termutakhir 6 Mengembangkan Strategi Pengembangan Kebijakan 7 Menjalankan Solusi Pemecahan Masalah	2. Bagaimana strategi pengembangan kebijakan siber nasional untuk mengatasi ancaman dalam bingkai pemutakhiran doktrin pertahanan negara?

Sumber : Pemetaan Relasi Pertanyaan Penelitian terhadap Proses SSM (disusun oleh peneliti)

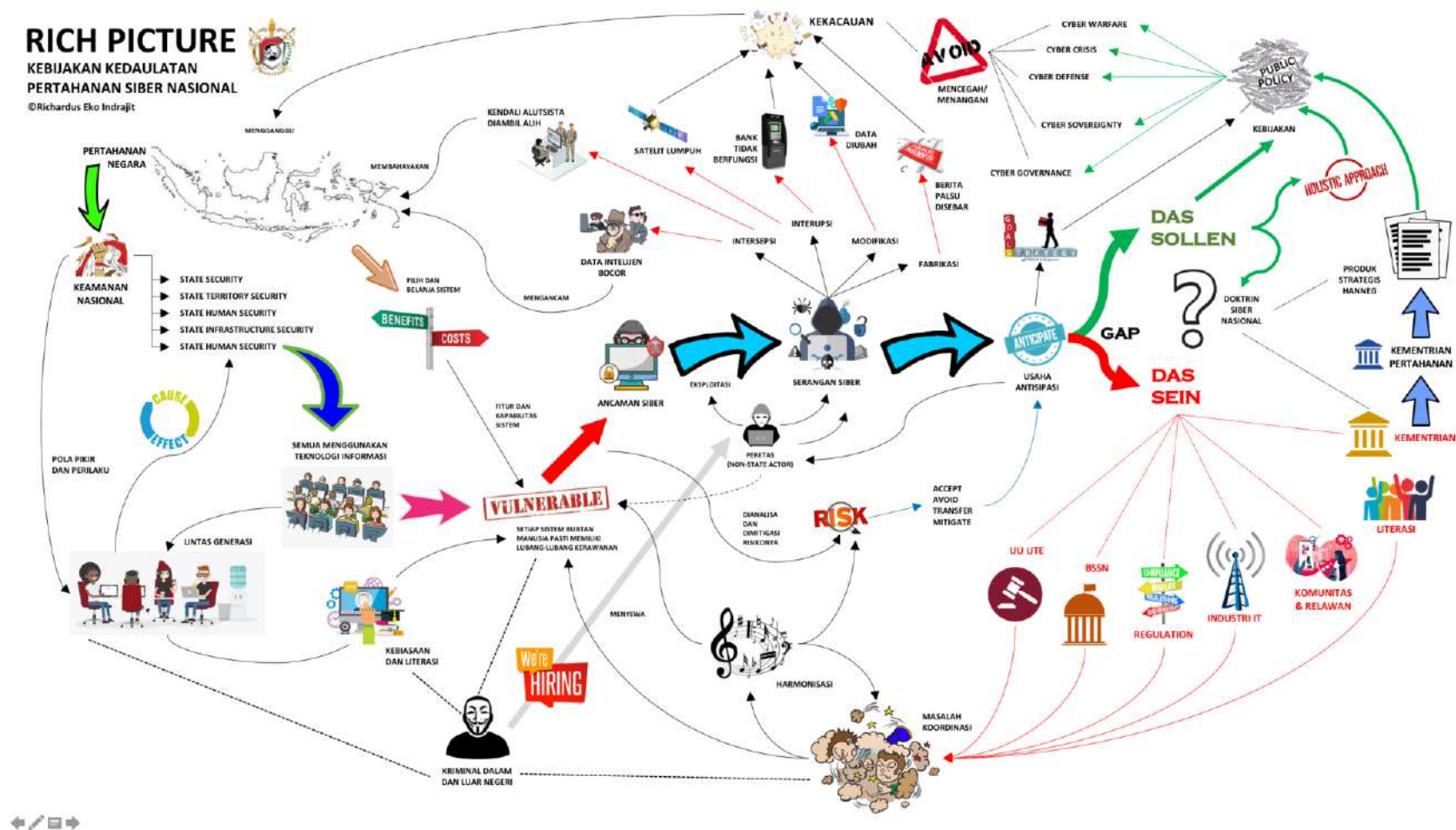
Tabel ini memperlihatkan bagaimana hubungan antara langkah-langkah yang ada pada SMM dengan keenam pertanyaan penelitian. Langkah pertama dan kedua dalam SMM dijalankan untuk menjawab empat pertanyaan penelitian, masing-masing adalah:

1. Seperti apakah potensi ancaman siber terhadap sistem pertahanan negara saat ini dan di masa mendatang?
2. Dampak apakah yang membahayakan pertahanan negara apabila serangan siber tersebut benar-benar terjadi?
3. Bagaimana tingkat kerawanan siber Indonesia dalam sektor pertahanan?
4. Seperti apakah kebijakan pertahanan siber nasional yang dimiliki Indonesia saat ini? Bagaimana tingkat efektivitas kebijakan pertahanan siber pada sektor pertahanan yang diterapkan di Indonesia sekarang?

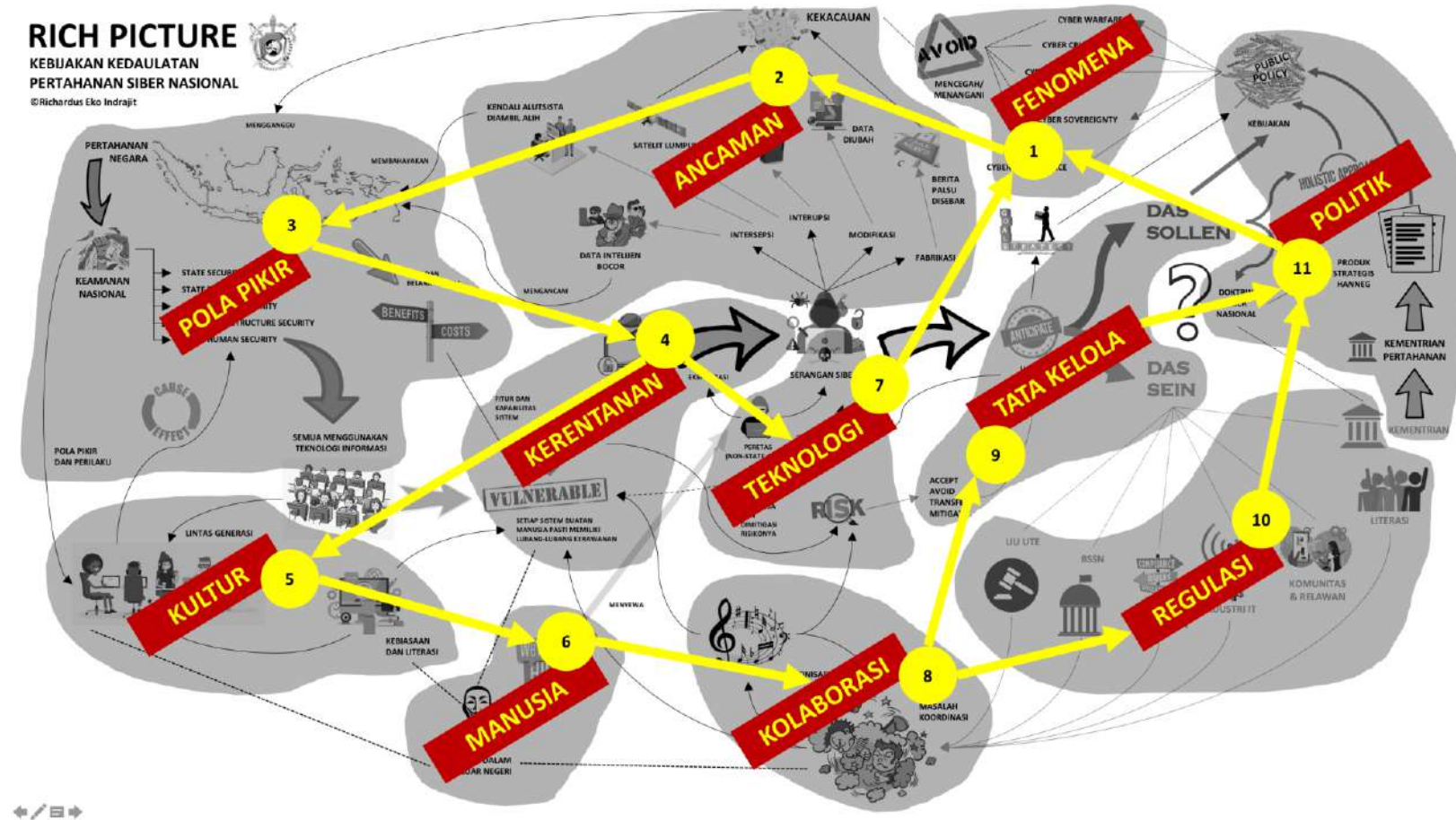
Sementara itu pertanyaan kelima yaitu “Seperti apakah ekosistem pertahanan dan kedaulatan siber yang holistik dan komprehensif? Seperti apakah model kebijakan pertahanan dan kedaulatan siber nasional yang ideal dalam sebuah negara?” dijawab dengan cara menjalankan langkah ketiga dan keempat pada SMM. Adapun pertanyaan keenam yang merupakan inti dari penelitian yaitu “Bagaimana strategi pengembangan kebijakan siber nasional untuk mengatasi

ancaman dalam bingkai pemutakhiran doktrin pertahanan negara?” terjawab melalui penerapan langkah kelima, keenam, dan ketujuh pada SMM. Pemetaan itu sendiri dimulai dengan pengembangan *Rich Picture* dan klasterisasi terhadapnya – untuk mendapatkan domain utama penelitian dan relasinya.

Gambar 4. 1 Rich Picture Kompleksitas Fenomena Pertahanan Siber



Gambar 4. 2 Klasterisasi terhadap Rich Picture



Penggambaran dan pemetaan *Rich Picture* memperlihatkan bagaimana fenomena permasalahan yang kompleks dapat dilihat lebih jelas dengan membaginya menjadi sejumlah klaster. Melalui analisa terhadap klaster dan hubungannya inilah dapat dipetakan antara permasalahan penelitian dengan langkah-langkah yang harus diambil untuk menyelesaikannya dengan menggunakan pendekatan *Soft System Methodology*. Adapun domain klaster dimaksud adalah sebagai berikut:

1. Domain Pertama berkaitan dengan adanya ancaman serangan siber terhadap keutuhan dan kedaulatan Negara Kesatuan Republik Indonesia (klaster Ancaman dan klaster Fenomena);
2. Domain Kedua berkaitan dengan dampak yang mengancam NKRI seandainya serangan siber tersebut berhasil diluncurkan oleh pihak lawan (klaster Pola Pikir);
3. Domain Ketiga berkaitan dengan kerentanan dan kerawanan pada sistem pertahanan siber nasional yang dapat dengan mudah dieksploitasi oleh para peretas maupun kriminal dunia siber (klaster Kerentanan dan klaster Kultur);
4. Domain Keempat berkaitan dengan efektivitas regulasi maupun kebijakan yang saat ini telah disusun dan diterapkan (klaster Regulasi);
5. Domain Kelima berkaitan dengan dibutuhkannya model pertahanan siber yang ideal sebagaimana telah diterapkan pada berbagai negara di dunia (klaster Teknologi, dan klaster Manusia); dan
6. Domain Keenam berkaitan dengan strategi pengembangan kebijakan pertahanan siber yang *agile*, dinamis, fleksibel, berdaulat, dan mandiri (klaster Tata Kelola, klaster Kolaborasi, dan klaster Politik).

Deskripsi Data Terkait Obyek dan Subyek

Sebagaimana disampaikan sebelumnya, obyek dari penelitian ini adalah serangkaian kebijakan dalam beragam jenis dan karakteristiknya. Subyeknya adalah seluruh *stakeholder* atau pemangku kepentingan yang berkaitan secara langsung maupun tidak langsung terhadap sistem pertahanan kedaulatan siber nasional. Oleh karena itulah maka dalam penelitian yang dilakukan dilakukan kajian terhadap seluruh kebijakan yang ada di Indonesia maupun di negara-negara lain sebagai bagian dari analisis komparasi, dan dilakukan wawancara terhadap beragam pemangku kepentingan mewakili kategori *stakeholder* dalam ekosistem pertahanan siber. Untuk memperjelas seperti apa situasi dan kondisi obyek maupun subyek yang menjadi fokus penelitian, dan memperjelas mengapa SSM dipilih sebagai metodologi adalah karena adanya sejumlah fenomena yang bersifat kompleks, *ill-structured*, tak beraturan, dan jauh dari keberadaan pola – ditambah dengan ekosistem global yang penuh dengan VUCA (*Volatile, Uncertain, Complex, Ambiguous*).

Hasil Pengumpulan Data Kualitatif dan Kuantitatif

Pengumpulan data penelitian dilakukan melalui berbagai pendekatan penelitian sesuai dengan ketujuh tahapan SSM yang dilakukan. Tabel berikut memperlihatkan bagaimana masing-masing proses pengumpulan data beserta sumber dan metodenya dilakukan selama penelitian berlangsung.

Tabel 4. 2 Pemetaan Model Pengumpulan Data terhadap Pertanyaan Penelitian

No	Pertanyaan Penelitian	Langkah SSM	Metoda Pengumpulan dan Sumber Data	Tool yang Dipakai
1	Seperti apakah potensi ancaman siber terhadap sistem pertahanan negara saat ini dan di masa mendatang?	1, 2	Mewawancara sejumlah pemangku kepentingan	Instrumen pertanyaan
			Mengakses catatan digital institusi pemantau siber	<i>Monitoring and reporting system</i>
			Mengadakan forum diskusi terbatas (FGD dan RTD)	Instrumen pertanyaan
			Mempelajari laporan studi kasus nasional dan internasional dari lembaga riset	<i>Internet browser</i>
2	Dampak apakah yang membahayakan pertahanan negara apabila serangan siber tersebut benar-benar terjadi?	1, 2	Membaca publikasi ilmiah yang relevan	<i>Digital library repository system</i>
			Mewawancara sejumlah pemangku kepentingan	Instrumen pertanyaan
			Mengadakan forum diskusi terbatas (FGD dan RTD)	Instrumen pertanyaan
			Mempelajari laporan studi kasus nasional dan internasional dari lembaga riset	<i>Internet browser</i>
			Membaca publikasi ilmiah yang relevan	<i>Digital library repository system</i>
			Mengakses catatan digital ahli bidang siber	<i>Internet</i>

			(blog, vlog)	<i>browser</i>
3	Bagaimana tingkat kerawanan siber Indonesia dalam sektor pertahanan?	1, 2	Mewawancara sejumlah pemangku kepentingan	Instrumen pertanyaan
			Menyelenggarakan survei kepada sejumlah <i>stakeholder</i>	Kuesioner
			Melakukan analisa intelijen dan forensik siber	<i>Penetration test and vulberability analysis software</i>
			Mempelajari laporan studi kasus kejahatan siber di Indonesia	<i>Internet browser</i>
			Mengakses catatan digital ahli bidang siber (blog, vlog)	<i>Internet browser</i>
4	Seperti apakah kebijakan pertahanan siber nasional yang dimiliki Indonesia saat ini? Bagaimana tingkat efektivitas kebijakan pertahanan siber pada sektor pertahanan yang diterapkan di Indonesia sekarang?	1, 2	Mewawancara sejumlah pemangku kepentingan	Instrumen pertanyaan
			Menyelenggarakan survei kepada sejumlah <i>stakeholder</i>	Kuesioner
			Mempelajari seluruh kebijakan terkait pertahanan siber	<i>Digital library repository system</i>
			Mengikuti diskursus percakapan para ahli, pelaku, dan praktisi siber	<i>Social media</i>
			Membaca laporan pemeringkatan lembaga independen dunia	<i>Digital library repository system</i>
5	Seperti apakah ekosistem pertahanan	3, 4	Mewawancara sejumlah pemangku	Instrumen

	dan kedaulatan siber yang holistik dan komprehensif? Seperti apakah model kebijakan pertahanan dan kedaulatan siber nasional yang ideal dalam sebuah negara?		kepentingan	pertanyaan
			Mengadakan forum diskusi terbatas (FGD dan RTD)	Instrumen pertanyaan
			Mempelajari sistem pertahanan siber berbagai negara di dunia	<i>Digital library repository system</i>
			Melakukan <i>benchmarking</i> antar berbagai institusi	<i>Digital library repository system</i>
6	Bagaimana strategi pengembangan kebijakan siber nasional untuk mengatasi ancaman dalam bingkai pemutakhiran doktrin pertahanan negara?	5, 6, 7	Mewawancara sejumlah pemangku kepentingan	Instrumen pertanyaan
			Mengadakan forum diskusi terbatas (FGD dan RTD)	Instrumen pertanyaan
			Mempelajari strategi pembuatan kebijakan pertahanan siber berbagai negara di dunia	<i>Digital library repository system</i>
			Melakukan <i>benchmarking</i> antar berbagai institusi	<i>Digital library repository system</i>

Sumber : Pemetaan Model Pengumpulan Data terhadap Pertanyaan Penelitian (disusun oleh peneliti)

Kurang lebih 50 (lima puluh) informan terlibat sebagai sumber data primer dalam penelitian ini, dimana masing-masing dikelompokkan ke dalam tiga jenis, yaitu: Informan Kunci (K), Informan Utama (U), dan Informan Pendukung. Tabel berikut memperlihatkan pemetaan informan dalam kaitannya dengan keenam pertanyaan penelitian.

Tabel 4. 3 Pemetaan Informan Penelitian

No	Nama Informan	Jabatan dan Asal Institusi	Pertanyaan Penelitian dan Tipe Informan (K=Kunci U=Utama P=Pendukung)					
			1	2	3	4	5	6
1.	Letjen TNI (Purn.) Agus Widjojo	Gubernur Lemhannas	U	K	P	K	P	K
2.	Letnan Jenderal TNI (Purn.) Hinsa Siburian	Kepala Badan Siber dan Sandi Negara	K	K	K	U	U	K
3.	Kemal Azis Stamboel	Ketua Komisi I DPR RI periode 2009-2014	U	K	P	K	P	K
4.	Brigadir Jenderal TNI Sarwono	Kepala Pusat Pertahanan Siber Kemhan	K	U	K	U	P	K
5.	Brigadir Jenderal TNI (Mar) Suaf Yanu Hardani	Komandan Satuan Siber TNI	K	U	K	U	P	K
6.	Brigjen TNI Dominggus Pakel	Kepala Pusdatin Kemhan (Periode 2018- 2019)	K	K	K	U	P	K
7.	Brigadir Jenderal TNI Bondan Widiawan	Direktur Pengendalian Informasi, Investigasi dan Forensik Digital BSSN	K	U	K	U	K	U
8.	Prof. Zainal A. Hasibuan	Anggota Dewan TIK Nasional (Wantiknas)	P	U	K	P	K	U
9.	Prof. Marsudi W. Kisworo	Komisaris Independen PT Telkom Indonesia	P	U	K	K	U	U

10.	Dr. Hammam Riza	Kepala BPPT	U	U	P	U	K	K
11.	Dr. Ismail	Direktur Jenderal Sumber Daya dan Perangkat Pos dan Informatika, Kemkominfo	P	U	K	U	K	K
12.	Dr. Rudi Luhmanto	Ketua Indonesia Security Incident Response Team on Internet Infrastructure - IDSIRTII (2011-2015)	K	K	K	P	K	U
13.	Arie Sutedja	Ketua Indonesia Cyber Security Forum (ICSF)	U	K	K	U	K	K
14.	Irjen Pol Muhammad Iqbal	Kepala Divisi Humas Kepolisian Republik Indonesia	P	K	K	U	P	P
15.	Prof. Yudho Giri Sucahyo	Ketua Pengelola Nama Domain Internet Indonesia (PANDI)	U	U	K	P	K	K
16.	Prof. Hoga Saragih	Kepala Program Studi Informatika Universitas Bakrie	P	P	P	K	K	P
17.	Dr. Connie Rahakundini Bakrie	Dosen Tetap Universitas Indonesia	P	U	K	P	K	U
18.	Dr. Charles Liem	Peneliti dan Ahli Forensik Digital Swiss-German University	P	P	K	P	K	P
19.	Dr. Bisyrton Wahyudi	Wakil Ketua CSIRT.id	U	P	K	P	U	K

20.	Muhammad Salahuddien	Wakil Ketua IDSIRTII	U	K	U	P	K	U
21.	IGN Mantra	Ketua Academic CERT	P	K	U	P	U	P
22.	Gildas Deograt Lumy	CEO XecureIT	P	K	K	P	U	K
23.	Prof. Eko K. Budiardjo	Ketua IPKIN dan Guru Besar Tetap Universitas Indonesia	P	P	P	K	P	P
24.	Prof. Suhono Supangkat	Advisor Forum TI BUMN, Guru Besar Institut Teknologi Bandung	P	P	P	K	U	K
25.	Prof. Benny Mutiara	Sekretaris Jenderal Asosiasi Pendidikan Tinggi Informatika dan Komputer	U	P	P	P	K	P
26.	Dr. Freddy Harris	Dirjen Kekayaan Intelektual, Kemenkumham	P	P	P	K	K	U
27.	Brigadir Jenderal Polisi Bambang Permantoro	Wakil Kepala Bidang Hukum dan Keadilan (PPATK)	P	P	K	P	P	P
28.	Tin Tin Hadijanto	Country Manager EC-Council	P	P	K	P	P	P
29.	Dr. Onno W. Purbo	Pakar IT Internasional, Dosen Tetap IIB Darmajaya	U	P	U	K	U	P
30.	Ismail Fahmi	Founder Drone Emprit	K	K	U	P	P	P

31.	Dr. Budi Rahardjo	Ketua ID-CERT	K	U	K	P	P	P
32.	Dr. Edmon Makarim	Pakar Cyberlaw, Dosen Tetap Universitas Indonesia	P	P	P	K	P	P
33.	Prof. Riyanarto Sarno	Peneliti Utama dan Guru Besar Tetap ITS Surabaya	P	P	P	K	U	U
34.	Heru Nugroho	Ketua APJII (1999-2002)	P	P	K	U	P	P
35.	Prof. Kalamullah Ramli	Chairman Indonesia Data Center Provider Association, Guru Besar Universitas Indonesia	U	U	U	K	U	U
36.	Djarot Soebiantoro	Ketua Asosiasi Piranti Lunak Informatika Indonesia (Aspiluki)	P	P	P	K	U	U
37.	Christian Octavianus Dono	Founder, Cyber Mantra	U	K	U	P	U	P
38.	Dr. Arko Djajadi	Ahli Internet-Of- Things IULI	P	P	P	P	K	P
39.	Prof. Adjat Daradjat	Ketua Badan Nasional Sertifikasi Profesi (BNSP)	P	P	P	K	P	P
40.	Dr. Heru Purnomo Ipung	Peneliti Utama Swiss-German University	P	P	P	P	K	P
41.	Dr. Ilham Akbar Habibie	Ketua Tim Pelaksana Dewan TIK Nasional (Wantiknas)	U	U	U	K	U	U

42.	Dr. Toto Atmodjo	Founder dan CEO Defenxor	K	P	U	P	K	P
43.	Dr. Handri Santoso	Senior Data Scientist Pradita University	P	K	P	P	P	P
44.	Sylvia W. Sumarlin	Founder Core Mediatech dan Xirka	P	P	P	U	P	P
45.	Teddy Sukardi	Ketua Ikatan Konsultan Teknologi Informasi Indonesia (IKTII)	P	P	P	K	P	P
46.	Dr. Yono Reksoprodjo	Kepala Bidang Ahli Teknologi dan Ofset KKIP	U	K	U	U	U	U
47.	Brigjen TNI Ferdinand Mahulette	Kepala Pusat Operasi Keamanan Siber Nasional BSSN	P	U	K	U	P	P
48.	Dr. Indra Utoyo	Direktur TI dan Digital, Bank Rakyat Indonesia	K	K	U	U	U	U
49.	Komjen. Pol. Dharma Pongrekun	Wakil Kepala Badan Siber dan Sandi Negara (Waka BSSN)	U	K	U	U	P	P
50.	Semuel Abrijani Pangerapan	Direktur Jenderal Aplikasi Informatika Kekominfo	U	U	U	K	K	K

Sumber : Pemetaan Informan Penelitian (hasil pemetaan peneliti)

Potensi Ancaman Serangan Siber terhadap Pertahanan Negara

Hasil pengumpulan data terkait dengan kebutuhan menjawab permasalahan dan pertanyaan penelitian sehubungan dengan potensi ancaman siber terhadap pertahanan negara sebagaimana dijelaskan sebagai berikut.

Tabel 4. 4 Metoda dan Hasil Pengumpulan Data
Pertanyaan Penelitian Pertama

Pertanyaan: "Seperti apakah potensi ancaman siber terhadap sistem pertahanan negara saat ini dan di masa mendatang?"		
Metoda Pengumpulan Data	Hasil Pengumpulan Data	Keterangan
Mewawancara sejumlah pemangku kepentingan	Hasil wawancara dengan sejumlah ahli dan praktisi pertahanan siber, akademisi, regulator, komunitas, dan sejumlah pemangku kepentingan dalam lingkungan Kementerian Pertahanan dan Militer.	Lampiran 1 dan 2
Mengakses catatan digital institusi pemantau siber	Catatan digital berupa perhitungan jumlah serangan dari <i>log file</i> diperoleh dari sejumlah lembaga pemantau trafik internet.	Lampiran 3
Mengadakan forum diskusi terbatas (FGD dan RTD)	Pernyataan, pandangan, dan jawaban terhadap permasalahan maupun pertanyaan penelitian yang disampaikan oleh perwakilan dari akademisi, praktisi, regulator, dan pengelola sistem pertahanan dan keamanan siber.	Lampiran 2
Mempelajari laporan studi kasus nasional dan internasional dari lembaga riset	Berbagai laporan studi terkait dengan ancaman, serangan, dan dampak yang pernah dialami Indonesia maupun negara-negara lain di dunia.	Lampiran 3
Membaca publikasi ilmiah yang relevan	Sebanyak 30 (tiga puluh) publikasi yang mengupas secara detil terkait fenomena serangan dalam dunia siber dan dampaknya terhadap pertahanan	Lampiran 3

serta kedaulatan negara.

Sumber : Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Pertama (disusun oleh peneliti)

Data yang diperoleh saat penelitian direpresentasikan dalam berbagai bentuk. Wawancara dengan sejumlah pemangku kepentingan dicatat dalam bentuk transkrip, sementara rekam jejak serangan sistem berbentuk file elektronik. FGD dan RTD yang menghadirkan sejumlah narasumber terekam dengan baik datanya dalam bentuk file video elektronik. Sementara itu laporan studi nasional dan internasional yang dihasilkan oleh lembaga independen disampaikan dalam bentuk dokumen elektronik. Demikian pula dengan publikasi ilmiah yang diperoleh dari berbagai sumber adalah merupakan file elektronik. Seluruh data tersebut disimpan dan dikelola dengan menggunakan aplikasi NVivo.

Dampak Serangan Siber terhadap Kedaulatan Negara

Hasil pengumpulan data terkait dengan kebutuhan menjawab permasalahan dan pertanyaan penelitian sehubungan dengan dampak serangan siber terhadap kedaulatan negara sebagaimana dijelaskan sebagai berikut.

Tabel 4. 5 Metoda dan Hasil Pengumpulan Data
Pertanyaan Penelitian Kedua

Pertanyaan: “Dampak apakah yang membahayakan pertahanan negara apabila serangan siber tersebut benar-benar terjadi?”		
Metoda Pengumpulan Data	Hasil Pengumpulan Data	Keterangan
Mewawancara sejumlah pemangku kepentingan	Data diperoleh dari hasil wawancara dengan sejumlah ahli dan praktisi pertahanan siber, akademisi, regulator, komunitas, dan sejumlah pemangku kepentingan dalam lingkungan Kementerian Pertahanan dan Militer.	Lampiran 1 dan 2
Mengadakan forum diskusi terbatas (FGD dan RTD)	Data diperoleh dari sejumlah pernyataan, pandangan, dan jawaban terhadap permasalahan maupun pertanyaan penelitian disampaikan oleh perwakilan dari akademisi, praktisi, regulator, dan pengelola sistem pertahanan dan keamanan siber.	Lampiran 2
Mempelajari laporan studi kasus nasional dan internasional dari lembaga riset	Data diperoleh dari berbagai laporan studi terkait dengan ancaman, serangan, dan dampak yang pernah dialami Indonesia maupun negara-negara lain di dunia.	Lampiran 3
Membaca publikasi ilmiah yang relevan	Data diperoleh dari 30 (tiga puluh) publikasi yang mengupas secara detil terkait fenomena serangan dalam dunia siber dan dampaknya terhadap pertahanan serta kedaulatan negara.	Lampiran 3
Mengakses catatan digital ahli bidang	Data diperoleh dari beragam pendapat pribadi para ahli dan praktisi terkait	Lampiran 3

siber (*blog, vlog*) dengan fenomena dunia siber.

Sumber : Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Kedua (disusun oleh peneliti)

Data yang diperoleh saat penelitian direpresentasikan dalam berbagai bentuk. Wawancara dengan sejumlah pemangku kepentingan dicatat dalam bentuk transkrip, sementara untuk FGD dan RTD terekam dengan baik datanya dalam bentuk file video elektronik. Adapun laporan hasil studi nasional dan internasional yang dihasilkan oleh lembaga independen disampaikan dalam bentuk dokumen elektronik. Demikian pula dengan tiga puluh publikasi ilmiah yang diperoleh dari berbagai sumber adalah merupakan file elektronik. Sementara itu data yang ada di internet baik dalam bentuk blog maupun vlog tersimpan alamat situsnya untuk sewaktu-waktu diakses. Seluruh data tersebut disimpan dan dikelola dengan menggunakan aplikasi NVivo.

Tingkat Kerawanan Pertahanan Siber di Indonesia

Hasil pengumpulan data terkait dengan kebutuhan menjawab permasalahan dan pertanyaan penelitian sehubungan dengan tingkat kerawanan pertahanan siber di Indonesia sebagaimana dijelaskan sebagai berikut.

Tabel 4. 6 Metoda dan Hasil Pengumpulan Data
Pertanyaan Penelitian Ketiga

Pertanyaan: “Bagaimana tingkat kerawanan siber Indonesia dalam sektor pertahanan?”		
Metoda Pengumpulan Data	Hasil Pengumpulan Data	Keterangan
Mewawancara sejumlah	Data diperoleh dari hasil wawancara	Lampiran 1

pemangku kepentingan	dengan sejumlah ahli dan praktisi pertahanan siber, akademisi, regulator, komunitas, dan sejumlah pemangku kepentingan dalam lingkungan Kementerian Pertahanan dan Militer.	dan 2
Menyelenggarakan survei kepada sejumlah <i>stakeholder</i>	Data diperoleh dari hasil survei yang melibatkan 500 responden di kalangan Kementerian Pertahanan dan Militer.	Lampiran 4
Melakukan analisa intelijen dan forensik siber	Data diperoleh dari hasil sejumlah aktivitas atau proses berbasis elektronik seperti <i>penetration test</i> terhadap sejumlah situs-situs penting di tanah air.	Lampiran 3
Mempelajari laporan studi kasus kejahatan siber di Indonesia	Data diperoleh dari berbagai sumber internet maupun laporan masyarakat terkait dengan terjadinya kejahatan siber di Indonesia.	Lampiran 3
Mengakses catatan digital ahli bidang siber (<i>blog</i> , <i>vlog</i>)	Data diperoleh dengan mempelajari catatan digital para praktisi, ahli, akademisi, maupun komunitas yang terbuka bebas di internet.	Lampiran 3

Sumber : Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Ketiga (disusun oleh peneliti)

Data yang diperoleh saat penelitian direpresentasikan dalam berbagai bentuk. Wawancara dengan sejumlah pemangku kepentingan dicatat dalam bentuk transkrip. Sementara itu data yang ada di internet baik dalam bentuk blog maupun vlog tersimpan alamat situsnya untuk sewaktu-waktu diakses. Disamping itu diperoleh pula data hasil analisa intelijen dan forensik siber terhadap sejumlah situs penting di Indonesia. Sementara itu laporan hasil studi kejahatan siber di Indonesia merupakan tautan internet terkait dengan detail mengenai peristiwa yang ada. Seluruh data tersebut disimpan dan dikelola

dengan menggunakan aplikasi NVivo. Sebagai tambahan, ketika FGD dan RTD dilaksanakan, dilakukan pula penyebaran survei kepada kurang lebih 500 responden di lingkungan Kementerian Pertahanan dan Militer yang hasilnya ditabulasikan dalam bentuk *spreadsheet*.

Efektivitas Kebijakan Kedaulatan Pertahanan Siber di Indonesia

Hasil pengumpulan data terkait dengan kebutuhan menjawab permasalahan dan pertanyaan penelitian sehubungan dengan efektivitas kebijakan kedaulatan pertahanan siber di Indonesia sebagaimana dijelaskan sebagai berikut.

Tabel 4. 7 Metoda dan Hasil Pengumpulan Data
Pertanyaan Penelitian Keempat

Pertanyaan: “Seperti apakah kebijakan pertahanan siber nasional yang dimiliki Indonesia saat ini? Bagaimana tingkat efektivitas kebijakan pertahanan siber pada sektor pertahanan yang diterapkan di Indonesia sekarang?”		
Metoda Pengumpulan Data	Hasil Pengumpulan Data	Keterangan
Mewawancara sejumlah pemangku kepentingan	Data diperoleh dari hasil wawancara dengan sejumlah ahli dan praktisi pertahanan siber, akademisi, regulator, komunitas, dan sejumlah pemangku kepentingan dalam lingkungan Kementerian Pertahanan dan Militer.	Lampiran 1 dan 2
Menyelenggarakan survei kepada sejumlah <i>stakeholder</i>	Data diperoleh dari hasil survei yang melibatkan 213 responden dari berbagai kalangan yang terlibat secara langsung maupun tidak langsung dengan pertahanan siber.	Lampiran 4
Mempelajari seluruh kebijakan terkait pertahanan siber	Data diperoleh dari repositori atau kumpulan seluruh peraturan (kebijakan) terkait dengan pengelolaan sistem siber di Indonesia yang telah diundangkan.	Lampiran 3
Mengikuti diskursus percakapan para ahli, digital di internet yang membahas pelaku, dan praktisi siber	Data diperoleh dari berbagai sumber digital di internet yang membahas mengenai pertahanan dan kedaulatan siber di Indonesia.	Lampiran 3

Membaca laporan pemeringkatan lembaga independen dunia	Data diperoleh dari hasil pemeringkatan sejumlah lembaga independen dunia terhadap negara-negara dunia terkait dengan berbagai aspek siber dan teknologi informasi komunikasi.	Lampiran 3

Sumber : Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Keempat (disusun oleh peneliti)

Data yang diperoleh saat penelitian direpresentasikan dalam berbagai bentuk. Wawancara dengan sejumlah pemangku kepentingan dicatat dalam bentuk transkrip. Sementara data mengenai regulasi dan kebijakan yang selama ini diundangkan di Indonesia disimpan secara rapi dalam repositori digital. Adapun data berupa percakapan, diskursus, dan pendapat para ahli dan praktisi terkait disimpan tautannya. File elektronik lain adalah dokumen elektronik terkait dengan laporan pemeringkatan sejumlah lembaga independen dunia. Seluruh data tersebut disimpan dan dikelola dengan menggunakan aplikasi NVivo. Sebagai tambahan, ketika FGD dan RTD dilaksanakan, dilakukan pula penyebaran survei kepada kurang lebih 213 responden dari berbagai kalangan akademisi dan praktisi untuk mendapatkan masukan yang hasilkan ditabulasikan ke dalam *spreadsheet*.

Model Pertahanan Siber Ideal yang Holistik dan Komprehensif

Hasil pengumpulan data terkait dengan kebutuhan menjawab permasalahan dan pertanyaan penelitian sehubungan dengan model pertahanan siber ideal yang holistik dan komprehensif sebagaimana dijelaskan sebagai berikut.

Tabel 4. 8 Metoda dan Hasil Pengumpulan Data
Pertanyaan Penelitian Kelima

Pertanyaan: “Seperti apakah ekosistem pertahanan dan kedaulatan siber yang holistik dan komprehensif? Seperti apakah model kebijakan pertahanan dan kedaulatan siber nasional yang ideal dalam sebuah negara?”		
Metoda Pengumpulan Data	Hasil Pengumpulan Data	Keterangan
Mewawancara sejumlah pemangku kepentingan	Data diperoleh dari hasil wawancara dengan sejumlah ahli dan praktisi pertahanan siber, akademisi, regulator, komunitas, dan sejumlah pemangku kepentingan dalam lingkungan Kementerian Pertahanan dan Militer.	Lampiran 1 dan 2
Mengadakan forum diskusi terbatas (FGD dan RTD)	Data diperoleh dari sejumlah pernyataan, pandangan, dan jawaban terhadap permasalahan maupun pertanyaan penelitian disampaikan oleh perwakilan dari akademisi, praktisi, regulator, dan pengelola sistem pertahanan dan keamanan siber.	Lampiran 2
Mempelajari sistem pertahanan siber berbagai negara di dunia	Data diperoleh dari berbagai buku putih atau <i>strategic documents</i> dari berbagai negara di dunia yang telah menerapkan konsep pertahanan sibernya dengan baik.	Lampiran 3
Melakukan <i>benchmarking</i> antar berbagai institusi	Data diperoleh dari berbagai institusi non negara (pemerintah) yang memiliki keterkaitan dengan perencanaan, pembangunan, pengembangan, pengelolaan, dan pengendalian pertahanan siber.	Lampiran 3

Sumber : Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Kelima (disusun oleh peneliti)

Data yang diperoleh saat penelitian direpresentasikan dalam berbagai bentuk. Wawancara dengan sejumlah pemangku kepentingan dicatat dalam bentuk transkrip, sementara untuk FGD dan RTD terekam dengan baik datanya dalam bentuk file video elektronik. Sejumlah buku putih terkait sistem pertahanan siber berbagai negara di dunia disimpan dalam bentuk file elektronik. Data lain yang dipakai sebagai sumber kajian adalah hasil studi komparasi berbagai lembaga non pemerintah terkait dengan tata kelola siber. Seluruh data tersebut disimpan dan dikelola dengan menggunakan aplikasi NVivo.

Strategi Pengembangan Kebijakan Pertahanan Siber Nasional

Hasil pengumpulan data terkait dengan kebutuhan menjawab permasalahan dan pertanyaan penelitian sehubungan dengan strategi pengembangan kebijakan pertahanan siber nasional yang efektif, efisien, dan terkendali sebagaimana dijelaskan sebagai berikut.

Tabel 4. 9 Metoda dan Hasil Pengumpulan Data
Pertanyaan Penelitian Keenam

Pertanyaan: “Bagaimana strategi pengembangan kebijakan siber nasional untuk mengatasi ancaman dalam bingkai pemutakhiran doktrin pertahanan negara?”		
Metoda Pengumpulan Data	Hasil Pengumpulan Data	Keterangan
Mewawancara sejumlah pemangku kepentingan	Data diperoleh dari hasil wawancara dengan sejumlah ahli dan praktisi pertahanan siber, akademisi, regulator, komunitas, dan sejumlah pemangku kepentingan dalam lingkungan Kementerian Pertahanan dan Militer.	Lampiran 1 dan 2
Mengadakan forum diskusi terbatas (FGD dan RTD)	Data diperoleh dari sejumlah pernyataan, pandangan, dan jawaban terhadap permasalahan maupun pertanyaan penelitian disampaikan oleh perwakilan	Lampiran 2

dari akademisi, praktisi, regulator, dan pengelola sistem pertahanan dan keamanan siber.

Mempelajari strategi pembuatan kebijakan pertahanan siber berbagai negara di dunia	Data diperoleh dari berbagai buku putih atau <i>strategic documents</i> dari berbagai negara di dunia yang telah menerapkan konsep strategi pembuatan kebijakan pertahanan sibernya dengan baik.	Lampiran 3
Melakukan <i>benchmarking</i> antar berbagai institusi	Data diperoleh dari berbagai institusi non-negara (pemerintah) yang memiliki keterkaitan dengan pengembangan kebijakan negara dalam bidang pertahanan siber.	Lampiran 3

Sumber : Metoda dan Hasil Pengumpulan Data Pertanyaan Penelitian Keenam (disusun oleh peneliti)

Data yang diperoleh saat penelitian direpresentasikan dalam berbagai bentuk. Wawancara dengan sejumlah pemangku kepentingan dicatat dalam bentuk transkrip, sementara untuk FGD dan RTD terekam dengan baik datanya dalam bentuk file video elektronik. Sejumlah buku putih terkait sistem pertahanan siber berbagai negara di dunia disimpan dalam bentuk file elektronik. Data lain yang dipakai sebagai sumber kajian adalah hasil studi komparasi berbagai lembaga non pemerintah terkait dengan strategi penyusunan kebijakan pertahanan siber. Seluruh data tersebut disimpan dan dikelola dengan menggunakan aplikasi NVivo.

Hasil Pengolahan Data Kualitatif dan Kuantitatif

Data yang telah berhasil dikumpulkan dalam penelitian untuk selanjutnya diolah dengan menggunakan sejumlah metoda. Berikut adalah

berbagai cara yang dipergunakan dalam mengelola data kualitatif (dan sejumlah data kuantitatif) dalam penelitian yang dilakukan.

Tabel 4. 10 Pemetaan Model Pengolahan Data terhadap Sumber Data

No	Sumber Data	Model Pengolahan Data
1	Transkrip Wawancara	Mencari kata atau kalimat kunci yang berkaitan secara langsung maupun tidak langsung terhadap permasalahan maupun pertanyaan penelitian
2	Rekaman FGR dan RTD	Mencatat saripati pendapat narasumber terkait dengan permasalahan dan pertanyaan penelitian
3	Survei Terbatas	Melakukan rangkuman hasil dengan menggunakan statistik deskriptif
4	Publikasi/Literatur	Mengutip pendapat ahli, pakar, dan akademisi yang berhubungan dengan permasalahan maupun pertanyaan penelitian
5	Laporan Penelitian	Meringkas hal-hal penting yang relevan dalam laporan penelitian terkait dengan permasalahan dan pertanyaan penelitian
6	Konferensi/Webinar	Menseleksi butir-butir pernyataan dari narasumber terkait dengan permasalahan dan pertanyaan penelitian
7	Blog/Vlog Internet	Mendengarkan dan mengidentifikasi sejumlah pernyataan maupun pendapat yang berkaitan dengan permasalahan dan pertanyaan penelitian
8	Diskursus Digital	Menyimpulkan makna yang tersurat maupun tersirat dalam percakapan atau diskusi dalam kaitannya dengan permasalahan dan pertanyaan penelitian
9	Rekam Jejak Digital	Mengolah data log file yang berasal dari sistem komputer untuk mendapatkan informasi terkait dengan permasalahan atau pertanyaan penelitian

Sumber : Pemetaan Model Pengolahan Data terhadap Sumber Data (disusun oleh peneliti)

Inti dari pengolahan data kualitatif adalah pada reduksi data. Sesuai dengan namanya, dengan melakukan reduksi data berarti memilih data mana saja yang relevan digunakan untuk memperkuat laporan penelitian. Menurut Miles, reduksi data merupakan proses pemilihan, pemusatan perhatian pada penyederhanaan, pengabstrakan, dan transformasi data kasar yang muncul dari data-data lapangan. Perlu dilakukannya reduksi data karena pada umumnya data kualitatif sangat banyak, terutama dari hasil wawancara dan observasi. Setelah melakukan reduksi data, maka dilanjutkan dengan proses kategorisasi data. Berikut adalah hasil pengolahan data per masing-masing aspek yang berkaitan langsung dengan permasalahan dan/atau pertanyaan penelitian.

Potensi Ancaman Serangan Siber terhadap Pertahanan Negara

Hasil pengolahan data yang berkaitan secara erat dengan isu ancaman maupun serangan siber dalam konteks pertahanan dan kedaulatan negara disaripatkan dalam tabel berikut ini.

Tabel 4. 11 Hasil Pengolahan Data Potensi Ancaman Serangan Siber

No	Hasil Pengolahan Data	Sumber
1	<i>“Trafik memperlihatkan bahwa perang siber telah dan sedang terjadi setiap hari. Sensor-sensor penting di BSSN dan lembaga dunia lainnya memperlihatkan hal tersebut. Sejumlah penelitian memperlihatkan adanya peningkatan serangan secara intens. Bahkan situasi sulit seperti pandemi saat ini justru meningkatkan ketegangan di dunia siber.”</i> <i>“Setiap harinya terdapat jutaan percobaan serangan ke situs-situs di Indonesia. Bahkan selama masa pandemi</i>	Charles Liem, Peneliti Swiss-German University, Wawancara Bondan Universitas Pertahanan RI

- terjadi kenaikan jumlah serangan secara sangat signifikan.”
- Widiawan,
Deputi BSSN,
RTD
- “Pada waktu ID-SIRTII didirikan pada tahun 2005, setiap harinya paling tidak terdapat 1.5 juta serangan. Disinyalir serangan ini terus bertambah dari tahun ke tahun.”
- Muhamamad
Salahuddien,
Mantan Wakil ID-SIRTII,
Wawancara
- 2 “Ancaman dalam konteks pertahanan negara perlu ditinjau dengan menggunakan perspektif manajemen risiko, terutama berkaitan dengan dampak yang terjadi ketika cyber war berlangsung dan melibatkan Indonesia. Konteks ancaman dalam dunia siber dapat dipelajari dengan menggunakan perspektif cyber threat intelligence model.”
- Ardi Sutedja,
Ketua ICSF,
Wawancara
- “Ancaman berupa serangan siber tidak berada di ruang hampa. Setiap terdapat konflik antara negara, kecil atau besar, selalu diikuti dengan aktivitas di dunia maya.”
- Rudi Luhmanto,
Ketua CSIRT.id,
Wawancara
- “Ancaman di dunia maya dapat sangat strategis dampaknya pada negara, terutama jika ditujukan untuk merusak infrastruktur nasional.”
- Gildas Deograt,
XecureIT,
Komunikasi Personal
- 3 “Perang siber terjadi setiap hari, namun secara formal dianggap tidak terjadi karena tidak adanya pernyataan perang sebagaimana dalam dunia fisik.”
- Bisyrn Wahyudi,
Mantan Manajer ID-SIRTII,
Wawancara
- “Karakteristik perang siber berbeda dengan konvensional, karena tidak dapat terlihat wujudnya, dan tidak dirasakan terjadinya.”
- Marsudi Kisworo,
Komisaris Telkom,
Wawancara
- “Ancaman siber tidak dianggap penting karena tidak ada yang tahu bahwa setiap hari sudah terjadi serangan menyerang antar negara. Hal ini dapat dilihat dalam monitoring berbagai sensor siber di dunia.”
- Heru Nugroho,
Mantan Ketua APJII,
Komunikasi Personal

4	<i>“Perang siber terjadi, dan biasanya selalu ada kaitannya dengan sponsor pada sebuah negara – secara langsung maupun tidak langsung. Peran Indonesia kebanyakan dijadikan platform antara dua pelaku perang siber, sehingga pada dasarnya Indonesia adalah korban. Lihatlah bagaimana jumlah phishing site yang ada di Indonesia dimana semakin meningkat dari hari ke hari.”</i> <i>“Di Indonesia banyak sekali komputer yang telah dijangkiti malware, dimana sewaktu-waktu dapat diperintahkan untuk melakukan serangan semacam DDOS.”</i> <i>“Pada berbagai kasus perang siber di masa lalu terdeteksi adanya banyak sumber serangan yang berasal dari IP address Indonesia. Kemungkinan besar berasal dari server yang terjangkiti malware.”</i>	Rudi Luhmanto, Ketua CSIRT.id, Wawancara Christian Dono, Pakar Siber, Komunikasi Personal IGN Mantra, Ketua ACA- CERT, Webinar
5	<i>“Banyak pimpinan tidak menyadari bahwa ancaman siber telah menjadi paradigma perang baru yang menjadi prioritas global.”</i> <i>“Sekarang itu adalah era perang informasi, dimana tidak perlu menggunakan berbagai senjata berat untuk melakukan agitasi ke negara lain.”</i> <i>“Perang sudah bergeser menuju perang mindset yang dilakukan melalui propaganda via media sosial.”</i>	Bondan Widiawan, Deputi BSSN, RTD Connie R. Bakrie, Pakar Militer, Webinar Dominggus Pakel, Mantan Kapusdatin Kemhan, Diskusi
6	<i>“Negara maju pencipta berbagai teknologi dan infrastruktur komunikasi melakukan penjajahan terhadap kedaulatan negara-negara berkembang melalui produk dan layanannya. Lihatlah bagaimana untuk perangkat jaringan hanya dikuasai oleh dua perusahaan besar, yaitu Cisco dan Huawei. Dengan kata lain, Indonesia tidak memiliki kendali terhadap ekosistem siber nasional.”</i> <i>“Indonesia harus memiliki kedaulatan di bidang siber dengan cara membuat dan menggunakan produksi</i>	Christian Dono, Pakar Siber, Komunikasi Personal Gildas Deograt, XecureIT,

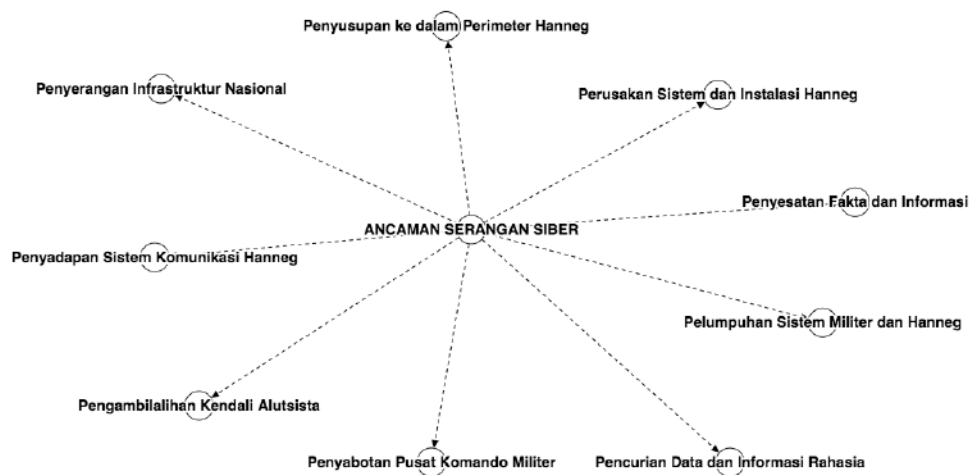
- buatan anak bangsa.”* Webinar
- “Hasil dari berbagai riset kampus di bidang IT memperlihatkan kemampuan putra putri Indonesia untuk membuat produk keamanan internet yang tidak kalah dengan bangsa lain.”* Handri Santoso,
Peneliti Pradita
University,
Komunikasi
Personal
- 7 *“Inti dari persaingan global tidak berubah dari masa ke masa, yaitu berusaha untuk memperebutkan sumber daya ekonomi dari negara lain. Internet dunia masih dikendalikan oleh Amerika Serikat dalam bentuk “peminjaman” alamat internet (dikenal sebagai IP address) agar individu maupun lembaga dapat terhubung dengan dunia maya. Tanpa adanya pengalokasian ini, mustahil masyarakat Indonesia dapat menggunakan internet.”* M.Salahuddien,
Mantan Wakil
Ketua ID-SIRTII,
Wawancara
- “Banyak pihak mulai memikirkan bagaimana caranya membuat jaringan internet alternatif seperti yang dilakukan China. Indonesia sebenarnya memiliki potensi untuk melakukan hal ini.”* Heru Nugroho,
Mantan Ketua
APJII,
Komunikasi
Personal
- “Penjajahan yang sebenarnya bukan terletak pada layer atas, tapi lebih pada pengaturan terhadap protokol internet global yang dimonopoli negara besar.”* Heru Purnomo
Ipung, Peneliti
Swiss-German
University,
Komunikasi
Personal
- 8 *“Indonesia di mata dunia dianggap sangat strategis karena posisinya dapat dimanfaatkan sebagai proksi dalam berbagai skenario serangan berskala besar dan masif. Memang kemungkinan besar Indonesia tidak menyerang kecuali jika diserang, tapi secara tidak sadar banyak entitas yang dijadikan sebagai proksi. Dimana ada perang fisik, di situ akan ada perang siber.”* Hoga Saragih,
Guru Besar
Universitas
Bakrie,
Wawancara
- “Indonesia pernah dianggap sebagai surga bagi para peretas, terutama ketika belum diterbitkan UU ITE.”* Muhammad
Salahuddien,
Mantan Wakil
Ketua ID-SIRTII,
Wawancara

“Perang proksi dapat dilakukan karena adanya kelemahan pada sejumlah negara yang tidak memiliki keamanan internet yang kuat.”

IGN Mantra,
Ketua ACA-
CERT, Webinar

Sumber : Hasil Pengolahan Data Potensi Ancaman Serangan Siber (disusun oleh peneliti)

Hasil pengolahan data yang dilakukan memperlihatkan bagaimana sebuah serangan siber dapat berpotensi menyebabkan terjadinya gangguan yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa. Hasil studi dan penelitian ini mengkategorikan klasifikasi ancaman terhadap pertahanan negara berdasarkan dampak bahaya yang ditimbulkan menjadi 9 (sembilan) kelompok besar sebagaimana diperlihatkan berikut.



Gambar 4. 3 Sembilan Jenis Ancaman dan Serangan Siber pada Haneg

Sumber : Sembilan Jenis Ancaman dan Serangan Siber pada Haneg

(hasil pengolahan data oleh peneliti)

Universitas Pertahanan RI

Pengelompokkan di atas didasarkan pada sejumlah peristiwa di masa lalu, yang telah direkam secara baik dalam berbagai publikasi ilmiah melalui pendekatan studi kasus. Selain mempelajari berbagai kasus riil yang menimpa berbagai negara di dunia, sebanyak 30 (tiga puluh) literatur utama dijadikan sumber peneliti dalam melakukan proses klasterisasi.

Tabel 4. 12 Ragam Ancaman terhadap Sektor Pertahanan dan Dampaknya

Jenis	Ancaman terhadap Sektor Pertahanan	Dampak yang Membahayakan Kedaulatan Negara, Keutuhan Wilayah Keselamatan Bangsa
A	Penyerangan terhadap infrastruktur vital/kritis nasional	Menghentikan operasional infrastruktur vital yang menguasai hajat hidup orang banyak seperti listrik, air, energi, transportasi, dsb.
B	Penyadapan sistem komunikasi dan koordinasi pertahanan	Mengetahui aktivitas dan kegiatan yang akan dilakukan berbagai pemangku kepentingan dalam kaitannya dengan pengelolaan pertahanan negara
C	Pengambilalihan kendali terhadap alutsista berbasis digital	Mengoperasikan dan mengontrol alutsista dari jarak jauh agar dapat melakukan aktivitas yang diinginkan tanpa dapat dicegah oleh pemiliknya
D	Penyabotan terhadap sistem pusat kendali (<i>command center</i>)	Membuat pusat kendali pertahanan dan militer tidak bekerja sebagaimana mestinya sehingga menghambat pemantauan, pengorganisasian, dan pengambilan keputusan strategis
E	Pencurian data dan informasi penting mengenai pertahanan negara	Mendapatkan data dan informasi rahasia mengenai pertahanan negara yang dapat dipergunakan sebagai referensi dalam melakukan berbagai kegiatan yang merugikan lawan
F	Pelumpuhan sistem informasi dan teknologi pada sektor pertahanan	Mengakibatkan tidak dapat dipergunakan atau terganggunya operasional sistem teknologi informasi yang berada dalam

		sector pertahanan
G	Penyesatan fakta melalui disinformasi dan misinformasi (propaganda)	Menyesatkan dan mengadu-domba berbagai pihak agar saling berseteru melalui penyebaran informasi yang salah atau bohong
H	Perusakan sistem dan fasilitas teknologi informasi pertahanan	Menghancurkan sumber daya komputasi (terutama perangkat keras, infrastruktur, jaringan, dan fasilitas sarana prasarana) secara fisik sehingga tidak dapat dipergunakan
I	Penyusupan ke dalam sistem dan fasilitas rahasia pertahanan negara	Menyamarkan identitas untuk dapat memperoleh akses terhadap berbagai situs, sistem, dan perimeter yang bersifat strategis dan bernilai tinggi.

Sumber : Ragam Ancaman terhadap Sektor Pertahanan dan Dampaknya (disusun oleh peneliti)

Tabel ini memperlihatkan bagaimana proses pengelompokan terjadi berdasarkan tiga puluh jurnal akademis yang di dalamnya mengupas tuntas mengenai fenomena serangan siber pada level nasional/negara yang berpengaruh secara langsung terhadap situasi dan kondisi pertahanan negara (Hughes & Shaffer, 2020; Park, 2016; Sigholm, 2016). Perlu diperhatikan bahwa dalam studi literatur yang dilakukan, terlihat bagaimana negara-negara di dunia membedakan antara serangan siber atau *cyber attack* yang bersifat mikro dan makro (Lilienthal & Ahmad, 2015b; Rosenfield, 2009). Dikatakan bersifat mikro ketika ruang lingkup dan dampaknya hanya bersifat terbatas sehingga tidak memiliki dampak signifikan terhadap keselamatan dan kedaulatan negara. Sementara serangan siber berada dalam kategori makro apabila keberadaannya membahayakan keutuhan dan kedaulatan negara. Dalam konteks pertahanan negara, serangan yang bersifat makro dan telah melibatkan dua atau lebih negara berpotensi menjadi *cyberwar* – perang antara sejumlah negara berdaulat dalam arena maya (Schulze, 2020; Sigholm, 2016). Oleh karena itulah maka dalam membedakan serangan mana yang bersifat mikro dan makro, dilakukan

pencirian terhadap karakteristik kejadian yang ada. Kenyataan memperlihatkan bahwa istilah *cyberwar* lebih tepat dipergunakan dibandingkan dengan *cyber attack* karena karakteristiknya yang selaras dengan definisi serangan dalam sistem pertahanan negara.

Cyberwar sendiri merupakan fenomena yang banyak mengemuka dalam konteks pertahanan moderen. Diskursus seputar konsep ini banyak dibahas dalam berbagai literatur dan komunitas. Fenomena ini didefinisikan sebagai:

“Penggunaan teknologi komputer untuk mengganggu aktivitas suatu negara atau organisasi, terutama penyerangan sistem informasi yang disengaja untuk tujuan strategis atau militer”.

Berdasarkan definisi inilah maka dapat dibedakan serangan mana saja yang berpotensi mengganggu pertahanan negara dan yang tidak.

Kajian terhadap sejumlah literatur di atas memperlihatkan bagaimana spektrum serangan siber terbentuk melalui proses pemetaan. Selain kajian literatur, sejumlah peristiwa di masa lalu yang menimpa sejumlah negara dalam kaitannya dengan perang siber juga menjadi penguat proses identifikasi jenis serangan yang ada (Beidleman, 2009). Terlihat secara jelas dalam tabel bagaimana klasifikasi dilakukan berdasarkan kejadian tak diinginkan atau risiko yang berpotensi memberikan dampak negatif dan signifikan terhadap kondisi pertahanan negara. Tentu saja sesuai dengan perkembangan teknologi informasi dan komunikasi yang sedemikian cepat dimungkinkan diperkenalkannya jenis ancaman baru. Tapi paling tidak kesembilan klasifikasi yang berhasil diidentifikasi telah secara nyata hadir di dunia pada masa lalu, saat ini, dan di kemudian hari.

Tabel 4. 13 Pemetaan Ragam Ancaman terhadap Literatur Ilmiah

		A	B	C	D	E	F	G	H	I
No.	Literatur, Referensi dan Publikasi Ilmiah	Penyerangan terhadap infrastruktur vital /kritis nasional	Penyadapan sistem komunikasi dan koordinasi pertahanan	Pengambilalihan kendali terhadap alutsista berbasis digital	Penyabotan terhadap pusat kendali pertahanan negara (<i>command center</i>)	Pencurian data dan informasi penting terkait pertahanan negara	Pelumpuhan sistem informasi dan teknologi terkait dengan pertahanan negara	Penyesatan fakta melalui disinformasi dan misinformasi (propaganda)	Perusakan sistem dan fasilitas teknologi informasi pertahanan	Penyusupan ke dalam sistem dan fasilitas rahasia pertahanan negara
1	“From Cyber War to Cyber Peace” (Reinhold & Reiter, 2019)	X	X	X	X	X			X	
2	“Cyber War and Nuclear Peace” (Gompert & Libicki, 2019)	X			X				X	
3	“The cyber arms race is	X								X

Universitas Pertahanan RI

9	Terror, and Risk” (Barnard-Wills & Ashenden, 2012)		X	X	X	X	X		X	X
10	“Generals in Cyberspace: Military Insights for Defending Cyberspace” (Campbell, 2018)	X		X	X		X			X
11	“Modelling and Simulation: Cyber War” (Mishra & Prajapati, 2013)				X	X	X		X	
12	“Mutual assured destruction in information, influence and cyber warfare: Compari ng, contrasting and combining relevant scenarios” (Straub, 2019)		X			X		X		
13	“Multi-paradigm Deception		X			X		X		X

	Modeling for Cyber Defense” (Faveri, Moreira, & Amaral, 2017)									
14	“The Principle of Distinction and Cyber War in	X	X	X		X	X		X	X
15	“International Armed Conflicts” (Dinstein, 2015)	X	X	X	X	X	X	X	X	X
16	“Violence, Just Cyber War and Information” (Dura nte, 2014)	X		X	X		X		X	X
17	“Cyber Situation Awareness: Modeling Detection of Cyber Attacks With Instance-Based Learning Theory” (Dutt, Ahn, & Gonzalez, 2013)	X					X		X	
18	“Limits to a cyber- threat” (Emerson,	X		X			X	X	X	X

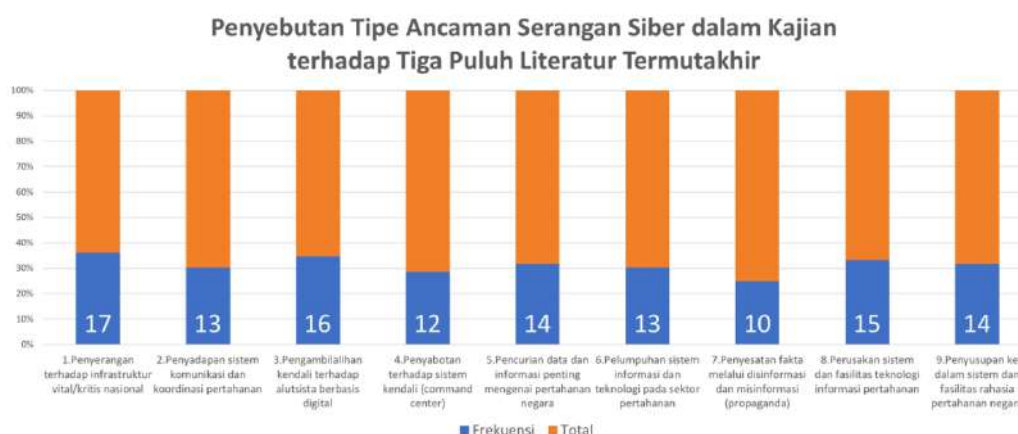
	2016)										
19	“Stuxnet and the Future of Cyber War” (Farwell & Rohozinski, 2011)	X	X	X	X	X	X	X	X	X	X
20	“The New Reality of Cyber War” (Farwell & Rohozinski, 2012)	X		X	X		X		X		
21	“Legitimate firms or hackers – who is winning the global cyber war?” (Majadillas, White, & Walsh, 2019)	X		X			X	X			
22	“Cyber war — When virtual fear of death turns into a real threat of life” (Grander, Schwaiger, Seeber, & Dünser, 2009)	X		X		X		X			X
23	“Active cyber defense with denial and		X		X		X		X		

	deception: A cyber-wargame experiment" (Heckman, Walsh, Stech, O'Boyle, DiCato, & xHerber, 13)									
24	"How Probable is Cyber xWar? Bringing IR Theory Back In to the Cyber Conflict Debate" (Junio, 2014)	X				X			X	X
25	"Cyber Deterrence in Times of Cyber Anarchy" (Kania, 2016)	X		X	X					
26	"Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures" (Lee & Shon,	X	X	X	X	X	X	X	X	X

	2016)									
27	“Cyber War is Inevitable (Unless We Build Security In)” (McGraw, 2013)	X		X	X				X	
28	“Modelling and Simulation: Cyber War” (Mishra & Prajapati, 2013)		X	X		X				X
29	“Finding the New High Ground in Cyber War: Malware as an Instrument of War” (Philbin & Philbin, 2012)	X		X	X			X		X
30	“A systematic review of cyber-resilience assessment frameworks” (Sepúlveda-Estay, RSahay, & Michael, 2020)	X	X	X	X	X	X	X	X	X

Sumber : Pemetaan Ragam Ancaman terhadap Literatur Ilmiah (hasil pengolahan data oleh peneliti)

Perlu dicatat pula bahwa kesembilan kelompok ancaman serangan siber yang teridentifikasi pada dasarnya merupakan sebuah “atom” yang dalam kejadian sebenarnya dapat terjadi secara bersamaan atau simultan, melahirkan berbagai kombinasi “molekul” serangan. Bahkan dalam sejumlah kejadian di masa lalu, terjadi serangan beruntun yang menimpa sebuah negara dimana hampir seluruh jenis serangan diperlihatkan melalui kombinasi strategi yang sangat kompleks (Dinstein, 2012; “The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case,” 2013). Berbeda dengan perang fisik, serangan menyerang dalam dunia siber – atau *cyberwar* – tidak dapat dilihat secara kasat mata. Keberadaannya secara jelas akan dapat dideteksi melalui berbagai teknologi *network monitoring system* yang dibangun melalui jejaring sensor trafik internet yang tertanam dalam berbagai titik *internet exchange* yang tersebar di ribuan lokasi. Serangan siber baru dapat dirasakan kehadirannya oleh manusia hanya dan apabila memberikan dampak langsung terhadap dunia nyata, seperti dalam bentuk: kejahatan, kerusakan, terorisme, pemberontakan, kehancuran, pencurian, dan lain sebagainya (Hathaway et al., 2012).



Gambar 4. 4 Frekuensi Penyebutan Jenis Serangan pada 30 Literatur

Sumber : Frekuensi Penyebutan Jenis Serangan pada 30 Literatur (hasil pengolahan data oleh peneliti)

Dampak Serangan Siber terhadap Kedaulatan Negara

Hasil pengolahan data yang berkaitan secara erat dengan isu dampak serius dari serangan siber dalam konteks pertahanan dan kedaulatan negara disaripatikan dalam tabel berikut ini.

Tabel 4. 14 Hasil Pengolahan Data Dampak Serangan Siber

No	Hasil Pengolahan Data	Sumber
1	<i>"Banyak orang berfikir bahwa kedaulatan negara akan terjaga sejauh tidak ada wilayah teritori yang berhasil diambil alih oleh negara lain. Padahal dalam konteks siber, teritori negara menjadi sangat tidak relevan. Dapat saja terjadi sebuah negara memiliki teritori yang terjaga, namun tergerus sumber daya ekonominya akibat ekosistem siber global yang tidak berpihak pada negara bersangkutan."</i> <i>"Dengan dipergunakannya aplikasi buatan dunia barat, pada dasarnya kedaulatan Indonesia sudah hilang karena semua informasi detil mengenai warga negara dan kegiatannya disimpan rapi oleh mereka."</i> <i>"Kedaulatan berarti adanya kontrol terhadap sumber daya yang dimiliki, termasuk data dan informasi publik."</i>	Muhammad Salahuddien, Mantan Wakil Ketua ID-SIRTII, Wawancara Gildas Deograt, XecureIT, Komunikasi Personal Ismail, Dirjen Kominfo, Komunikasi Personal
2	<i>"Banyak orang lupa akan terjadinya serangan masif dan berbahaya untuk menghancurkan negara seperti peristiwa di Estonia dan Georgia. Motivasi penyerang kebanyakan adalah finansial atau ekonomi, dengan cara memanfaatkan ketidaktahuan masyarakat akan cara siber beroperasi."</i> <i>"Jangan pernah meremehkan kemampuan serangan siber. Berbagai negara sudah porak poranda akibat diserang secara DDOS oleh para peretas bayaran atau"</i>	Charles Liem, Peneliti Swiss-German University, Wawancara Keisuke Kamata, Pakar Siber, Pelatihan

	<i>komunitas bawah tanah.”</i>	CSIRT/CERT
	<i>“Setiap serangan siber pada level nasional biasanya dilatarbelakangi oleh motivasi tertentu.”</i>	Panarith, Pakar Siber, Webinar
3	<i>“Salah satu tujuan para hacker yang dibayar oleh negara atau pihak lain adalah membuat pertahanan dan keamanan negara lain menjadi lemah, agar berpengaruh terhadap kondisi riilnya. Negara penyerang biasanya yang memiliki kepentingan terhadap aksinya – dimana di belakang layar didukung oleh militer.”</i>	Bisyron Wahyudi, Mantan Manajer ID-SIRTII, Wawancara
	<i>“Alustsista moderen diperlengkapi dengan teknologi digital. Selain memberikan manfaat dan daya saing, mengandung risiko pula karena mudah diserang oleh pihak lain melalui penetrasi siber.”</i>	Hoga Saragih, Guru Besar Universitas Bakrie, Wawancara
	<i>“Sektor pertahanan adalah salah satu infrastruktur vital nasional yang harus dijaga keamanannya, agar tidak menjadi sasaran empuk para peretas.”</i>	Suaf Yanu, Komandan Satsiber TNI, RTD
4	<i>“Pemutakhiran doktrin berjalan sangat lambat. Situasi dan kondisi dapat membahayakan keselamatan bangsa dan negara. Jelas ancaman siber sangat terlihat nyata dapat membahayakan kedaulatan dan persatuan komponen bangsa dan negara. Oleh karena itu revisi terhadap doktrin agar sesuai dengan kemajuan jaman harus dilakukan segera.”</i>	Agus Widjojo, Gubernur Lemhannas, Wawancara
	<i>“Doktrin pertahanan negara harus disesuaikan dengan situasi dan kondisi ancaman masa kini.”</i>	Zainal Hasibuan, Anggota Wantiknas, RTD
	<i>“Setiap negara memiliki doktrin siber yang berbeda-beda, sesuai dengan aliran politik yang dimilikinya – bahkan Korea Utara berani mengatakan bahwa doktrin sibernya adalah melakukan penyerangan aktif ke berbagai negara besar dunia sebagai bentuk pertahanan.”</i>	Muhammad Salahuddien, Mantan Wakil Ketua ID-SIRTII, Wawancara

Sumber : Hasil Pengolahan Data Dampak Serangan Siber (disusun oleh peneliti)

Beraneka ragam jenis ancaman serangan siber sebagaimana dijelaskan sebelumnya memiliki tujuan akhir atau *ultimate goal* yang berbeda-beda. Hasil wawancara terhadap berbagai pakar di bidang pertahanan dan serangan siber menghasilkan kesimpulan mengenai berbagai tujuan yang relevan dengannya. Tabel berikut memperlihatkan target akhir dari serangan siber yang diluncurkan.

Tabel 4. 15 Ancaman dan Tujuan Serangan Siber pada Sektor Pertahanan

Jenis	Ancaman terhadap Sektor Pertahanan	Tujuan
1	Penyerangan terhadap infrastruktur vital/kritis nasional	Menghentikan operasional infrastruktur vital yang menguasai hajat hidup orang banyak seperti listrik, air, energi, transportasi, dsb.
2	Penyadapan sistem komunikasi dan koordinasi pertahanan	Mengetahui aktivitas dan kegiatan yang akan dilakukan berbagai pemangku kepentingan dalam kaitannya dengan pengelolaan pertahanan negara
3	Pengambilalihan kendali terhadap alutsista berbasis digital	Mengoperasikan dan mengontrol alutsista dari jarak jauh agar dapat melakukan aktivitas yang diinginkan tanpa dapat dicegah oleh pemiliknya
4	Penyabotan terhadap system pusat kendali (command center)	Membuat pusat kendali pertahanan dan militer tidak bekerja sebagaimana mestinya sehingga menghambat pemantauan, pengorganisasian, dan pengambilan keputusan strategis
5	Pencurian data dan informasi penting mengenai pertahanan negara	Mendapatkan data dan informasi rahasia mengenai pertahanan negara yang dapat dipergunakan sebagai referensi dalam melakukan berbagai kegiatan yang merugikan lawan
6	Pelumpuhan sistem informasi dan teknologi pada sektor pertahanan	Mengakibatkan tidak dapat dipergunakan atau terganggunya operasional sistem teknologi informasi yang berada dalam sector pertahanan
7	Penyesatan fakta melalui disinformasi dan misinformasi (propaganda)	Menyesatkan dan mengadu-domba berbagai pihak agar saling berseteru melalui penyebaran informasi yang salah atau bohong
8	Perusakan sistem dan fasilitas teknologi informasi pertahanan	Menghancurkan sumber daya komputasi (terutama perangkat keras, infrastruktur, jaringan, dan fasilitas sarana prasarana) secara fisik sehingga tidak dapat dipergunakan
9	Penyusupan ke dalam sistem dan fasilitas rahasia pertahanan negara	Menyamarkan identitas untuk dapat memperoleh akses terhadap berbagai situs, sistem, dan perimeter yang bersifat strategis dan bernilai tinggi.

Sumber : Ancaman dan Tujuan Serangan Siber pada Sektor Pertahanan (hasil pengolahan data oleh peneliti)

Jika tujuan akhir tersebut berhasil diraih, maka potensi gangguan yang akan terjadi terhadap negara yang diserang adalah sebagai berikut:

1. Lumpuhnya infrastruktur kritis atau vital yang menguasai hajat hidup orang banyak seperti jaringan listrik, air, transportasi, distribusi, perbankan/keuangan, dan lain-lain yang berpotensi mengakibatkan *chaos* dalam masyarakat;
2. Konflik horisontal secara masif antar komunitas masyarakat sebagai dampak keberhasilan adu domba yang dilakukan melalui berbagai propaganda berbasis disinformasi, misinformasi, dan malinformasi;
3. Terganggunya manajemen sistem pertahanan negara karena banyaknya sumber daya militer yang tidak terkendali dan pusat-pusat pertahanan negara yang malfungsi;
4. Rentannya terjadi serangan bertubi-tubi dari negara lain maupun dari musuh yang ada di dalam negeri akibat bocornya sejumlah informasi rahasia mengenai pertahanan negara; dan
5. Melemahnya situasi dan kondisi pertahanan negara karena begitu banyak aset dan sumber daya yang dimiliki telah berhasil diakses dan dikendalikan oleh musuh atau lawan negara.

Kelima situasi di atas tentu saja sangat membahayakan keselamatan, keutuhan, dan kedaulatan negara karena begitu besar dampaknya bagi masyarakat secara langsung. Keseluruhan gambaran situasi dan kondisi tersebut bukanlah merupakan sebuah suasana hipotetikal, namun sudah pernah menimpa sejumlah negara besar di dunia yang mengalami secara langsung

serangan siber. Berikut ini adalah sejumlah serangan yang pernah terjadi di berbagai negara yang dikumpulkan informasinya selama proses penelitian.

Paling tidak studi ini telah mencatat adanya 30 (tiga puluh) peristiwa penyerangan siber di masa lalu yang melibatkan dua atau lebih negara yang berseteru. Perlu diperhatikan bahwa tidak semua serangan dilakukan oleh negara, karena begitu banyaknya pihak-pihak independen *non-state actors* yang bergerak atas dasar motivasi beragam – baik berbasis politik, ekonomi, sosial, dan budaya. Beberapa serangan yang terjadi tidak saja memicu keresahan masyarakat dari negara yang terlibat, namun telah meningkatkan ketegangan antar sejumlah pihak. Menarik untuk dicermati bahwa serangan berbasis siber yang terjadi di masa lalu kebanyakan dipicu oleh situasi, kondisi, atau peristiwa yang terjadi di dunia fisik.

Tabel berikut ini memperlihatkan bagaimana masing-masing serangan dengan beragam modusnya memberikan dampak yang membahayakan keselamatan, keutuhan, dan kedaulatan negara. Mereka yang tidak siap mengantisipasi atau berhadapan dengan agenda lawan akan mengalami kerugian yang sangat besar – termasuk adanya potensi terjadinya kekacauan masal dan peperangan antar negara-negara yang berseteru atau terlibat. Sejumlah serangan yang berhasil diidentifikasi ini bahkan berlanjut menjadi perang siber yang baru usai setelah beberapa tahun. Bahkan ada beberapa *event* yang dampaknya masih terasa hingga saat ini karena *magnitude*-nya yang begitu besar dan masif.

Tabel 4. 16 Kasus Perang dan Serangan Siber antar Negara di Masa Lalu

No	Tahun	Penyerang	Target	Deskripsi	Dampak
1	2007	Rusia	Estonia	Serangan masif <i>botnet</i> yang menyerang berbagai institusi penting pemerintahan dan industri seperti parlemen, perbankan, kementerian, surat kabar/ penyiaran (media) – termasuk	Terjadinya <i>chaos</i> dan kerusuhan di seluruh negeri karena masyarakat tidak dapat membeli makanan karena jaringan teknologi perbankan tidak bekerja. Ketidaksiapan mereka

				melumpuhkan jaringan infrastruktur listrik.	menyimpan uang tunai berakibat pada penjarahan berbagai pusat-pusat perbelanjaan.
2	2003	China	Amerika	Peristiwa yang dinamakan Titan Rain ini adalah serangkaian serangan terkoordinasi pada sistem komputer di Amerika Serikat yang dimulai semenjak tahun 2003, dan berlangsung selama tiga tahun. Serangan disinyalir berasal dari dari Guangdong, Cina.	Peretas Titan Rain berhasil memperoleh akses ke banyak jaringan komputer kontraktor pertahanan Amerika Serikat, sehingga mereka berhasil mendapatkan informasi rahasia dan sensitif, termasuk data milik Lockheed Martin, Laboratorium Nasional Sandia, Gudang Senjata Redstone, dan NASA.
3	2017	Rusia	Ukraina Perancis Jerman Italia Polandia Rusia Inggris Amerika Australia	Serangkaian serangan dunia maya <i>malware</i> Petya yang terjadi pada tanggal 27 Juni 2017, dimana keberadaannya membanjiri situs web organisasi penting di Ukraina, seperti: bank, kementerian, surat kabar, dan perusahaan listrik. Penularan <i>malware</i> serupa dilaporkan pula oleh negara Perancis, Jerman, Italia, Polandia, Rusia, Inggris, Amerika Serikat, dan Australia .	Serangan berbasis <i>ransomware</i> ini berhasil menyandera sejumlah sistem teknologi informasi sehingga tidak dapat dipergunakan. Tercatat Ukraina dan Jerman adalah kedua negara yang paling terpukul dengan adanya serangan ini.
4	2018	Amerika	Rusia	The New York Times melaporkan bahwa peretas Amerika dari Komando Siber Amerika Serikat menanam <i>malware</i> yang berpotensi	Rusia mengalami gangguan sementara dalam memasok listriknya ke sejumlah lokasi akibat adanya serangan <i>malware</i> dimaksud.

				mengganggu jaringan listrik Rusia. Rusia pada Juni 2019 mengkalim bahwa telah ada penyerangan terhadap infrastruktur jaringan listriknya. Serangan ini merupakan balasan atas serangan Rusia ketika diselenggarakan Olimpiade Musim Dingin 2018 yang merugikan sejumlah bisnis Amerika.
5	2010	Amerika Israel	Iran	Sebuah virus komputer bernama Stuxnet sangat canggih yang awalnya dikira sebagai sebuah <i>worm</i> tersebut disinyalir “menyasar” fasilitas nuklir Iran. Penelitian lebih lanjut oleh Symantec Security yang lebih serius dan memperlihatkan bahwa ternyata serangan tersebut ditujukan untuk merusak sistem pengendali reaktor nuklir berbasis aplikasi SCADA (<i>Supervisory Control And Data Acquisition</i>). Virus ini dinilai sangat canggih sehingga diyakini dihasilkan oleh sebuah negara maju. PLTN Bushehr atau Natanz di Iran sempat mengalami kerusakan. Untung saja spesialis Iran berhasil mengentikan virus tersebut sebelum mendatangkan dampak yang lebih serius dan membahayakan kehidupan masyarakat. Secara hipotetikal dapat dibayangkan apabila sampai berhasil mengganggu proses PLTN dan terjadi kebocoran radio aktif, maka berpotensi terjadi perang antara Iran dengan negara yang diyakini melakukan penyerangan yaitu Amerika Serikat dan Israel.
6	2001	Amerika	Inggris	Gary McKinnon adalah seorang <i>hacker</i> asal Inggris yang dikenal berhasil melancarkan serangan terhadap komputer militer terbesar sepanjang Otoritas AS mengklaim bahwa peretas berhasil menghapus berkas elektronik atau <i>file</i> sangat penting serta berhasil mematikan atau melumpuhkan

				masa. McKinnon menyerbu 97 komputer milik NASA dan militer AS. Ia melakukannya selama 13 bulan antara Februari 2001 sampai Maret 20012 melalui rumah kekasihnya di London.	2,000 komputer milik militer selama 24 jam. McKinnon juga berhasil menyalin berbagai data penting dan <i>password</i> ke komputer pribadinya.
7	2012	Pejuang Siber Izz Ad-Din Al Qassam	Amerika	Operasi Ababil merupakan rangkaian serangan dunia maya yang dimulai pada tahun 2012. Serangan ini menyasar berbagai lembaga keuangan Amerika yang dilakukan oleh kelompok yang menamakan dirinya Pejuang Siber Izz Ad-Din Al Qassam (Qassam Cyber Fighters). Serangan berbasis <i>denial of services</i> ini merupakan pesan kritikan mereka terhadap Israel dan Amerika Serikat atas tanggapan terhadap video <i>Innocence of Muslim</i> yang dirilis oleh pendeta Amerika kontroversial, Terry Jones.	Serangan menargetkan agar Bursa Efek New York serta sejumlah bank termasuk JP Morgan Chase mengalami gangguan operasional. Hasil dari serangan tersebut adalah gangguan terbatas pada situs <i>web</i> yang ditargetkan.
8	2009	Korea Utara	AS Korsel	Serangkaian serangan dunia maya terkoordinasi selama Juni 2009 terhadap situs-situs utama pemerintah, media berita, dan situs web keuangan Korea Selatan dan Amerika Serikat. Serangan tersebut melibatkan	Sebagian besar komputer yang dibajak berada di Korea Selatan. Perkiraan jumlah komputer yang dibajak sangat bervariasi: sekitar 20,000 komputer menurut South Korea National Intelligence Service, 50,000

				aktivasi <i>botnet</i> yang diluncurkan untuk melumpuhkan server-server utama berbagai institusi tersebut.	menurut kelompok Respon Teknologi Keamanan Symantec, dan lebih dari 166,000 menurut seorang peneliti keamanan komputer Vietnam yang menganalisis <i>log files</i> dari dua server yang dikendalikan penyerang. Penyelidikan mengungkapkan bahwa setidaknya 39 situs <i>web</i> menjadi sasaran serangan berdasarkan <i>file</i> yang disimpan di sistem yang disusupi. Waktu serangan ditargetkan pada hari yang sama dengan uji coba rudal balistik jarak pendek Korea Utara.
9	2013	Singapura	James Raj Arokiasamy (India)	Merupakan serangan siber yang diprakarsai oleh organisasi peretas Anonymous yang dilakukan sebagian tanggapan atas peraturan sensor yang diberlakukan Singapura. Seorang anggota Anonymous yang dikenal dengan nama "The Messiah" mengaku bertanggung jawab sebagai ujung tombak serangan tersebut.	Sejumlah serangan secara paralel dan simultan diluncurkan, yaitu: 1. Serangan ke <i>web</i> Yayasan Komunitas Partai Aksi Rakyat diretas, yang diikuti serangan berikutnya terhadap situs web resmi Dewan Kota Ang Mo Kio . 2. Peretas mengunggah video berdurasi empat menit di YouTube, dimana yang bersangkutan mengenakan topeng Guy Fawkes, mengancam akan "meruntuhkan

infrastruktur utama di Singapura".

3. Reporter berita The Straits Times Irene Tham yang mengkritik video terkait diubah konten artikelnya sehingga menimbulkan kegemparan setempat.

4. Pada 3 November, situs *web* Bandara Seletar juga diretas. Halaman mukanya diganti dengan latar belakang hitam dan hijau dengan gambar di tengahnya yang menyerupai tengkorak berkerudung.

5. Pada 5 November, akun Twitter dan YouTube penghibur Singapura Ridhwan Azman diretas pula, dan disebarkan berita yang memicu protes masyarakat.

6. Dua hari kemudian, para peretas merusak sub-halaman di situs *web* Perdana Menteri Singapura Lee Hsien Loong, dan juga konten pada *website* istana.

10	2018	Korea Utara	Amerika Inggris Meksiko	Tiga <i>programmer</i> Korea Utara karena melakukan peretasan untuk mencuri uang senilai 1,3 miliar dolar	Departemen Kehakiman AS mengatakan, para peretas bertanggung jawab atas berbagai

Asia AS dan *cryptocurrency*. aktivitas kriminal dan gangguan profil serius, Mereka adalah Jon termasuk serangan Chang-hyok (31 tahun), terhadap Sony Pictures Kim Il (27 tahun), dan Entertainment pada Park Jin-hyok (36 tahun). Aktivitas 2014. Kelompok itu pembobolan dilakukan diduga menargetkan saat ketiganya bekerja staf AMC Theatres dan di dinas intelijen Korea membobol komputer Utara. milik Mammoth Screen, yaitu perusahaan film Inggris yang sedang mengerjakan serial drama tentang Korut. Departemen Kehakiman AS juga menuduh ketiganya berpartisipasi dalam pembuatan *ransomware* WannaCry 2.0 yang menyerang Layanan Kesehatan Nasional Inggris ketika diluncurkan pada 2017. Surat dakwaan menyatakan, para peretas turut membobol bank di Asia Selatan, Asia Tenggara, Meksiko, dan Afrika. Mereka melakukan peretasan dengan menembus jaringan lembaga keuangan dan menyalahgunakan protokol SWIFT untuk mencuri uang. Mereka juga diduga telah menyebarkan aplikasi destruktif dari Maret 2018 hingga September 2020 untuk menargetkan pengguna mata uang kripto.

11	2020	China	Taiwan	Taiwan mengatakan kelompok peretas yang terkait dengan Pemerintah China telah melakukan serangan siber terhadap 10 lembaga negara. Kelompok peretas itu juga menyerang 6,000 akun e-mail pejabat pemerintah dalam upaya infiltrasi untuk mencuri data yang penting.	Infiltrasi tersebut melibatkan mulai dari kampanye media yang didukung Beijing hingga serangan dunia maya. Kelompok peretas China telah menyusup ke lembaga pemerintah dan menyadap sejumlah informasi untuk waktu yang lama. Kelompok peretas tersebut bertujuan untuk mendapatkan dokumen dan data penting pemerintah. Kantor Investigasi Keamanan Siber Biro Investigasi Taiwan mengatakan serang siber tersebut dimulai pada awal 2018. Kantor tersebut menambahkan pihaknya belum dapat mengidentifikasi data apa yang berhasil dicuri karena para peretas menyembunyikan jejak mereka. Setidaknya ada empat perusahaan teknologi yang memberikan layanan informasi kepada pemerintah yang dilaporkan diserang dan disusupi oleh dua kelompok peretas tersebut. Kantor Urusan Taiwan China tidak menanggapi permintaan komentar.
12	2013	China	Jerman	Pada 2013, Jerman membentuk unit khusus Operasi Jaringan Komputer	Para penyerang berusaha untuk mengakses data dan menyatakan

				yang bekerjasama dengan Badan intelijen Jerman (BND). Unit ini mempekerjakan 130 peretas yang bemarkas di stasiun pertahanan siber baru . Pada Maret 2013, presiden BND Gerhard Schindler mengumumkan bahwa agensinya telah mengamati hingga lima serangan sehari terhadap otoritas pemerintah yang sebagian besar diperkirakan berasal dari China.	ancamannya bahwa informasi yang dicuri dapat digunakan sebagai modal meluncurkan serangan sabotase di masa depan yang ditargetkan terhadap produsen senjata, perusahaan telekomunikasi, serta badan pemerintah dan militer.
13	1982	Amerika	Uni Soviet	Bom logika ditanamkan Amerika Serikat di instalasi pompa dan pipa minyak Uni Soviet yang menyebabkan kerusakan akibat serangan pada modul pengendali kecepatan pompa dan pengaturan katup.	Kerusakan pada pompa dan pipa minyak berpengaruh terhadap pasokan minyak Uni Soviet yang terganggu, sehingga terjadinya kerugian finansial yang sangat besar.
14	1991	Amerika	Iraq	Serangan udara Amerika Serikat terhadap sistem komando dan kontrol Irak yang berfungsi mengendalikan sistem telekomunikasi dan infrastruktur nasional – dengan didukung oleh teknologi komunikasi dan sistem satelit.	Lumpuhnya sistem puskodal tentara dan pemerintahan Irak yang menyebabkan kehancuran di mana-mana.
15	2002	Rusia	Chechnya	Sistem Keamanan Rusia merobohkan dua situs <i>web</i> Chechnya yang di-<i>hosting</i> di	Ketegangan antara Rusia, Amerika, dan Chechnya akibat terjadinya insiden yang dianggap melibatkan

				Amerika Serikat.	ketiga negara.
16	2008	Russian Nationalist Hackers	Lithuania	Ratusan peretas Rusia merusak situs <i>web</i> pemerintah Lithuania maupun perusahaan-perusahaan besar yang dimilikinya.	Terjadi keresahan pada masyarakat Lithuania yang berpotensi menimbulkan kerusuhan akibat menyebarnya aktivitas disinformasi.
17	2008	Rusia Lithuania	Georgia	Serangan siber langsung dikoordinasikan dengan menggunakan <i>botnet</i> menyerang sejumlah media utama di Georgia. Serangan DDoS dilakukan serempak dengan peretasan dengan menggunakan metoda SQL Injection dan Cross Sites Scripting (XSS).	Terganggunya <i>web</i> pemerintah, aplikasi keuangan, sistem pada institusi pendidikan, dan beragam teknologi informasi yang dipergunakan bisnis media berita (termasuk BBC dan CNN).
18	2009	Rusia	Kyrgyzstan	Serangan DDoS berfokus pada tiga dari empat Penyedia Layanan Internet (ISP) terbesar di Kirgizstan.	Terganggunya semua lalu lintas internet sehingga pemerintah dan masyarakat tidak dapat berkomunikasi dan berinteraksi.
19	2014	Rusia	Ukraina	Serangan DDoS Rusia terhadap Ukraina ini memiliki <i>magnitude</i> 32 kali lebih besar dari serangan terbesar yang pernah terjadi di masa lalu, ketika pasukan pro-Rusia bersenjata Rusia menguasai Krimea.	Serangan ini berusaha untuk menjatuhkan sistem komisi pemilihan umum Ukraina dan teknologi cadangannya. Serangan itu merupakan upaya untuk menciptakan kekacauan dan membantu kandidat yang pro-Rusia.
20	2015	Rusia	Jerman	Penyelidik Jerman menemukan bahwa peretas telah menyusup ke jaringan	Sebagian informasi penting dan rahasia tentang cara kerja Bundestag, para

				komputer Bundestag Jerman. Dinas intelijen domestik Jerman mengatakan bahwa serangan itu dilakukan oleh Rusia.	pemimpin Jerman, NATO, dan lainnya – berhasil dicuri.
21	2015	China	Amerika	Peretas China mencuri sejumlah data mengenai para pelamar pekerjaan untuk menjadi pegawai negeri Amerika Serikat yang gagal direkrut.	Sebanyak 21,5 juta catatan karyawan dan pelamar yang tidak berhasil diterima pemerintah Amerika Serikat dicuri dari Kantor Manajemen Personal AS.
22	2016	Russia	Ukraina	Desember 2016, pemadaman listrik kedua yang disebabkan oleh Rusia di Ukraina: Diperkirakan bahwa peretas Rusia bersembunyi di jaringan pemasok listrik tanpa terdeteksi selama enam bulan sebelum mematikan listrik.	Pemadaman listrik berjumlah sekitar seperlima dari konsumsi daya Kiev malam itu yang hilang. Serangan ini terjadi hampir satu tahun hingga tanggal serangan dunia maya pada Desember 2015 yang memutus aliran listrik ke 225.000 orang di Ukraina bagian barat.
23	1982	Amerika	Uni Soviet	Ditanamkannya <i>malware</i> komputer berbasis Trojan Horse dalam perangkat lunak bajakan Kanada yang dilakukan oleh Central Intelligence Agency (CIA). <i>Malware</i> tersebut menyebabkan sistem SCADA yang menjalankan <i>pipeline</i> tidak berfungsi. "Farewell Dossier" memberikan informasi tentang serangan ini, dan menulis bahwa <i>chip</i> komputer yang	Ketika Rusia masih menjadi bagian dari Uni Soviet pada tahun 1982, sebagian dari pipa Trans-Siberia di dalam wilayahnya meledak. Peristiwa ini dianggap sebagai ledakan non-nuklir paling monumental yang apinya dapat dilihat dari luar angkasa.

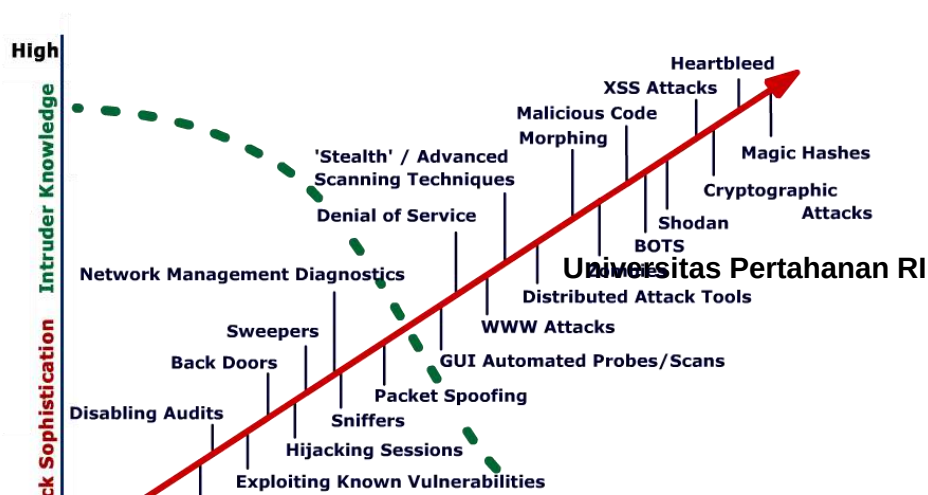
				dikompromikan akan menjadi bagian dari peralatan militer Soviet.	
24	2020	Korea Utara	Korea Selatan	Grup peretasan Korea Utara secara bersama-sama meluncurkan serangan berantai terhadap sejumlah lunak sistem keamanan Korea Selatan.	Sistem perangkat lunak keamanan yang dimiliki Korea Selatan dicoba untuk diambil alih agar Korea Utara dapat masuk mengakses seluruh situs-situs penting pemerintahan.
25	2020	China	Amerika	Pejabat AS melaporkan adanya lonjakan serangan oleh peretas China terhadap penyedia layanan kesehatan, produsen farmasi, Departemen Kesehatan, dan Layanan Kemanusiaan AS di tengah pandemi Covid-19.	Dicurigai adanya usaha untuk meretas sistem yang berisi data mengenai usaha Amerika dalam mengembangkan vaksin Covid-19.
26	2015	Rusia	Perancis	Layanan media penyiaran Perancis yang berbasis di Paris diserang oleh peretas yang menggunakan perangkat lunak berbahaya untuk menyerang dan menghancurkan sistem jaringan dan mematikan semua dua belas salurannya dari udara.	Situs kampanye Emmanuel diretas. Kabar tentang kebocoran tersebut menyebar dengan cepat melalui Internet karena difasilitasi oleh <i>botnet</i> dan akun <i>spam</i> . Pelanggaran tersebut telah menyebabkan sebagian besar sistem penyedia teknologi informasi, terutama penyedia <i>web hosting</i> , tidak berfungsi. Rusia membantah berada di balik serangan dunia maya. Centreon mengatakan dalam sebuah pernyataan bahwa mereka "telah mencatat informasinya," dan

					telah terbukti secara tidak sah melibatkan versi komersial dari perangkat lunak Centeron.
27	2009	Russia	Korea Selatan	Menurut dua pejabat intelijen Amerika Serikat yang berbicara dengan The Washington Post dan juga temuan analisis keamanan siber Michael Matonis, Rusia berada di balik serangan dunia maya terhadap Olimpiade Musim Dingin 2018 di Korea Selatan. <i>Worm</i> yang bertanggung jawab atas serangan <i>cyber</i> ini dikenal sebagai "Perusak Olimpiade".	<i>Worm</i> tersebut menargetkan semua infrastruktur teknologi informasi Olimpiade, dan berhasil mematikan WiFi, sistem tiket, dan sistem teknologi Olimpiade lainnya.
28	2019	Rusia	Polandia	Kampanye disinformasi pro-Rusia selama tiga tahun di Facebook dengan penonton 4,5 juta orang Polandia ditemukan pada awal 2019 oleh OKO Press dan Avaaz. Kampanye tersebut menerbitkan berita palsu dan mendukung tiga politisi pro-Rusia Polandia dan situs <i>web</i> mereka.	Propaganda ini diluncurkan untuk mengadu domba rakyat Polandia agar saling menyerang satu dan lainnya.
29	2013	China	Australia	Pada Mei 2013, ABC News mengklaim bahwa China mencuri cetak biru markas besar Organisasi Intelijen Keamanan Australia.	Dokumen penting, strategis, dan rahasia negara ini bocor ke tangan musuh – sehingga membahayakan pertahanan negara Australia.

30	2010	India	Pakistan	Pada 26 November 2010, sebuah kelompok yang menamakan dirinya Tentara Siber India meretas situs <i>web</i> milik Angkatan Darat Pakistan dan yang lainnya - termasuk milik Kementerian Luar Negeri, Kementerian Pendidikan, Kementerian Keuangan, Biro Komputer Pakistan, Dewan Ideologi Islam, dan lain-lain. Serangan itu dilakukan sebagai balas dendam atas serangan teroris Mumbai .	Rusaknya berbagai situs militer, pertahanan, dan pemerintahan Pakistan sehingga mendatangkan kekacauan birokrasi yang mencoreng muka para pimpinan politik.

Sumber : Kasus Perang dan Serangan Siber antar Negara di Masa Lalu (hasil pengolahan data oleh peneliti)

Sejalan dengan perkembangan teknologi, tren jenis dan modus serangan siber pun berevolusi secara sangat cepat. Jenis kejahatan paling kuno adalah “menebak *password*” yang kemudian diikuti dengan sederetan modus serangan berbasis komputer maupun siber. Serangan ini semakin lama semakin kompleks, karena selain melibatkan skenario canggih, para peretas menggunakan sumber daya komputasi berteknologi tinggi.



Gambar 4. 5 Evolusi dan Kompleksitas Jenis Serangan Siber

Sumber : Evolusi dan Kompleksitas Jenis Serangan Siber (James, 2005)

ENISA (The European Union Agency for Cybersecurity) pada laporan terakhirnya di penghujung tahun 2020 mendeteksi dan menganalisa adanya 15 (lima belas) jenis serangan yang paling banyak mengemuka di dunia – dan akan tetap bertahan dalam lima tahun ke depan. Kelimabelas serangan tersebut adalah sebagai berikut:

1. Malware: penanaman virus atau peluncuran *software* dengan intensi jahat ke dalam sistem komputer dengan berbagai tujuan untuk merusak atau merugikan pihak yang diserang (Aslan & Samet, 2020; Kalash et al., 2018);
2. Web-Based Attacks: penyerangan ke dalam sistem yang dibangun berbasis internet yang berjalan di atas protokol web dengan berbagai variasi penetrasinya (Kruegel et al., 2005; Kruegel & Vigna, 2003; Tekerek, 2021);

3. Phishing: pengelabuan pihak lawan dengan berbagai cara agar terjerembab ke dalam jebakan digital yang telah disiapkan sebelumnya (Alabdan, 2020; Williams et al., 2018; Williams & Joinson, 2020);
4. Web Application Attacks: penyerangan secara khusus yang ditujukan kepada beraneka-ragam aplikasi yang berjalan di atas protokol *web* (Al-Khurafi & Al-Ahmad, 2016; Tekerek, 2021);
5. Spam: pengiriman berbagai sampah elektronik secara masif ke berbagai tempat untuk mendapatkan perhatian khusus bagi calon korban sehingga mereka terlena dengan pesan yang dikirimkan (Dada et al., 2019; Hussain et al., 2019);
6. DDoS: pelumpuhan sistem melalui pengiriman paket digital dengan frekuensi dan volume tinggi ke dalam satu fokus target yang biasanya merupakan pusat komputasi atau *server* utama (Bawany et al., 2017; Polat et al., 2020; Zargar et al., 2013);
7. Identity Theft: pencurian identitas rahasia yang menjadi dasar kunci akses rahasia kepada aset dan sumber daya penting dalam lingkungan sistem teknologi informasi (Gupta & Kumar, 2020; Irshad & Soomro, 2018);
8. Data Breach: pelanggaran pemberian data secara sengaja maupun tak sengaja karena adanya aktivitas yang dilakukan oleh peretas dengan tujuan mengalirkannya ke pihak-pihak atau sumber yang berbahaya (Edwards et al., 2016; Juma'h & Alnsour, 2020);
9. Insider Threat: penyusupan individu melalui akses rahasia ke dalam sistem musuh sehingga dapat melakukan kerusakan dari dalam (internal) (Homoliak et al., 2018; Liu et al., 2018);
10. Botnets: penggunaan jejaring ribuan bahkan jutaan robot *software* di seluruh titik internet yang dipersiapkan untuk menjalankan

perintah serangan secara terkoordinasi (Alieyan et al., 2017; Hoang & Nguyen, 2018);

11. Physical Manipulation, Damage, Theft, and Loss: pencurian, pelumpuhan, manipulasi, dan kerusakan secara fisik terhadap aset dan sumber daya penting yang berada di sekitar perimeter sistem informasi (Hutter, 2019; S. Lee, 2020);
12. Information Leakage: pembocoran informasi secara sengaja oleh peretas untuk diperjualbelikan atau membuat huru-hara karena sifatnya yang rahasia dan sensitif (Issa et al., 2020; Wong et al., 2019);
13. Ransomware: penyanderaan sistem aplikasi dan teknologi oleh penyerang dengan tujuan adanya balas jasa finansial untuk membebaskannya agar kembali berjalan normal (Hull et al., 2019; Paquet-Clouston et al., 2019);
14. Cyberespionage: pemantauan dan penyadapan digital selayaknya aktivitas mata-mata berbasis intelijen untuk mengetahui kekuatan lawan (Aucsmith, 2017; Banks, 2017); dan
15. Cryptojacking: pengambilalihan aset finansial digital dari berbagai tempat untuk memperkaya diri (Carlin et al., 2020; Tuttle, 2018).

Sejumlah pertanyaan mengemuka terkait dengan posisi serangan *social engineering* dalam konteks kelimabelas modus yang dihasilkan oleh ENISA. Dalam penjelasannya dikatakan bahwa mayoritas dari seluruh jenis serangan dimaksud selalu melibatkan aktivitas *social engineering* dalam prosesnya. Menurut definisi, “*social engineering*” adalah suatu teknik ‘pencurian’ atau pengambilan data atau informasi penting/krusial/rahasia dari seseorang dengan cara menggunakan pendekatan manusiawi melalui mekanisme interaksi sosial - ringkasnya memanipulasi manusia melalui pendekatan sosial. Atau dengan kata lain *social engineering* adalah suatu teknik memperoleh data/informasi rahasia dengan cara mengeksploitasi kelemahan manusia.

Serangan ini sangat sulit diantisipasi karena “menyerang” kelemahan dan/atau manusia yang memiliki naluri dan karakteristik sebagai makhluk sosial, yang cenderung memiliki :

1. Rasa Takut – jika seorang pegawai atau karyawan dimintai data atau informasi dari atasannya, polisi, atau penegak hukum yang lain, biasanya yang bersangkutan akan langsung memberikan tanpa merasa sungkan;
2. Rasa Percaya – jika seorang individu dimintai data atau informasi dari teman baik, rekan sejawat, sanak saudara, atau sekretaris, biasanya yang bersangkutan akan langsung memberikannya tanpa harus merasa curiga; dan
3. Rasa Ingin Menolong – jika seseorang dimintai data atau informasi dari orang yang sedang tertimpa musibah, dalam kesedihan yang mendalam, menjadi korban bencana, atau berada dalam duka, biasanya yang bersangkutan akan langsung memberikan data atau informasi yang diinginkan tanpa bertanya lebih dahulu.

Ketiga contoh hal tersebut menjadi episentrum atau pusat utama eksploitasi kerawanan manusia karena melekat pada sifat sosial seorang individu dan insan sosial. Apalagi di dalam konteks kultur manusia Indonesia yang bersifat sosial-kolektif, dimana kerjasama dan hubungan antar pribadi relatif dekat karena diikat oleh berbagai pertalian persaudaraan seperti: suku, golongan, agama, almamater, komunitas, organisasi, dan lain sebagainya.

Pada dasarnya teknik *social engineering* dapat dibagi menjadi dua jenis, yaitu: berbasis interaksi sosial dan berbasis interaksi komputer. Berikut adalah sejumlah teknik *social engineering* yang biasa dipergunakan oleh kriminal, musuh, penjahat, penipu, atau mereka yang memiliki intensi tidak baik. Setelah mengetahui isu *social engineering* di atas, timbul pertanyaan mengenai bagaimana cara menghindarinya. Berdasarkan sejumlah pengalaman, berikut adalah hal-hal yang biasa disarankan kepada mereka yang merupakan pemangku kepentingan aset-aset informasi penting perusahaan, yaitu:

1. Selalu hati-hati dan mawas diri dalam melakukan interaksi di dunia nyata maupun di dunia maya. Tidak ada salahnya perilaku “ekstra hati-hati” diterapkan di sini mengingat informasi merupakan aset sangat berharga yang dimiliki oleh organisasi atau perusahaan;
2. Organisasi atau perusahaan mengeluarkan sebuah buku saku berisi panduan mengamankan informasi yang mudah dimengerti dan diterapkan oleh pegawainya, untuk mengurangi insiden-insiden yang tidak diinginkan;
3. Belajar dari buku, seminar, televisi, internet, maupun pengalaman orang lain agar terhindar dari berbagai penipuan dengan menggunakan modus *social engineering*;
4. Pelatihan dan sosialisasi dari perusahaan ke karyawan dan unit-unit terkait mengenai pentingnya mengelola keamanan informasi melalui berbagai cara dan kiat;
5. Memasukkan unsur-unsur keamanan informasi dalam standar prosedur operasional sehari-hari – misalnya “*clear table and monitor policy*” - untuk memastikan semua pegawai melaksanakannya; dan lain sebagainya.

Selain usaha yang dilakukan individu tersebut, perusahaan atau organisasi yang bersangkutan perlu pula melakukan sejumlah usaha, seperti:

1. Melakukan analisa kerawanan sistem keamanan informasi yang ada di perusahaannya (baca: *vulnerability analysis*);
2. Mencoba melakukan uji coba ketangguhan keamanan dengan cara melakukan “*penetration test*”;
3. Mengembangkan kebijakan, peraturan, prosedur, proses, mekanisme, dan standar yang harus dipatuhi seluruh pemangku kepentingan dalam wilayah organisasi;

4. Menjalin kerjasama dengan pihak ketiga seperti vendor, ahli keamanan informasi, institusi penanganan insiden, dan lain sebagainya untuk menyelenggarakan berbagai program dan aktivitas bersama yang mempromosikan kebiasaan peduli pada keamanan informasi;
5. Membuat standar klasifikasi aset informasi berdasarkan tingkat kerahasiaan dan nilainya;
6. Melakukan audit secara berkala dan berkesinambungan terhadap infrastruktur dan suprastruktur perusahaan dalam menjalankan keamanan informasi; dan lain sebagainya.

Tabel berikut ini memperlihatkan bagaimana hubungan antara kelimabelas jenis serangan dengan ancaman yang berpotensi terjadi. Pemetaan ini didasarkan pada kajian terhadap serangan yang selama ini terjadi dan mengancam keselamatan masyarakat maupun kedaulatan negara

Tabel 4. 17 Pemetaan Jenis Serangan terhadap Modus Serangan

No	Nama Jenis Ancaman/Serangan berdasarkan Terminologi dan Hasil Penelitian ENISA dan Potensi Dampaknya	1. Perusakan terhadap infrastruktur vital/risiko nasional	2. Penyusutan data: kompromi dan kerahasiaan pertahanan	3. Pengambilalihan kendali terhadap sistem digital	4. Perusakan terhadap sistem kendali (control center)	5. Perusakan data dan informasi penting mengenai pertahanan negara	6. Perusakan sistem informasi dan teknologi pada aspek pertahanan	7. Perusakan data penting, dokumen, dan komunikasi strategis	8. Perusakan sistem dan fasilitas teknologi informasi pertahanan	9. Perusakan sistem dan fasilitas pertahanan negara
1	Malware									
2	Web-based attacks									
3	Phishing									
4	Web application attacks									
5	Spam									
6	DDoS									
7	Identity theft									
8	Data breach									
9	Insider threat									
10	Botnets									
11	Physical manipulation, damage, theft and loss									
12	Information leakage									
13	Ransomware									
14	Cyberespionage									
15	Cryptjacking									

Sumber : Pemetaan Jenis Serangan terhadap Modus Serangan (hasil pengolahan data oleh peneliti)

Berbasis pada kelimabelas tren serangan tersebut, dilakukanlah analisa risiko dengan menggunakan pendekatan *risk matrix*. Matrik risiko ini

memetakan risiko ancaman siber berdasarkan dua hal utama, yaitu: (i) probabilitas terjadinya serangan; dan (ii) dampak kerusakan yang dihasilkan (Lyu et al., 2019; Sen & Borle, 2015). Kedua hal tersebut berhubungan secara langsung dalam tabel terkait yang telah dijelaskan sebelumnya. Untuk melakukan pemetaan ini, dilibatkan lima orang pakar keamanan siber yang memiliki pengetahuan relatif detil terhadap situasi dan kondisi keamanan informasi dalam lingkungan Kementerian Pertahanan dan militer di Indonesia. Dikatakan berpengalaman karena selain mereka pernah terlibat dalam sejumlah program atau proyek pengembangan sistem pertahanan keamanan, para profesional ini juga memiliki latar belakang dan jam terbang tinggi dalam bidang *cyber security* di bidang pertahanan dan militer. Mereka berasal dari beranekaragam latar belakang, seperti akademisi, praktisi, dan peneliti.



		SEVERITY →		
		1	2	3
LIKELIHOOD ↓	1	LOW - 1 -	LOW - 2 -	MEDIUM - 3 -
	2	LOW - 2 -	MEDIUM - 4 -	HIGH - 6 -
	3	MEDIUM - 3 -	HIGH - 6 -	HIGH - 9 -

Gambar 4. 6 Matrik Asesmen Risiko

Sumber : Matrik Asesmen Risiko (Lyu et al., 2019; Sen & Borle, 2015)

Pada penelitian ini masing-masing pakar individu melakukan pemetaan terhadap kemungkinan terjadinya kelima belas tren serangan tersebut ke situs-situs militer dan pertahanan Indonesia di masa mendatang (aspek *likelihood*). Dan terhadap masing-masing jenis ancaman serangan tersebut, diperkirakan dampak kehancurannya (aspek *severity*). Aspek *likelihood* dapat dinilai dengan cara melihat catatan sejarah terkait dengan berbagai jenis serangan yang terjadi di dunia, terutama pernah menimpa berbagai institusi atau sektor di Indonesia. Probabilitas ini juga dapat dilihat dari persepsi terhadap tingkat kerawanan atau *vulnerabilities* sistem informasi dan teknologi yang dimiliki berbagai institusi di tanah air. Sementara aspek dampak dapat diperkirakan dengan melihat bagaimana konteks keberhasilan penyerangan berpotensi merugikan masyarakat, bangsa dan negara – terutama dalam sektor pertahanan yang bertumpu pada keutuhan dan kedaulatan NKRI. Tabel 4.18 berikut ini memperlihatkan hasil pemetaan para pakar ke dalam matrik asesmen risiko dimaksud.

Tabel 4. 18 Hasil Pemetaan Risiko Pakar Pertahanan Siber

PAKAR #1: MUHAMMAD SALAHUDDIN

No	The Threats/Events	MINISTRY OF DEFENSE						MILITARY (ARMY, NAVY, AIR FORCE)					
		Probability of Occurrence			The Level of Impacts (Damages) in Case of the Event Occurred			Probability of Occurrence			The Level of Impacts (Damages) in Case of the Event Occurred		
		Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
1	Malware			1			1			1			1
2	Web-Based Attacks		1		1			1			1		
3	Phishing		1			1			1			1	
4	Web Application Attacks		1		1			1			1		
5	SPAM		1		1			1			1		
6	Distributed Denial of Services			1			1			1			1
7	Identify Theft			1			1			1			1
8	Data Breach			1			1			1			1
9	Insider Threat			1			1			1			1
10	Botnets	1			1			1			1		
11	Physical Manipulation, Damage, Theft, and Loss	1			1			1			1		
12	Information Leakage		1										
13	Ransomware			1			1			1			1
14	Cyber Espionage			1			1			1			1
15	Cryptotacking			1			1			1			1

PAKAR #2: DUJDI

No	The Threats/Events	MINISTRY OF DEFENSE						MILITARY (ARMY, NAVY, AIR FORCE)					
		Probability of Occurrence			The Level of Impacts (Damages)			Probability of Occurrence			The Level of Impacts (Damages) in		
		Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
1	Malware			1			1			1			1
2	Web-Based Attacks			1		1				1		1	
3	Phishing		1			1			1			1	
4	Web Application Attacks			1		1			1			1	
5	SPAM		1		1				1		1		
6	Distributed Denial of Services			1			1			1			1
7	Identify Theft			1			1			1			1
8	Data Breach			1			1			1			1
9	Insider Threat			1			1			1			1
10	Botnets	1			1			1			1		
11	Physical Manipulation, Damage, Theft, and Loss	1			1			1			1		
12	Information Leakage			1			1			1			1
13	Ransomware			1			1			1			1
14	Cyber Espionage			1			1			1			1
15	Cryptotacking			1			1			1			1

PAKAR #3: RUDIANTO

No	The Threats/Events	MINISTRY OF DEFENSE						MILITARY (ARMY, NAVY, AIR FORCE)					
		Probability of Occurrence			The Level of Impacts (Damages)			Probability of Occurrence			The Level of Impacts (Damages) in		
		Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
1	Malware			1			1			1			1
2	Web-Based Attacks			1			1			1			1
3	Phishing		1			1			1			1	
4	Web Application Attacks			1		1			1			1	
5	SPAM		1		1				1		1		
6	Distributed Denial of Services			1			1			1			1
7	Identify Theft			1			1			1			1
8	Data Breach			1			1			1			1
9	Insider Threat			1			1			1			1
10	Botnets	1			1			1			1		
11	Physical Manipulation, Damage, Theft, and Loss	1			1			1			1		
12	Information Leakage		1						1				
13	Ransomware			1			1			1			1
14	Cyber Espionage		1			1			1			1	
15	Cryptotacking		1			1			1			1	

PAKAR #4: BISYRON

No	The Threats/Events	MINISTRY OF DEFENSE						MILITARY (ARMY, NAVY, AIR FORCE)					
		Probability of Occurrence			The Level of Impacts (Damages)			Probability of Occurrence			The Level of Impacts (Damages) in		
		Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
1	Malware			1		1				1		1	
2	Web-Based Attacks			1	1					1	1		
3	Phishing		1		1				1		1		
4	Web Application Attacks			1		1				1		1	
5	SPAM			1	1					1	1		
6	Distributed Denial of Services			1		1				1		1	
7	Identify Theft			1			1			1			1
8	Data Breach			1			1			1			1
9	Insider Threat		1			1			1			1	
10	Botnets			1		1				1			1
11	Physical Manipulation, Damage, Theft, and Loss		1			1		1				1	
12	Information Leakage			1			1			1			1
13	Ransomware	1				1			1			1	
14	Cyber Espionage		1			1			1			1	
15	Cryptotacking	1				1			1			1	

PAKAR #5: CHARLES LIM

No	The Threats/Events	MINISTRY OF DEFENSE						MILITARY (ARMY, NAVY, AIR FORCE)					
		Probability of Occurrence			The Level of Impacts (Damages)			Probability of Occurrence			The Level of Impacts (Damages) in		
		Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
1	Malware			1			1			1			1
2	Web-Based Attacks			1		1				1		1	
3	Phishing			1		1				1			1
4	Web Application Attacks			1		1				1			1
5	SPAM		1			1				1			1
6	Distributed Denial of Services		1			1			1			1	
7	Identify Theft			1			1			1			1
8	Data Breach			1			1			1			1
9	Insider Threat			1		1			1			1	
10	Botnets		1			1			1			1	
11	Physical Manipulation, Damage, Theft, and Loss		1			1			1			1	

Sumber : Hasil Pemetaan Risiko Pakar Pertahanan Siber (hasil olahan data oleh peneliti)

Berdasarkan hasil pemetaan yang telah dilakukan para pakar, dilakukanlah proses pengolahan data sebagai berikut.

1. Penetapan Prioritas: berdasarkan matrik asesmen risiko yang dipergunakan, ditetapkanlah urutan prioritas berdasarkan tingkat kepentingan dan urgensi sebagai berikut (i) Prioritas I adalah yang *likelihood*-nya H dan *severity*-nya H; (ii) Prioritas II adalah *likelihood* M dan *severity* H; (iii) Prioritas III adalah *likelihood* H dan *severity* M; (iv) Prioritas IV adalah *likelihood* M dan *severity* M; dan (v) Prioritas V adalah *likelihood* L dan *severity* H. Angka “1” diberikan pada masing-masing hasil pemetaan.
2. Penghitungan Nilai Parsial: dilakukan penjumlahan nilai masing-masing pakar terhadap setiap lembaga (Kementerian Pertahanan dan Militer) berdasarkan masing-masing kelompok prioritas. Nilai total parsial ini sangat penting untuk dapat melihat ancaman mana saja yang perlu untuk diperhatikan karena tingkat kepentingan dan kegentingannya.
3. Penghitungan Nilai Total: merupakan penggabungan dari seluruh hasil pemetaan pakar terhadap setiap ancaman. Nilai agregat ini

akan memperlihatkan ancaman mana saja yang disepakati penting untuk diprioritaskan penanganannya.

4. Pemilihan Aspek Ancaman: dilakukan pemilihan terhadap sejumlah ancaman yang paling perlu untuk diperhatikan dalam jangka pendek. Nilai total akhir per ancaman menjadi indikator dalam menentukan mana saja yang dianggap penting untuk didahulukan.

Tabel 4. 19 Hasil Konversi Skor Asesmen Risiko

PRIORITY 1		PRIORITY 2		PRIORITY 3		PRIORITY 4		PRIORITY 5		SCORE	
MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL
2	2	1	1	1	1	0	0	1	1	5	5
0	0	1	0	0	0	1	0	0	1	2	1
0	0	1	1	1	1	2	2	0	0	4	4
0	0	1	0	0	0	1	0	0	1	2	1
0	0	1	0	0	0	1	0	0	1	2	1
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
0	0	0	0	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1
0	0	1	0	0	0	1	0	0	0	2	0
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5

PRIORITY 1		PRIORITY 2		PRIORITY 3		PRIORITY 4		PRIORITY 5		SCORE	
MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL
2	2	1	1	1	1	0	0	1	1	5	5
1	1	0	0	2	2	1	1	0	0	4	4
0	0	1	1	1	1	2	2	0	0	4	4
1	1	0	0	2	2	1	1	0	0	4	4
0	0	1	1	0	0	1	1	0	1	2	3
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
0	0	0	0	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5

PRIORITY 1		PRIORITY 2		PRIORITY 3		PRIORITY 4		PRIORITY 5		SCORE	
MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
0	0	1	1	1	1	2	2	0	0	4	4
2	2	1	1	1	1	0	0	1	1	5	5
0	0	1	1	0	0	1	1	0	1	2	3
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
2	2	1	1	1	1	0	0	1	1	5	5
0	0	0	0	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	2	2
2	2	1	1	1	1	0	0	1	1	5	5
0	0	1	1	1	1	2	2	0	0	4	4
0	0	1	1	1	1	2	2	0	0	4	4

PRIORITY 1		PRIORITY 2		PRIORITY 3		PRIORITY 4		PRIORITY 5	
MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL
1	1	0	0	2	2	1	1	0	0
1	1	0	0	1	1	0	0	0	1
0	0	1	1	0	0	1	1	0	1
1	1	0	0	2	2	1	1	0	0
1	1	0	0	1	1	0	0	0	1
1	1	0	0	2	2	1	1	0	0
2	2	1	1	1	1	0	0	1	1
2	2	1	1	1	1	0	0	1	1
1	1	2	2	0	0	1	1	1	1
2	2	1	1	1	1	0	0	1	1
1	1	2	2	1	1	0	0	1	1
2	2	1	1	1	1	0	0	1	1
0	0	0	1	1	1	1	2	1	0
1	1	2	2	0	0	1	1	1	1
0	0	0	1	1	1	1	2	1	0

SCORE	
MOD	MIL
4	4
2	3
2	3
4	4
2	3
4	4
5	5
5	5
5	5
5	5
5	5
5	5
5	5
3	4
5	5
3	4

PRIORITY 1		PRIORITY 2		PRIORITY 3		PRIORITY 4		PRIORITY 5	
MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL	MOD	MIL
2	0	1	1	0	0	0	2	1	0
1	1	0	0	2	2	1	1	0	0
2	2	0	0	1	0	0	0	1	0
1	2	0	1	0	1	0	0	0	0
0	2	0	1	0	0	2	0	0	0
0	0	1	0	0	0	2	2	0	0
2	2	1	1	1	1	0	0	1	1
2	2	1	1	1	1	0	0	1	1
0	0	0	0	2	1	0	2	0	0
0	0	0	0	0	0	2	2	0	0

SCORE	
MOD	MIL
4	3
4	4
4	3
4	3
2	3
3	3
5	5
5	5
2	3
2	3

an RI

Sumber : Hasil Konversi Skor Asesmen Risiko (hasil olahan data oleh peneliti)

Tabel berikut memperlihatkan hasil perhitungan dan pemilihan aspek dimaksud. Pada Tabel terlihat bahwa nilai terbesar yaitu “2” diberikan terhadap ancaman dengan *likelihood* tinggi dan *severity* tinggi. Sementara lainnya diberikan nilai “1” atau “0” berdasarkan tingkatan *likelihood* dan *severity*. Tabel terkait memperlihatkan hasil prioritisasi terhadap masing-masing lembaga – Kementerian Pertahanan dan Militer – dimana hanya yang memperoleh nilai agregat total di atas 4,00 yang terpilih sebagai prioritas.

Tabel 4. 20 Prioritisasi Serangan

RESPONDEN AHLI	MINISTRY OF DEFENSE														
	ANCAMAN 1	ANCAMAN 2	ANCAMAN 3	ANCAMAN 4	ANCAMAN 5	ANCAMAN 6	ANCAMAN 7	ANCAMAN 8	ANCAMAN 9	ANCAMAN 10	ANCAMAN 11	ANCAMAN 12	ANCAMAN 13	ANCAMAN 14	ANCAMAN 15
PAKAR #1: MUHAMMAD SALAHUDDIN	5	2	4	2	2	5	5	5	5	1	1	2	5	5	5
PAKAR #2: DUDI	5	4	4	4	2	5	5	5	5	1	1	5	5	5	5
PAKAR #3: RUDJANTO	5	5	4	5	2	5	5	5	5	1	1	2	5	4	4
PAKAR #4: BISHKON	4	2	2	4	2	4	5	5	5	5	5	5	5	5	3
PAKAR #5: CHARLES LIM	4	4	4	4	2	3	5	5	2	2	3	2	3	5	4
RATA-RATA	4,60	3,40	3,60	3,80	2,00	4,40	5,00	5,00	4,40	2,00	2,20	3,20	4,20	4,80	4,30



- Prioritas #1 : Ancaman Serangan **IDENTITY THEFT**
- Prioritas #2 : Ancaman Serangan **DATA BREACH**
- Prioritas #3 : Ancaman Serangan **CYBER ESPIONAGE**
- Prioritas #4 : Ancaman Serangan **MALWARE**
- Prioritas #5 : Ancaman Serangan **DDOS**
- Prioritas #6 : Ancaman Serangan **INSIDER THREAT**
- Prioritas #7 : Ancaman Serangan **RANSOMWARE**
- Prioritas #8 : Ancaman Serangan **CRYPTOJACKING**

MILITARY															
RESPONDEN AHLI	ANCAMAN 1	ANCAMAN 2	ANCAMAN 3	ANCAMAN 4	ANCAMAN 5	ANCAMAN 6	ANCAMAN 7	ANCAMAN 8	ANCAMAN 9	ANCAMAN 10	ANCAMAN 11	ANCAMAN 12	ANCAMAN 13	ANCAMAN 14	ANCAMAN 15
PAKAR #1: MUHAMMAD SALAHUDDIN	5	1	4	1	1	3	5	3	5	1	1	0	3	5	5
PAKAR #2: DUDI	5	4	4	4	3	5	5	5	5	1	1	5	5	5	5
PAKAR #3: RUDIANTO	5	5	4	5	3	5	5	5	5	1	1	2	5	4	4
PAKAR #4: BSYRON	4	3	3	4	3	4	5	5	5	5	3	5	4	5	4
PAKAR #5: CHARLES LIM	3	4	3	3	3	3	5	5	3	2	5	2	3	2	4
RATA-RATA	4,40	3,40	3,60	3,40	2,60	4,40	5,00	5,00	4,80	2,60	2,20	2,80	4,40	4,20	4,40



- Prioritas #1 : Ancaman Serangan **IDENTITY THEFT**
 Prioritas #2 : Ancaman Serangan **DATA BREACH**
 Prioritas #3 : Ancaman Serangan **INSIDER THREAT**
 Prioritas #4 : Ancaman Serangan **MALWARE**
 Prioritas #5 : Ancaman Serangan **DDOS**
 Prioritas #6 : Ancaman Serangan **RANSOMWARE**
 Prioritas #7 : Ancaman Serangan **CYBER ESPIONAGE**
 Prioritas #8 : Ancaman Serangan **CRYPTOJACKING**

Sumber : Prioritisasi Serangan (hasil pengolahan data oleh peneliti)

Berdasarkan tabel prioritisasi tersebut, dapat ditetapkan 8 (delapan) ancaman utama dari 15 (lima belas) tren ancaman yang harus diperhatikan secara sungguh-sungguh oleh negara, yaitu: (i) *Identity Theft*; (ii) *Data Breach*; (iii) *Cyber Espionage*; (iv) *Malware*; (v) *DDOS*; (vi) *Insider Threat*; (vii) *Ransomware*; dan (viii) *Cyryptojacking*. Keseluruhan ancaman tersebut harus benar-benar diperhatikan dan dimitigasi agar tidak membahayakan keselamatan, keutuhan, dan kedaulatan bangsa dan negara.

Langkah selanjutnya yang dilakukan dalam penelitian ini adalah mendalami dampak serius yang berpotensi dihadapi institusi atau sektor yang diserang dengan menggunakan kedelapan jenis serangan ini. Berbeda dengan dampak ancaman yang disampaikan terdahulu, pada bagian ini dilakukan kajian dan investigasi lebih mendalam hingga ke dua level.

Level pertama disebut sebagai dampak langsung, yaitu situasi dan kondisi yang diakibatkan karena adanya serangan yang berhasil masuk ke perimeter organisasi atau aset komputasi/informasi yang dilindungi. Tentu saja akan terdapat cukup banyak variasi dampak dimaksud. Dalam studi ini dilakukan pemilihan dua dampak yang paling membahayakan.

Level kedua adalah dampak yang disebabkan dari kejadian level pertama, sebagai sebuah efek domino yang terjadi. Sering kali terlihat bahwa justru pada dampak tak langsung itulah terjadi kerusakan yang jauh lebih besar daripada pertama. Oleh karena itu dilakukan kajian mendalam mengenai potensi dimaksud dengan menggunakan metoda *network analysis*.

Perlu diperhatikan bahwa jika ditinjau secara sungguh-sungguh, dampak langsung maupun tidak langsung tersebut memiliki potensi yang membahayakan kedaulatan, keutuhan, dan keselamatan bangsa dan negara. Dampak ini diperoleh dari kasus yang dialami sejumlah negara di masa lalu, hasil wawancara dengan para pakar, dan laporan pada berbagai publikasi terkait dengan serangan siber dan *impact*-nya bagi institusi, komunitas, dan negara. Berikut adalah masing-masing hasil *network analysis* dari kedelapan tren ancaman yang diprioritaskan untuk diantisipasi dan dihadapi oleh Indonesia sebagai sebuah negara berdaulat.

Tingkat Kerawanan Pertahanan Siber di Indonesia

Hasil pengolahan data yang berkaitan secara erat dengan tingkat kerawanan kedaulatan dan pertahanan siber di Indonesia disaripatikan dalam tabel berikut ini.

Tabel 4. 21 Hasil Pengolahan Data Tingkat Kerawanan Pertahanan Siber

No	Hasil Pengolahan Data	Sumber
1	<i>“Pertahanan siber Indonesia sangatlah lemah. Dapat dianalogikan bahwa siber di Indonesia itu sangat ‘telanjang’ karena dapat mudah ditembus dengan mudah oleh para peretas.”</i>	Gildas Deograt, XecureIT, Wawancara
	<i>“Lemahnya pertahanan siber Indonesia karena masih tidak dianggap seriusnya potensi kerusakan negara yang diakibatkan oleh serangan siber, walaupun beberapa negara telah berhasil dihancurkan musuh dengan menggunakan senjata moderen ini.”</i>	Christian Dono, Pakar Siber, Komunikasi Personal
	<i>“Mudah sekali menembus situs-situs di sektor pertahanan dan militer di tanah air.”</i>	Anonymous, Peretas, Blog Personal
2	<i>“Pada tingkat mikro, Indonesia memiliki potensi sumber daya manusia yang kuat, karena mempunyai kesempatan yang sama dengan seluruh negara dalam mendalami ilmu berbasis siber. Namun kultur keamanan masyarakatnya yang masih sangat beragam membuat negara sangat rentan mendapatkan serangan, terutama yang bernuansa social engineering.”</i>	Muhammad Salahuddien, Mantan Wakil Ketua ID-SIRTII, Wawancara
	<i>“Banyak serangan siber berhasil mencapai targetnya karena menggunakan teknik social engineering, yaitu menggunakan kelemahan manusia yang memiliki literasi rendah di bidang keamanan internet.”</i>	Tintin, EC-Council, Komunikasi Personal
	<i>“Literasi masyarakat Indonesia harus ditingkatkan agar</i>	Didiek Partono,

- tidak menjadi sasaran empuk serangan siber.”* Inixindo, Webinar
- 3 *“Ketidadaan doktrin yang jelas berakibat pada ketidakadaan konsolidasi usaha untuk membangun pertahanan kedaulatan siber yang kuat bagi Indonesia. Disamping itu, dengan tidak adanya doktrin, akan terjadi kegamangan dalam menghadapi berbagai ancaman yang terkait dengan serangan siber terhadap sebuah negara.”* Christian Dono, Pakar Siber, Komunikasi Personal
- “Doktrin siber akan melandasi tindakan negara dan komunitas dalam bersikap maupun beraktivitas.”* Hoga Saragih, Guru Besar Universitas Bakrie, Komunikasi Personal
- “Doktrin sishankamrata di era digital harus dirumuskan agar relevan dengan kebutuhan strategis Indonesia di masa sekarang.”* Kemal Stamboel, Mantan Ketua Komisi I DPR RI, Wawancara
- 4 *“Jaringan internet adalah segalanya. Menguasai protokol dalam tataran infrastruktur teknis merupakan kunci dari kedaulatan.”* Toto Atmodjo, Defenxor, Wawancara
- “Rawannya internet Indonesia adalah karena kebanyakan teknologi bukan merupakan karya anak bangsa.”* Gildas Deograt, XecureIT, Wawancara
- “Palapa Ring yang sedang dibangun akan menjadi kekuatan tersendiri bagi Indonesia dalam mengembangkan kedaulatan sibernya.”* Zainal Hasibuan, Anggota Wantiknas, RTD
- 5 *“Negara kurang menganggap pentingnya infrastruktur kritis dilindungi secara sungguh-sungguh, padahal entitas inilah yang menjadi target utama para penjahat siber yang ingin mengganggu keberlangsungan hidup sebuah bangsa. Tidak ada standar sama sekali yang diterapkan untuk melindungi infrastruktur siber nasional yang berhubungan erat dengan berbagai infrastruktur kritis dimaksud.”* Rudi Luhmanto, Ketua CSIRT.id, Wawancara
- “Setiap institusi dan lembaga penting negara harus menerapkan standar keamanan informasi yang prima.”* Eko Budiarto, Ketua IPKIN, RTD

- “Infrastruktur kritis yang berhasil dilumpuhkan atau diambil alih akan sangat membahayakan kedaulatan NKRI.”* Victor, Direktur BSSN, Diskusi
- 6 *“Kunci kekuatan siber terletak pada tata kelola dan regulasi negara yang mengaturnya, dimana Indonesia berada dalam posisi sangat lemah dalam hal tersebut. Contohnya adalah peraturan terhadap pihak swasta yang menjadi pemilik dan pengatur infrastruktur telekomunikasi dan internet di tanah air. Dengan kata lain adalah Indonesia sangat jauh dari kedaulatan siber sebagaimana seharusnya.”* Bisyron Wahyudi, Mantan Manajer ID-SIRTII, Wawancara
- “Tata kelola siber dapat dilakukan dengan membentuk dua layer governance, yaitu policy council yang memberikan arahan, dan tingkatan eksekutif yang mengeksekusinya.”* Kemal Stamboel, Mantan Ketua Komisi I DPR RI, Wawancara
- “Pertahanan siber dapat terbentuk melalui tata kelola yang baik.”* Suhono, Guru Besar ITB, Webinar
- 7 *“Salah satu penyebab lemahnya otoritas dan koordinasi bukan sekedar karena kekurangan atau ketiadaan organisasi, melainkan lebih disebabkan karena lemahnya leadership. Di belakang negara-negara berkembang maupun maju yang berhasil memiliki perkembangan siber yang cepat terdapat seorang leader yang sangat visioner – dan mampu meyakinkan penguasa maupun masyarakat akan pentingnya penguasaan terhadap arena virtual ini.”* Bambang Permantoro, Mantan Penasehat ID-SIRTII, Komunikasi Personal
- “Pimpinan negara sangat berpengaruh dalam menggerakkan dunia siber nasional.”* Carlia, Pengurus Aspiluki, Komunikasi Personal
- “Keberadaan pimpinan negara yang paham mengenai siber dapat mempercepat implementasi pertahanan siber karena memiliki kemampuan mengembangkan kebijakannya secara top-down.”* Muh. Adli, Konsultan Siber, Komunikasi Personal
- 8 *“Dalam peta penelitian dan perkembangan teknologi, tidak terlihat adanya perencanaan untuk berdaulat dalam industri telekomunikasi. Dengan sendirinya maka ketergantungan akan pihak asing menjadi sangat tinggi. Kondisi dahulu ketika Indonesia* Charles Liem, Peneliti Swiss-German University, Wawancara

memiliki Satelit Palapa perlu direalisasikan kembali masa kini.”

“Banyak program studi di tanah air yang mulai membuka konsentrasi di bidang teknologi siber dan internet. Fenomena ini dapat menjadi peluang bagus bagi Indonesia untuk menjadi tuan rumah di negara sendiri.”

Benny Mutiara,
Sekjen APTIKOM,
Komunikasi
Personal

“Indonesia telah memiliki peta Artificial Intelligence di bidang pertahanan siber sebagai bentuk manifestasi untuk menjaga kedaulatan negara.”

Hammam Riza,
Kepala BPPT, FGD

- 9 *“Infrastruktur fisik dalam bentuk transmisi telekomunikasi yang berhubungan dengan dunia siber masih sangat tergantung negara lain. Lebih dari 90% trafik ke dan dari Indonesia dilalui via negara Singapura dan Hongkong. Jika terjadi sesuatu dengan koneksi ini, jaringan internet Indonesia akan lumpuh. Akibatnya akan terjadi chaos dalam sejumlah sektor industri yang bergantung padanya.”*

Heru Nugroho,
Mantan Ketua APJII,
Wawancara

“Salah satu masalah yang sering ditemui adalah ketika jaringan kabel laut yang menjadi backbone internet Indonesia putus karena terkena jangkar kapal.”

Marsudi Kisworo,
Komisaris Telkom,
Wawancara

“Tidak mudah bagi Indonesia untuk dapat mengawasi seluruh infrastruktur internet tanpa teknologi yang memadai.”

Muhammad
Salahuddien,
Mantan Wakil Ketua
ID-SIRTII,
Wawancara

Sumber : Hasil Pengolahan Data Tingkat Kerawanan Pertahanan Siber (disusun oleh peneliti)

Setelah mengetahui tren ancaman dan serangan yang berpotensi mengganggu sistem pertahanan negara, langkah selanjutnya adalah melakukan kajian terhadap tingkat kerawanan atau *vulnerabilities* dari sistem informasi pertahanan negara yang dimiliki Indonesia. Sebagai sebuah sistem yang terdiri

dari berbagai komponen yang terkait satu dan lainnya, mengukur tingkat kerawanan harus dilakukan secara holistik, komprehensif, dan *end-to-end*.

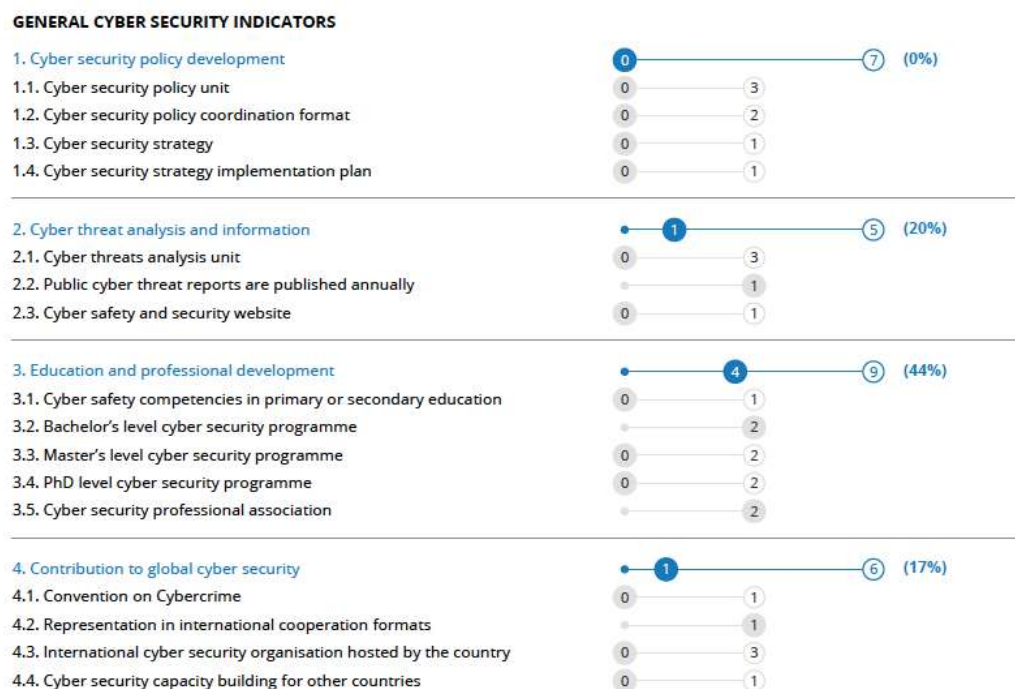
Semenjak kurang lebih satu dasawarsa yang lalu, terdapat sejumlah lembaga internasional yang melakukan kajian terhadap situasi dan kondisi terkait dengan keamanan siber dari suatu negara. Sejumlah institusi independen ini melakukan pemeringkatan global berdasarkan beraneka ragam indikator pengukuran. Hasil kajian dan pemeringkatan ini dapat menjadi referensi untuk memperlihatkan situasi dan kondisi pertahanan dan keamanan siber nasional yang dimiliki.

National Cyber Security Index

Hasil asesmen pada tahun 2020 menempatkan Indonesia pada peringkat 77 dari 160 negara yang dikaji. Nilai total yang diperoleh adalah 38,96 dari skala maksimum 100. Indikator yang dipergunakan untuk menilai terbagi menjadi tiga, masing-masing adalah: (i) *General Cyber Security Indicators*; (ii) *Baseline Cyber Security Indicators*; dan (iii) *Incident and Crisis Management Indicators*.

Pada Tabel berikut terlihat bagaimana Indonesia mendapatkan nilai sangat rendah dalam aspek Pengembangan Kebijakan Keamanan Siber. Empat komponen utama yang dianggap belum serius ditangani oleh pemerintah dan negara, yaitu terkait dengan: (i) unit penyusun kebijakan keamanan siber; (ii) mekanisme koordinasi penyelerasan kebijakan keamanan siber; (iii) strategi terkait dengan keamanan siber; dan (iv) rencana implementasi strategi keamanan siber yang komprehensif. Untuk ketiga aspek yang lain pun Indonesia mendapatkan nilai rendah di bawah 50, yaitu: Kajian dan Informasi terkait Ancaman Siber (20%), Pengembangan Profesionalisme dan Pendidikan di Bidang Keamanan Siber (44%), dan Kontribusi Keamanan Siber terhadap Kondisi Global (17%).

Tabel 4. 22 Skor NCSI Indonesia terkait Indikator Umum



Sumber : Skor NCSI Indonesia terkait Indikator Umum (NCSI Report, 2020)

Domain berikutnya yang tidak kalah menarik untuk dipelajari adalah terkait dengan indikator dasar. Tabel berikut memperlihatkan bahwa dari empat indikator yang ada, baru satu indikator dimana Indonesia memperoleh nilai sangat baik, yaitu terkait dengan aspek Layanan Terpercaya dan Identifikasi Personal berbasis Elektronik (89%). Sementara ketiga aspek lainnya masih dinilai sangat rendah. Paling rendah nilainya yaitu 0% diberikan kepada aspek Proteksi Layanan Esensial atau Kritis. Dalam dunia pertahanan dan keamanan siber, yang dimaksud dengan layanan ini berkaitan erat dengan infrastruktur krisis nasional. Nilai rendah berikutnya yaitu 20% diberikan terhadap aspek Proteksi Layanan Digital – baik di sektor publik maupun swasta. Dan yang terakhir dengan nilai 25% berkaitan dengan Proteksi Data Personal.

Tabel 4. 23 Skor NCSI Indonesia terkait Indikator Dasar

BASELINE CYBER SECURITY INDICATORS**5. Protection of digital services**

- 5.1. Cyber security responsibility for digital service providers
- 5.2. Cyber security standard for the public sector
- 5.3. Competent supervisory authority

**6. Protection of essential services**

- 6.1. Operators of essential services are identified
- 6.2. Cyber security requirements for operators of essential services
- 6.3. Competent supervisory authority
- 6.4. Regular monitoring of security measures

**7. E-identification and trust services**

- 7.1. Unique persistent identifier
- 7.2. Requirements for cryptosystems
- 7.3. Electronic identification
- 7.4. Electronic signature
- 7.5. Timestamping
- 7.6. Electronic registered delivery service
- 7.7. Competent supervisory authority

**8. Protection of personal data**

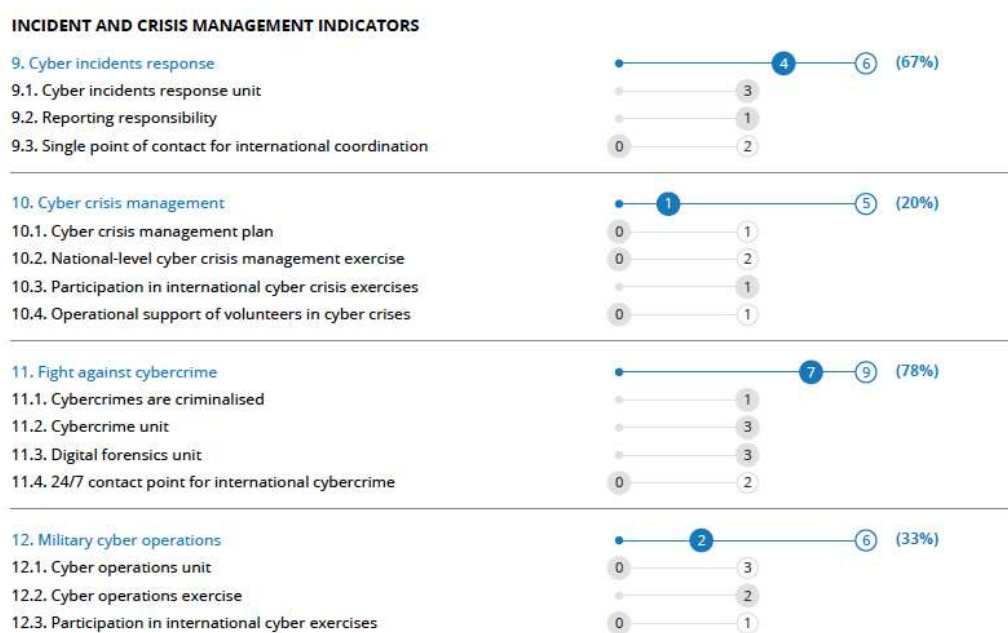
- 8.1. Personal data protection legislation
- 8.2. Personal data protection authority



Sumber : Skor NCSI Indonesia terkait Indikator Dasar (NCSI Report, 2020)

Domain terakhir yang dijadikan sebagai dasar pengukuran indeks adalah indikator yang berkaitan dengan kemampuan negara dalam Pengelolaan Insiden dan Krisis Siber.

Tabel 4. 24 Skor NCSI Indonesia terkait Indikator Manajemen Krisis dan Insiden

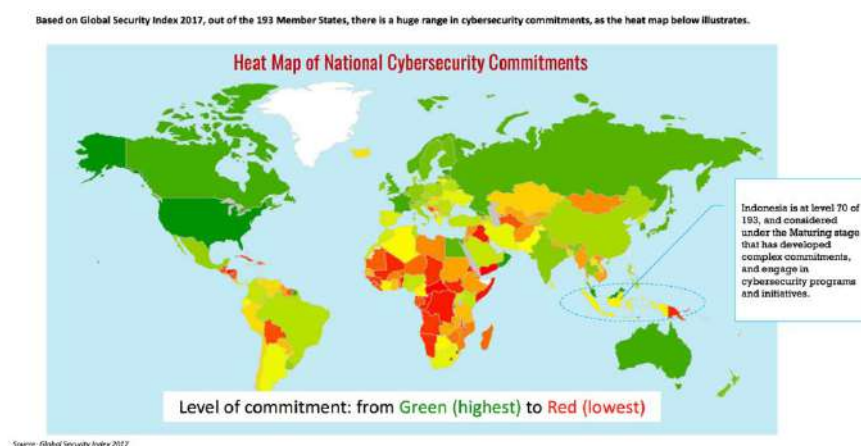


Sumber : Skor NCSI Indonesia terkait Indikator Manajemen Krisis dan Insiden (NCSI Report, 2020)

Ada empat hal yang dinilai dalam domain ini, dimana Indonesia mendapatkan nilai baik 78% untuk aspek yang berkaitan dengan Perang terhadap Kejahatan Siber atau yang lebih dikenal dengan istilah *cyber crime*. Aspek kedua yang dianggap cukup baik dengan nilai 67% terkait dengan adanya Tim Tanggap Insiden Siber, mengingat semenjak lima belas tahun yang lalu Indonesia telah memiliki ID-SIRTII di bawah koordinasi Kementerian Komunikasi dan Informatika. Sementara dua aspek lain masih jauh dari harapan, terutama terkait dengan Keandalan Operasi Siber Militer (33%) dan Manajemen Penanganan Krisis Siber (20%).

Global Security Index

Berita baik diperoleh Indonesia setelah pembentukan Badan Siber dan Sandi Negara (BSSN). Sebelum badan ini didirikan, Global Security Index Indonesia berada di peringkat 70 dari 193 negara. Pada saat itu Indonesia hanya memperoleh 47,4 dari skala 100. Indikator yang dijadikan sebagai basis penilaian terdiri dari 5 (lima) domain utama, masing-masing terkait dengan aspek: (i) Legal; (ii) Teknis; (iii) Organisasi; (iv) Kapasitas; dan (v) Kooperasi. Hal-hal yang dianggap kurang dari negara Indonesia dan perlu mendapatkan perhatian sungguh-sungguh adalah berhubungan dengan isu sebagai berikut:



Gambar 4. 7 Peta Komitmen Keamanan Siber Dunia menurut GSI

Sumber : Peta Komitmen Keamanan Siber Dunia menurut GSI (GSI Report, 2020)

1. *Sectoral CERT/CIRT/CSIRT*: keberadaan tim tanggap darurat untuk insiden maupun krisis yang berbasis pada sektor industri seperti perbankan, militer, transportasi, kesehatan, pendidikan, dan lain sebagainya;
2. *Standards for Organisations*: persyaratan, penerapan, dan penegakan hukum terkait dengan kewajiban mengikuti standar bagi organisasi atau perusahaan yang memberikan layanan elektronik atau digital secara masif;
3. *Child Online Protection*: perlindungan terhadap anak-anak ketika mereka berinteraksi di dunia maya melalui berbagai mekanisme dan pendekatan yang efektif;
4. *Strategy*: penetapan formulasi strategi pertahanan dan keamanan siber yang komprehensif, holistik, serta *end-to-end* berbasis kolaborasi antar institusi atau lembaga negara dan pemangku kepentingan lainnya;
5. *Cybersecurity Metrics*: pemantauan situasi keamanan siber dipandang dari berbagai indikator yang dapat diukur kondisinya;
6. *Cybersecurity Good Practices*: kisah sukses pengelolaan keamanan siber organisasi yang dijadikan sebagai rujukan atau referensi bagi institusi lain yang ingin menerapkan secara baik;
7. *Education Programs*: penyelenggaraan program edukasi keamanan siber yang berjenjang dan berkelanjutan, dimana

Universitas Pertahanan RI

diperuntukkan bagi berbagai latar belakang masyarakat yang berbeda-beda;

8. *Home-Grown Industry*: tumbuhnya industri informatika dalam negeri yang bergerak dalam mengembangkan berbagai aplikasi dan teknologi terkait dengan keamanan informasi dan internet;
9. *Bilateral Agreements*: kerjasama bilateral antar Indonesia dengan negara lain dalam rangka berkolaborasi di bidang penanganan dan pengelolaan keamanan siber;
10. *Multilateral Agreements*: kerjasama multilateral antara Indonesia dengan berbagai negara lainnya untuk berkoordinasi, berkooperasi, dan berkolaborasi dalam penanganan keamanan siber;
11. *Public-Private Partnerships*: penyelenggaraan pola kemitraan strategis antara pemerintah dan swasta dalam mengelola keamanan siber bersama bagi kepentingan masyarakat luas; dan
12. *Cooperation*: kemitraan strategis antar berbagai pihak di dalam negeri yang bersepakat secara intens dan masif secara kolektif mengelola keamanan negara demi keselamatan masyarakat, bangsa, dan negara.

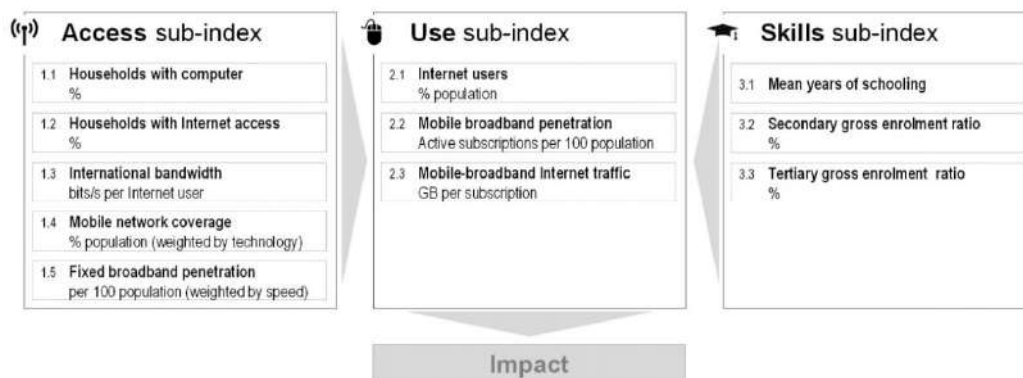
Terlepas dari berbagai kekurangan tersebut, di tahun 2020 ini setelah terbentuknya BSSN, Indonesia mengalami lompatan peringkat yang sangat signifikan – yaitu sebanyak 29 tingkat. Pada saat ini Indonesia berhasil menempati urutan 41, sehingga berada dalam papan tengah pengelolaan keamanan siber di dunia. Walaupun demikian, masih banyak yang harus dilakukan karena masih begitu banyak aspek yang rendah nilainya.

ICT Development Index

Pembangunan Teknologi Informasi dan Komunikasi (*Information and Communications Technology/ICT*) Indonesia tertinggal dibandingkan negara

Universitas Pertahanan RI

anggota Group Twenty (G20) lainnya. Indeks yang didapatkan Indonesia pada 2017 sebesar 4,33 poin. Angka ini berada di posisi 111 dunia dari 176 negara atau kedua terendah di G20 setelah India. IDI 2017 terdiri dari 3 kelompok penilaian yaitu 5 indikator kesiapan akses infrastruktur, 3 indikator intensitas penggunaan, dan 3 indikator kemampuan atau keahlian. Pada tahun 2020 sedang dipersiapkan penghitungan indeks dengan menggunakan 1 indikator baru, sesuai dengan kemajuan teknologi informasi dan komunikasi yang sedemikian pesat. Kesebelas indikator yang dimaksud diperlihatkan pada gambar 4.6 berikut ini. Diperkirakan dengan metoda dan indikator baru ini Indonesia akan dapat meningkatkan peringkatnya.

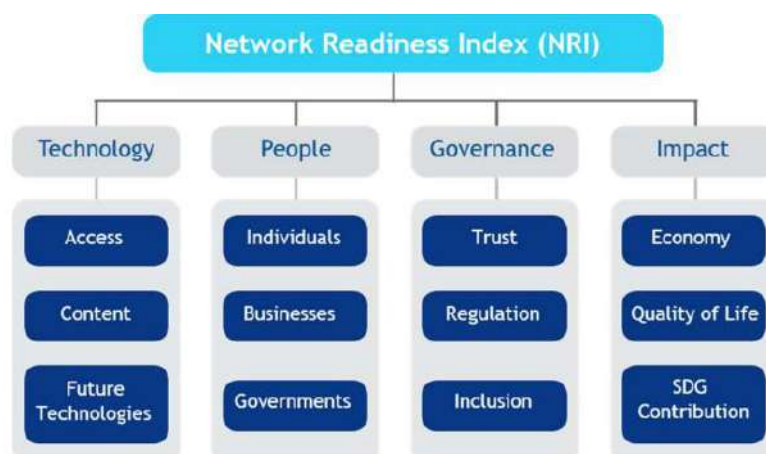


Gambar 4. 8 Skor Indonesia menurut ICT Development Index

Sumber : Skor Indonesia menurut ICT Development Index (ICT-DI Report, 2020)

Networked Readiness Index

NRI merupakan salah satu indeks terkemuka global yang dipergunakan untuk melihat tingkat kesiapan jaringan teknologi informasi sebuah negara. Secara keseluruhan, terdapat empat indikator yang diukur sebagaimana diperlihatkan pada Gambar 4.18. Pengukuran indeks ini sangatlah penting karena arena siber terbentuk akibat adanya jaringan dari jejaring sumber daya komputasi yang terhubung satu dan lainnya.

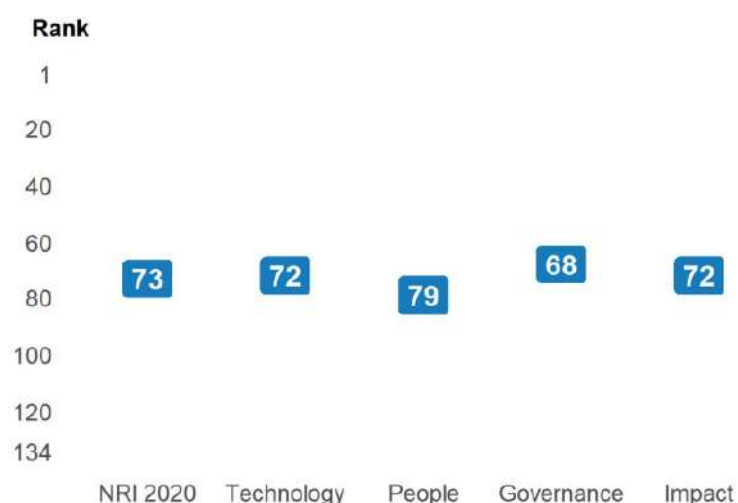


an RI

Gambar 4. 9 Struktur Komponen Network Readiness Index

Sumber : Struktur Komponen Network Readiness Index (NRI Report, 2020)

Domain pertama adalah teknologi, dimana diukur jangkauan aksesibilitas, kekayaan konten, dan pemanfaatan teknologi masa depan. Sementara domain kedua berkaitan dengan sumber daya manusia, menyangkut kompetensi individual, kesiapan profesionalisme bisnis, dan kehandalan para birokrat dalam memanfaatkan teknologi. Selanjutnya domain ketiga adalah tata kelola, menyangkut aspek-aspek seputar tingkat kepercayaan lembaga dan masyarakat, keberadaan dan kelengkapan regulasi, serta inklusivitas pemanfaatan teknologi informasi dan komunikasi. Dan yang terakhir yaitu domain keempat terkait dengan dampak, meliputi aspek kontribusi terhadap pertumbuhan ekonomi, peningkatan kualitas hidup, dan sumbangan terhadap pencapaian *Sustainable Development Goals*.



Gambar 4. 10 Skor Indonesia pada Sejumlah Komponen NRI

Sumber : Skor Indonesia pada Sejumlah Komponen NRI (NRI Report, 2020)

Secara keseluruhan Indonesia pada tahun 2020 menempati urutan 73 dari 134 negara yang dianalisa – dengan nilai 46,71 dari skala 100. Gambar 4.8 memperlihatkan peringkat per masing-masing domain kategori. Sementara Tabel 4.23 memperlihatkan rincian peringkat pada masing-masing sub-pilar. Terlihat di sana bahwa ranking terbaik Indonesi adalah pada pemanfaatan teknologi masa depan (peringkat 52), sementara yang paling rendah peringkatnya terkait dengan kehandalan bisnis dalam memanfaatkan teknologi yang ada secara masif dan berdampak langsung terhadap pertumbuhan ekonomi (peringkat 102).

Tabel 4. 25 Nilai Indonesia pada Sejumlah Pilar NRI

Sub-pillar	Rank	Sub-pillar	Rank
Future Technologies	52	Inclusion	80
Governments	53	Individuals	81
Economy	57	Quality of Life	82
Trust	66	SDG Contribution	89
Access	68	Content	92
Regulation	80	Businesses	102

Sumber : Nilai Indonesia pada Sejumlah Pilar NRI (NRI Report, 2020)

Secara rata-rata, Indonesia dinilai masih di bawah rata-rata dibandingkan negara berkembang lainnya maupun yang berada di wilayah Asia Pasifik. Tabel 4.24 berikut ini memperlihatkan kondisi dimaksud.

Tabel 4. 26 Nilai Indonesia pada Sejumlah Dimensi NRI

Dimension	Indonesia	Upper-middle-income countries	Asia & Pacific
NRI	46.71	47.39	52.76
Technology	38.38	38.42	45.33
People	43.26	46.66	49.64
Governance	54.99	54.31	59.20
Impact	50.20	50.17	56.86

Sumber : Nilai Indonesia pada Sejumlah Dimensi NRI (NRI Report, 2020)

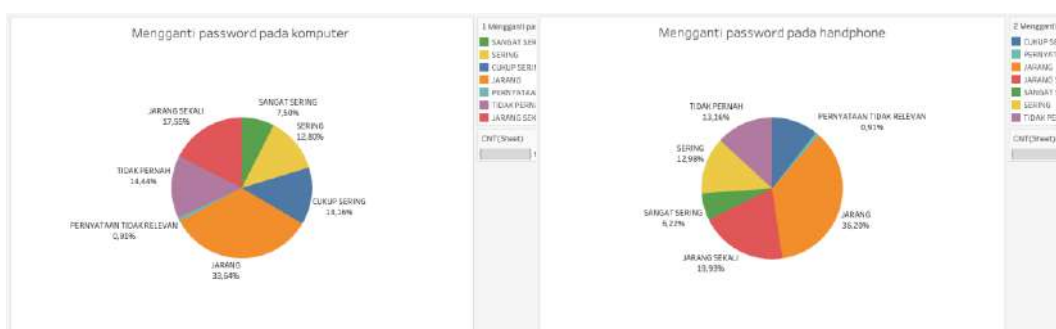
Tingkat kerawanan sebuah sistem siber juga sangat ditentukan oleh literasi dari masyarakat yang menggunakannya. Tidak ada gunanya jika dikembangkan teknologi keamanan yang canggih dan proses yang berbasis standar, tanpa diimbangi dengan literasi dan kultur keamanan informasi dari para penggunanya. Manusia dianggap sebagai *“the weakest link”* atau komponen terlemah dari sebuah sistem informasi, sehingga mudah dijadikan sebagai sasaran eksploitasi bagi para kriminal atau penjahat siber. Hampir semua kejahatan siber besar di Indonesia dimulai dengan aktivitas *social engineering*

atau usaha mengeksploitasi kelemahan manusia dalam berinteraksi dengan menggunakan sumber daya digital. Oleh karena itulah perlu dilakukan kajian terkait dengan kelemahan dimaksud.

Pada penelitian ini dilakukan survei terhadap lebih dari 500 pengguna atau *user* di lingkungan militer dan Kementerian Pertahanan. Tujuannya adalah untuk mendapatkan gambaran mengenai kultur keamanan informasi dari mereka. Ringkasan hasilnya dapat dilihat sebagai berikut.

Mengelola Password

Password adalah satu komponen penting dan mendasar dalam ekosistem keamanan siber. Pemilihan, pemeliharaan, pengelolaan, dan pemutakhiran kata kunci rahasia ini harus menjadi sebuah kepedulian bersama bagi setiap individu yang menggunakan piranti digital serta mengakses internet. Pada studi ini dicoba dilihat bagaimana perilaku atau kebiasaan responden dalam memutakhirkan *password*. Salah satu prinsip yang perlu dipegang teguh oleh pengguna aplikasi dalam lingkungan internet terkait dengan pengelolaan *password* adalah “semakin sering diganti, semakin baik”.





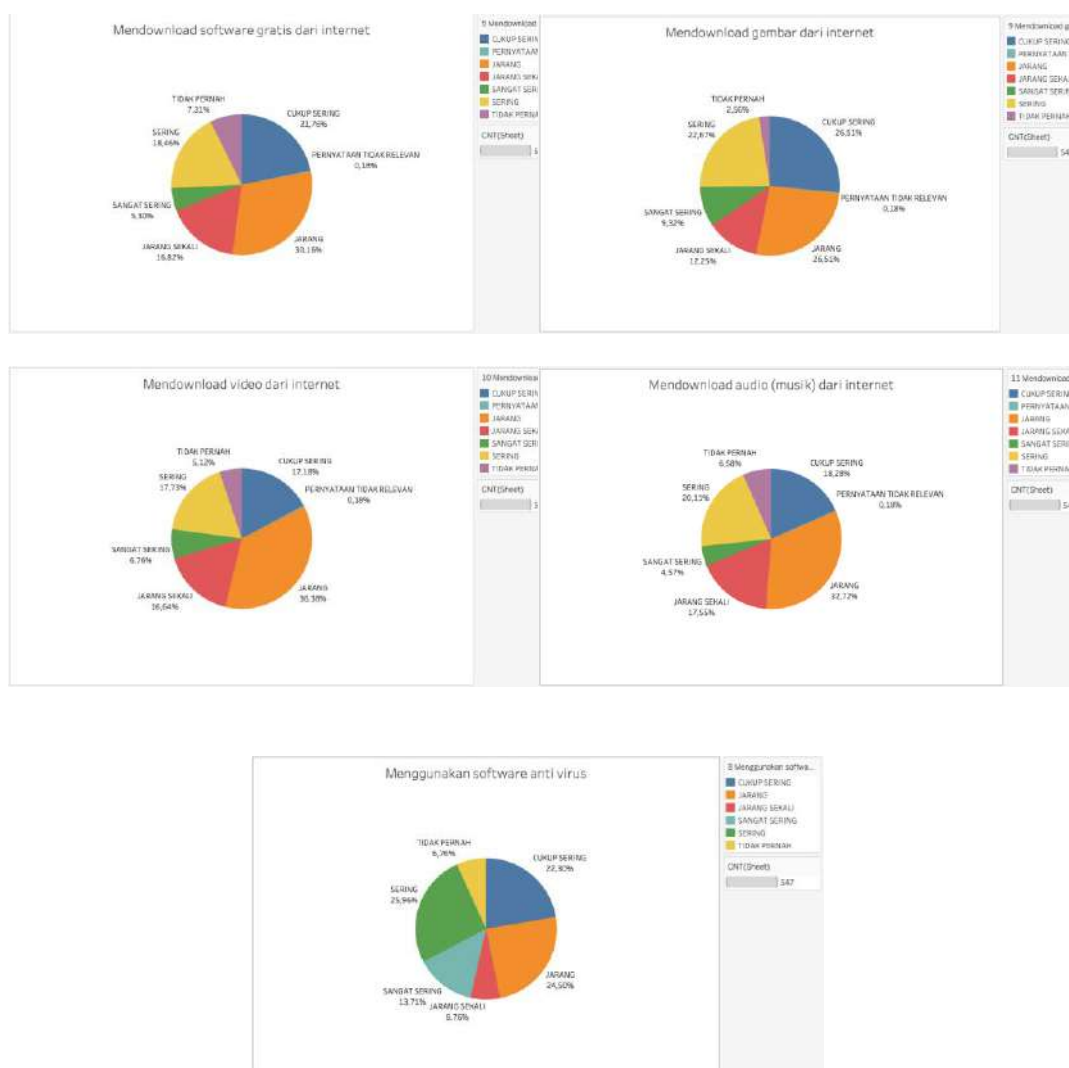
Gambar 4. 11 Grafik Kultur Mengelola Password

Sumber : Grafik Kultur Mengelola Password (hasil pengolahan data oleh peneliti)

Hasil dari survei yang dilakukan cukup mengejutkan, karena terlihat bahwa lebih dari 50% responden mengatakan bahwa mereka sangat jarang mengganti *password*-nya, baik yang dipergunakan di komputer, *handphone*, email, dan media sosial. Bahkan terdapat 15% yang tidak pernah mengganti sama sekali *password* yang dimilikinya. Tentu saja kultur ini menjadi sebuah kelemahan yang perlu diwaspadai.

Mengunduh File dari Internet

Dunia siber memberikan keleluasaan kepada penggunanya untuk saling berkomunikasi dan berinteraksi secara bebas. Salah satu fitur yang dapat dilakukan pengguna adalah mengunduh atau *download* berbagai berkas digital atau yang biasa disebut sebagai *files* secara bebas. *Files* dimaksud dapat berupa *software* atau aplikasi, gambar, video, maupun audio. Melihat adanya kebiasaan ini, para penjahat menggunakan *files* yang cenderung gratis ini untuk meletakkan *malware* atau aplikasi beritensi jahat. Semakin sering seseorang mengunduh sesuatu yang gratis dari internet, semakin tinggi risiko yang dihadapinya karena dapat terpapar oleh *malware*.



Gambar 4. 12 Grafik Kultur Mengunduh File dari Internet

Sumber : Grafik Kultur Mengunduh File dari Internet (hasil pengolahan data oleh peneliti)

Hasil yang ditemukan cukup menarik, karena rata-rata 40% responden merasa cukup sering mengunduh beragam *files* dimaksud. Dari semua jenis artefak *file*, terlihat bahwa yang paling banyak diunduh adalah gambar. Kemudian masing-masing diikuti oleh mengunduh aplikasi atau *software*, musik dalam bentuk audio, dan video. Dalam konteks keamanan informasi, ada sejumlah prinsip yang harus diterapkan dalam mengunduh sesuatu yang gratis di internet agar terhindar dari bahaya *malware*, seperti: instalasi *software* anti-virus,

identifikasi situs sumber *files*, teknik mengunduh yang efektif namun aman, dan lain sebagainya.

Meminjamkan dan Dipinjami *Flash Disk*

Sejumlah kajian memperlihatkan bahwa virus atau *malware* paling banyak ditularkan ke sistem atau jaringan komputer adalah melalui *flash disk*. Oleh karena itulah maka perilaku pinjam meminjam *flash disk* haruslah dihindari.



Gambar 4. 13 Grafik Kultur Meminjamkan dan Dipinjami *Flash Disk*

Sumber : Grafik Kultur Meminjamkan dan Dipinjami *Flash Disk*

(hasil pengolahan data oleh peneliti)

Gambar terkait memperlihatkan bagaimana para responden pernah menggunakan atau meminjamkan *flash disk* yang dimilikinya ke pihak lain. Artinya adalah bahwa risiko tertular atau tertanam *malware* pada komputer yang mengakses *flash disk* dimaksud relatif tinggi. Jika sudah masuk ke dalam sebuah sistem, maka penularannya ke perangkat lain akan lebih cepat karena sifat jejaring yang menghubungkan satu komputer dengan yang lain.

Mem-backup File Penting

Sebagaimana telah disampaikan sebelumnya, salah satu jenis serangan yang belakangan ini menimpa dunia adalah *ransomware*. Ketika

sebuah sistem tereksplorasi dengan serangan ini, maka tidak ada cara lain melepaskan “sandera” lawan kecuali membayar tuntutan finansial yang diminta penyandera. Satu-satunya cara mengantisipasi atau memitigasi serangan ini adalah melalui kebiasaan mem-*backup* file-file penting – sehingga jika sistem diambil alih, data penting yang dibutuhkan masih terselamatkan. Hasil penelitian memperlihatkan rendahnya kebiasaan responden melakukan proses *backup* baik terhadap berkas elektronik (data, informasi, dan konten) yang disimpan pada komputer maupun *handphone* – hanya di bawah 50% yang melakukannya.

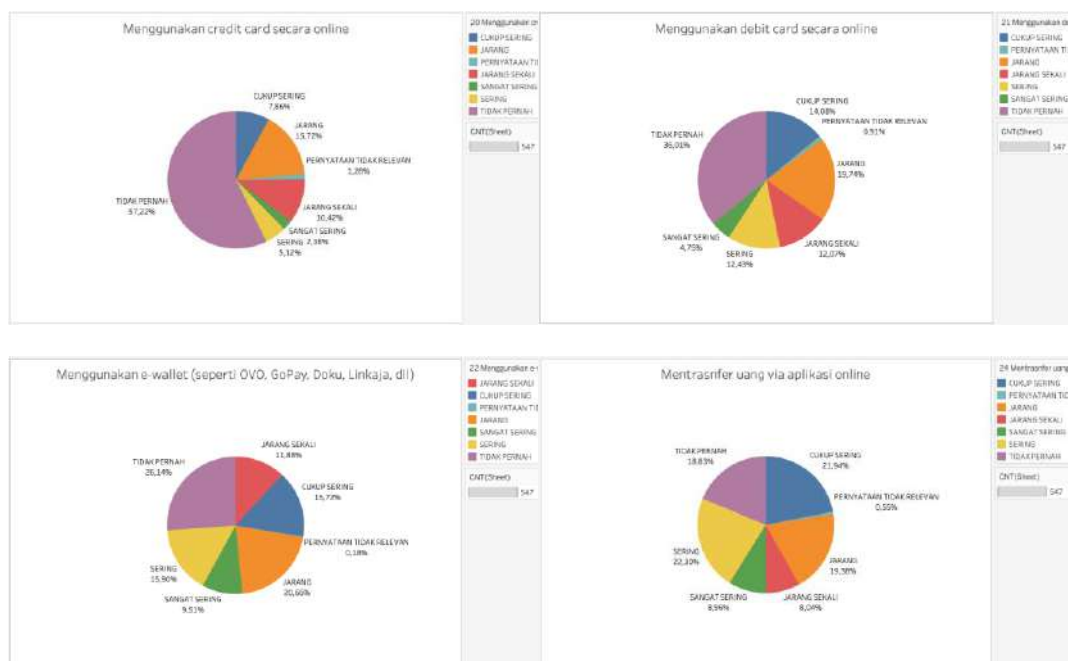


Gambar 4. 14 Grafik Kultur Membakup File Penting

Sumber : Grafik Kultur Membakup File Penting (hasil pengolahan data oleh peneliti)

Menggunakan Kartu dan Uang Digital

Indonesia adalah salah satu negara yang dikenal dengan tingkat pertumbuhan *e-commerce* tertinggi di dunia, melebihi rata-rata global. Dikatakan sebagai *e-commerce* apabila dalam kegiatannya terdapat jual beli produk atau layanan yang melibatkan transaksi keuangan. Mengetahui seberapa banyak masyarakat yang aktif menggunakan kartu atau uang digital sangatlah penting karena sejumlah alasan.



Gambar 4. 15 Grafik Kultur Menggunakan Kartu dan Uang Digital

Sumber : Grafik Kultur Menggunakan Kartu dan Uang Digital

(hasil pengolahan data oleh peneliti)

Alasan pertama adalah untuk memastikan bahwa tidak ada pihak yang mengetahui akses terhadap uang digital – baik dalam bentuk kartu kredit, debit, atau dompet digital – karena dapat merugikan secara finansial pihak bersangkutan. Sementara alasan kedua adalah karena cukup banyak terjadi peristiwa kebobolan data yang menimpa *platform e-commerce* besar seperti Bukalapak dan Tokopedia, dimana jutaan *password* pengguna telah terpapar. Lebih dari 40% rata-rata responden mengaku pernah melakukan transaksi *e-commerce* dengan melakukan pembayaran *online* via kartu kredit, kartu debit, maupun uang digital.

Memindahkan Data antar Perangkat

Setiap individu biasanya memiliki lebih dari satu perangkat digital, apakah berupa komputer, *notebook*, *handphone*, tablet, atau gawai lainnya. Keperluan memindahkan data antara satu perangkat ke perangkat lainnya adalah merupakan suatu keniscayaan, karena adanya keperluan seperti *backup* atau memutakhirkan piranti baru yang baru saja dibeli atau dimiliki.



Gambar 4. 16 Grafik Kultur Memindahkan Data antar Perangkat

Sumber : Grafik Kultur Memindahkan Data antar Perangkat

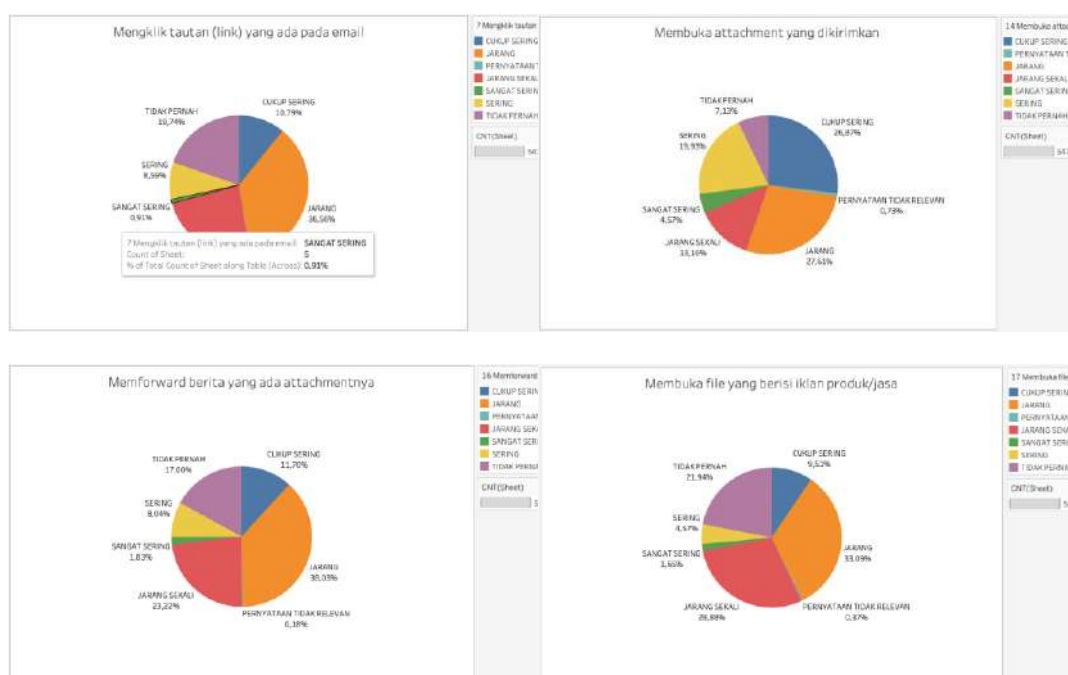
(hasil pengolahan data oleh peneliti)

Dalam konteks keamanan informasi, terdapat sejumlah kerawanan serius dalam proses pemindahan data dimaksud. Pertama adalah begitu banyaknya proses pemindahan data yang dilakukan oleh pihak lain, bukan pemilik perangkat yang bersangkutan. Risiko dari aktivitas ini adalah adanya kemungkinan pihak tersebut untuk menyalin data elektronik yang ada tanpa sepengetahuan pemilik. Kedua adalah karena dimungkinkan terjadi *men-in-the-middle attack* ketika pemindahannya dilakukan melalui medium nirkabel atau *wireless*. Sementara yang ketiga adalah lupanya menghapus data dari perangkat

lama yang diputuskan untuk tidak dipergunakan lagi (bahkan direncanakan untuk dijual atau diberikan kepada orang lain). Hasil penelitian memperlihatkan adanya rata-rata 25% responden yang melakukan aktivitas ini secara berkala.

Mengklik Tautan dan Membuka Attachment Files

Penjahat siber paling senang menggunakan taktik *phishing* dalam menipu masyarakat agar secara tidak sengaja masuk ke dalam perangkap atau jerat program jahatnya. Salah satu teknik *phishing* yang terbukti aktif dan banyak dilakukan adalah melalui jeratan tautan dalam bentuk *link* atau *attachment* yang menyertai sebuah pesan elektronik seperti email atau *whatsapp*.



Gambar 4. 17 Grafik Kultur Mengklik Tautan dan Membuka Attachment

Sumber : Grafik Kultur Mengklik Tautan dan Membuka Attachment

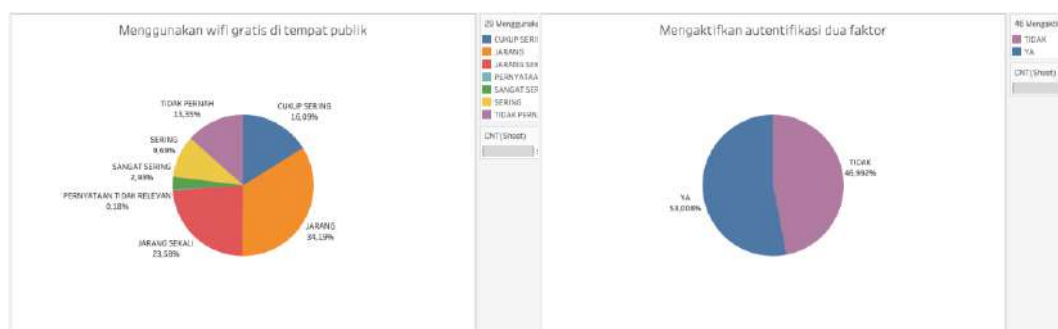
(hasil pengolahan data oleh peneliti)

Hasil penelitian memperlihatkan bahwa kurang lebih 50% responden mengaku biasa membuka *attachment* yang menyertai email yang dikirimkan, sementara sekitar 20% meneruskannya atau *mem-forward* ke pihak lain. Demikian pula terkait dengan ajakan mengklik *link* baik berisi ajakan tertentu

atau berkaitan dengan penawaran produk/layanan, yaitu sekitar 20%-an. Tentu saja kecenderungan ini meningkatkan risiko masuknya virus atau *malware* sejenis lainnya.

Menggunakan Wifi Publik

Kebiasaan menggunakan wifi gratis juga menjadi permasalahan tersendiri, karena tidak semuanya dikonfigurasi dengan baik, berbasis prinsip-prinsip keamanan internet. Disamping itu ditanyakan pula ke responden apakah mereka mengaktifkan autentifikasi dua faktor untuk mengamankan dari pencurian data atau informasi penting. Penelitian memperlihatkan bahwa sekitar 47% responden tidak melakukan hal tersebut, sehingga mereka sangat rawan terekspos ancaman pencurian data.



Gambar 4. 18 Grafik Kultur Menggunakan Wifi Publik

Sumber : Grafik Kultur Menggunakan Wifi Publik (hasil pengolahan data oleh peneliti)

Menggunakan Identitas Biometrik

Salah satu cara paling ampuh untuk melindungi data, informasi, maupun perangkat teknologi yang dimiliki adalah menggunakan fitur pengamanan berbasis biometrik – disamping hanya berpegang teguh pada pendekan konvensional menggunakan *username* dan *password*.



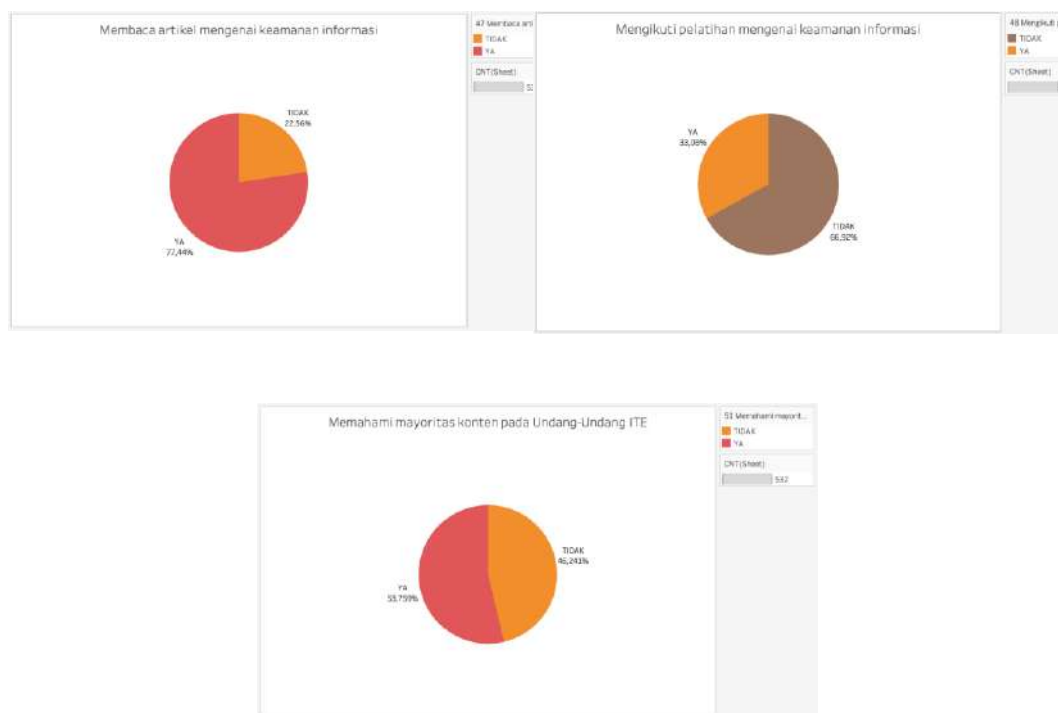
Gambar 4. 19 Grafik Kultur Menggunakan Identitas Biometrik

Sumber : Grafik Kultur Menggunakan Identitas Biometrik (hasil pengolahan data oleh peneliti)

Survei memperlihatkan bahwa mayoritas 75% responden tidak menggunakan fitur biometrik yang ada pada komputer, dan 34% pengguna telepon genggam juga tidak melakukannya. Artinya adalah bahwa mereka harus benar-benar melakukan pengelolaan terhadap *password* yang dimilikinya agar tidak diketahui orang lain.

Membaca dan Mengikuti Pelatihan

Literasi dan keperdulian terhadap keamanan informasi dibangun melalui pengetahuan seseorang akan isu penting tersebut. Sering membaca artikel dan mengikuti pelatihan adalah contoh cara meningkatkan wawasan, pengetahuan, dan penguasaan terhadap keamanan informasi. Gambar 4.18 memperlihatkan bahwa kebiasaan membaca responden terhadap berbagai hal terkait keamanan informasi relatif tinggi, yaitu 77,44%. Namun demikian, kesempatan mereka mengikuti pelatihan terkait hal yang sama cukup rendah, yaitu 33,08%. Satu pertanyaan tambahan diajukan terkait dengan pemahaman mereka akan konten Undang-Undang tentang Informasi dan Transaksi Elektronik. Sebanyak 46,24% merasa belum memahami mayoritas isi dari peraturan tersebut. Tentu saja kenyataan ini memperlihatkan bagaimana perlunya dilakukan serangkaian aktivitas untuk meningkatkan pengetahuan dan kompetensi tentang keamanan informasi dan UU-ITE kepada masyarakat terkait.



Gambar 4. 20 Grafik Kultur Membaca dan Mengikuti Pelatihan

Sumber : Grafik Kultur Membaca dan Mengikuti Pelatihan (hasil pengolahan data oleh peneliti)

Menggunakan Situs E-Commerce

Hasil kajian berikutnya yang menarik adalah ketika mengetahui bahwa cukup banyak responden berbelanja secara *online* melalui situs *e-commerce* yang tersedia. Situs yang paling banyak dipergunakan adalah Tokopedia (60,34%). Shopee (57,36%), dan Bukalapak (38,36%). Lebih dari 60% responden menegaskan kebiasaannya berbelanja via situs-situs ini.



Gambar 4. 21 Grafik Kultur Menggunakan Situs E-Commerce

Sumber : Grafik Kultur Menggunakan Situs E-Commerce (hasil pengolahan data oleh peneliti)

Kebiasaan berbelanja dengan memanfaatkan situs *online* harus diiringi dengan kultur mengganti *password* secara berkala, dan terus memonitor keamanan situs dimaksud – mengingat situs-situs ternama ini kerap menjadi sasaran *hacking* dari para penjahat siber. Hal yang sama perlu pula dilakukan untuk kebiasaan mengakses beragam situs terkemuka baik yang dimiliki oleh institusi dalam maupun luar negeri.

Menggunakan Aplikasi *Virtual Meeting*

Semenjak masa pandemi, terdapat kebiasaan baru di masyarakat, yaitu marak dan intensif-nya penggunaan aplikasi *teleconference* seperti Zoom atau Google Meet. Hasil penelitian mengkonfirmasi kenyataan ini, dimana 74,67% responden mengaku menggunakan aplikasi Zoom dan 48,05% menggunakan Google Meet.



Gambar 4. 22 Grafik Kultur Menggunakan Aplikasi Virtual Meeting

Sumber : Grafik Kultur Menggunakan Aplikasi Virtual Meeting

(hasil pengolahan data oleh peneliti)

Mereka yang kerap menggunakan berbagai aplikasi *teleconference* dimaksud perlu memahami sejumlah hal terkait dengan isu keamanan informasi di seputarnya. Misalnya adalah pernah terjadinya pembobolan data *private* dari aplikasi Zoom beberapa waktu yang lalu. Atau kebiasaan pihak *host* melakukan *recording* tanpa sepengetahuan atau seijin seluruh pihak yang berinteraksi. Belum lagi tereksposnya foto wajah karena saling bertatap muka via virtual yang harus menjadi pertimbangan plus minusnya.

Menggunakan *Proprietary Software*

Semenjak komputer diperkenalkan ke masyarakat sebagai alat membantu aktivitas individu di sekitar awal tahun 1980-an, aplikasi untuk meningkatkan produktivitas begitu banyak digemari dan dipergunakan. Salah satu seri aplikasi yang paling banyak dipergunakan adalah produk Microsoft

untuk keperluan mengetik, menghitung, presentasi, email, *database*, dan lain sebagainya. Aplikasi seperti Microsoft Word, Microsoft Excel, dan Microsoft Powerpoint menjadi seperti program wajib yang perlu dimiliki dan diinstal dalam komputer personal. Hingga saat ini, pengguna aplikasi Microsoft dunia masih menempati urutan teratas karena kemudahan dan fitur-fitur yang dimilikinya. Karena perannya yang begitu penting dan berharga bagi masyarakat, maka pada saat yang sama, risiko banyak pihak yang ingin menggonggonya pun meningkat.



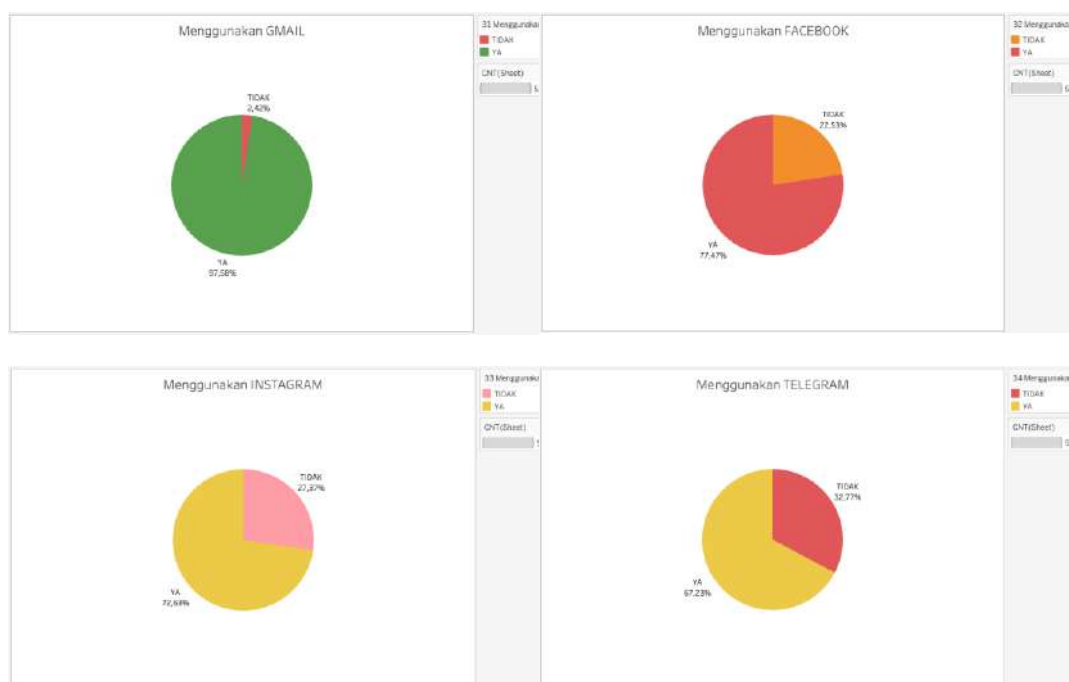
Gambar 4. 23 Grafik Kultur Menggunakan Proprietary Software

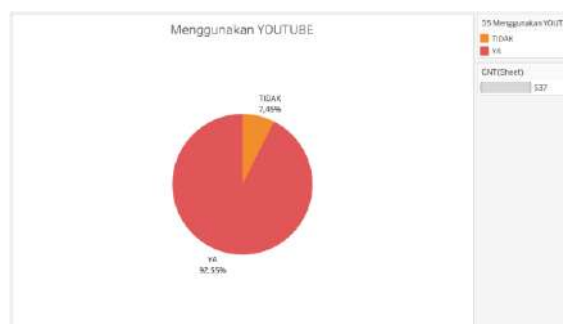
Sumber : Grafik Kultur Menggunakan Proprietary Software (hasil pengolahan data oleh peneliti)

Survei memperlihatkan bagaimana rata-rata 90% responden menggunakan seluruh program Microsoft tersebut, yang kerap menjadi sasaran utama atau antara dari para penjahat siber. Oleh karena itulah mereka harus ekstra ketat dalam menjaga keamanan yang terkait dengannya.

Menggunakan Media Sosial dan Aplikasi Komunikasi

Selain *e-commerce*, Indonesia juga sangat dikenal sebagai pengguna media sosial yang fanatik. Masyarakat Indonesia pun dikenal gemar menggunakan berbagai aplikasi komunikasi gratis yang ditawarkan via internet. Sejalan dengan manfaat yang diperoleh tersebut, menyertai pula risiko keamanan bersamanya. Hasil dari survei cukup mengejutkan. Hampir semua responden yaitu sekitar 95,58% menggunakan aplikasi gmail sebagai alamat *email* mereka. Sementara 77,47% dari mereka adalah pengguna Facebook dan 72,63% menggunakan aplikasi Instagram. Disamping itu 92,51% dari mereka juga aktif memanfaatkan Youtube dan 67,23% dari mereka pun aktif memanfaatkan aplikasi *group messenger* Telegram dalam berkomunikasi.





Gambar 4. 24 Grafik Kultur Menggunakan Media Sosial dan Aplikasi Komunikasi

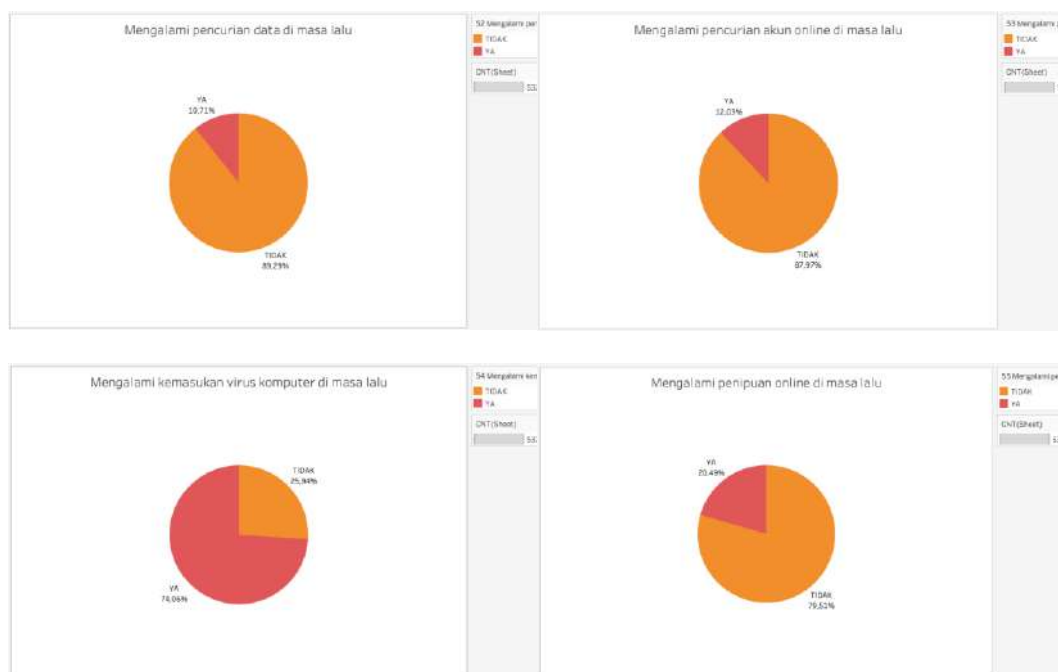
Sumber : Grafik Kultur Menggunakan Media Sosial dan Aplikasi Komunikasi

(hasil pengolahan data oleh peneliti)

Kenyataan ini memperlihatkan kecenderungan masyarakat Indonesia dalam memilih dan menggunakan aplikasi gratis yang dikembangkan negara lain. Tentu saja hal ini jika terus berlanjut akan berpotensi membahayakan kedaulatan negara karena seluruh data dan informasi penting mengalir melalui *software* dan aplikasi terkait.

Mengalami Kasus Kejahatan Siber

Pertanyaan terakhir yang diajukan dalam survei berkaitan dengan pengalaman para responden di masa lampau. Pengalaman dimaksud berhubungan dengan pernah tidaknya mereka terlibat menjadi korban kejahatan siber. Hasil survei memperlihatkan walaupun tidak banyak, yaitu sekitar 10-12%, mereka pernah mengalami kejadian pencurian data dan akun *online* di masa lalu.



Gambar 4. 25 Grafik Pengalaman Mengalami Kasus Kejahatan Siber

Sumber : Grafik Pengalaman Mengalami Kasus Kejahatan Siber

(hasil pengolahan data oleh peneliti)

Sementara 74,06% dari mereka mengaku pernah kemasukan virus komputer. Data lain memperlihatkan bahwa 20,49% dari responden pernah mengalami penipuan *online* di masa lalu. Arti dari data ini adalah bahwa pada dasarnya para responden telah dan pernah terekspos keamanan informasinya dalam dunia siber. Kenyataan ini memperlihatkan bagaimana rentannya tingkat risiko keamanan informasi masyarakat Indonesia.

Efektivitas Kebijakan Kedaulatan Pertahanan Siber di Indonesia

Hasil pengolahan data yang berkaitan secara erat dengan tingkat efektivitas keberadaan dan implementasi kebijakan kedaulatan pertahanan siber di Indonesia disaripatikan dalam tabel berikut ini.

Tabel 4. 27 Hasil Pengolahan Data Efektivitas
Kebijakan Pertahanan Siber

No	Hasil Pengolahan Data	Sumber
1	<i>“Langkah paling utama dan pertama yang dibutuhkan untuk membuat pertahanan siber yang kuat adalah dengan membenahi regulasi terlebih dahulu. Misalnya adalah dalam hal penanganan krisis siber nasional. Undang-undang yang paling penting untuk dibenahi adalah: UU Telekomunikasi, UU Siber, dan UU Perlindungan Data Publik – serta National Cyber Policy Strategy.”</i> <i>“Indonesia membutuhkan peraturan dan kebijakan yang jelas di bidang pertahanan siber, agar seluruh stakeholder menerapkannya secara bersungguh-sungguh.”</i> <i>“BSSN dan Kominfo diharapkan bekerjasama dalam mengembangkan berbagai peraturan terkait dengan pertahanan dan keamanan siber nasional.”</i>	Bisyrton Wahyudi, Mantan Manajer ID-SIRTII, Wawancara Djarot Soebiantoro, Ketua Aspiluki, Komunikasi Personal Eko Budiardjo, Ketua IPKIN, RTD
2	<i>“Pada dasarnya, hanya ada satu undang-undang yang berkaitan erat dengan siber, yaitu Undang-Undang tentang Transaksi Elektronik tahun 2008 yang telah diadendum beberapa kali. Regulasi ini didasarkan pada peraturan lawas yaitu Undang-Undang tentang Telekomunikasi tahun 1999 yang di dalamnya tidak ada sama sekali membahas masalah internet. Negara lain seperti Malaysia misalnya, setiap tahun mengeluarkan berbagai peraturan terkait dengan siber dan internet dalam sebuah wadah konsep cyberlaw peraturan terkait dengan siber dan internet dalam sebuah wadah konsep cyberlaw yang sangat komprehensif. Ada baiknya mulai dipikirkan diberlakukannya model omnibus law dalam konteks ini, mengingat begitu banyaknya sebaran peraturan yang terkait secara langsung maupun tidak langsung dengan dunia siber, seperti undang-undang mengenai: informasi publik, kerahasiaan informasi, transaksi elektronik, pertahanan negara, perdagangan elektronik, penyiaran, dan lain sebagainya.”</i>	Muhammad Salahuddien, Mantan Wakil Ketua ID-SIRTII, Wawancara

- “Sesungguhnya Indonesia baru memiliki satu regulasi terkait cyberlaw, yaitu Undang-Undang Informasi dan Transaksi Elektronik. Tentu saja ini sangat tidak memadai untuk dapat membentuk pertahanan dan keamanan siber yang kuat.”* Freddy Harris, Dirjen Kekayaan Intelektual, Komunikasi Personal
- “UU-ITE harus dilengkapi dengan undang-undang lain karena tidak semua permasalahan dan tantangan siber dapat diselesaikan olehnya.”* Mizamil, Pakar Cyber Law, Komunikasi Personal
- 3 *“UU PDP dan UU KIP yang saling berlawanan dikembangkan secara terbalik. Dimana UU KIP dulu baru UU PDP, sementara di tempat lain justru UU PDP dahulu baru UU KIP. Di sinilah ada kesalahan paradigma yang mendasar. Bahkan disinyalir UU PDP tidak perlu karena ada 30 UU di Indonesia yang memiliki unsur PDP di dalamnya.”* Rudi Luhmanto, Ketua CSIRT.id, Wawancara
- “Banyak masyarakat Indonesia terutama kalangan milenial yang tidak begitu peduli dengan privacy-nya, apalagi belum ada undang-undang yang mengaturnya.”* Mizamil, Pakar Cyber Law, Komunikasi Personal
- “Regulasi dan Undang-Undang dalam bidang kerahasiaan informasi, keterbukaan publik, dan keamanan privacy harus disusun serta dikembangkan secara simultan.”* Eko Budiardjo, Ketua IPKIN, Komunikasi Personal
- 4 *“Kerjasama antara institusi di Indonesia dengan berbagai pihak masih bersifat sporadis, sektoral, dan tidak terkoordinasi dengan baik. Ada berbagai jenis kerjasama yang harus segera dibangun, dengan kategori sebagai berikut: intra-state cooperation, multilateral agreements, international fora, public-private partnerships, dan inter-agency partnerships.”* Ardi Sutedja, Ketua ICSF, Wawancara
- “Isu siber bukan hanya milik BSSN atau Kominfo semata, melainkan harus menjadi perhatian seluruh sektor pemerintahan.”* Dominggus Pakel, Mantan Kapusdatin Kemhan, Diskusi
- “Sangat perlu dikembangkan public-private partnerships untuk meningkatkan kualitas pertahanan dan keamanan siber di Indonesia.”* Soegiharto Santoso, Ketua Apkomindo,

		Personal Komunikasi
5	<i>“Masalah legal yang harus diperhatikan sungguh-sungguh tidaklah sebatas pada ada tidaknya peraturan atau kebijakan, namun memiliki sejumlah spektrum seperti: cyber criminal legislation, substantive law, procedural cybercriminal law, dan cybersecurity regulation.”</i> <i>“Negara harus melindungi warganegaraanya di bidang siber melalui berbagai regulasi yang mengaturnya.”</i> <i>“Masyarakat dan komunitas harus turut berperan aktif dalam mendorong agar kebijakan di bidan siber benar-benar disusun dan dikembangkan oleh pemerintah dan/atau wakil rakyat.”</i>	Freddy Harris, Dirjen Kekayaan Intelektual, Komunikasi Personal Ahmad Ramli, Dirjen Kominfo, Webinar Rapim Mudiardjo, Pakar Cyber Law, Wawancara

Sumber : Hasil Pengolahan Data Efektivitas Kebijakan Pertahanan Siber

(hasil pengolahan data oleh peneliti)

Kajian berikutnya yang dilakukan dalam penelitian ini adalah menginventarisasi berbagai regulasi dan kebijakan pokok yang berkaitan secara langsung dengan pertahanan dan keamanan siber. Regulasi dimaksud dibatasi pada tingkatan undang-undang, peraturan pemerintah, peraturan presiden, dan perturan menteri. Tabel 4.28 memperlihatkan sebagian besar dari regulasi penting yang berkaitan dengan pertahanan dan keamanan siber yang diundangkan di Indonesia semenjak tahun 1999 hingga sekarang.

Tabel 4. 28 Daftar Peraturan dan Kebijakan Seputar Siber

No	Regulasi	Tentang/Ruang Lingkup
UNDANG-UNDANG REPUBLIK INDONESIA		
1	Undang-Undang Republik Indonesia Nomor 36 tahun 1999	Telekomunikasi

2	Undang-Undang Republik Indonesia Nomor 11 tahun 2008	Informasi dan Transaksi Elektronik
3	Undang-Undang Republik Indonesia Nomor 8 tahun 2010	Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang
4	Undang-Undang Republik Indonesia Nomor 3 tahun 2011	Transfer Dana
5	Undang-Undang Republik Indonesia Nomor 19 tahun 2016	Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
6	Undang-Undang Republik Indonesia Nomor 9 tahun 2017	Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 tahun 2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan menjadi Undang-Undang
7	Undang-Undang Republik Indonesia Nomor 5 tahun 2018	Perubahan atas Undang-Undang Nomor 15 tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang

PERATURAN PEMERINTAH REPUBLIK INDONESIA

1	Peraturan Pemerintah Republik Indonesia Nomor 52 tahun 2000	Penyelenggaraan Telekomunikasi
2	Peraturan Pemerintah Republik Indonesia Nomor 58 tahun 2012	Penyelenggaraan Sistem dan Transaksi Elektronik
3	Peraturan Pemerintah Republik Indonesia Nomor 71 tahun 2019	Penyelenggaraan Sistem dan Transaksi Elektronik
4	Peraturan Pemerintah Republik Indonesia Nomor 46 tahun 2021	Pos, Telekomunikasi, dan Penyiaran

PERATURAN PRESIDEN REPUBLIK INDONESIA

1	Peraturan Presiden Republik	Badan Siber dan Sandi Negara

Indonesia Nomor 53 Tahun 2017

2	Peraturan Presiden Republik Indonesia Nomor 133 Tahun 2017	Perubahan Peraturan Republik Indonesia Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara
3	Peraturan Presiden Republik Indonesia Nomor 95 tahun 2018	Sistem Pemerintahan Berbasis Elektronik

PERATURAN MENTERI REPUBLIK INDONESIA

1	Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 tahun 2014	Pedoman Pertahanan Siber
2	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 26/Per/M.Kominfo/5/2007 tanggal 4 Mei 2007	Pengamanan Pemanfaatan Jaringan Telekomunikasi berbasis Protokol Internet
3	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 29/Per/M.Kominfo/12/2010	Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet
4	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 14/ Per/M. Kominfo /04/2011 tanggal 2 Mei 2011	Standar Kualitas Pelayanan Jasa Internet Teleponi untuk Keperluan Publik
5	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 24/ Per/M. Kominfo /12/2011 tanggal 7 Desember 2011	Perubahan Ketiga atas Peraturan Menteri Komunikasi dan Informatika Nomor 26/ Per /M.Kominfo/05/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi berbasis Protokol Internet
6	Peraturan Menteri Komunikasi dan Informatika Nomor 8 tahun 2014 tanggal 4 Februari 2014	Persyaratan Teknis Alat dan Perangkat Penyadapan yang Sah atas Informasi berbasis Protokol pada Penyelenggaraan Jaringan Bergerak Seluler dan Jaringan Tetap Lokal Tanpa Kabel dengan Mobilitas

		Terbatas
7	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 19 tahun 2014 tanggal 17 Juli 2014	Penanganan Situs Internet Bermuatan Negatif
8	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 2 tahun 2016	Penyampaian Informasi Kebencanaan melalui Jaringan Bergerak Seluler
9	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 tahun 2016	Sistem Manajemen Pengamanan Informasi
10	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 6 tahun 2017 tanggal 7 Februari 2017	Penyelenggaraan Layanan Televisi Protokol Internet
11	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 8 tahun 2017 tanggal 7 Februari 2017	Penyelenggaraan Jasa Internet Teleponi untuk Keperluan Publik
12	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 14 tahun 2017	Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 12 tahun 2016 tentang Registrasi Pelanggan Jasa Telekomunikasi
13	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 3 tahun 2018 tanggal 5 Juni 2018	Organisasi dan Tata Kerja Badan Aksesibilitas Telekomunikasi dan Informasi
14	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 12 tahun 2018 tanggal 24 September 2018	Penyelenggaraan Telekomunikasi Khusus untuk Keperluan Instansi Pemerintah atau Badan Hukum
15	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 14 tahun 2018 tanggal 2 Oktober 2018	Rencana Dasar Tekniks Telekomunikasi Nasional
16	Peraturan Menteri Komunikasi	Ketentuan Operasional Sertifikasi Alat

	dan Informatika Republik Indonesia Nomor 16 tahun 2018 tanggal 31 Desember 2018	dan/atau Perangkat Telekomunikasi
17	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 tahun 2019 tanggal 28 Juni 2019	Persyaratan Teknis Alat dan/atau Perangkat Telekomunikasi untuk Keperluan Penyelenggaraan Televisi Siaran dan Radio Siaran
18	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 tahun 2020	Penyelenggara Sistem Elektronik Lingkup Privat
19	Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 1 tahun 2021	Perubahan Kedua atas Peraturan Menteri Komunikasi dan Informatika Nomor 13 tahun 2019 tentang Penyelenggaraan Jasa Telekomunikasi

PERATURAN DAN KEPUTUSAN PANGLIMA TNI

1	Peraturan Panglima TNI Nomor 17 tahun 2017 tanggal 18 Maret 2017	Organisasi dan Tugas Satuan Siber Tentara Nasional Indonesia
2	Keputusan Panglima TNI Nomor Kep/874/IX/2018 tanggal 3 September 2018	Grand Design Satuan Siber TNI
3	Keputusan Panglima TNI Nomor Kep/1355/XII/2018 tanggal 18 Desember 2018	Doktrin Siber Tentara Nasional Indonesia
4	Peraturan Panglima TNI Nomor 71 tahun 2019 tanggal 30 Desember 2019	Organisasi Satuan Satuan Penindakan Siber

PERATURAN BADAN SIBER DAN SANDI NEGARA

1	Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2018	Visi Misi Badan Siber dan Sandi Negara
2	Peraturan Badan Siber dan Sandi Negara Nomor 5 tahun 2018	Rencana Strategis Badan Siber dan Sandi Negara tahun 2018-2019
3	Peraturan Badan Siber dan Sandi Negara Nomor 7 tahun 2018	Pembentukan Regulasi Badan Siber dan Sandi Negara

4	Peraturan Badan Siber dan Sandi Negara Nomor 12 tahun 2018	Organisasi Pengelola Informasi dan Dokumentasi Badan Siber dan Sandi Negara
5	Peraturan Badan Siber dan Sandi Negara Nomor 1 tahun 2019	Organisasi dan Tata Kerja Balai Deteksi Sinyal
6	Peraturan Badan Siber dan Sandi Negara Nomor 2 tahun 2019	Organisasi dan Tata Kerja Sertifikasi Elektronik
7	Peraturan Badan Siber dan Sandi Negara Nomor 7 tahun 2019	Pengadaan Barang/Jasa yang Bersifat Rahasia di Badan Siber dan Sandi Negara
8	Peraturan Badan Siber dan Sandi Negara Nomor 10 tahun 2019	Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah
9	Peraturan Badan Siber dan Sandi Negara Nomor 13 tahun 2019	Penghapusan Barang Milik Negara yang Bersifat Rahasia di Lingkungan Badan Siber dan Sandi Negara
10	Peraturan Badan Siber dan Sandi Negara Nomor 14 tahun 2019	Pengelolaan Kinerja di Badan Siber dan Sandi Negara
11	Peraturan Badan Siber dan Sandi Negara Nomor 5 tahun 2020	Rencana Strategis Badan Siber dan Sandi Negara tahun 2020-2024
12	Peraturan Badan Siber dan Sandi Negara Nomor 7 tahun 2020	Pemberian Rekomendasi dan Pemberian Register Lemabga Sertifikasi Profesi Bidang Keamanan Siber
13	Peraturan Badan Siber dan Sandi Negara Nomor 8 tahun 2020	Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik
14	Peraturan Badan Siber dan Sandi Negara Nomor 9 tahun 2020	Organisasi dan Tata Kerja Badan Siber dan Sandi Negara
15	Peraturan Badan Siber dan Sandi Negara Nomor 10 tahun 2020	Tim Tanggap Insiden Siber
16	Peraturan Badan Siber dan Sandi Negara Nomor 11 tahun 2020	Kamus Kompetensi Teknis Bidang Keamanan Siber dan Persandian

REGULASI TERKAIT LAINNYA

- A Keputusan Panglima Tentara Nasional Indonesia
- B Keputusan Kepala Kepolisian Republik Indonesia
- C Keputusan Kepala Badan Intelijen Negara
- D Peraturan Badan Nasional Penanggulangan Terorisme
- E Keputusan Kepala Badan Narkotika Nasional
- F Peraturan Kepala Pusat Pelaporan dan Analisis Transaksi Keuangan

Sumber : Daftar Peraturan dan Kebijakan Seputar Siber (hasil pengolahan data oleh peneliti)

Jika dilakukan kajian secara sungguh-sungguh terkait dengan peraturan yang ada, ruang lingkup, beserta sejarah kelahirannya, maka dapat disimpulkan bahwa lahirnya seluruh peraturan perundang-undangan yang berlaku lebih bersifat sporadis dan insidental. Tidak ada kerangka komprehensif dan holistik yang dikembangkan sebagai dasar dalam menyusun seluruh undang-undang dan peraturan yang berlaku. Pada penelitian ini dilakukan pula survei untuk melihat pandangan masyarakat terkait dengan efektivitas regulasi yang selama ini disusun dan diterapkan. Sebanyak kurang lebih 213 responden dari para praktisi dan komunitas terkait dengan pertahanan siber ditanyakan pendapatnya dan di bawah ini adalah hasilnya.

Pertama, hampir semua responden (95,74%) sepakat bahwa serangan siber berpotensi membahayakan kedaulatan bangsa dan negara. Hasil ini selaras dengan berbagai studi di dunia yang beranggapan bahwa serangan siber tidak akan pernah berhenti sejalan dengan perkembangan teknologi informasi dan komunikasi. Setiap teknologi yang memberikan manfaat pasti mengandung risiko yang menyertainya. Perang siber adalah model agitasi antar negara dalam abad global yang akan terus terjadi karena mudah diluncurkannya, murah biayanya, dan masif dampaknya.

Tabel 4. 29 Hasil Survei terkait Bahaya Serangan Siber terhadap Hanneg

Apakah anda setuju serangan siber dapat membahayakan kedaulatan bangsa dan keselamatan masyarakat?

Jawaban	Persentase
Setuju	95,74%
Tidak Setuju	0,00%
Ragu-Ragu	4,26%

Sumber : Hasil Survei terkait Bahaya Serangan Siber terhadap Hanneg (hasil pengolahan data oleh peneliti)

Kedua, mayoritas responden menganggap bahwa ancaman terhadap serangan siber berasal dari dalam maupun luar negeri (76,60%). Hal ini mengandung arti bahwa Indonesia harus mampu membuat pertahanan yang kuat untuk mencegah serangan musuh yang datang dari luar negara maupun dari dalam negeri sendiri. Data serangan dari ID-SIRTII memperlihatkan tingginya serangan terhadap situs-situs negara yang berasal dari dalam negeri Indonesia sendiri.

Tabel 4. 30 Hasil Survei terkait Sumber Serangan Siber

Menurut anda, mayoritas ancaman siber datang dari mana?

Jawaban	Persentase
Luar Negeri	19,15%
Dalam Negeri	4,26%
Kombinasi Keduanya	76,60%

Sumber : Hasil Survei terkait Sumber Serangan Siber (hasil pengolahan data oleh peneliti)

Ketiga, hal menarik ditemukan dalam survei ini ketika sebagian besar responden berpendapat bahwa pada hakekatnya Indonesia saat ini belum berdaulat di bidang pertahanan siber (83,83%). Kenyataan tersebut tidak begitu mengejutkan bila sering mengikuti konferensi atau seminar di bidang pertahanan siber yang memperlihatkan banyaknya kekhawatiran para pemangku kepentingan terhadap tidak dapatnya negara mengendalikan isu dimaksud. Jika hal ini dibiarkan berlarut-larut akan sangat membahayakan pertahanan negara dan keselamatan masyarakat.

Tabel 4. 31 Hasil Survei terkait Kedaulatan Siber

Menurut anda, apakah Indonesia sudah berdaulat di bidang pertahanan siber?

Jawaban	Persentase
Sudah	10,64%
Belum	83,83%
Ragu-Ragu	25,53%

Sumber : Hasil Survei terkait Kedaulatan Siber (hasil pengolahan data oleh peneliti)

Keempat, walaupun dipersepsikan belum berdaulatnya negara di ranah siber, namun mayoritas responden (89,36%) percaya bahwa pada dasarnya SDM Indonesia mampu membangun pertahanan siber yang kuat. Keyakinan ini sangatlah penting di tengah-tengah kenyataan bahwa hampir seluruhnya perangkat teknologi yang berada dalam ekosistem siber adalah produksi luar negeri.

Tabel 4. 32 Hasil Survei terkait Potensi Kemampuan SDM Indonesia

Apakah menurut anda SDM Indonesia mampu membangun pertahanan siber yang kuat?

Jawaban	Persentase
Mampu	89,36%
Tidak Mampu	4,26%
Ragu-Ragu	6,38%

Sumber : Hasil Survei terkait Potensi Kemampuan SDM Indonesia (hasil pengolahan data oleh peneliti)

Kelima, kurang lebih 61,70% responden merasa bahwa saat ini Indonesia belum memiliki kebijakan siber yang efektif. Kebijakan yang dimaksud adalah seluruh bentuk peraturan dari mulai undang-undang hingga peraturan atau keputusan menteri. Masih banyaknya kejadian tak diinginkan adalah bukti dari kepercayaan ini.

Tabel 4. 33 Hasil Survei terkait Kebijakan Siber di Indonesia

Apakah menurut anda Indonesia telah memiliki kebijakan siber yang efektif untuk mengatasi serangan siber?

Jawaban	Persentase
Sudah	8,51%
Belum	61,70%
Ragu-Ragu	29,79%

Sumber : Hasil Survei terkait Kebijakan Siber di Indonesia (hasil pengolahan data oleh peneliti)

Keenam, jawaban berbeda-beda terlihat ketika responden ditanyakan mengenai pendapat mereka terkait pihak mana yang perlu mengambil alih pimpinan apabila terjadi serangan masif ke infrastruktur kritis nasional. Sebanyak 31,91% mengatakan bahwa Panglima TNI yang harus memimpin, sementara

27,66% lebih memilih Ketua BSSN. Sementara pada layer kedua yang dikatakan pantas menjadi pimpinan adalah Presiden RI (17,02%) dan Menteri Kominfo (14,89%).

Tabel 4. 34 Hasil Survei terkait Pimpinan pada Serangan Siber Masif

Siapakah yang bertanggung jawab untuk menjadi pimpinan dalam menghadapi serangan siber masif yang mengganggu infrastruktur kritis/vital nasional?

Jawaban	Persentase
Presiden RI	17,02%
Ketua BSSN	27,66%
Panglima TNI	31,91%
Menteri Kominfo	14,89%
Kapolri	2,13%
Lain-Lain (Ketua Satgas, Institusi Independen, Semua Pihak)	6,39%

Sumber : Hasil Survei terkait Pimpinan pada Serangan Siber Masif (hasil pengolahan data oleh peneliti)

Ketujuh, terkait dengan strategi pertahanan siber, sangat menarik ketika mayoritas menganggap bahwa Indonesia perlu menggunakan kedua pendekatan ofensif dan defensif dalam menghadapi serangan yang terjadi (76,60%). Tentu saja pandangan ini menarik untuk dicermati terutama jika dikaitkan dengan prinsip politik luar negeri Indonesia yang bebas dan aktif.

Tabel 4. 35 Hasil Survei terkait Strategi Pertahanan Siber

Strategi pertahanan siber seperti apakah yang tepat untuk Indonesia?

Jawaban	Persentase
Ofensif	0,00%

Defensif	23,40%
Keduanya	76,60%

Sumber : Hasil Survei terkait Strategi Pertahanan Siber (hasil pengolahan data oleh peneliti)

Model Pertahanan Siber Ideal yang Holistik dan Komprehensif

Hasil pengolahan data yang berkaitan secara erat dengan pencarian model pertahanan siber ideal yang holistik dan komprehensif dalam sebuah ekosistem disaripatikan dalam tabel berikut ini.

Tabel 4. 36 Hasil Pengolahan Data Model Pertahanan Siber Ideal

No	Hasil Pengolahan Data	Sumber
1	<i>“Ekosistem pertahanan siber yang holistik dan komprehensif harus terdiri dari dua unsur utama, masing-masing adalah infrastruktur dan suprastuktur. Infrastruktur negara yang dikembangkan tidak diimbangi dengan bangunan suprastruktur yang kuat. Suprastruktur yang kuat harus dibangun dengan pola pikir yang benar, kehendak yang kokoh, dan motivasi tinggi untuk membangun negara. Semangat merah putih harus menjadi dasar bagi segalanya.”</i> <i>“Pemutakhiran dan doktrin pertahanan negara harus cepat diselesaikan agar Indonesia terhindar dari berbagai ancaman kontemporer yang membahayakan. Melihatnya harus secara utuh dan komprehensif, jangan sporadis dan sepotong-sepotong.”</i> <i>“Siber adalah sebuah ekosistem dimana di dalamnya terdiri dari berbagai komponen yang saling mempengaruhi satu dan lainnya.”</i>	Kemal Stamboel, Mantan Ketua Komisi I DPR-RI, Wawancara Agus Widjojo, Gubernur Lemhannas, Wawancara Hinsa Siburian, Kepala BSSN, Wawancara
2	<i>“Badan siber nasional harus diberikan wewenang yang cukup untuk dapat berfungsi secara efektif dalam</i>	Charles Liem,

- mencegah, menghadapi, dan mengantisipasi berbagai serangan siber. Disamping itu koordinasi antar institusi pemerintah dan stakeholder lain sangat lemah. Sangat jarang dilakukan latihan atau drill di bidang insiden siber misalnya.” Peneliti Swiss-German University, Wawancara
- “Setiap negara memiliki leading sector yang berperan aktif dalam memperkuat dan mengamankan sistem siber negara.” Muhammad Salman, Pakar Siber Universitas Indonesia, Diskusi
- “BSSN sangat diharapkan menjadi institusi yang akan memimpin Indonesia dalam bidang siber, sebagaimana telah diamanatkan oleh regulasi.” Bambang Permantoro, Mantan Penasehat ID-SIRTII, Komunikasi Personal
- 3 “Sumber daya manusia adalah segalanya dalam ekosistem siber, karena merekalah yang merencanakan, mengatur, dan mengendalikan tata kelola pertahanan maupun ketahanan dalam dunia maya. Oleh karena itulah maka pelaku kuncinya harus memiliki kompetensi yang sesuai dengan kebutuhan. Standar Kompetensi Kerja Nasional Indonesia (SKKNI) di bidang keamanan siber merupakan salah satu referensi yang dapat dijadikan sebagai acuan pengembangan SDM.” Eko Budiardjo, Ketua IPKIN, RTD
- “Indonesia memiliki modal yang kuat untuk dapat mengembangkan profesional di bidang siber.” Made Wiryana, Pakar Siber Universitas Gunadarma, Diskusi
- “Perguruan tinggi harus memiliki kurikulum di bidang keamanan internet agar dapat menciptakan SDM yang handal dalam bidang yang sangat dibutuhkan tersebut.” Tintin, EC-Council, Diskusi
- 4 “Memahami isu pertahanan dan keamanan siber nasional tidak dapat dilakukan secara sporadis atau sepotong-sepotong. Hal tersebut harus dilihat secara utuh ‘end-to-end’ atau dari hulu ke hilir, terutama dalam menghadapi yang disebut sebagai perang generasi

kelima”.

<i>“Indonesia perlu memiliki kerangka pertahanan siber yang holistik dan komprehensif, yang melibatkan beragam stakeholder yang saling bekerjasama satu dan lainnya.”</i>	Zainal Hasibuan, Anggota Wantiknas, RTD
<i>“Cyber Roadmap ke depan harus dimiliki Indonesia agar dapat berdaulat secara penuh di ruang siber.”</i>	Hammam Riza, Kepala BPPT, FGD
5 <i>“BSSN harus memilih salah satu dari tiga layer (kebijakan, teknologi, dan kesiapan personal), bukan ingin mengurus semua. Layer dimaksud adalah sesuai dengan kewenangannya.”</i>	Rudi Luhmanto, Ketua CSIRT.id, RTD
<i>“Sebagai institusi yang diberikan amanah di bidang keamanan siber, BSSN bekerja keras untuk dapat belajar dan melayani masyarakat yang membutuhkannya.”</i>	Hinsa Siburian, Kepala BSSN, FGD
<i>“Jika BSSN bertanggung jawab terhadap keamanan siber, Kemenhan harus dapat menjaga pertahanan siber agar kuat dan kokoh, serta berdaulat penuh.”</i>	Ardi Sutedja, Ketua ICSF, RTD

Sumber : Hasil Pengolahan Data Model Pertahanan Siber Ideal (hasil pengolahan data oleh peneliti)

Doktrin adalah prinsip dasar yang dipergunakan oleh institusi negara seperti militer dan lembaga terkait lainnya dalam mengambil langkah-langkah strategis dalam rangka mewujudkan tujuan negara. Prinsip ini akan menjadi pijakan dalam melakukan sejumlah operasional siber yang dianggap perlu bagi kepentingan negara (Andreas, 2004). Ada empat hal utama yang harus dipertimbangkan setiap kali sebuah operasional siber diluncurkan, yaitu: (i) *method of delivery*; (ii) *strict liability*; (iii) *direct result*; dan (iv) *consequences* (Durante, 2014; Gervais, 2011). Keberadaan perang siber harus menjadi sebuah kesadaran sebagai sesuatu yang sedang terjadi di seluruh dunia, sehingga tingkat kepentingan dan kegentingan harus dinaikkan ke level negara. Prinsip-

prinsip perang siber harus dimasukkan ke dalam doktrin pertahanan negara secara eksplisit (Dinstein, 2012). Perang siber harus didefinisikan secara tegas dan dihubungkan keterkaitannya dengan ancaman serius yang dihadapi negara pada masa kini dan mendatang (Hughes, 2017). Konsep kedaulatan siber harus didefinisikan dan disosialisasikan sebagai bagian tak terpisahkan dari doktrin siber demi menjaga keutuhan negara dan pencapaian tujuan negara (Khanna, 2018).

Dalam sektor pertahanan, doktrin menjadi panduan militer dalam merancang dan menjalankan peran strategisnya dalam kehidupan berbangsa maupun bernegara. Doktrin militer konvensional biasanya bertumpu pada tiga domain wilayah, yaitu: darat, laut, dan udara. Sejumlah negara besar seperti Amerika memiliki tambahan dua arena, yaitu: antariksa dan siber. Siber dianggap sebagai sebuah arena virtual dimana peperangan dan perebutan kekuasaan moderen terjadi. Fenomena mengenai peran penting dan kriticalnya dunia siber dalam kehidupan manusia moderen telah menempatkan keberadaanya sebagai sebuah wilayah yang harus dikelola secara serius dan sungguh-sungguh.

Doktrin siber Amerika Serikat menempatkan keberadaan dan peran strategis siber dalam dua aspek inti, yaitu dalam konteks *Cyberspace Operation (CO)* dan *Information Assurance (IA)*. Dalam konteks CO, dunia siber dianggap sebagai sebuah wilayah global yang dibangun dari berbagai jejaring digital yang terhubung satu dan lainnya. CO dianggap begitu penting karena seluruh agenda pertahanan Amerika Serikat dapat diwujudkan melalui aktivitas operasional yang terjadi dalam ranah virtual ini. Disamping itu melalui operasi siber, Amerika Serikat dapat mewujudkan seluruh agenda militernya melalui berbagai cara, seperti: manipulasi informasi, penyerangan sumber daya komputasi, penyadapan intelijen, pelaksanaan propaganda, dan lain sebagainya. Sementara aspek IA bertumpu pada prinsip bahwa negara harus memiliki superioritas terhadap penguasaan data dan informasi global. Karena dengan menguasai informasi, maka sebuah negara dapat menguasai dunia (Andress & Winterfeld, 2014a).

Doktrin negara China bermula dari ambisi untuk mengejar ketertinggalannya atau inferioritasnya terhadap musuh besarnya, yaitu Amerika

Serikat. Pemerintah China memutuskan untuk “membangun sendiri” arena dan teknologi sibernya agar tidak memiliki ketergantungan dari negara besar manapun. Mereka memiliki sebuah doktrin yang bertumpu pada prinsip bahwa keberadaan siber membawa sebuah fenomena baru yaitu “*unrestricted warfare*” – wilayah dan cara perang tanpa ruang dan batas. Senada dengan Taiwan, kedua negara besar ini membangun doktrinnya di atas sejumlah prinsip, seperti: informasi adalah alat untuk mengendalikan negara lain, perang moderen pada dasarnya adalah perang elektronik, perang informasi adalah inti dari integrasi kekuatan politik-ekonomi-diplomatik-militer, kunci sukses adalah kemenangan pada *intagible war* yang tak terlihat tapi dapat dirasakan akibatnya, dan semua orang adalah serdadu dalam perang siber (Shen, 2016; Zeng et al., 2017).

Jepang mengembangkan doktrin sibernya di atas prinsip untuk melindungi negara – terutama pemerintah – dari berbagai serangan, terutama yang melibatkan kekuatan militer. Pembentukan NISC (National Information Security Center) menggambarkan keseriusan pemerintah Jepang dalam mengintegrasikan doktrin siber yang diadopsi dengan doktrin pertahanan negara yang dimiliki oleh Kementerian Pertahanan (Andress & Winterfeld, 2011).

Dua negara musuh bebuyutan yaitu Korea Utara dan Korea Selatan memiliki kemiripan dalam konteks doktrin sibernya ditujukan untuk memperkuat kekuatan militernya melalui penguasaan terhadap perang siber dan perang asimetrik, keduanya melalui pendekatan ofensif dan intelijen. Pihak Korea Utara sadar bahwa hanya dengan perang asimetrilah mereka bisa memiliki *leverage* terhadap Korea Selatan. Sebaliknya Korea Selatan paham betul bahwa dengan metoda ofensif berbasis intelijen, maka mereka dapat senantiasa membaca dan memprediksi gerak gerak Korea Utara.

Negara-negara Eropa memiliki pendekatan doktrin yang cukup berbeda, yaitu dengan secara kolektif membentuk CCD COE (Cooperative Cyber Defense Center of Excellence) yang berpusat di Tallinn-Estonia untuk memperkuat kapabilitas pertahanan siber NATO. Mereka sadar bahwa serangan terhadap NATO dapat dilakukan via siber dengan menggunakan negara-negara kecil di Eropa sebagai batu loncatan virtualnya. Dalam CCD COE inilah seluruh doktrin siber negara-negara NATO diselaraskan, terlepas dari perbedaan politik

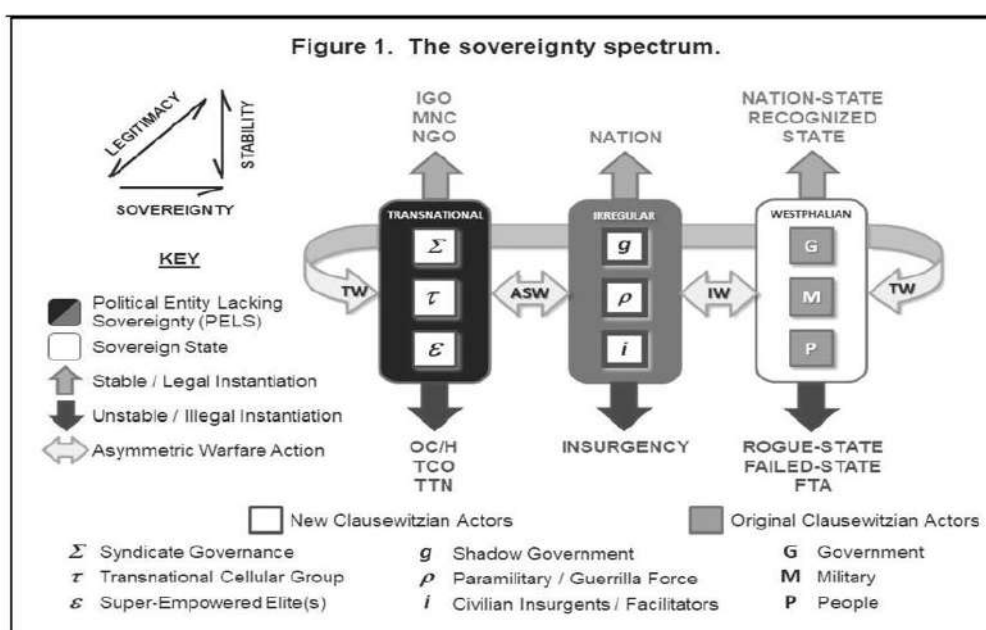
dan hukum yang dianut masing-masing anggotanya. Butuh waktu bertahun-tahun bagi mereka untuk menyelaraskan gerakannya (Hunker, 2010; Lewis, 2015). Inggris di pihak lain menyusun doktrin sibernya bersamaan dengan strategi keamanan siber, dimana keamanan dan ketahanan dunia siber merupakan kunci dari keamanan nasional karena merupakan arena lalu lintas informasi penting. Doktrin dikembangkan untuk melindungi berbagai sistem informasi strategis dari eksploitasi kriminal dari dalam maupun luar negara. Penanggungjawabnya adalah UK Office of Cybersecurity dan UK Cybersecurity Operations Center (Al-Shamisi, 2014).

Sementara negara tetangganya yaitu Perancis menempatkan doktrinnya dalam konteks perang siber. Buku putih mengenai dua aspek penting yaitu konsep baru pertahanan siber dan pengembangan kemampuan penyerangan dalam perang siber dijadikan dasar dalam melakukan berbagai gerakan maupun inisiatif militer. Pemerintah Perancis merasa yakin bahwa siber harus diintegrasikan ke dalam domain militer karena keselarasan peran dan fungsinya bagi negara (Laudrain, 2019).

Adapun negara-negara Nordik seperti Finlandia, Norwegia, dan Swedia memiliki doktrin yang bervariasi. Finlandia berusaha untuk menjadi pemain unggul dalam bidang keamanan informasi dan pertahanan siber secara kolektif nasional maupun dalam kematangan literasi masing-masing individu masyarakatnya. Sementara Norwegia bertujuan untuk melindungi masyarakatnya dari serangan siber yang dapat mengganggu keberlangsungan negaranya yang memiliki banyak sumber daya ekonomi. Swedia lebih tertarik memfokuskan doktrinnya pada kemampuan melakukan serangan dan bertahan terhadap berbagai serangan siber canggih dari pihak lawan. Di sinilah maka mereka menyusun strategi siber yang disatukan dengan kekuatan militer yang dimiliki ("Securing a Small Nation Scotland, Democratic Politics," 2017). Doktrin menarik dimiliki oleh Cekoslovakia, dimana doktrin siber mereka ditujukan untuk melindungi ancaman terhadap infrastruktur teknologi informasi yang dimiliki. Mereka menganggap pentingnya melindungi sistem teknologi informasi dan komunikasi dimaksud karena merupakan urat nadi dari jalannya pemerintahan dan penyelenggaraan negara (Boeke, 2018). Indonesia dianggap belum memiliki

doktrin siber atau politik siber sebagaimana diperlihatkan pada negara-negara lain. Ada dua pilihan yang biasa diambil dalam rangka mengelola sistem pertahanan siber yang berdaulat. Pertama adalah memutakhirkan doktrin pertahanan negara yang dimiliki sehingga unsur siber terintegrasi di dalamnya. Atau pendekatan kedua dimana terdapat doktrin pertahanan siber sendiri yang berdiri sejajar atau menjadi sub-bagian dari doktrin pertahanan negara terkait.

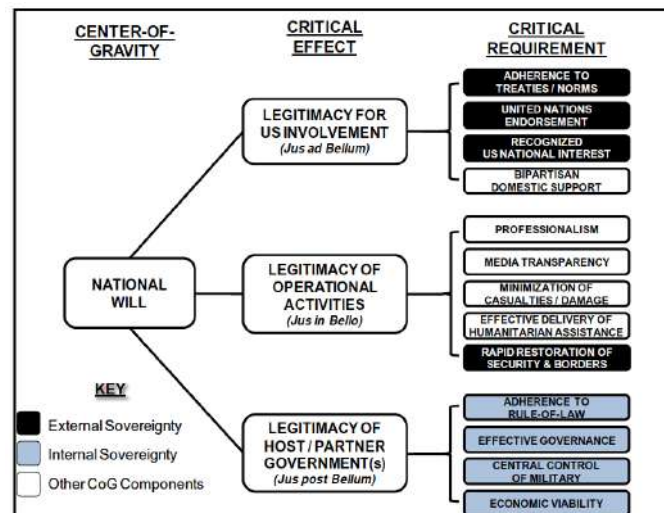
Kedaulatan siber tidak berada di ruang hampa, melainkan memiliki sejumlah spektrum yang melibatkan berbagai aktor.



Gambar 4. 26 Spektrum Kedaulatan Siber Amerika Serikat

Sumber : Spektrum Kedaulatan Siber Amerika Serikat (Khanna, 2018)

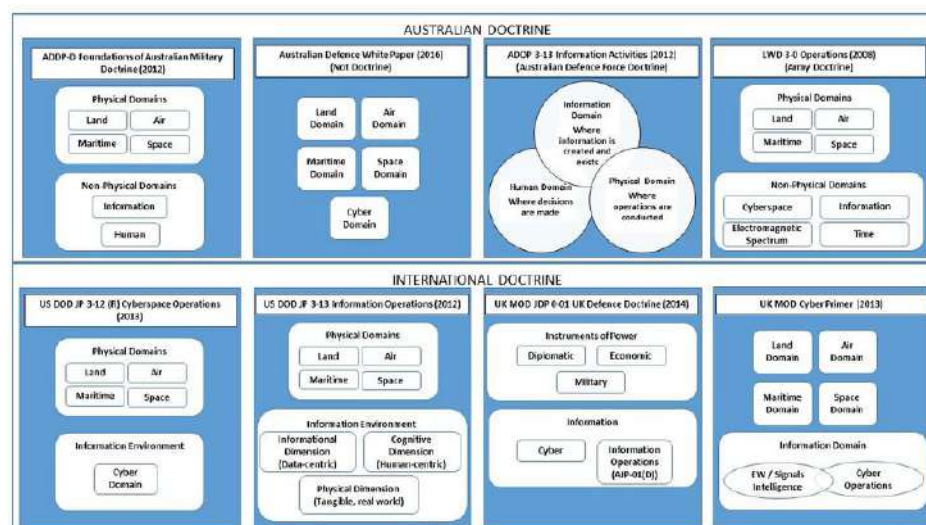
Contohnya adalah Amerika Serikat yang secara jelas dan detil mengidentifikasi komponen dari kedaulatan dimaksud.



Gambar 4. 27 Komitmen Nasional dan Politik Pertahanan Siber

Sumber : Komitmen Nasional dan Politik Pertahanan Siber (Ormrod, 2016)

Australia, UK, dan US (internasional) mengembangkan kerangka doktrin yang sangat jelas dan komprehensif, serta mudah dipahami banyak orang (Ormrod, 2016).



Gambar 4. 28 Anatomi Doktrin Pertahanan Siber Australia dan Global

Sumber : Anatomi Doktrin Pertahanan Siber Australia dan Global (Ormrod, 2016)

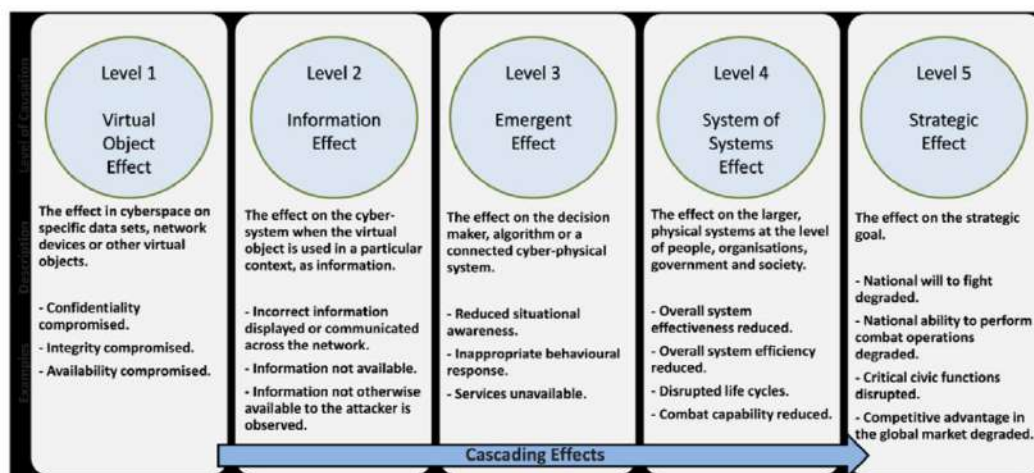
Disamping itu dikembangkan pula sejumlah kerangka komprehensif sebagai pendukungnya, seperti *Cyber conceptual framework components and effects of a cyber-attack*, sebagai berikut:



Gambar 4. 29 Kerangka Konseptual Serangan Siber Nasional

Sumber : Kerangka Konseptual Serangan Siber Nasional (Ormrod, 2016)

dan *The cyber conceptual framework cyber-attack causal chain* sebagai berikut:



Gambar 4. 30 Tingkatan Serangan Siber Negara

Sumber : Tingkatan Serangan Siber Negara (Ormrod, 2016)

Doktrin bukan merupakan sesuatu yang dogmatis dan tidak terbantahkan, justru sebaliknya, doktrin militer yang baik akan menyesuaikan dengan lingkungan operasi yang aktual, adaptif dengan segala bentuk situasi dan dapat dipahami serta dilaksanakan mulai dari pimpinan TNI sampai dengan prajurit pelaksana di lapangan dan doktrin harus aplikatif menyesuaikan dengan sifat peperangan. Sehingga untuk mendukung kesiapan TNI dalam menghadapi fenomena perang hibrida, doktrin TNI harus dapat menyesuaikan dengan perkembangan peperangan yang aplikatifnya pada taktik yang dioperasionalkan di lapangan. Taktik harus menyesuaikan dengan lingkungan operasi dan sifat dari musuh yang akan dihadapi, jangan sampai taktik peperangan yang digunakan oleh TNI tidak sinkron dengan pola peperangan hibrida yang cenderung menembus ruang dan waktu (Sa'diyah & Vinata, 2016).

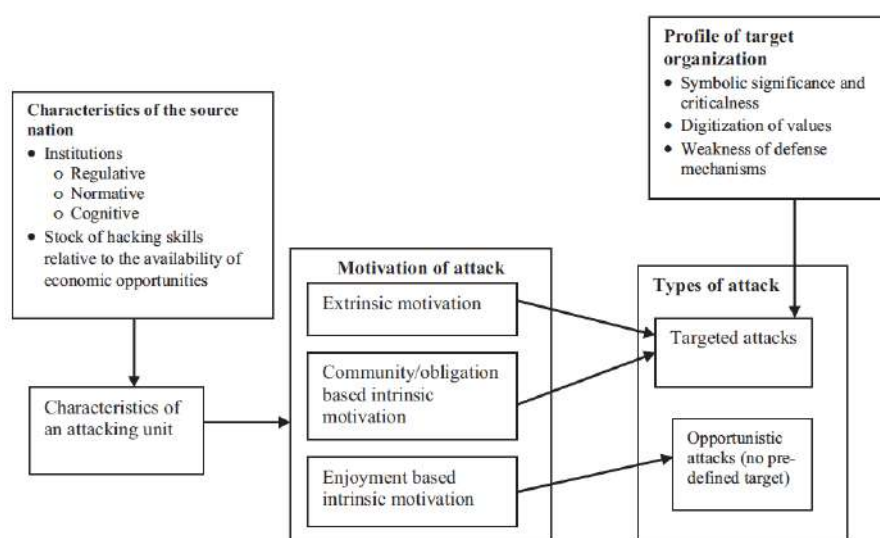
Penetrasi wilayah siber sebuah negara dapat dianggap sebagai pelanggaran hukum kedaulatan sebagaimana ditetapkan dalam *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Namun dokumen tersebut bertentangan dengan doktrin siber Amerika yang bertumpu di atas *International Law Framework for Employing Cyber Capabilities in Military Operations*. Artinya adalah bahwa penetrasi dibenarkan dalam situasi operasi militer (Schmitt & Vihul, 2017). Sesuai dengan teori perang, tingkatan yang sama terjadi dalam konteks perang siber, yaitu pada tataran strategis, operasional, dan

taktikal. Pada tingkatan strategis, tujuannya adalah untuk meraih obyektif utama yaitu melemahkan lawan melalui serangan yang bersifat esensial, yaitu pada infrastruktur krisis negara. Sementara pada tataran operasional, tujuan utamanya adalah untuk menggalang atau mendapatkan sumber daya yang dibutuhkan dalam peperangan. Biasanya yang menjadi target utama adalah sektor militer, yang banyak memiliki alutsista dan sumber daya pertahanan negara. Sementara dalam tataran taktikal, tujuannya sangat fokus yaitu untuk menguasai atau memenangkan sejumlah misi – seperti perebutan wilayah, pengambilalihan markas, penguasaan aset, dan lain sebagainya (Schulze, 2020).

Pada dasarnya domain siber telah menjadi ruang independen tersendiri tempat peperangan yang melibatkan negara dapat terjadi. Arena ini tidak bersifat statis, tetapi berkembang terus “luas dan spektrumnya” secara dinamis. Posisi negara yang dulu cenderung pada *active defense*, sekarang telah pindah modus menuju *offensive capabilities*. Namun demikian, peperangan dalam dunia siber tetap beririsan dengan fenomena peperangan atau konflik yang terjadi di dunia nyata (Siroli, 2018). Perdebatan mengenai ada tidaknya cyber war didasarkan pada konsep “*the act of war*” yang harus memenuhi tiga syarat utama, yaitu: *it must be political in motivation, instrumental in character and lethal in potential*. Sementara Clausewitz mendefinisikannya dengan berbeda: “*War is an act of force to compel our enemy to do our will*”, wrote Carl von Clausewitz on the first page of *On War*. *All war, pretty simply, is violent. If an act is not potentially violent, it is not an act of war . . . A real act of war is always potentially or actually lethal, at least for some participants on at least one side.*” Dalam konteks inilah dikatakan bahwa cyberwar dapat dan sedang terjadi.

Negara perlu memiliki kerangka strategi pertahanan siber nasional yang di dalamnya terdapat empat hal utama, yaitu: (i) *set of ideas*; (ii) *instruments of power*; (iii) *synchronised efforts*; dan (iv) *objectives and direction* (Souza, 2013). Menurut Bodley, kedaulatan terdiri dari kedaulatan eksternal dan internal. Di mana kedaulatan eksternal adalah semua hal yang berkaitan dengan luar negeri serta kekuatan pertahanan untuk melindungi teritorial negara dari serangan negara lain. Sedangkan kedaulatan yang internal adalah kewenangan yang dimiliki oleh suatu negara untuk menjalankan fungsinya dalam lingkup

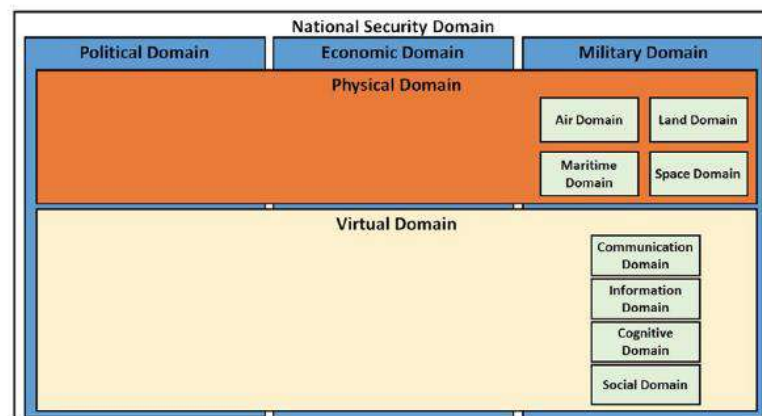
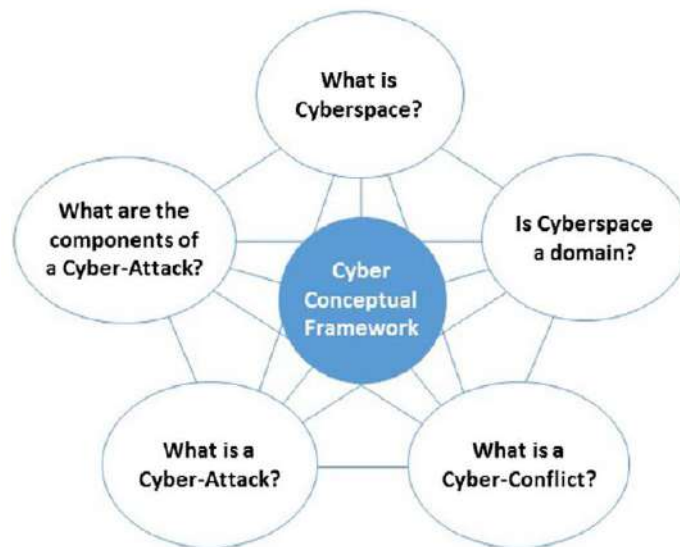
nasional. Dalam *“Tallinn Manual The International Law Applicable to Cyber Warfare Rule Sovereignty”* menyatakan bahwa *“State may exercise control over cyber infrastructure and activities within its sovereign territory”* (Sa'diyah & Vinata, 2016). Peraturan tersebut menjelaskan bahwa, suatu negara dapat menjalankan kontrol terhadap infrastruktur cyber dan aktivitas cyber di dalam wilayah kedaulatannya. Dari definisi yang diberikan oleh Bodley dan aturan yang tercantum dalam Tallinn Manual dapat disimpulkan bahwa, ketika suatu negara memiliki kapabilitas dalam hal infrastruktur cyber dan aktivitas cyber, negara tersebut dapat dikatakan telah memiliki kedaulatan di dalam cyberspace, dan syarat umum yang terdapat dalam hukum internasional mengenai cyberspace untuk dapat dikatakan sebagai domain terpenuhi. Modus ancaman siber bersifat dinamis dan cepat berkembang, sehingga perlu dipikirkan cara paling efektif dalam mendefinisikan, mengenali, mencegah, memitigasi, dan mengantisipasi ancaman dimaksud (Kim, 2016). Kerangka ancaman dinamis di atas harus digambarkan secara jelas agar dipahami konstelasinya dalam pertahanan negara (Kshetri, 2005).



Gambar 4. 31 Anatomi Serangan Siber

Sumber : Anatomi Serangan Siber (Ormrod, 2016)

Kerangka konseptual mengenai apa yang dimaksud dengan siber dan hubungan keterkaitannya dengan komponen lainnya perlu dikembangkan – dengan menjawab lima pertanyaan fundamental sebagai berikut (Ormrod, 2016):

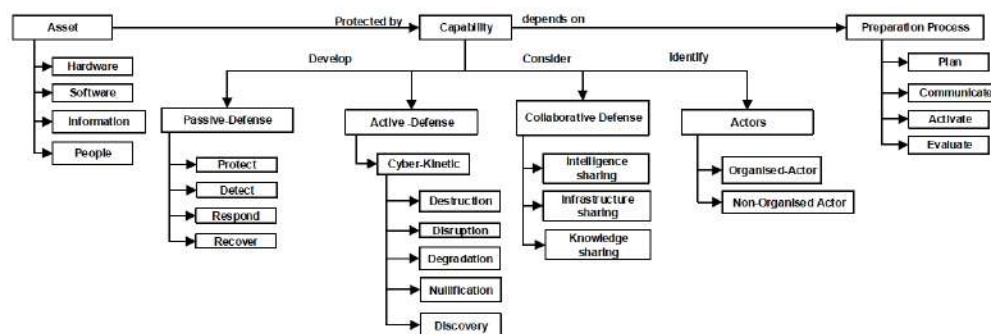


Gambar 4. 32 Kerangka Konseptual Ruang Siber

Sumber : Kerangka Konseptual Ruang Siber (Ormrod, 2016)

Salah satu strategi yang dapat diadopsi oleh Indonesia adalah berbasis berbasis *cyber deterrence* yang dapat dibagi menjadi lima jenis, yaitu: (i) *deterrence by punishment*; (ii) *deterrence by denial*; (iii) *deterrence by association*; (iv) *deterrence by norms and taboos*; dan (v) *deterrence by entanglement* (Ryan, 2017; Geers, 2010; Janeliunas, 2020). Setiap negara harus memiliki kemampuan dalam menyerang (*offensive*) dan bertahan (*defensive*) di dunia siber, dimana kapabilitas ini merupakan kemampuan kolektif dari berbagai pemangku kepentingan. Perlu pula dipikirkan implementasi dari konsep “*active defense*” (Janeliunas, 2020). Kapabilitas pertahanan siber harus dimodelkan dalam bentuk kerangka taksonomi yang holistik, seperti (Kolin, 2015):

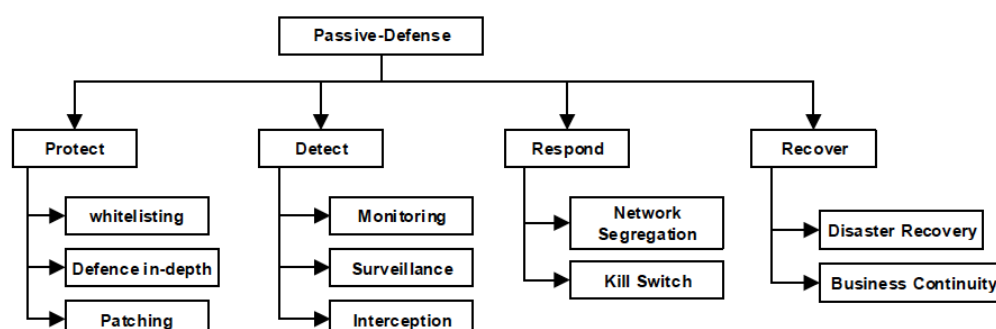
1. Cyber Capability Defense Model and Taxonomy Overview



Gambar 4. 33 Model Kapabilitas Pertahanan Siber

Sumber : Model Kapabilitas Pertahanan Siber (Kolin, 2015)

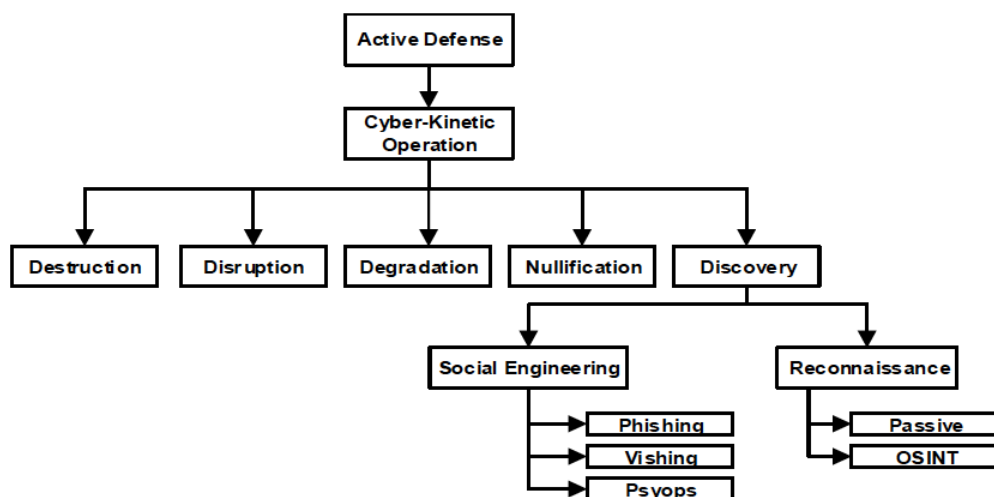
2. Passive Defense Classification



Gambar 4. 34 Klasifikasi Pertahanan Pasif Siber

Sumber : Klasifikasi Pertahanan Pasif Siber (Kolin, 2015)

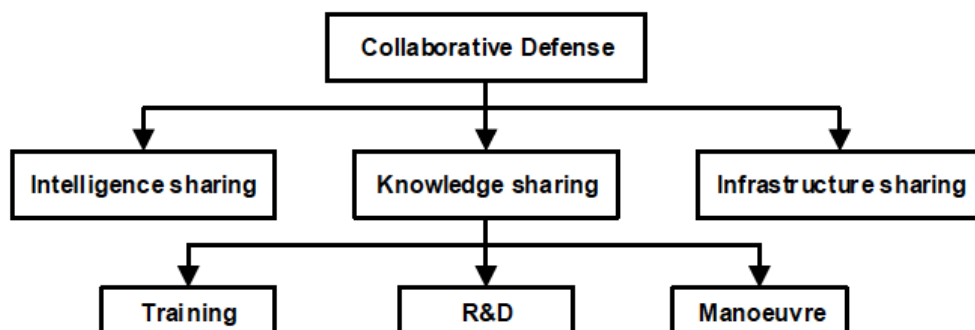
3. Active Defense Classification



Gambar 4. 35 Klasifikasi Pertahanan Aktif Siber

Sumber : Klasifikasi Pertahanan Aktif Siber (Kolin, 2015)

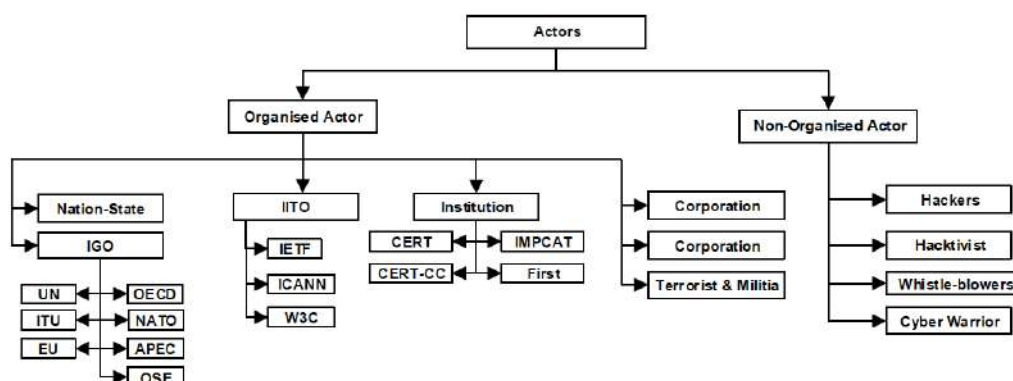
4. Collaborative Defense Classification



Gambar 4. 36 Klasifikasi Kolaborasi Pertahanan Siber

Sumber : Klasifikasi Kolaborasi Pertahanan Siber (Kolin, 2015)

5. Actor Classification



Gambar 4. 37 Klasifikasi Aktor Pertahanan Siber

Sumber : Klasifikasi Aktor Pertahanan Siber (Li, 2019)

Setiap jenis serangan memiliki rangkaian proses dimana masing-masing proses tersebut perlu ditopang dengan sumber daya yang memadai (Li, 2019).

Kedaulatan siber tidak semata-mata akan terjadi apabila sebuah negara menciptakan atau memproduksi teknologinya sendiri, namun lebih pada kualitas pengetahuan kolektif yang dimiliki dalam memahami ekosistem siber dunia (Schlager, 2018). Berdasarkan studi, ada sejumlah strategi perang siber yang patut untuk diadopsi, yaitu berdasarkan prinsip sebagai berikut:

1. *First-strike and sequential use of cyber capabilities seem easier to pull off, even for low-capacity actors, because the force-synchronization required for parallel use is hard to achieve.*

2. *The more preparation time there is, the more likely is the success of a cyber operation.*
3. *High operational complexity increases the risk of failure of any sustained cyber campaign.*
4. *If military commanders have alternative options to cyber operations with high complexity and thus uncertain reliability, they tend to choose the safer option (that is, using kinetic means to disable targets instead).*

Tabel 4. 37 Tahapan Proses Serangan Siber

Intrusion kill chains	Serial	The attack procedures and techniques
Reconnaissance	1	External information acquisition
	2	Vulnerability scanning
	3	Password cracking
	4	Port scanning
Weaponization	5	Carrier selection (file carrier, flow package)
	6	Choices about vulnerabilities and ways to exploit
	7	Choices about penetration tools
	8	Choices about the control weapons
	9	Anti-antivirus techniques (packing, feature confusion etc.)
Delivery	10	Spear Phishing attack
	11	Watering Hole attack
	12	Supply chain attack
	13	Proximity attack
	14	Ferry attack (USB ferry attack etc.)
Exploitation	15	Overflow vulnerabilities exploit
	16	Web vulnerabilities exploit
	17	Logical vulnerabilities combined exploit
	18	Verity of elevated privileges techniques
Installation	19	Botnets, Trojans, worms
	20	Backdoors of operation systems or devices
	21	RootKit embed
	22	WebShell
	23	Advanced Trojans
Command & Control	24	Command and Control
	25	Covert channels
	26	Abnormal communication modes
Actions on objectives	27	Destroyed the data or devices
	28	Data leakage
	29	Data defacement
	30	Long-term monitoring

Sumber : Tahapan Proses Serangan Siber (Li, 2019)

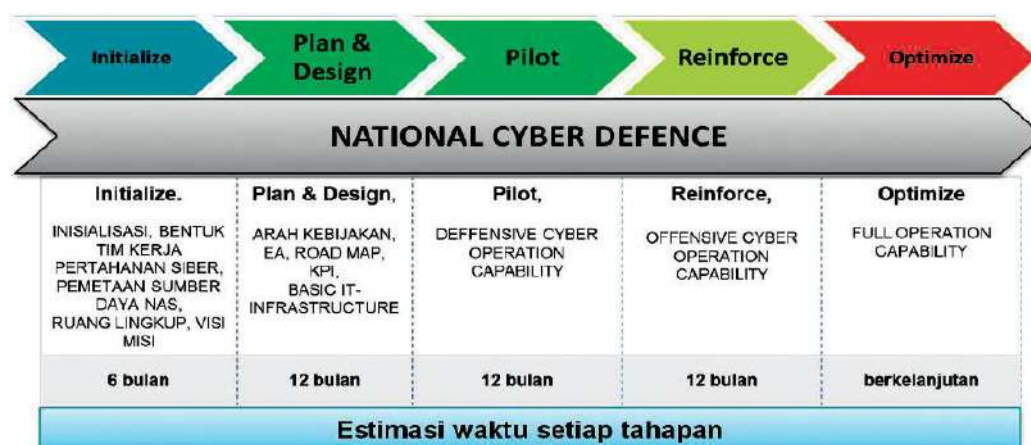
Strategi mempertahankan diri harus disesuaikan dengan jenis serangan yang cenderung mentargetkan sejumlah entitas berbasis perangkat teknologi (Shaji, Dev, & Brindha; 2018).

Tabel 4. 38 Ragam Model Pertahanan Siber

Defense methods	Attacks				
	APT	BYOD	IoT	Smart grid	RFID
Denial and deception	✓				
SVM and CSOACN	✓			✓	
Security intelligence		✓			
Two player sum game			✓	✓	
Moving target defense (MTD)			✓	✓	
Ant based defense			✓	✓	
Fusion based defense			✓		
Privacy policy enforcement			✓		
Sensor data correlation					✓

Sumber : Ragam Model Pertahanan Siber (Shaji, Dev, & Brindha; 2018)

Pertahanan siber harus dikembangkan secara holistik dan komprehensif, dengan memperhatikan komponennya secara *end-to-end* (Soewardi, 2013).



Gambar 4. 38 Proses Pertahanan Siber secara End-to-End

Sumber : Proses Pertahanan Siber secara End-to-End (Soewardi, 2013)

Negara perlu memiliki TI (*Threat Intelligence*) – yang terdiri dari *Strategic Threat Intelligence*, *Operational Threat Intelligence*, *Tactical Threat*

Intelligence, dan *Technical Threat Intelligence* - untuk memastikan selalu berada dalam garda terdepan dalam memahami dan mengidentifikasi berbagai ancaman siber yang mengemuka, seperti: *advanced persistent threats*, *polymorphic threats*, *zero-day threats*, dan *composite threats* (Tounsi & Rais, 2010).

Tabel 4. 39 Bentangan Infrastruktur Telekomunikasi Indonesia

No.	Indonesia's Submarine Cable List	Owner(s)	Landing Point(s)	
			Domestic	International
1	Jambi-Batam Cable System (JIBA)	MorateIndo	Batam, Jambi,	N/A
2	Jakarta-Bangka-Bintan-Batam-Singapore (B3JS)	MorateIndo	Batam, Bratu Prah, Jakarta, Pesaren	Singapore
3	SEA-US	RAM Telecom International, Globe Telecom, Hawaiian Telcom, Telkom Indonesia, GTA TeleGuam	Manado	Philippines, United States, Guam
4	Mataram Kupang Cable System (MKCS)	Telkom Indonesia	Ambalawi, Ende, Kupang, Mataram, Saraemee, Sumbawa Besar, Waingapu	N/A
5	JaKa2LaDeMa	Telkom Indonesia	Bali, Banjarmasin, Beculuk, Jimbaran, Ketapang, Mataram, Pankalan, Pontianak, Sangata, Toweli	N/A
6	PGASCOM	PGASCOM	Batam, Kuala Tungkal	Singapore
7	SeaMeWe-5	Telekom Malaysia, Bangladesh Telegraph & Telephone Board, China Mobile, China Telecom, Orange, Myanmar Post and Telecommunication, Saudi Telecom, Sri Lanka Telecom, Telkom Indonesia, TOT, SingTel, Telecom Italia Sparkle, TeleYemen, China Unicom, du, Turk Telekom International, TransWorld Associates (Pvt.) Limited	Batam	Egypt, Yemen, Oman, Italy, Djibouti, United Arab Emirates, Pakistan, Bangladesh, Sri Lanka, Malaysia, India, Myanmar, Thailand, France, Singapore, Saudi Arabia
8	Batam-Singapore Cable System (BSCS)	Telkom Indonesia	Batam	Singapore
9	SeaMeWe-3	Orange, BT, KDDI, SingTel, Telecom Italia Sparkle, Telekom Malaysia, OTEGLOBE, AT&T, Belgacom, Communications Authority of Thailand, China Telecom, Deutsche Telekom, Etisalat, Telecom Egypt, CTM, PT Indonesia Satellite Corp., Jabatan Telekom Brunei, KT, Portugal Telecom, Maroc Telecom, PLDT, Saudi Telecom, Sri Lanka Telecom, Turk Telekom, Tata Communications, Chunghwa Telecom, Verizon, KPN, Telekom Austria, SingTel Optus, Telstra, Vietnam Telecom International, Omantel, PCCW, Pakistan Telecommunications Company Ltd., Cyta, eircom, LG Uplus, Softbank Telecom, Telkom South Africa, Rostelecom, Orange Polska, SingTel Optus, Telecom Argentina, Myanmar Post and Telecommunication, Sprint, Vocus Communications, Djibouti Telecom, Embratel, Vodafone	Ancol, Medan	Egypt, Philippines, Greece, India, Vietnam, Hong Kong, Djibouti, Taiwan, United Arab Emirates, United Kingdom, Saudi Arabia, Pakistan, Korea, Turkey, Italy, Malaysia, Sri Lanka, India, Oman, Germany, Japan, Belgium, France, Australia, Myanmar, Thailand, Portugal, China, Singapore, Brunei, Morocco, Cyprus
10	Thailand-Indonesia-Singapore (TIS)	SingTel, Communication Authority of Thailand, Telkom Indonesia	Batam	Singapore, Thailand
11	Dumai-Melaka Cable System	Telkom Indonesia	Dumai	Malaysia
12	Matrix Cable System	Matrix Network Pte., Ltd.	Batam, Jakarta	Singapore
13	Australia-Singapore Cable (ASC)	Nextgen Networks	Jakarta	Australia, Singapore
14	APX-West	SubPartners	Jakarta	Australia, Singapore
15	MorateIndo International Cable System-1 (MIC-1)	MorateIndo	Batam	Singapore
16	Batam-Rengit Cable System (BRCS)	PT. Excelcomindo Pratama	Batam	Malaysia
17	JAKABARE	PT. Indonesia Satellite Corp.	Sungai Kakap, Tanjung Bemban, Tanjung Pakis	Singapore
18	Batam Dumai Melaka (BDM) Cable System	MorateIndo, Telekom Malaysia	Batam, Dumai	Malaysia

Sumber : Bentangan Infrastruktur Telekomunikasi Indonesia (Cuihong, 2019)

Negara perlu merancang dan membangun jaringan “internet lokal” yang dapat dikendalikan dan berada sepenuhnya dalam penguasaan negara. Salah satu cara termudah adalah menjadi bagian dari pengembangan jaringan internet global (Cuihong, 2019). Kedaulatan data memiliki sejumlah komponen yang harus diperhatikan, masing-masing adalah: *(i) system and communications protection; (ii) national cryptographic standards; (iii) local applications platform; (iv) national infrastructures platform; (v) control of international traffic; (vi) domestic hosting and domains; dan (vii) data centre localisation.*

Penggunaan ruang udara dan angkasa luar dalam pengembangan perang hibrida tidak lepas dari penggunaan teknologi satelit. Setidaknya terdapat empat jenis satelit yang dapat digunakan untuk kepentingan perang hibrida yaitu: Pertama, paling awal adalah satelit untuk tujuan mempelajari ruang angkasa.

Kedua, satelit telekomunikasi. Ketiga, satelit militer yang dibekali dengan senjata laser. Keempat, satelit pemantau langit atau satelit astronomi. Dengan satelit ini diharapkan pelanggaran wilayah laut oleh kapal-kapal asing, baik penyelundupan maupun penangkapan ikan secara liar atau *illegal fishing*, pembalakan hutan atau *illegal logging*, penambangan liar atau *illegal mining* hingga bencana alam, kecelakaan transportasi dan kerusakan dapat di monitor secara terus menerus (Sa'diyah & Vinata, 2016). Di dalam konsep *cyber warfare*, penggunaan teknologi sistem informasi dimanfaatkan untuk mendukung kepentingan komunikasi antar prajurit atau jalur komando yang difasilitasi oleh satu sistem komando kendali militer modern, yaitu sistem NCW atau Network Centric Warfare.⁵¹ Dengan adanya teknologi NCW yang didukung infrastruktur SIPRNet, berbagai komponen atau elemen militer di mandala operasi dapat saling terhubung atau *get connected* secara *online system* dan *realtime*, sehingga keberadaan lawan dan kawan dapat saling diketahui melalui visualisasi di layar komputer atau laptop. Dengan adanya teknologi Internet SIPRNet serta penggunaan satelit mata-mata dan satelit GPS, memungkinkan NCW memvisualisasikan seluruh kegiatan operasi militer gabungan yang sedang berlangsung di medan pertempuran atau *battle field* ke layar lebar ruang yudha atau *military operation room*, yang mungkin jaraknya terpisahkan ribuan kilometer jauhnya. Sehingga konsep NCW pada akhirnya akan merubah paradigma militer lama yang menyatakan bahwa suatu medan pertempuran dapat dimenangkan hanya oleh satu komponen militer saja.

Untuk memastikan terpenuhinya unsur-unsur *good practices* dalam penanganan dan pengelolaan siber, perlu diadopsi dan diterapkan sejumlah standar utama, seperti NIST, FIPS, SP800, ITL, FISMA, dan lain sebagainya (Andreas, 2004). Negara perlu membutuhkan *cyber warrior* baik yang bersifat resmi maupun informal, dimana mereka bekerja secara efektif dalam semangat bela negara untuk mempertahankan kedaulatan bangsa (Souza, 2013).

Salah satu cara efektif untuk melihat adanya ancaman adalah melalui analisa terhadap CTI (*Cyber Threat Intelligence*), dimana dalam manifestasinya membutuhkan semacam unit “intelijen siber” untuk melakukannya secara rutin (Ramsdale, 2020).

Tabel 4. 40 Sistem pada *Cyber Threat Intelligence*

CTI	Systems	Description
System logs and events	All systems	System activity, principally errors and security events
Network events	Network equipment, (switches, routers, firewalls)	devices connecting/disconnecting, ACL alert, login/failed login, etc.
Network utilisation and traffic profiles	Network equipment, (switches, routers, probes)	SNMP, NetFlow, RMON, etc. to Network management platform
Alerts from boundary devices	IDS/IPS, Firewall, WAF	Alerts/events collected and analysed by SIEM or vendor-specific management portal
AV, system alerts	Corporate AV software installed on host systems, (client and Server)	Corporate AV system alerts from host AV software
Human	All systems	Observed anomalies or events
Forensic	All systems	Artefacts and intelligence gathered after an event

Sumber : Sistem pada Cyber Threat Intelligence (Ramsdale, 2020)

Setiap negara harus memiliki kebijakan mengenai definisi serta penetapan *national critical infrastructure* yang tegas dan jelas. Sementara kebijakan lain yang perlu ditetapkan berkaitan dengan *cyberscurity deterrence* dan *cyber offensive and defensive capabilities*. Besarnya anggaran untuk pembentukan dan operasional *cyberforces* juga perlu didukung oleh kebijakan yang efektif (Janeliunas, 2020). Indonesia harus mulai memilih dalam meratifikasi berbagai peraturan internasional dalam bidang *cyberlaw* – disamping mulai membuat daftar regulasi apa saja yang dibutuhkan oleh negara untuk jangka pendek, menengah, dan panjang (Khanna, 2018). Kesenjangan juga dapat terjadi bila ada ketentuan hukum baru yang ditetapkan yang tidak sesuai dengan

tingkah laku manusia di dalam masyarakat. Dalam hal demikian tuntutan keharusan hukum yang baru ditetapkan tidak sesuai dengan tingkah laku yang hidup dalam masyarakat. Hal itu berarti kehidupan masyarakat tertinggal dari ketentuan hukum yang berlaku. Untuk mengatasi kesenjangan itu hukum dapat menetapkan tiga alternatif. Pertama, tetap berpegang pada hukum yang berlaku dan merubah tingkah laku kehidupan dalam masyarakat yang ada. Kedua, melegalsir perubahan kehidupan yang ada dan meniadakan ketentuan hukum yang berlaku. Dan yang Ketiga, sebagian ketentuan hukum yang berlaku dipertahankan dengan juga menerima sebagian perubahan kehidupan dalam masyarakat yang terjadi. Peran hukum dalam merubah kehidupan masyarakat dapat dilakukan secara langsung dan dapat juga dilakukan secara tidak langsung (Sa'diyah & Vinata, 2016). Walaupun ruang siber bersifat *borderless*, tapi dalam konteks regulasi tetap dilakukan secara berjenjang sesuai dengan sistem perundang-undangan yang berlaku dalam dunia nyata.



-
- ```

graph TD
 1[1 Cyber Security Regulation] --> 1.1[1.1 Regulation of the Specific Information Domains]
 1 --> 1.2[1.2 Security Regulation]
 1 --> 1.3[1.3 Privacy Regulation]
 1 --> 1.4[1.4 Accountability Regulation]
 1.1 --> 1.1.1[1.1.1 Classified Information]
 1.1 --> 1.1.2[1.1.2 Unclassified Information]
 1.1 --> 1.1.3[1.1.3 Personnel Data]
 1.1 --> 1.1.4[1.1.4 Intellectual Property]
 1.2 --> 1.2.1[1.2.1 Cybercrime]
 1.2 --> 1.2.2[1.2.2 Lawful Interception]
 1.2 --> 1.2.3[1.2.3 Critical Infrastructure (CI)]
 1.2 --> 1.2.4[1.2.4 Critical Information Infrastructure (CII)]
 1.3 --> 1.3.1[1.3.1 Service providers' infrastructure protection]
 1.3 --> 1.3.2[1.3.2 Protection of end-to-end users' communication]
 1.4 --> 1.4.1[1.4.1 «Due Diligence» responsibility of continuing assesment and understanding of the risks that company faces]
 1.4 --> 1.4.2[1.4.2 «Due Care» responsibility of service providers in implementing security regulation]
 1.4 --> 1.4.3[1.4.3 Encouragement of the security awareness development in the widest social groups]

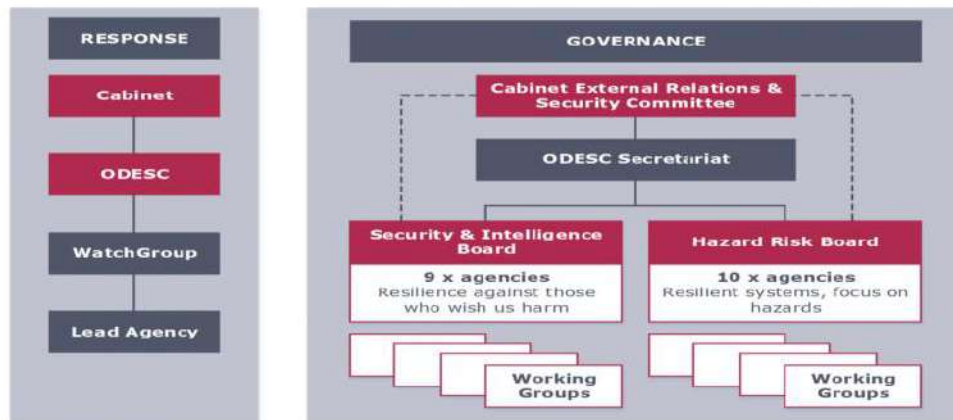
```
- 1 Cyber Security Regulation**
    - 1.1 Regulation of the Specific Information Domains**
      - 1.1.1 Classified Information
      - 1.1.2 Unclassified Information
      - 1.1.3 Personnel Data
      - 1.1.4 Intellectual Property
    - 1.2 Security Regulation**
      - 1.2.1 Cybercrime
      - 1.2.2 Lawful Interception
      - 1.2.3 Critical Infrastructure (CI)
      - 1.2.4 Critical Information Infrastructure (CII)
    - 1.3 Privacy Regulation**
      - 1.3.1 Service providers' infrastructure protection
      - 1.3.2 Protection of end-to-end users' communication
    - 1.4 Accountability Regulation**
      - 1.4.1 «Due Diligence» responsibility of continuing assesment and understanding of the risks that company faces
      - 1.4.2 «Due Care» responsibility of service providers in implementing security regulation
      - 1.4.3 Encouragement of the security awareness development in the widest social groups

Gambar 4. 39 Komponen Regulasi Pertahanan dan Keamanan Siber

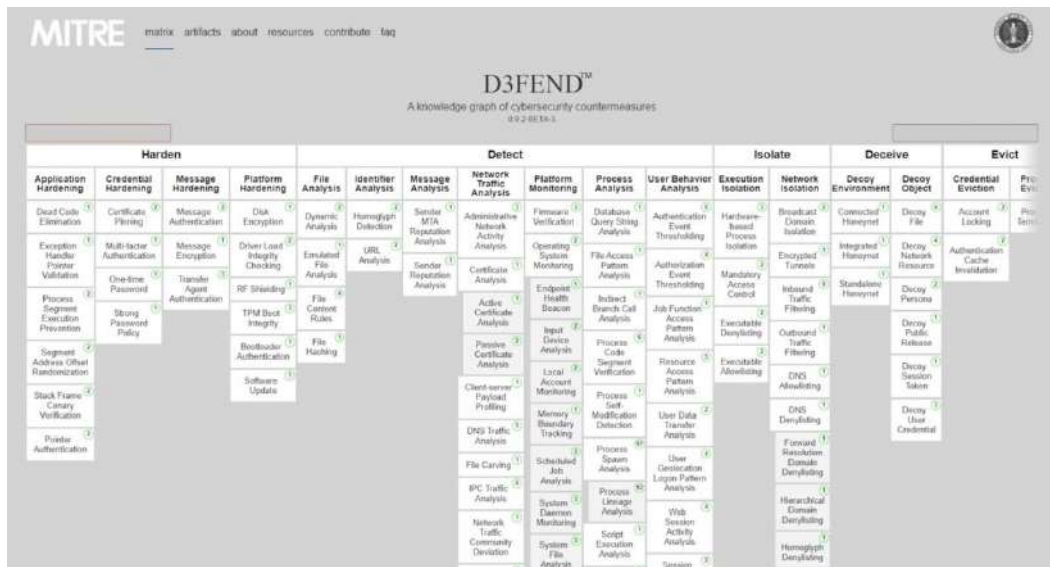
Sumber : Komponen Regulasi Pertahanan dan Keamanan Siber (Sa'diyah & Vinata, 2016)

Dalam menghadapi kondisi insiden, negara-negara maju melibatkan koordinasi dari empat lembaga negara, yaitu: kementerian dalam negeri, badan intelijen negara, kementerian pertahanan, dan penegak hukum (Andreas, 2004). Badan Pertahanan Cyber Nasional sebenarnya sangat diperlukan oleh Indonesia. Badan Pertahanan Cyber Nasional atau apapun namanya harus segera dipikirkan untuk dibentuk agar terwujud mekanisme koordinasi, komunikasi, dan sinergi antar berbagai aktor keamanan dan pertahanan dalam melindungi kedaulatan dunia maya Indonesia dari berbagai ancaman serangan cyber. Kementerian Pertahanan, TNI, Polri, BIN, Kemenkominfo, Lembaga Sandi Negara, dan berbagai instansi

terkait lainnya harus mampu bersinergi untuk menangkis, menangkal, dan mencegah serangan siber dari pihak tertentu atau dari negara lain yang mencoba untuk mengganggu kedaulatan dunia maya Indonesia saat ini dan di masa depan. Dalam kaitan ini, maka perlu sebuah analisis mendalam tentang penggunaan media sosial yang luar biasa pada masyarakat Indonesia dengan potensi perang siber (Sa'diyah & Vinata, 2016). Kementerian Pertahanan bersama lembaga, pihak, dan instansi terkait lainnya harus saling bahu membahu memberdayakan potensi dunia maya dan potensi digital yang dimiliki, sebagai sumber daya buatan, untuk diberdayakan dalam membendung dan menghadapi perang siber. Pemerintah, kementerian pertahanan, TNI, Polri, BIN, Kemenkominfo, dan lain-lain harus melakukan berbagai inventarisasi, identifikasi, pembinaan, dan pengelolaan berbagai potensi kekuatan dunia maya yang dimiliki oleh Indonesia, khususnya masyarakat pengguna media sosial, netizen, dan berbagai komunitas informasi komunikasi dunia maya untuk saling bersinergi dalam menghadapi perang siber. Sudah saatnya Indonesia membutuhkan Badan Pertahanan Siber Nasional, seiring dengan semakin bertumbuhnya ekonomi di Indonesia dan tingginya intensitas pemanfaatan teknologi informasi dan komunikasi di segala bidang (Subagyo, 2015). Adanya urgensi pembentukan Komando Pertahanan Siber atau *cyber defense command* untuk menghadapi peperangan siber dan asimetris di dunia maya (Sutrisno, 2016).



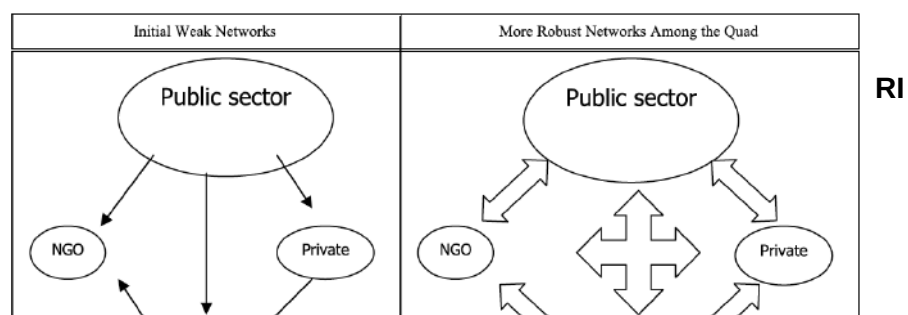
| Level       | Australia                                                                                                                                                                                                                                                                                                    | UK                                                                                                                                                                                                                                                                                                          | Indonesia                       |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Strategic   | <p>Cyber Security Policy and Coordination Committee (Lead Agency: The Attorney-General's Department)</p> <p>Function: interdepartmental committee that coordinates the development of cyber security policy for the Australian Government.</p>                                                               | <p>Office of Cyber Security (OCS)</p> <p>function: to provide strategic leadership for and coherence across Government;</p>                                                                                                                                                                                 | Undefined                       |
| Tactical    | <p>Cyber Security Operations Centre (CSOC) (Under Directorate: Defense Signals Directorate)</p> <p>Function: provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance.</p> | <p>Cyber Security Operations Centre (CSOC)</p> <p>Function: actively monitor the health of cyber space and co-ordinate incident response; to enable better understanding of attacks against UK networks and users; to provide better advice and information about the risks to business and the public.</p> | Undefined                       |
| Operational | CERT Australia                                                                                                                                                                                                                                                                                               | GovCertUK                                                                                                                                                                                                                                                                                                   | ID-SIRTII<br>GovCert<br>ID-Cert |



Gambar 4. 40 Spektrum Pertahanan dan Keamanan Siber

Sumber : Spektrum Pertahanan dan Keamanan Siber (Mitre, 2018)

Militer perlu mulai membangun industri teknologi siber agar negara dapat memiliki pertahanan siber yang ampuh maupun penyerangan siber yang handal dalam situasi terjadinya “perang siber” setiap harinya (Kanniainen, 2018). Tata kelola internet atau *internet governance* hanya akan diperoleh apabila terbangun ekosistem industri telekomunikasi dan teknologi informasi nasional yang merupakan kolaborasi antara The Quad (public sector, private, NGO, dan R&D) (Wilson, 2005).

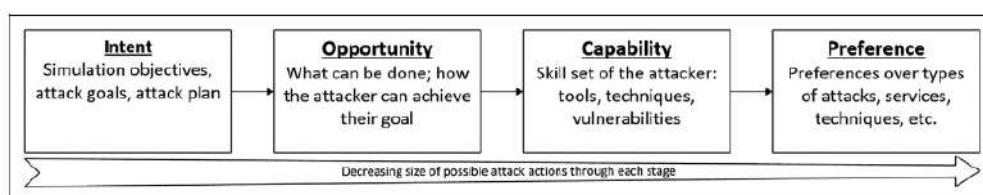
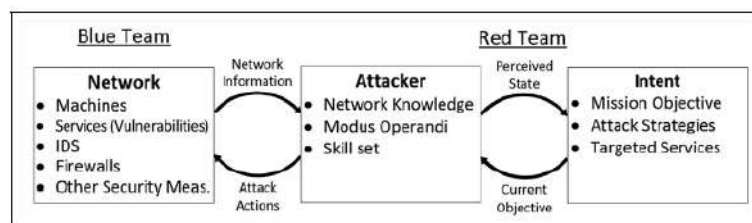


Gambar 4. 41 Perbandingan Topologi Jaringan Kerjasama

Sumber : Perbandingan Topologi Jaringan Kerjasama (Wilson, 2005)

Cara China membentuk kedaulatan sibernya adalah melalui pembangunan *cyber governance* yang berada dalam teritori negaranya. Kebijakan China dibangun berdasarkan ketidaknyamanan domestik karena kekuatan siber global yang berada di luar negara (Zeng, Stevens, & Chen; 2017).

Kerjasama antar institusi dalam satu negara atau antar negara dapat dilakukan terutama dalam latihan perang siber bersama, dimana ada pihak yang berperan sebagai penyerang (*red team*) dan yang diserang/bertahan (*blue team*) (Moska, 2018).



Gambar 4. 42 Skenario Latihan Perang Siber

Sumber : Skenario Latihan Perang Siber (Moska, 2018)

Berbagai institusi harus bekerjasama dalam menghadapi berbagai serangan siber yang semakin marak, sesuai dengan tupoksinya masing-masing (Subagyo, 2015).

Tabel 4. 41 Pembagian Peran Penanganan Ancaman Siber

| No | Jenis Ancaman                          | Intansi Utama Penanganan                                           |
|----|----------------------------------------|--------------------------------------------------------------------|
| 1  | Ancaman Cyber ( <i>Cyber Threat</i> )  | Kemenkominfo, Kemlu, Komunitas Informasi, Instansi Terkait Lainnya |
| 2  | Kejahatan Cyber ( <i>Cyber Crime</i> ) | Polri & Interpol                                                   |
| 3  | Perang Cyber ( <i>Cyber Warfare</i> )  | Kemhan, TNI, BIN                                                   |

Sumber : Pembagian Peran Penanganan Ancaman Siber (Subagyo, 2015)

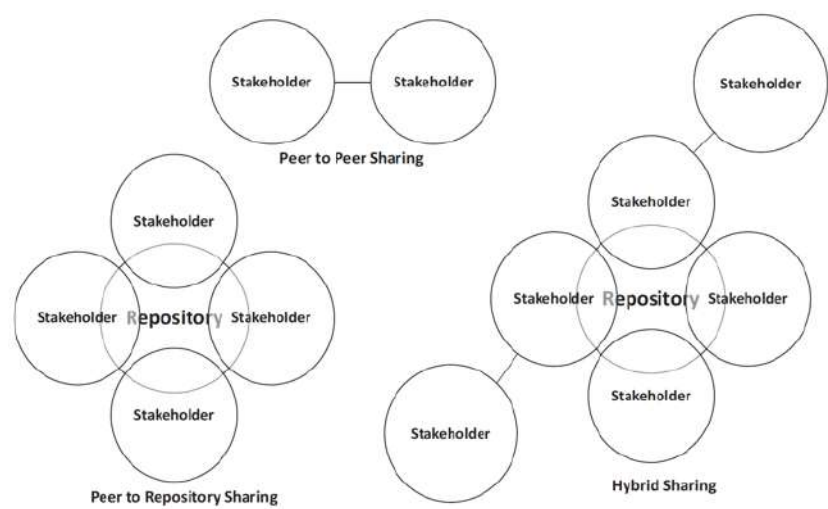
*Cyber Threat Intelligence* harus dilakukan melalui koordinasi antar berbagai pihak yang berbeda, terutama dalam melakukan *information sharing* (Wagner et al., 2019).

Tabel 4. 42 Protokol *Cyber Intelligence*

| CTI protocols.                                              |                                                                                                              |                                                                         |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Title                                                       | Description                                                                                                  | URL                                                                     |
| Structured Threat Information eXpression                    | Structured language for CTI sharing (human and machine readable in JSON)                                     | <a href="https://tinyurl.com/ybjgmoc7">https://tinyurl.com/ybjgmoc7</a> |
| Trusted Automated eXchange of Indicator Information         | Language to share CTI (open transport mechanism with native support for HTTP and HTTPS)                      | <a href="https://tinyurl.com/ybjgmoc7">https://tinyurl.com/ybjgmoc7</a> |
| Open Threat Partner Exchange (OpenTPX)                      | Open source language that supports machine-readable threat intelligence sharing in JSON                      | <a href="https://tinyurl.com/yd5uopkc">https://tinyurl.com/yd5uopkc</a> |
| Malware Attribution Enumeration and Characterization (MAEC) | A standardized language for sharing structured information about malware (human and machine readable in XML) | <a href="https://tinyurl.com/yb35uj9k">https://tinyurl.com/yb35uj9k</a> |
| Incident Object Description Exchange Format (IODEF)         | Framework for sharing computer security incidents in XML                                                     | <a href="https://tinyurl.com/yeh8ekus">https://tinyurl.com/yeh8ekus</a> |
| Vocabulary for Event Recoding and Incident Sharing (VERIS)  | Language to describe structured security events                                                              | <a href="https://tinyurl.com/y9uvh9yx">https://tinyurl.com/y9uvh9yx</a> |

Sumber : Protokol Cyber Intelligence (Wagner et al., 2019)

Model *sharing* yang dipilih dapat disesuaikan dengan tupoksi masing-masing pihak agar tidak memberikan kompleksitas dalam penyelenggaraannya.



Gambar 4. 43 Model Kerjasama Saling Berbagi Sumber Daya



Sumber : Model Kerjasama Saling Berbagi Sumber Daya (Wagner et al., 2019)

CTI yang baik dan efektif mengandung sejumlah komponen dan atribut yang harus dipertimbangkan.



Gambar 4. 44 Karakteristik dan Indikator *Cyber Threat Intelligence*

Sumber : Karakteristik dan Indikator Cyber Threat Intelligence (Wagner et al., 2019)

Hirarki regulasi terkait dengan information sharing dalam CTI juga harus dikembangkan.

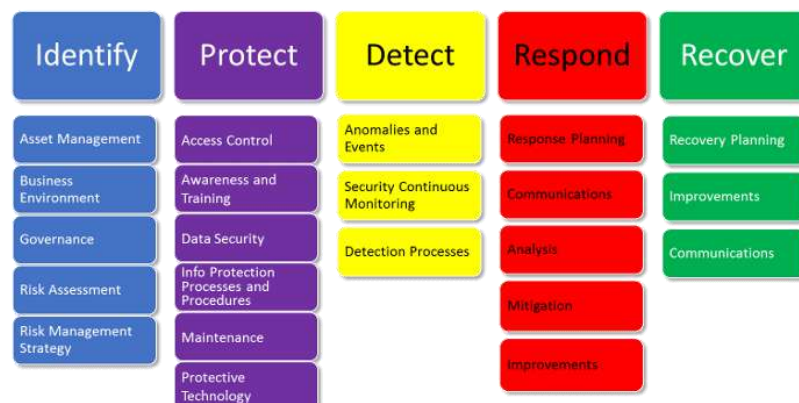
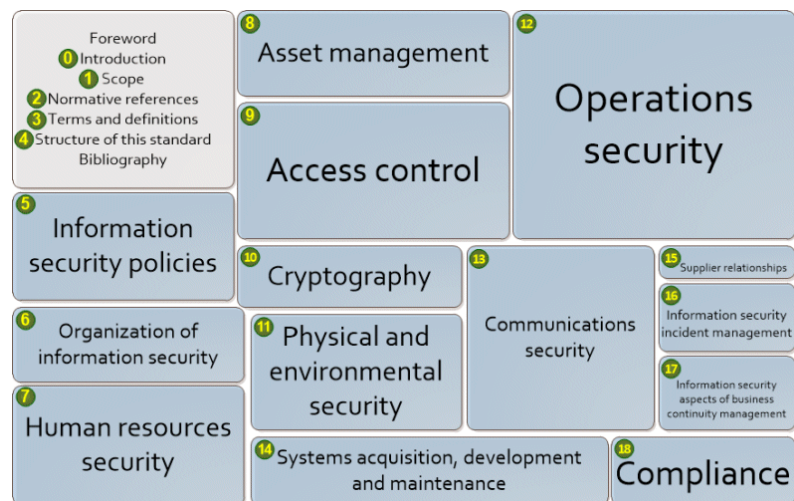


Gambar 4. 45 Hirarki Regulasi terkait *Cyber Threat Intelligence*

Sumber : Hirarki Regulasi terkait Cyber Threat Intelligence (Wagner et al., 2019)

Entitas yang berada dalam ekosistem pertahanan harus memenuhi standar keamanan siber yang bertujuan untuk memastikan terjadinya tiga aspek utama, yaitu: (i) *confidentiality*; (ii) *integrity*; dan (iii) *availability*. Agar ketiga hal tersebut tercapai, ada sejumlah pra-kebutuhan yang harus terpenuhi, yaitu menyangkut aspek: (i) *authentication*; (ii) *authenticity*; (iii) *authorisation*; (iv) *accountability*; (v) *privacy*; (vi) *dependability*; (vii) *survivability*; dan (viii) *safety criticality* (Gunduz, 2020). Keberadaan dan kepatuhan terhadap sejumlah

standar adalah sebuah keniscayaan untuk memastikan tercapainya kualitas yang diinginkan. Pastikan sejumlah standar berskala nasional (seperti NIST) diadopsi oleh negara (Srinivas, Das, & Kumar; 2018).

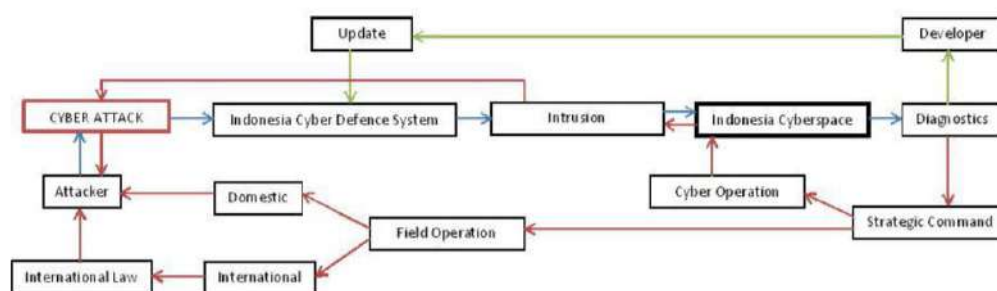


Gambar 4. 46 Domain Pertahanan dan Keamanan Siber

Sumber : Domain Pertahanan dan Keamanan Siber (Limnell, 2016)

Sumber daya manusia adalah komponen terpenting dalam ekosistem pertahanan siber. Negara perlu memiliki strategi khusus cara mengadakan, melatih, dan mengembangkan kompetensi mereka. SDM dimaksud dapat berasal dari dalam maupun luar negeri, baik yang digodok melalui pendidikan formal, informal, maupun non-formal, atau yang memiliki pengalaman panjang dalam bidang pertahanan dan keamanan siber (Limnell, 2016). Peningkatan SDM melalui pendidikan dan latihan di dalam dan luar negeri. Personel TNI mulai dari sekarang harus mulai memahami apa yang dimaksud dengan perang hibrida, bagaimana mengawaki Alusista untuk perang hibrida, bagaimana menghadapi *cyber warfare* dan perang informasi. Tuntutan kemajuan perang telah memaksa TNI untuk memiliki *nonwar skills*. Selain itu hubungan sipil dan militer perlu dilatihkan dalam wujud latihan yang terintegrasi, dimana dalam pola operasi yang dilakukan, instansi-instansi nonmiliter akan memberikan dukungan dalam bentuk personel, keahlian dan perlengkapan yang tidak dimiliki oleh TNI dalam menghadapi perang hibrida (Sa'diyah & Vinata, 2016). *Tentara siber harus* direkrut oleh Kementerian Pertahanan melalui berbagai cara. Cara pertama adalah melalui tata cara pendaftaran sebagaimana yang umum dilakukan oleh TNI. Cara kedua adalah dengan cara menginventarisasi, mendata dan merekrut para anggota TNI aktif yang memang sudah memiliki keahlian dan kemampuan di bidang IT di berbagai kesatuan masing-masing sehingga dijadikan satu untuk dilakukan pelatihan khusus sehingga dapat mengisi unit khusus tentara siber atau *cyber force*.

Tentara Siber sangatlah dibutuhkan segera, terutama untuk menghadapi berbagai ancaman teroris global yang menggunakan dunia maya sebagai medium maupun instrumen peperangan (Setiawan, 2018).



Gambar 4. 47 Relasi Keterkaitan antar Proses Pertahan Siber

Sumber : Relasi Keterkaitan antar Proses Pertahan Siber (Setiawan, 2018)

Tentara siber selain berhadapan dengan tentara serupa dari pihak lawan, harus pula menghadapi komunitas *hackers* yang kerap menyerang dengan berbagai motivasi (Shaji, Dev, & Brindha; 2018).

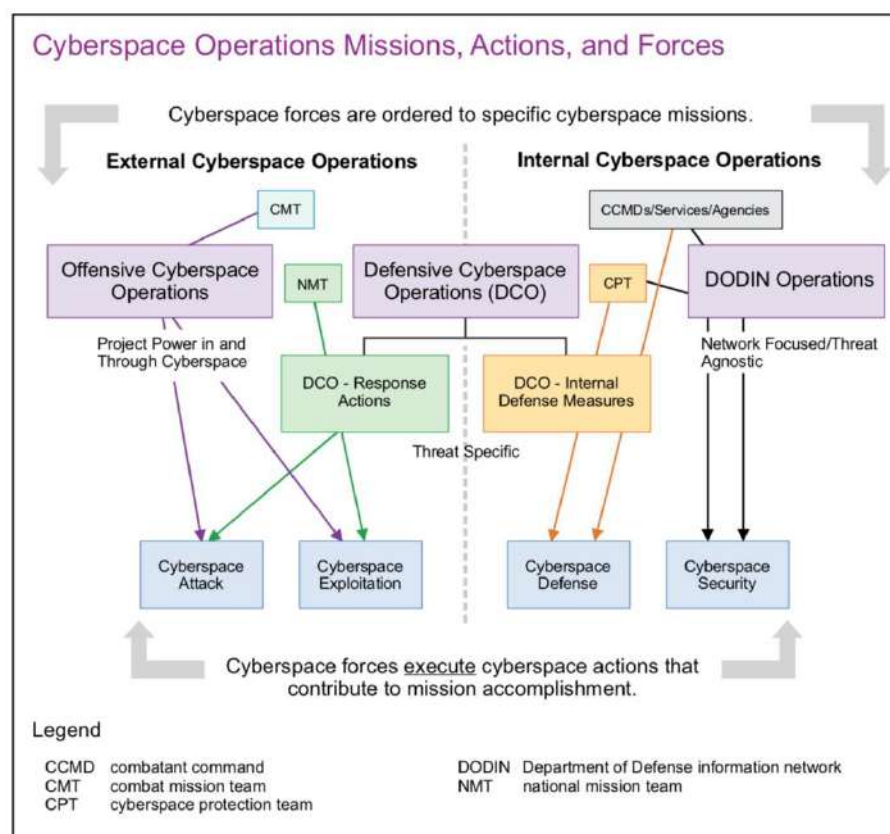
Tabel 4. 43 Tipe Peretas, Motivasi, dan Keahliannya

| Hacker types                   | Motivations |            |          |         |        |           | Skill level        |
|--------------------------------|-------------|------------|----------|---------|--------|-----------|--------------------|
|                                | Ideology    | Recreation | Prestige | Revenge | Profit | Curiosity |                    |
| Novices                        |             |            |          |         |        | ✓         | Low                |
| Crowd sourcers                 |             | ✓          |          | ✓       |        |           | Below intermediate |
| Cyberpunk (hightech outsiders) |             |            |          |         |        | ✓         | Very low           |
| Hacktivists                    | ✓           |            |          | ✓       |        |           | Very high          |
| Insiders                       |             |            |          | ✓       | ✓      |           | Intermediate       |
| Coders                         |             |            | ✓        | ✓       |        |           | Upper intermediate |
| Cyber warriors                 | ✓           |            |          |         | ✓      |           | High               |

Sumber : Tipe Peretas, Motivasi, dan Keahliannya (Shaji, Dev, & Brindha; 2018)

Satu demi satu negara maju membentuk Angkatan Siber sebagai matra keempat atau kelimanya. China membentuk pasukan yang diberi nama Blue Army, Israel memiliki Unit 8200, Amerika memiliki US CyberCom, Australia dan Inggris memiliki CSOC, dan lain sebagainya (Soewardi, 2013).

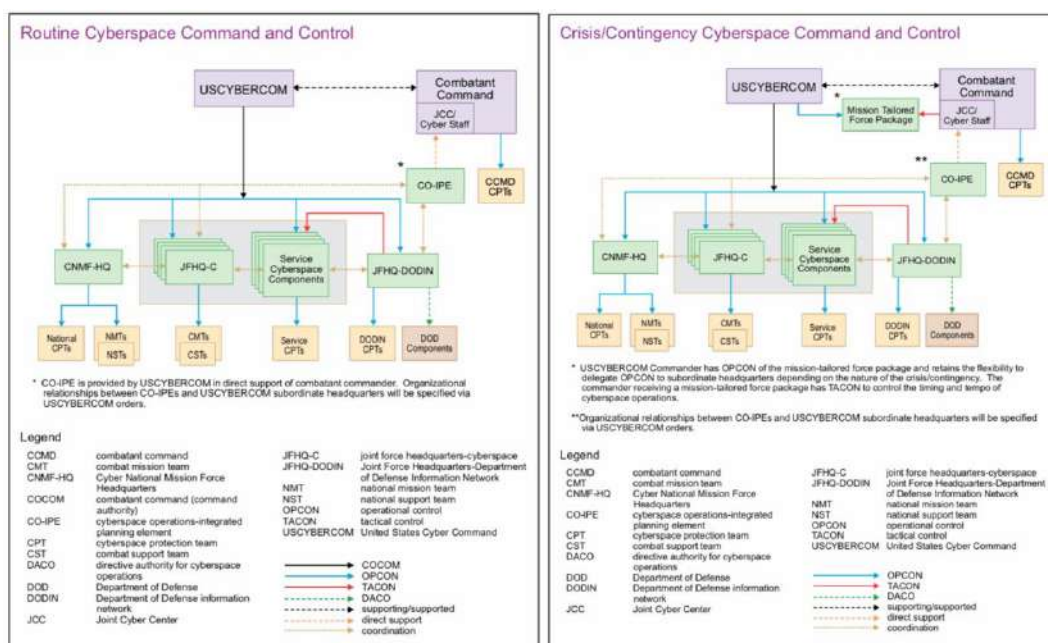
Sebagaimana setiap peristiwa konflik, dalam perang siber pun dikenal istilah tentara siber. Bentuknya dapat beraneka ragam, sesuai dengan peran serta karakteristik dari lembaga yang bertanggung jawab terhadapnya. Misalnya adalah konsep dari Department of the Navy USA, yang memiliki berbagai unit operasi militer dalam dunia siber, seperti: *cyber protection force*, *cyber national mission force*, *cyber combat mission force*, dan lain sebagainya (Barrett, 2013; Robert Kehler et al., 2017; Samaan, 2010). Intinya adalah unit-unit ini saling berkoordinasi dalam menjalankan misi dari sebuah perang siber. Misi internal berkaitan dengan kegiatan operasional sehari-hari untuk melindungi keamanan teritori siber dalam ruang lingkup organisasi seperti satuan militer atau yang lebih luas. Sementara misi eksternal terkait usaha penyerangan dan eksploitasi sumber daya siber pihak musuh atau sasaran yang telah ditetapkan.



Gambar 4. 48 Domain Teritori Operasi Siber

Sumber : Domain Teritori Operasi Siber (USA Navy, 2018)

*Cyber Space* pada dasarnya terbentuk dari adanya jejaring komputer yang dikoneksi melalui infrastruktur transmisi digital. Dalam konteks pengelolaan siber, dikenal dua jenis peristiwa atau status. Status pertama adalah situasi dimana siber dalam keadaan aman, dimana terjadi aktivitas rutin menjaga keamanan di dalamnya. Sementara status kedua adalah ketika terjadi peristiwa krisis, yang membutuhkan penanganan khusus secara cepat dan tepat. Dalam kondisi normal, struktur organisasi yang telah dirancang menjalankan tugas pokoknya masing-masing. Sementara dalam kondisi kritis, diperlukan satu unit taktis untuk menangani insiden yang terjadi. Contohnya adalah dibentuknya CERT (Computer Emergency Response Team) dan/atau CSIRT (Computer Security Insident Response Team). Istilah yang biasa dipakai dalam dunia militer adalah *mission tailored force package* (Allen, 2001; West-Brown et al., 2003).



Gambar 4. 49 Contoh Struktur Organisasi Siber dalam Kondisi Normal dan Krisis

Sumber : Contoh Struktur Organisasi Siber dalam Kondisi  
Normal dan Krisis (US Navy, 2018)

Berdasarkan konsep ini, konteks ketika berada dalam keadaan krisis menjadi fokus pengelolaan dunia siber. Suatu kondisi dikatakan krisis nasional apabila keadaan tersebut dapat berimplikasi serius terhadap keberadaan, keutuhan, dan kedaulatan sebuah negara. Sementara krisis siber nasional didefinisikan sebagai suatu situasi dan kondisi yang mengancam aktivitas operasional rutin aset siber sehingga menyebabkan kerusakan atau kehancuran terhadap reputasi, ekonomi, dan jiwa manusia secara masif. Kata kunci dalam definisi ini adalah aset siber, yang pada dasarnya menjalankan aktivitas penting (*core processes*) yang berkaitan secara langsung dengan hajat hidup orang banyak. Dalam konteks pertahanan siber, penetapan aset siber utama merupakan proses yang harus dilalui. Bahasa yang kerap dipakai untuk mendeskripsikan entitas ini adalah infrastruktur kritis nasional. Infrastruktur ini adalah sistem berbasis fisik maupun siber yang vital bagi operasi ekonomi dan pemerintah, termasuk tapi tidak terbatas pada telekomunikasi, energi, perbankan, keuangan, militer, transportasi, sistem air, maupun layanan darurat – baik dalam kendali manajemen pemerintah maupun swasta (Bhardwaj et al., 2016; Wiśniewski, 2020). Banyak infrastruktur kritis nasional yang secara historis merupakan sistem yang berdiri sendiri telah dimutakhirkan menjadi



berbasis teknologi digital, sehingga bersamanya terdapat kerawanan atau risiko baru.

Mengingat bahwa fasilitas dan sarana parasarana militer adalah merupakan infrastruktur kritikal, maka Amerika Serikat memiliki struktur organisasi khusus untuk mengatasi permasalahan krisis yang berpotensi menimpa perimeter pertahanan mereka (Bendrath, 2001; Tatar et al., 2019; Weed, 2017).

**International Organization for Standardization:** Organizations and facilities that are essential to the functioning of society and the economy as a whole. The standard elaborates that a failure or malfunction of such organizations or facilities would result in sustained supply shortfalls, make a significant impact on public security, and have other wide ranging impacts.

**International Telecommunication Union:** The key systems, services, and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these.

**NATO:** Physical or virtual systems and assets under the jurisdiction of a state that are so vital that their incapacitation or destruction may debilitate a state's security, economy, public health or safety, or the environment.

**EU:** An asset, system, or part thereof located in a member state that is essential to vital societal functions, health, safety, security, economic, or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions.

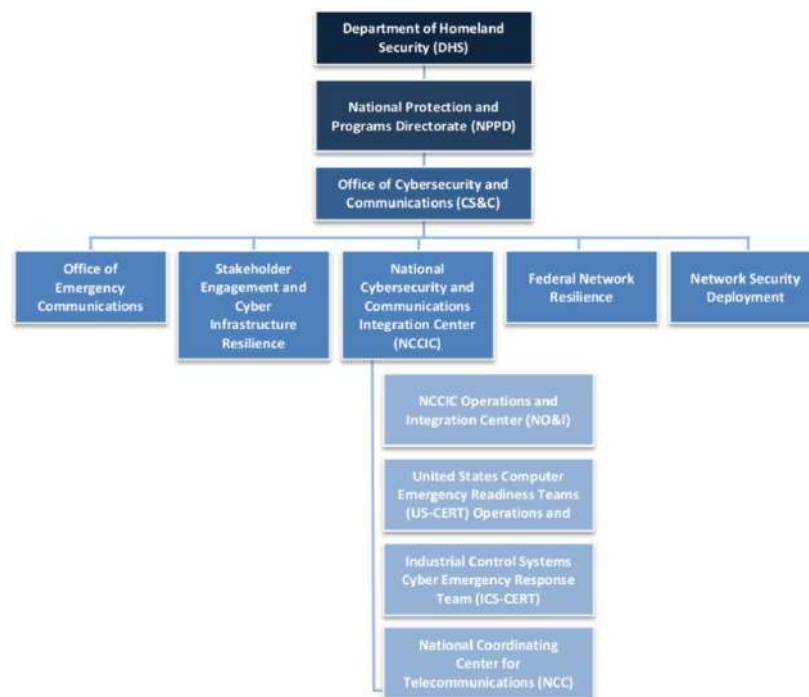
**United States:** The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Gambar 4. 50 Ragam Definisi Infrastruktur Kritis Nasional

**Sumber :** Ragam Definisi Infrastruktur Kritis Nasional

(Bhardwaj et al., 2016; Wiśniewski, 2020)

Sejumlah peristiwa memperlihatkan bahwa krisis siber adalah jalan masuk untuk mengganggu pertahanan negara maupun keamanan nasional sebuah teritori yang berdaulat. Paling tidak kejadian luar biasa di Estonia memperlihatkan bagaimana ketika terjadi krisis akibat diserangnya infrastruktur publik yang menguasai hajat hidup orang banyak, meledaklah kerusuhan besar yang hampir melumpuhkan negara karena sulitnya mengendalikan amukan massa yang begitu besar.



Gambar 4. 51 Struktur Organisasi Penanganan Krisis Siber Amerika Serikat

Sumber : Struktur Organisasi Penanganan Krisis Siber Amerika Serikat

(Bendrath, 2001; Tatar et al., 2019; Weed, 2017)

Beberapa ilmuwan telah mencoba untuk melakukan studi mendalam terhadap pengembangan kerangka tata kelola untuk pertahanan siber. Gomez dari De La Salle University melakukan studi khusus terkait dengan “*Arming Cyberspace*” dalam hubungannya dengan kegiatan pengelolaan pertahanan di dunia siber (Gomez, 2016). Yang bersangkutan mendapatkan tiga komponen

utama dalam menjaga dunia siber, yaitu: (i) doktrin dan kebijakan militer; (ii) strategi keamanan siber nasional; dan (iii) unit siber. Penelitian ini menegaskan kembali apa yang telah dilakukan sebelumnya oleh sejumlah ilmuwan. Pernik menyarankan tiga dokumen disusun untuk melindungi pertahanan siber dari berbagai serangan, masing-masing adalah: (i) dokumen yang mengatur aspek keamanan seluruh jaringan utama negara; (ii) dokumen yang secara khusus mengatur pengendalian terhadap infrastruktur kritis nasional; dan (iii) dokumen militer yang secara khusus membahas persoalan keamanan dan pertahanan nasional dalam kaitannya dengan dunia siber (Pernik, 2020). Dalam Pemerintahan Obama, lahir satu pemikiran mengenai perlunya langkah-langkah strategis dalam menjaga kedaulatan siber (Lilli, 2020; “Obama: Cyber-Czar to Be Hand-Picked,” 2009), yaitu:

1. Membuat sistem yang mendukung adanya semangat berbagi situasi dan kondisi siber antar berbagai pemangku kepentingan, terutama dalam kaitannya untuk mendukung komunikasi antara pemerintah dan pihak swasta;
2. Meningkatkan kapabilitas dalam merespon secara cepat jika terjadi insiden atau permasalahan di dunia siber yang mengganggu kondisi pertahanan negara;
3. Memperbaiki kapabilitas aktivitas “*counterintelligence*” di dalam dunia siber;
4. Mengembangkan sistem rantai pasokan informasi terkait dengan keamanan siber yang melibatkan berbagai *stakeholder* lintas institusi;
5. Mensosialisasikan secara masif aspek edukasi siber ke segenap masyarakat dan pemangku kepentingan kunci;
6. Mengkoordinasikan dan mengembangkan riset di bidang pertahanan siber; dan
7. Mengembangkan strategi *deterrence* yang efektif, efisien, dan terkendali.



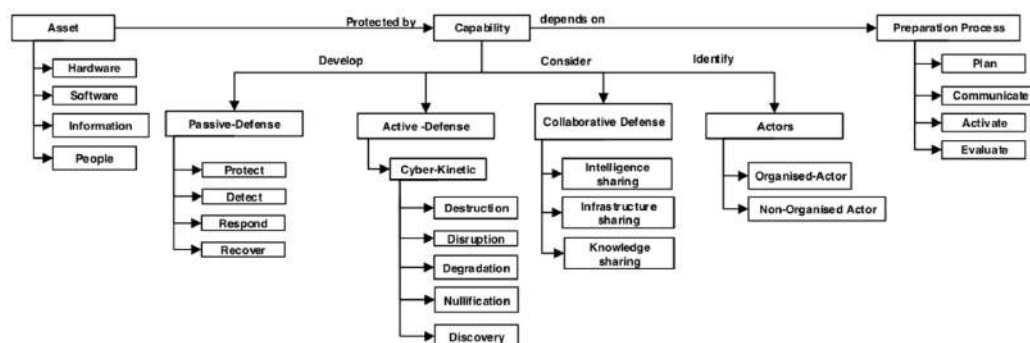
Tabel 4. 44 Komponen Militerisasi di Dunia Siber

| Component                               | Score | Description                                                                                                                   |
|-----------------------------------------|-------|-------------------------------------------------------------------------------------------------------------------------------|
| <i>Military doctrine/policy</i>         | (1)   | Has a dedicated doctrine/policy that recognize cyberspace as a unique domain of warfare or as a source of existential threats |
|                                         | (0.5) | Has a separate doctrine/policy where cyberspace is recognized as a domain of warfare or as a source of existential threats    |
|                                         | (0)   | Has no doctrine/policy that recognizes cyberspace as a domain of warfare or as a source of existential threats                |
| <i>National cyber security strategy</i> | (1)   | Has an existing national strategy recognizing state or state-sponsored OCOs as a threat                                       |
|                                         | (0.5) | Has an existing national strategy but does not recognize state or state-sponsored OCOs as a threat                            |
|                                         | (0)   | Has no existing national strategy                                                                                             |
| <i>Cyber units</i>                      | (1)   | Has an existing military organization responsible for cyberspace                                                              |
|                                         | (0.5) | Has an existing civilian organization responsible for cyberspace                                                              |
|                                         | (0)   | No existing organization responsible for cyberspace                                                                           |

Sumber : Komponen Militerisasi di Dunia Siber (Gomez, 2016)

Kolini dan Janczewski beserta beberapa ilmuwan memulai penelitian pengembangan tata kelola siber dengan memperkenalkan konsep *Cyber*

*Defense Capability Model*. Pendekatan yang diperkenalkannya ini berpegang pada satu premis utama, dimana aset berharga harus dilindungi oleh pihak tertentu yang memiliki kapabilitas, dimana kinerjanya akan sangat tergantung dari serangkaian proses perencanaan yang matang (Dube & Mohanty, 2020; Ghaffari & Arabsorkhi, 2019).



Gambar 4. 52 Cyber Capability Defense Model

Sumber : Cyber Capability Defense Model

(Dube & Mohanty, 2020; Ghaffari & Arabsorkhi, 2019)

Terlihat dalam model ini bahwa aset siber yang dimaksud adalah perangkat keras, perangkat lunak, informasi, dan sumber daya manusia. Sementara kapabilitas yang harus dimiliki dalam konteks pertahanan dan kedaulatan siber adalah kemampuan melindungi (*passive-defense*) dan menyerang (*active-defense*) dengan berbekal aktivitas kolaborasi (*collaborative defense*) antar sejumlah pihak atau aktor (Hey, 2004).

Tabel 4. 45 Ragam Aktivitas IGO

| IGOs                                                         | Liability                                       | Cyber Activity                                                            | Members                         |
|--------------------------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------|---------------------------------|
| United Nations (UN)                                          | International treaty based with legal authority | Policy maker , Disputes, and Reports                                      | 193 countries                   |
| International Telecommunication Union(ITU)                   | Treaty based organization                       | Coordination ,Guidelines, technical standards and education               | 193 countries and 700 companies |
| European Union (EU)                                          | Governing body                                  | Legislation, policy maker                                                 | 28 countries                    |
| North Atlantic Treaty Organization (NATO)                    | Treaty based organization                       | Guidelines, education, cyber/military Prevention and Response cooperation | 33 countries                    |
| Organization for Economic Co-operation and Development(OECD) | International Forum                             | Publications and reports                                                  | 34 countries                    |
| Asia-Pacific Economic Cooperation(APEC)                      | International Forum                             | Publications and reports                                                  | 21 countries                    |
| Organization for Security Co-operation in Europe (OSCE)      | Regional Security Organization                  | Training , workshops and reports                                          | 57 countries<br>11 partners     |

Sumber : Ragam Aktivitas IGO (Hey, 2004)

Dan ketika berbicara aktor, maka terlihat tiga pihak yang paling berperan dalam mengelola “kedaulatan” siber. Pihak pertama adalah jejaring organisasi pemerintahan atau *Intergovernmental Organization (IGO)* yang terdiri dari sejumlah komunitas besar. Sementara pihak kedua adalah organisasi teknis pengelola jejaring internet dunia, yang kerap disebut sebagai *the International Internet Technical Organization (IITO)*, yang bertanggung jawab terhadap pengembangan standar dan protokol tata kelola dunia siber.

Tabel 4. 46 Ragam Aktivitas IITO

| IITO                                                       | Structure              | Cyber Activity                                         |
|------------------------------------------------------------|------------------------|--------------------------------------------------------|
| Internet Corporation for Assigned Names and Numbers(ICANN) | Non-Profit corporation | Manage IP addresses and DNS                            |
| Internet Engineering Task Force (IETF)                     | Non-Profit corporation | Design and develop technology, protocols and guideline |
| The World Wide Web Consortium (W3C)                        | Committee              | Web Standards                                          |

Sumber : Ragam Aktivitas IITO (Hey, 2004)

Dan yang ketiga adalah institusi-institusi lain yang terlibat secara langsung maupun tidak langsung dengan pengelolaan keamanan di dunia siber,



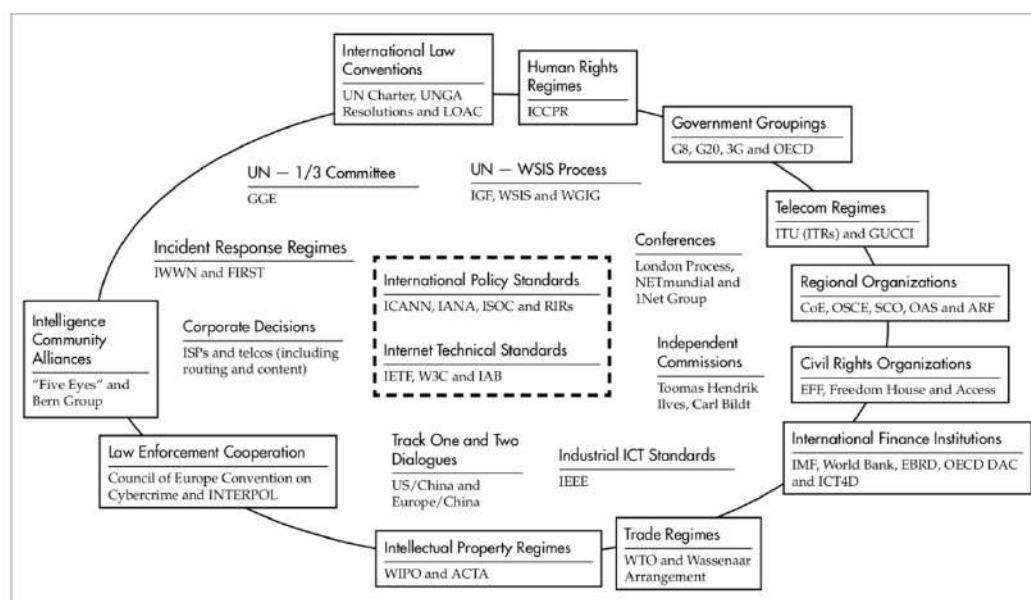
khususnya adalah CSIRT dan/atau CERT dari berbagai komunitas dan negara (Allen, 2001; West-Brown et al., 2003)

Tabel 4. 47 Ragam Aktivitas CSIRT/CERT

| Institutions                                                         | Scope            | Cyber Activity                 |
|----------------------------------------------------------------------|------------------|--------------------------------|
| Computer Emergency Response Team Coordination Centre (CERT – CC)     | International    | Coordination of global CERT    |
| Asia Pacific (AP)-CERT                                               | Regional -Asia   | Asian Regional coordination    |
| TF-CSIRT                                                             | Regional -Europe | European regional coordination |
| Forum of Incident Response and Security Teams (FIRST)                | International    | Forum and Information sharing  |
| International Multilateral Partnership Against Cyber Threat (IMPACT) | International    | Global threat response centre  |

Sumber : Ragam Aktivitas CSIRT/CERT (Allen, 2001; West-Brown et al., 2003)

Dalam karyanya berjudul *“The Regime Complex for Managing Global Cyber Activities”*, Nye menggambarkan bagaimana seluruh pihak ini berperan, berkolaborasi, dan bekerjasama dalam mengelola dunia siber. Terlihat secara jelas bahwa perkembangan teknologi siber yang sedemikian pesat terjadi akibat adanya kerjasama berbagai pihak, sehingga membentuk sebuah ekosistem dengan tingkat ketergantungan tinggi antar satu dan lainnya (Nye, 2014).



Gambar 4. 53 Kolaborasi Stakeholder Utama Pengelola Siber

Sumber : Kolaborasi Stakeholder Utama Pengelola Siber (Nye, 2014)

Sementara itu hasil studi KPMG terhadap fenomena kedaulatan siber di China berhasil mengidentifikasi sejumlah komponen penting yang harus ada dalam kerangka tata kelola pertahanan siber. Kerangka dimaksud dibagi menjadi 4 (empat) domain utama, yaitu: (i) Strategi dan Tata Kelola; (ii) Transformasi Keamanan; (iii) Layanan Pertahanan Siber; dan (iv) Asesmen dan Jaminan Kinerja. Masing-masing domain ini selanjutnya dibagi menjadi sejumlah sub-domain yang saling terkait satu dan lainnya. Berbeda dengan negara-negara barat yang cenderung berkolaborasi dalam mengelola dunia siber, China berusaha untuk membangun sendiri ekosistem sibernya (Kanwal, 2009; Zeng et al., 2017).

Sebuah pendekatan lain bernama *distributed cyber-security framework for heterogeneous environments* ditawarkan sebagai landasan dalam menggambarkan model tata kelola siber. Kerangka ini membagi siber menjadi sejumlah *layer* atau lapisan (R. Bolla et al., 2019; Raffaele Bolla et al., 2018).

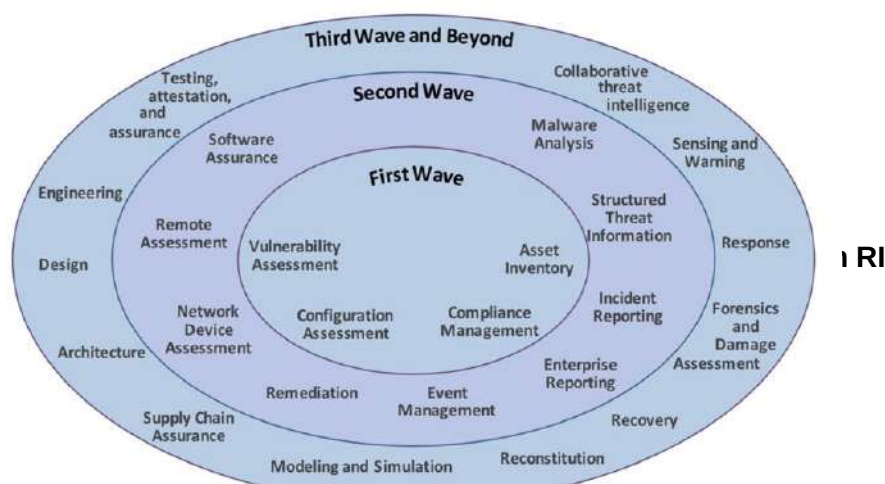


Gambar 4. 54 Kerangka Filosofi Tata Kelola Siber di China

Sumber : Kerangka Filosofi Tata Kelola Siber di China

(R. Bolla et al., 2019; Raffaele Bolla et al., 2018)

Pada lapisan Strategi dan Tata Kelola, terdapat komponen *governance*, ruang kendali siber, manajemen risiko, proteksi data *privacy*, serta ketahanan siber. Sementara dalam lapisan Transformasi Keamanan terapat komponen arsitektur keamanan, program perubahan, manajemen akses identitas, edukasi dan sosialisasi, serta perangkat infrastruktur teknologi. Pada lapisan Layanan Pertahanan Siber, terdapat latihan perang siber, keamanan aplikasi, tes penetrasi, dan penanganan insiden. Dan pada lapisan Layanan dan Jaminan Kinerja, terdapat komponen standar industri, audit internal siber, rantai pasokan keamanan, asesmen kematangan keamanan siber, dan kajian regulasi (Dilisen, 2018). Pentagon menggambarkan kondisi serupa dalam sebuah ilustrasi ekosistem strategis keamanan siber yang harus dikendalikan secara otomatis dengan menggunakan teknologi informasi dan komunikasi termutakhir (X. Hu & Wang, 2018; Mohd Nizam et al., 2015).

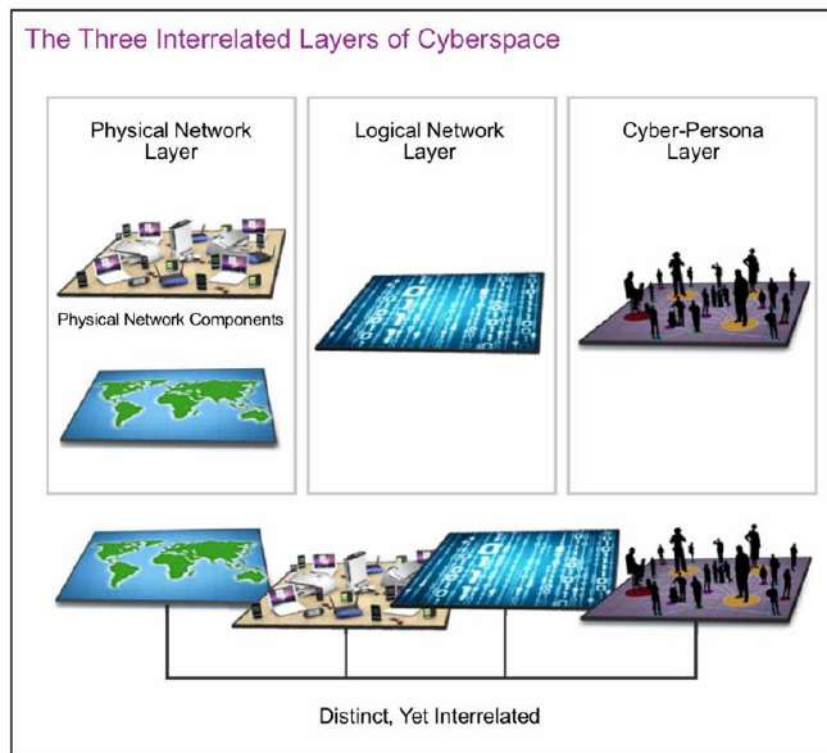


Gambar 4. 55 Ekosistem Strategis Tata Kelola Keamanan Siber

Sumber : Ekosistem Strategis Tata Kelola Keamanan Siber

(X. Hu & Wang, 2018; Mohd Nizam et al., 2015)

Terlihat dalam ekosistem ini bagaimana model pertahanan dan keamanan siber bergerak dari yang bersifat reaktif menuju pada yang lebih preventif. Pandangan menarik lainnya digambarkan oleh Pentagon untuk memberikan gambaran pada kaum awam bagaimana dunia fisik dan siber saling berkaitan satu dan lainnya. Pada dasarnya dalam dunia siber terdapat tiga *layer*, yaitu: lapisan jejaring fisik, lapisan jejaring logika, dan lapisan jejaring manusia. Ketiga lapisan ini saling bersinggungan sehingga aktivitas dalam dunia siber yang pada dasarnya bermain di jaringan logika, akan berpengaruh secara nyata pada dunia fisik yang terdiri dari manusia dan entitas fisik lainnya (Arnold, 2013; Ma et al., 2015).

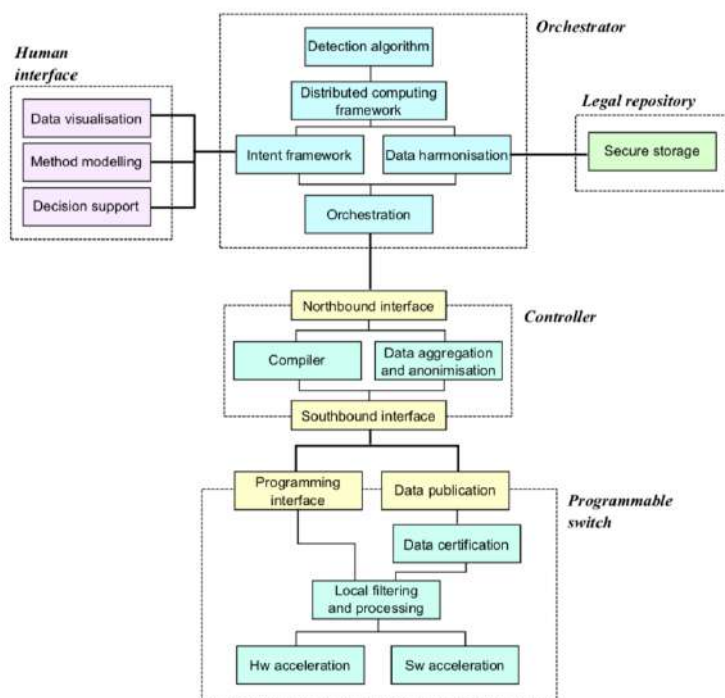


Gambar 4. 56 Tiga Lapisan Interkoneksi dalam Dunia Siber

Sumber : Tiga Lapisan Interkoneksi dalam Dunia Siber (Arnold, 2013; Ma et al., 2015)

Lapisan terbawah berisi aset utama yang harus dilindungi, yaitu data dan informasi yang berada dalam ekosistem perangkat keras dan perangkat lunak terkait dengannya. *Layer* terbawah ini dinamakan sebagai *programmable switch* dengan sifatnya yang dapat diaktifkan atau dinonaktifkan secara mudah. Keseluruhan aset strategis inilah yang selanjutnya akan dikendalikan oleh layer berikutnya yaitu *controller*, yang berfungsi melakukan pengolahan atau operasi

terkait lainnya terhadap aset digital yang ada (R. Bolla et al., 2019; Raffaele Bolla et al., 2018).



Gambar 4. 57 Kerangka Heterogen Terdistribusi

Sumber : Kerangka Heterogen Terdistribusi

(R. Bolla et al., 2019; Raffaele Bolla et al., 2018)

Hasil olahan ini kelak akan dipakai oleh manusia sebagai pengguna (*human interface*) dimana proses pengaksesan, pengorganisasian, dan pendistribusian aset digital harus dilakukan melalui prosedur baku `harmonis inilah maka diperlukan satu layer terpenting yang bernama *orchestrator* – dengan fungsi selayaknya sistem syaraf dalam tubuh manusia.

Dalam karyanya yang fenomenal berjudul “Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance”, pakar siber Jayawardane mengatakan perlunya dibuat matrik “siapa melakukan

**Universitas Pertahanan RI**

aktivitas apa” dalam penggambaran kerangka tata kelola siber. Yang bersangkutan memberikan contoh bagaimana dunia siber saat ini dikelola oleh sejumlah pihak kunci yang saling berbagi peran.



| Actors                                                                  | Activity                                              |                                             |                                                                                           |                                                                            |                                    |
|-------------------------------------------------------------------------|-------------------------------------------------------|---------------------------------------------|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|------------------------------------|
|                                                                         | NORM DEVELOPMENT<br>(OR CONTESTING<br>EXISTING RULES) | NORM<br>DISSEMINATION AND<br>IMPLEMENTATION | AGREEING ON<br>"SOFT" NORMS (E.G.,<br>INFORMAL CODES OF<br>CONDUCT OR SOCIAL<br>COMPACTS) | AGREEING<br>ON BINDING<br>INTERNATIONAL<br>LEGAL OBLIGATIONS<br>(TREATIES) | ENFORCING LEGALLY<br>BINDING RULES |
| STATES                                                                  |                                                       |                                             |                                                                                           |                                                                            |                                    |
| INTERNATIONAL /<br>REGIONAL ORGANIZATIONS<br>(E.G., UN, ITU, EU)        |                                                       |                                             |                                                                                           |                                                                            |                                    |
| PRIVATE SECTOR<br>ORGANIZATIONS (SUCH AS<br>BUSINESSES, BUT ALSO ICANN) |                                                       |                                             |                                                                                           |                                                                            |                                    |
| CIVIL SOCIETY ORGANIZATIONS<br>(THINK TANKS, ADVOCACY<br>GROUPS)        |                                                       |                                             |                                                                                           |                                                                            |                                    |
| TECHNICAL COMMUNITY                                                     |                                                       |                                             |                                                                                           |                                                                            |                                    |

Gambar 4. 58 Berbagai Peran dalam Pengelolaan Siber

Sumber : Berbagai Peran dalam Pengelolaan Siber (Jayawardane, 2015)

Pandangan umum para praktisi internet di Indonesia mengatakan bahwa negara tidak memiliki kedaulatan penuh terhadap tata kelola dan manajemen sibernya. Berbagai fakta dan kenyataan memperlihatkan bahwa tidak dimilikinya strategi siber nasional yang holistik dan komprehensif telah menyebabkan begitu rapuhnya sistem pertahanan siber Indonesia sehingga mudah sekali diintervensi oleh institusi asing maupun berbagai pihak lain yang tidak bertanggung jawab.



## Strategi Pengembangan Kebijakan Pertahanan Siber Nasional

Hasil pengolahan data yang berkaitan secara erat dengan pengembangan strategi pertahanan siber ideal yang holistik dan komprehensif dalam sebuah ekosistem disaripatikan dalam tabel berikut ini.

Tabel 4. 48 Hasil Pengolahan Data Strategi Pengembangan Kebijakan Pertahanan Siber Nasional

| No | Hasil Pengolahan Data                                                                                                                                                                                                                                                                                                                                  | Sumber                                             |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| 1  | <i>“Ekosistem pertahanan siber yang holistik dan komprehensif harus terdiri dari dua unsur utama, masing-masing adalah infrastruktur dan suprastuktur. Doktrin pertahanan rakyat semesta dalam jaman digital harus disusun dan dikembangkan, karena hanya dengan demikian maka Indonesia akan memiliki postur pertahanan yang kuat dan berdaulat.”</i> | Kemal Stamboel,<br>Anggota DPR-RI, Wawancara       |
|    | <i>“Harus dibedakan antara penyusun kebijakan dan pelaksana kebijakan, agar secara tata kelola dapat berjalan dengan baik dan efektif.”</i>                                                                                                                                                                                                            | Suhono<br>Supangkat, Guru Besar ITB, Webinar       |
|    | <i>“Teknologi dapat membantu terkelolanya kebijakan dengan baik dengan berpegang pada smart regulation”</i>                                                                                                                                                                                                                                            | Marsudi<br>Kisworo,<br>Komisaris Telkom, Wawancara |
| 2  | <i>“Kolaborasi dan kooperasi di Indonesia sangatlah mahal harganya, karena masih banyak pihak yang bekerja sendiri-sendiri dalam menangani permasalahan siber. Paling tidak harus terbentuk quadhelix stakeholder relationships, yaitu antara pemerintah, bisnis, akademisi, dan masyarakat dalam menangani berbagai isu di dunia virtual.”</i>        | Bondan<br>Widiawan,<br>Deputi BSSN, RTD            |
|    | <i>“Kerjasama antara pemerintah, industri, dan akademisi adalah sebuah kenischayaan dalam membangun sistem</i>                                                                                                                                                                                                                                         | Benny Mutiara,<br>Sekjen Aptikom, Komunikasi       |

- siber yang berdaulat penuh serta mandiri.” Personal
- “Silos-silos dalam pemerintahan harus dikikis habis jika ingin memiliki ekosistem pertahanan dan keamanan siber yang kuat.” Gildas Deograt, Xecure.id, Diskusi
- 3 “Banyak organisasi dan institusi penting di Indonesia yang belum mengadopsi standar keamanan yang baik sehingga sangat rentan dari serangan siber. Perlu diperhatikan bahwa sejumlah standar nasional telah diadopsi menjadi Standar Nasional Indonesia.” Eko Budiardjo, Ketua IPKIN, RTD
- “Cukup banyak standar keamanan informasi dan internet yang harus diimplementasikan oleh institusi penting dan terkemuka di tanah air – salah satunya adalah ISO-27001 dan ISO-27002.” Agung Martono, Ketua LSP Komputer, Diskusi
- “Standar adalah kriteria minimum yang harus dipenuhi oleh institusi kritikal nasional. Tanpanya akan sulit melindungi aset-aset digital strategis yang mempengaruhi hidup masyarakat banyak.” Adjat Daradjat, Mantan Ketua BNSP, Diskusi
- 4 “Ekonomi digital tidak saja merupakan hasil dari perkembangan serta kemajuan teknologi, tetapi merupakan bagian dari skenario negara maju dalam menguasai dunia. Transformasi digital yang dilakukan berbagai pihak, baik pemerintah maupun swasta, harus dilandasi dengan keberpihakan terhadap kepentingan dalam negeri. China adalah salah satu contoh sebagai negara yang mencoba untuk keluar dari jeratan negara Barat melalui pengembangan sistem sibernya secara mandiri.” Ardi Sutedja, Ketua ICSF, Wawancara
- “Indonesia memiliki potensi mengikuti China membuat sistem internetnya sendiri, khusus untuk melayani kebutuhan masyarakat dalam negeri.” Heru Purnomo Ipung, Peneliti Swiss-German University, Diskusi
- “Peta jalan AI nasional salah satunya bertujuan agar Indonesia dapat melakukan transformasi digital secara menyeluruh sehingga memberikan daya saing tinggi di waktu mendatang.” Hammam Riza, Kepala BPPT, FGD
- 5 “Harus ada keberpihakan negara terhadap inovasi dalam negeri yang berusaha mengembangkan berbagai

- perangkat hardware dan software di bidang pertahanan maupun keamanan siber. Ekosistem peraturan lebih banyak berpihak pada produk asing. Perlu dilihat pula masalah sumber energi komputasi, yaitu listrik yang merupakan bagian dari infrastruktur kritis (bagian dari *physical risk, application risk, dan services risk*).”
- Ketua CSIRT.id,  
Wawancara
- “Indonesia telah berhasil menciptakan sejumlah software dan hardware yang dapat dipergunakan untuk mengurangi ketergantungan dari negara lain sekaligus menurunkan risiko bocornya data.”
- Gildas Deograt,  
Xecure IT,  
Diskusi
- “Akan sulit bagi sebuah negara untuk dapat berdaulat di bidang siber tanpa kemampuan dalam mengembangkan industri teknologi informasi dan komunikasinya”
- Arko Djajadi,  
IULI, Diskusi
- 6 “Perlu ada rencana strategis yang komprehensif terhadap pertahanan dan keamanan siber, terutama terkait dengan peta jalan pengembangannya. Misalnya terkait dengan Indonesia 4.0 selain keamanan siber, perlu juga ada roadmap untuk pertahanan siber – yang melibatkan seluruh stakeholder pada ekosistem.”
- Charles Liem,  
Peneliti Swiss-German University,  
Wawancara
- “Roadmap AI Nasional sangat berkaitan erat dengan Revolusi Industri 4.0 yang sedang melanda Indonesia dan dunia.”
- Hamman Riza,  
Kepala BPPT,  
FGD
- “Kombinasi antara pendekatan top-down dan bottom-up dibutuhkan dalam membuat peta jalan yang efektif dan didukung oleh banyak stakeholder.”
- Zainal Hasibuan,  
Anggota Wantiknas, RTD
- 7 “Kultur SDM Indonesia dalam hal keamanan informasi sangatlah rendah. Dalam peningkatan *capacity building*, diperlukan sejumlah inisiatif yang berkaitan dengan: *public awareness, professional training, national education programmes, research and development, incentive mechanism, dan home-grown industry*. Indonesia sejauh ini masih terlalu banyak fokus pada usaha edukasi dan sosialisasi.”
- Zainal Hasibuan,  
Anggota Wantiknas,  
RTD
- “Literasi digital masyarakat Indonesia perlu ditingkatkan secara signifikan melalui program pendidikan dan sosialisasi yang bersifat masif dan berkesinambungan.”
- Muhaemin,  
Ketua LSP Informatika,  
Diskusi

*“SKKNI dan KKNi terkait dengan pertahanan dan keamanan siber harus disusun serta diberlakukan di seluruh wilayah tanah air.”*

Eko Budiardjo,  
Ketua IPKIN,  
RTD

Sumber : Hasil Pengolahan Data Strategi Pengembangan Kebijakan Pertahanan Siber Nasional (hasil pengolahan data oleh peneliti)

Hasil olahan data kualitatif yang dikumpulkan memperlihatkan pula adanya sejumlah fenomena yang memiliki keterkaitan dengan usaha menyusun dan mengembangkan strategi pertahanan siber di Indonesia selama ini. Berikut adalah sejumlah fenomena dimaksud.

#### Fenomena 1: Serangan Siber Tanpa Akhir

Semenjak peristiwa peretasan sistem Pemilu tahun 2004, terjadi serangan siber tanpa henti dalam ekosistem siber atau internet di tanah air. Lembaga pengawas internet Indonesia yaitu ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure) mensinyalir bahwa pada tahun 2005-2010, paling tidak terjadi kurang lebih rata-rata 1.5 juta serangan per hari. Dewasa ini, jumlah serangan siber yang terjadi pun semakin banyak – jauh dari berkurang frekuensi dan volumenya. Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa selama tahun 2020 paling tidak terjadi 400 juta serangan yang ditujukan ke dalam situs-situs Indonesia. Sementara The Communication and Information System Security Research Center (CISSReC) memperkirakan bahwa terdapat lebih dari 1 milyar serangan di tahun yang sama. Salah satu hasil laporan BSSN yang menarik untuk dicermati adalah bahwa pada masa pandemi, tren serangan di dunia siber Indonesia meningkat enam kali lipat dari kondisi normal. Fenomena serangan siber di Indonesia pun mendapatkan perhatian khusus di level global. Paling tidak Indonesia tercatat sebagai negara dengan kasus *malware* tertinggi di Asia Pasifik – berdasarkan data di tahun 2019 yang mencatat bahwa 10,68% *malware* yang ada di kawasan regional berasal dari Indonesia. Serangan *ransomware* WannaCry yang mengguncang dunia juga

menarik untuk dicermati, karena ternyata Indonesia menempati urutan kedua dari negara yang paling banyak terjangkiti virus ini – dilihat dari ribuan alamat IP yang menjadi target dan korban. Intinya adalah bahwa sejalan dengan perkembangan teknologi, fenomena ancaman dan serangan siber di tanah air bukannya menurut, namun justru bertambah frekuensi, volume, dan kompleksitasnya. Penyebab dan motivasi dari terjadinya serangan pun beraneka ragam, seperti: ekonomi, politik, sosial budaya, maupun pertahanan-keamanan.

Serangan yang terjadi di masa lalu pun menyisakan begitu banyak kerugian dan permasalahan yang belum teratasi. Buktinya adalah masih terjadinya peristiwa serupa di masa kini walaupun telah lebih dari dua windu Indonesia menekuni perkembangan pertahanan dan keamanan siber. Ketika serangan Sistem Pemilu 2004 yang menimbulkan ketegangan nasional terjadi, banyak hal yang dapat dipelajari daripadanya (Arianto & Anggraini, 2019). Namun beberapa kali pemilu yang terjadi setelahnya pun tidak luput dari berbagai serangan dan menyita begitu banyak perhatian karena keberhasilan peretas dalam menembus sistem teknologi yang diberitakan telah dilindungi dengan teknologi pengaman yang berkualitas. Masih teringat pula betapa besar kerugian material maupun immaterial yang disebabkan serangan *malware* WannaCry yang menimpa Indonesia, karena kehadirannya tidak saja merugikan berbagai institusi secara finansial, namun ada pula yang mengancam jiwa manusia karena ditargetkan ke pusat-pusat kemanusiaan seperti rumah sakit dan puskesmas (Kenway, 2019). Belum lagi terhitung berbagai serangan yang menimpa dunia perbankan dan telekomunikasi, yang telah mendatangkan banyak kerugian di kalangan masyarakat. Pembobolan akun-akun pribadi di situs media sosial pun membuat jutaan data pribadi milik masyarakat Indonesia jatuh ke tangan pihak-pihak lain yang tidak berhak memilikinya.

Wakil Ketua ID-SIRTII periode pertama, Muhammad Salahuddien, memberikan pendapatnya mengenai fenomena dimaksud dalam wawancara sebagai berikut:

“Sebagian besar serangan ke situs-situs pemerintahan di Indonesia justru berasal dari dalam negeri. Faktor pemicu yang paling besar adalah karena masalah politik. Artinya adalah bahwa ancaman serangan siber akan selalu membayangi

negara sejalan dengan hiruk pikuk dinamika politik yang terjadi. Selain politik, faktor lain yang kerap memicu adanya serangan siber dari dalam negeri karena maraknya aktivitas 'hactivism' yang dilakukan anak-anak muda praktisi teknologi informasi dan komunikasi dengan berbagai alasan motivasi yang didominasi oleh militansi dan idealisme yang tinggi".

Pendapat ini sejalan dengan yang disampaikan Bisyrn Wahyudi selaku peneliti di Academic-CERT yang secara jelas mengatakan dalam keterlibatannya dalam penelitian ini bahwa:

"Seluruh pihak harus waspada selama 24/7 karena sewaktu-waktu serangan siber dari dalam negeri dapat terjadi. Isu yang sedang memanas di tanah air, yang diwarnai dengan pro dan kontra, berpotensi memicu terjadinya serangan-menyerang di dunia internet antar para pihak yang berseteru. Negara dengan berbagai komponennya harus memahami situasi ini dan memiliki kemampuan dalam mengantisipasi maupun menghadapinya".

Artinya adalah bahwa siap atau tidak siap, negara akan selalu dibayangi oleh berbagai ancaman serangan siber dari dalam maupun luar negeri sejalan dengan dinamika penyelenggaraan negara.

### Fenomena 2: Perangkat Regulasi Siber Nasional

Dibandingkan dengan negara lain, Indonesia termasuk negara yang sangat sedikit memiliki perangkat regulasi terkait dengan tata kelola, manajemen, dan ekosistem siber. Satu-satunya "regulasi pamungkas" yang paling banyak dipergunakan adalah Undang-Undang Informasi dan Transaksi Elektronik yang dilahirkan pada tanggal 25 Maret 2008 dan telah diadendum beberapa kali. Sementara regulasi lainnya yang terkait dengan *cyber law* tersebar dalam berbagai peraturan dan perundang-undangan lainnya secara parsial. Padahal sebagai sebuah domain kehidupan masyarakat moderen yang sangat penting, ekosistem siber dan teknologi informasi komunikasi harus dikelola secara holistik dan komprehensif – dimana di dalamnya membutuhkan begitu banyak peraturan dan perundang-undangan yang berlaku. Contohnya undang-undang yang



diperlukan misalnya terkait dengan aspek: kejahatan siber, kedaulatan siber, perlindungan data pribadi, rahasia negara, infrastruktur informasi kritis nasional, telekomunikasi berbasis internet, industri teknologi informasi dalam negeri, tata kelola internet nasional, perang siber, dan lain sebagainya (Corn & Taylor, 2017; Rizal & Yani, 2016). Ketiadaan atau kekosongan peraturan ini mendatangkan permasalahan tersendiri bagi institusi negara dalam menjalankan peran dan fungsinya. Pakar hukum siber, Freddy Harris, secara jelas mengatakan bahwa:

“Indonesia perlu memiliki sejumlah peraturan selevel undang-undang yang berbicara mengenai berbagai komponen dalam cyberlaw. Undang-Undang ITE sangat jauh dari memadai untuk mengatasi berbagai isu termutakhir di bidang teknologi internet. Keberadaannya harus dilengkapi dengan berbagai regulasi lain setara dengannya agar berbagai permasalahan hukum yang berkaitan dengan internet dan dunia siber dapat diselesaikan”.

Contohnya adalah Badan Siber dan Sandi Negara yang telah dibentuk serta ditetapkan pemerintah sebagai *leading sektor* merasa kesulitan dalam menjalankan tugas dan wewenangnya karena belum adanya undang-undang yang mendasari aktivitasnya. Pembentukannya yang didasarkan pada Peraturan Presiden ini sulit beraktivitas secara efektif karena begitu banyaknya tugas pokok dan fungsi yang bersinggungan dengan undang-undang sektor lain yang menjadi wewenang lembaga negara dan pemerintah lainnya. Kasus lain menimpa Kementerian Komunikasi dan Informatika yang mengalami kesulitan dalam mengatur infrastruktur kritis nasional karena keberadaannya diatur dalam sistem perundang-undangan yang berkaitan erat dengan Kementerian Badan Usaha Milik Negara. Karakteristik siber yang sifatnya lintas sektor dan teritorial mempersulit pemerintah dalam mengatur dan mengelola sistem perundang-undangan yang selaras dengannya.

### Fenomena 3: Kendali Global Ekosistem Siber

Arena siber terbentuk dari adanya interkoneksi antar berbagai pusat komputasi melalui infrastruktur telekomunikasi lokal, nasional, dan global. Artinya adalah bahwa internet Indonesia terbentuk karena adanya jejaring infrastruktur

telekomunikasi yang dikelola oleh berbagai pihak, terutama perusahaan telekomunikasi dan Internet Service Provider (ISP). Perlu dipahami bahwa di antara perusahaan-perusahaan telekomunikasi besar di Indonesia, hanya tinggal PT Telkom Tbk yang kepemilikan saham terbesarnya dimiliki oleh bangsa Indonesia. Sementara perusahaan yang lain sudah menjadi milik bersama antara Indonesia dengan negara lain, seperti: PT Telkomsel (Singapore Telecom), PT Indosat Ooredoo (Qatar Telecom), dan PT XL Axiata (Malaysia). Kepemilikan asing tersebut membuat negara sulit memiliki keleluasan untuk mengendalikan perusahaan-perusahaan tersebut sehingga kerap kali dalam sejumlah kesempatan terjadi ketegangan ketika negara mengharuskan korporasi dimaksud melakukan aksi-aksi tertentu untuk mengantisipasi berbagai hal yang mengancam keselamatan bangsa dan negara.

Kepemilikan asing pula yang menciptakan tantangan tersendiri, karena berdasarkan undang-undang perseroan terbatas, kekuasaan tertinggi terletak pada Rapat Umum Pemegang Saham. Artinya adalah bahwa segala aksi korporasi yang dilakukan, baik dalam kondisi normal maupun darurat, pemerintah Indonesia tidak dapat melakukan intervensi terhadapnya ketika terjadi situasi dan kondisi tertentu yang membahayakan keselamatan bangsa dan negara. Contoh klasiknya adalah ketika dalam beberapa situasi perusahaan diminta pemerintah untuk memutuskan sejumlah koneksi karena alasan untuk mencegah terjadinya kerusuhan lebih besar sebagaimana sering mengemuka dalam kasus separatisme, pemberontakan, kerusuhan, dan lain sebagainya. Pada situasi ini, korporasi tidak dapat dengan mudahnya mengikuti perintah tersebut karena harus mempertanggung jawabkannya secara komersial karena berpotensi merugikan perusahaan dan pelanggan yang dilayaninya.

Hal serius lainnya adalah terkait dengan adanya dominasi perusahaan-perusahaan raksasa internasional yang menjadi produsen berbagai perangkat teknologi *hardware* maupun *software* yang dimaknai mayoritas masyarakat Indonesia. Pada *layer* infrastruktur misalnya, perusahaan Amerika Serikat seperti AT&T dan MCI mendominasi jejaring dunia. Sementara untuk *layer* piranti jaringan, perusahaan seperti Cisco (Amerika Serikat) dan Huawei (China) mendominasi berbagai *network system* di tanah air. Belum lagi jika berbicara

mengenai sistem operasi, dimana cengkraman Microsoft Windows dan Apple IOS tetap tidak terelakkan, walaupun telah ada berbagai alternatif *open source* yang banyak dipergunakan. Berbicara mengenai komputer *server*, merek seperti IBM, Dell, dan Hewlett-Packard adalah yang paling banyak dipergunakan. Sementara pada domain gawai, tidak dapat dimungkiri adanya dominasi Samsung, Apple, OVO, dan Vivo di Indonesia. Kenyataan ini semakin meningkatkan kompleksitas pengendalian data dan informasi milik masyarakat Indonesia yang sehari-harinya mengalir melalui ragam perangkat buatan asing ini. Wawancara dengan Gildas Deograt, selaku pakar keamanan dan pertahanan siber, menghasilkan sejumlah pernyataan penting, di antaranya adalah:

“Jika ingin berdaulat dan memiliki kendali penuh terhadap sistem siber nasional, Indonesia harus berani menciptakan dan menggunakan berbagai produk teknologi informasi dan komunikasi buatan anak bangsa. Walaupun kalah bersaing dengan negara maju, paling tidak dalam sejumlah aspek pertahanan negara, banyak hal yang dapat diselamatkan – terutama dalam menghadapi ancaman yang bersifat multi-dimensi di bidang teknologi informasi akibat dipergunakannya secara masif berbagai produk buatan negara lain”.

Melalui kacamata ini dapat dipahami bagaimana negara semacam China memutuskan untuk membangun sendiri infrastruktur dan suprastrukturnya dari nol, agar tidak terjadi ketergantungan dengan negara lain yang bermuara pada hilangnya kedaulatan negara yang dimiliki.

#### Fenomena 4: Doktrin Pertahanan Siber Negara

Pada beberapa kejadian serangan siber yang menimpa institusi negara, kerap kali terjadi kegamangan dan keraguan dari lembaga-lembaga negara dalam menanganinya. Kenyataan di masa lalu memperlihatkan bahwa semakin banyaknya pihak pemangku kepentingan yang terlibat, semakin mempersulit terjadinya koordinasi untuk memecahkan masalah. Demikian pula dalam kondisi dimana sejumlah insiden terjadi pada sektor tertentu. Fenomena yang terlihat adalah kebingungan dan ketidaktahuan para pihak mengenai apa yang harus dilakukan, karena belum adanya prinsip atau panduan yang

dipegang dalam mengatasi masalah yang sebelumnya tidak pernah terjadi. Perlu dipahami bahwa hal ini terjadi sebelum maupun sesudah BSSN didirikan sebagai *leading sector*. Berkaca dari literatur yang membahas pengalaman *good practices* di negara lain, permasalahan lintas sektoral dalam menghadapi peristiwa siber hanya dapat diatasi secara cepat apabila terjadi kesamaan pandangan, prinsip, dan pola pikir di antara segenap pemangku kepentingan negara. Artinya adalah bahwa negara perlu memiliki doktrin yang menjadi pegangan bersama dalam mengelola berbagai peristiwa yang terjadi pada dunia siber (Andress & Winterfeld, 2014b).

Ketiadaan doktrin khususnya dalam konteks pertahanan dan kedaulatan siber membuat terjadinya berbagai isu koordinasi dan kooperasi di Indonesia. Alasan yang paling banyak mengemuka setiap kali institusi negara dihadapkan pada peristiwa siber adalah karena belum adanya peraturan perundang-undangan yang mengatur peran dan tanggung jawab masing-masing pihak. Seandainya pun ada, berbagai perdebatan tanpa akhir kerap terjadi yang bermuara pada tidak dilakukan tindakan eksekusi apapun karena landasan hukum yang tidak mencukupi. Dalam kondisi yang dilematis, negara-negara besar dan maju berpegang pada prinsip-prinsip yang termaktub dalam doktrin sibernya. Dengan demikian, ketika negara menghadapi berbagai situasi yang belum diatur regulasinya, doktrin siber menjadi panduan prinsip dalam melakukan berbagai aksi yang diperlukan (Alford, 2001; Ormrod & Turnbull, 2016).

Studi memperlihatkan bahwa doktrin dimaksud memiliki posisi yang berbeda-beda di setiap negara. Tipe pertama adalah yang memposisikan doktrin siber setara dengan konstitusi tertinggi – baik merupakan sebuah produk khusus atau bagian dari doktrin negara secara keseluruhan. Tipe kedua adalah memposisikan doktrin siber sebagai bagian tak terpisahkan dari doktrin pertahanan negara, karena sifatnya yang berkaitan erat dengan ancaman non-militer yang mengemuka. Tipe ketiga adalah yang memposisikan doktrin siber sebagai sebuah dokumen strategis tersendiri yang sejajar dengan doktrin-doktrin lainnya dalam konteks bernegara. Sementara tipe keempat adalah yang merupakan kombinasi atau gabungan di antaranya. Ketidadaan doktrin siber

dan/atau doktrin pertahanan siber yang dapat menjadi pegangan bersama seluruh pemangku kepentingan akan mempersulit negara dalam melakukan pengelolaan terhadap kedaulatan sibernya.

#### Fenomena 5: Infrastruktur dan Suprastruktur

Sejarah perkembangan internet di Indonesia cukup unik. Kehadirannya berbeda dengan negara-negara maju yang cenderung bersifat *top-down*. Indonesia membangun infrastruktur dan suprastruktur internetnya secara *bottom-up* – dalam arti kata dilakukan oleh para praktisi dan akademisi berbasis komunitas yang memiliki pengetahuan dalam bidang teknologi informasi dan komunikasi. Karena sifatnya yang *bottom-up*, maka dapat dilihat bagaimana terjadi perkembangan yang sporadis dan tidak terancang. Berdasarkan catatan whois ARIN dan APNIC, protokol Internet (IP) pertama dari Indonesia, UI-NETLAB (192.41.206/24) didaftarkan oleh Universitas Indonesia pada 24 Juni 1988. RMS Ibrahim, Suryono Adisoemarta, Muhammad Ihsan, Robby Soebiakto, Putu, Firman Siregar, Adi Indrayanto, dan Onno W. Purbo merupakan beberapa nama-nama pada awal pembangunan Internet Indonesia sekitar tahun 1992 hingga 1994. Mereka telah mengontribusikan keahlian dan dedikasinya dalam membangun cuplikan-cuplikan sejarah jaringan komputer di Indonesia. Pada sekitar tahun 1994 mulai beroperasi IndoNet yang dipimpin oleh Sanjaya. IndoNet merupakan ISP komersial pertama Indonesia. Pada waktu itu pihak POSTEL belum mengetahui tentang bisnis Internet & masih sedikit sekali pengguna Internet di Indonesia. Sambungan awal ke Internet dilakukan menggunakan dial-up oleh IndoNet. Lokasi IndoNet masih di daerah Rawamangun di kompleks dosen UI. Akses awal di IndoNet mula-mula memakai mode teks dengan shell account, browser lynx, dan klien surel pine serta *chatting* dengan *conference* pada *server* AIX. Pada tahun 1995, pemerintah Indonesia melalui Departemen Pos Telekomunikasi menerbitkan izin untuk ISP yang diberikan kepada IndoNet yang dipimpin oleh Sanjaya dan Radnet pimpinan BRM.

Semenjak tahun 1995, terjadi ledakan pembentukan ISP di seluruh wilayah tanah air, yang jumlahnya melebihi 350 ketika itu. Hal yang perlu dicatat adalah bahwa perkembangan internet semenjak itu sedemikian cepatnya melampaui ketersediaan infrastruktur dan suprastruktur yang memadai. Akibatnya adalah terjadi banyak keruwetan (kompleks), kesimpangsiuran, dan “kekacauan” yang terjadi karena belum diterapkannya sejumlah standar yang disepakati bersama. Situasi tersebut “diperparah” dengan literasi dunia internet yang berbeda dan beragam di antara pelaku industri, pemerintah, dan masyarakat. Sejumlah ketegangan banyak terjadi di lapangan, terutama ketika berhadapan dengan isu-isu seputar perijinan, lisensi, ruang lingkup, pajak, dan lain sebagainya. Pelaku dan praktisi sejarah, Heru Nugroho, yang merupakan mantan Ketua APJII mengatakan dalam wawancara bahwa:

“Pada saat itu, seluruh pemangku kepentingan di Indonesia sama-sama belajar mengenai bagaimana caranya mengatur internet secara baik. Gesekan antara berbagai pihak kerap terjadi. Namun semua dapat diselesaikan karena adanya kesamaan cita-cita yaitu ingin memajukan dunia siber di tanah air. Perlu diketahui bahwa dalam awal-awal perkembangannya, belum ada kementerian khusus yang mengurus berbagai hal terkait dengan internet dan teknologi informasi”.

Semenjak dibentuknya Kementerian Komunikasi dan Informatika, mulailah secara perlahan-lahan pemerintah mengatur berbagai hal terkait dengan dunia siber dan internet. Walaupun demikian, kompleksitas sejarah yang terjadi masih menyisakan berbagai pekerjaan rumah di bidang pengelolaan infrastruktur dan suprastruktur yang harus diselesaikan oleh berbagai pihak terkait.

#### Fenomena 6: Rezim dan Agenda Politik

Sejarah memperlihatkan pula bahwa pasang surut situasi siber dan internet di Indonesia sangat dipengaruhi oleh rezim yang berkuasa – terutama mereka yang dipercaya untuk menjadi nakhoda kementerian yang berkaitan dengan urusan komunikasi dan informatika. Contoh klasiknya adalah bagaimana

sulitnya melahirkan undang-undang terkait dengan *cyberlaw*. Walaupun internet Indonesia telah mulai berkembang semenjak tahun 1994, namun baru pada tahun 2008 lahir regulasi terkait dengannya, yaitu Undang-Undang Informasi dan Transaksi Elektronik. Undang-Undang yang lahir semasa pemerintahan Presiden Megawati Soekarnoputri ini harus melalui begitu banyak jalan berliku, dari mulai dibahas, direncanakan, disusun, hingga pada akhirnya berhasil diundangkan. Tidak dapat dipungkiri bahwa salah satu pemicu yang mempercepat lahirnya undang-undang ini adalah tekanan dari dunia yang ketika itu diwakili oleh World Trade Organisation. Hingga saat ini, telah begitu banyak usulan peraturan dan perundang-undangan terkait dengan internet, teknologi informasi, dan siber yang diajukan, namun belum ada tanda-tanda yang memperlihatkan seluruh peraturan tersebut akan segera diundangkan.

Pendulum keberpihakan negara terhadap dunia siber nasional sangat ditentukan oleh agenda politik pemerintah yang berkuasa. Lihatlah fenomena penjualan perusahaan Indosat ke negara lain terjadi ketika proses *recovery* krisis ekonomi dijalani. Praktis jejaring infrastruktur yang telah dibangun di seluruh negeri pindah pengendaliannya dari tangan negara ke pihak asing. Hal yang sama pun terjadi pada Excelcomindo dan Telkomsel. Contoh lain adalah ketika kejayaan Indonesia di angkasa melalui satelitnya tidak seperti dahulu, terlihat dengan begitu banyaknya institusi dan perusahaan di Indonesia yang lebih memilih memanfaatkan satelit milik negara lain dibandingkan dengan kepunyaan sendiri. Walaupun telah ada mekanisme USO (Universal Service Obligation) yang seharusnya mampu membebaskan Indonesia dari *blank spot* akses telekomunikasi, kenyataannya masih banyak wilayah Indonesia yang belum terjangkau sinyal telekomunikasi – walaupun telah beberapa kali berganti presiden dan Menkominfo. Proyek Palapa Ring yang sudah lebih dari satu dasawarsa dibicarakan akhirnya dijalankan secara serius selama masa pemerintahan Presiden Jokowi belakangan ini.

Keseluruhan fenomena di atas pada dasarnya tidak berdiri sendiri namun saling terkait satu dan lainnya. Sebenarnya masih banyak fenomena lain dalam ekosistem siber Indonesia yang menambah kompleksitas isu yang dihadapi, misalnya terkait dengan:

1. Literasi siber yang berbeda-beda di antara masyarakat Indonesia yang terbentang dari Sabang hingga Merauke, sehingga berpengaruh terhadap kematangan mereka dalam menghadapi perkembangan teknologi informasi;
2. Gap digital yang cukup besar terlihat di berbagai daerah di Indonesia, baik dalam konteks kesediaan akses, kinerja infrastruktur, literasi digital masyarakat, dan lain sebagainya;
3. Ragam generasi yang ada di masyarakat dengan pandangan dan pola pikir yang berbeda, dimana kerap terjadi gesekan antara kelompok *Veteran*, *Baby Boomers*, dan *X-Generation* dengan *Millenials* dan sesudahnya;
4. Situasi VUCA (*Volatile, Uncertain, Complex, dan Ambiguous*) yang mendominasi situasi global yang tidak dapat diprediksi maupun dikendalikan oleh siapapun; dan lain sebagainya.

*Rich Picture* sebagaimana tergambaran memperlihatkan besarnya kompleksitas yang dihadapi dunia pertahanan dan keamanan siber nasional. Gambaran tersebut memperlihatkan adanya sejumlah situasi sebagai berikut:

1. Besar dan rumitnya ekosistem dunia siber di Indonesia, terutama dalam kaitannya dengan pertahanan negara dan keamanan nasional;
2. Tingginya relasi keterhubungan antara puluhan bahkan ratusan komponen dalam sistem pertahanan dan keamanan siber nasional; dan
3. Banyaknya pihak yang terlibat secara langsung maupun tidak langsung dalam tata kelola masing-masing komponen yang tergambar dalam sistem.

Situasi dan kondisi “benang kusut” sebagaimana diperlihatkan dalam *rich picture* hanya dapat diselesaikan dengan pendekatan berbasis sistem, yaitu melihat keseluruhan lingkungan tersebut secara holistik dan komprehensif, yang





serangan non-militer, dimana penggunaan teknologi informasi menjadi kunci dalam meluncurkan serangan siber. Kejadian yang menimpa sejumlah negara di masa lalu memperlihatkan bagaimana fenomena ini akan terus menjadi tren dalam hubungan antar negara, terutama yang telah lama berselisih. Perang siber terjadi setiap hari, tak terlihat, dan tak terelakkan.

Kedua, statistik memperlihatkan bahwa frekuensi dan volume serangan siber di dalam maupun terhadap Indonesia meningkat secara pesat. Ancaman ini jika terjadi sungguh-sungguh akan memberikan dampak membahayakan bagi kesatuan dan persatuan bangsa. Oleh karena itulah maka keberadaan potensi serangan dimaksud merupakan ancaman serius bagi kedaulatan dan keutuhan NKRI.

Ketiga, pola pikir, pandangan, atau paradigma terhadap situasi global akan menentukan bagaimana pimpinan negara memandang fenomena maupun ancaman siber yang terjadi saat ini – dan di kemudian hari – harus dipandang sebagai sebuah situasi dan kondisi yang harus mendapatkan perhatian serius. Peristiwa serangan siber yang pernah hampir meruntuhkan sendi-sendi pertahanan berbagai negara tidak mustahil akan dipergunakan untuk menghancurkan Indonesia.

Keempat, pertanyaan terbesar dari sebuah negara terkait dengan kenyataan di atas adalah seberapa kuat dan rentan pertahanan maupun keamanan siber yang dimiliki Indonesia saat ini. Kondisi ini hanya dapat diketahui apabila dilakukan proses asesmen risiko secara sungguh-sungguh.

Kelima, studi dan kajian mendalam memperlihatkan bahwa kultur manusia dalam menjaga pertahanan dan keamanan siber yang melingkupi dirinya serta lingkungan masyarakatnya sangat menentukan ketahanan siber sebuah negara. Indonesia yang merupakan negara bangsa memiliki kultur yang di satu pihak menjadi kekuatan bersama sebagai modal sosial namun di sisi lain menjadi sebuah kerentanan yang mudah dieksploitasi oleh pihak lawan.

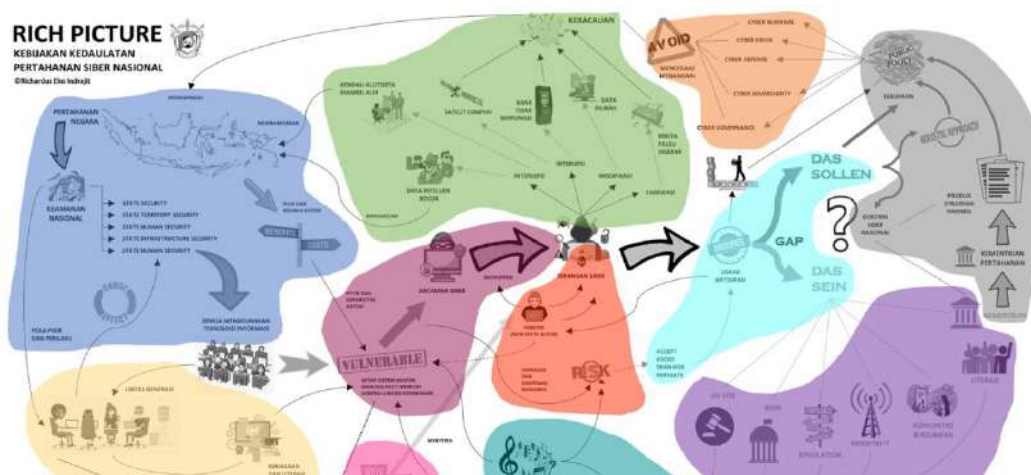
Keenam, komponen terlemah atau *the weakest link* dalam rantai jejaring arena siber bukan terletak pada teknologi atau proses, namun ada pada komponen manusia. Manusia dianggap komponen terlemah karena mudah

ditipu, diperdaya, dikelabui, dan dibohongi melalui berbagai cara dan teknik *social engineering*. Terutama masyarakat Asia yang dikenal ramah, mudah percaya, menghindari konflik, dan berfikir positif dalam hal bermasyarakat dan berinteraksi dengan orang lain, menjadi sasaran empuk bagi para penjahat siber. Merekapun sadar bahwa rata-rata literasi keamanan informasi masyarakat Indonesia relatif masih sangat rendah.

Ketujuh, karena siber merupakan arena berbasis teknologi, maka faktor kepemilikan, pengendalian, kinerja, dan industri terkait dengan komponen ini sangatlah penting untuk diperhatikan. Bukan merupakan rahasia umum bahwa hampir semua kalau tidak bisa dikatakan seluruhnya piranti komputasi seperti perangkat keras, perangkat lunak, dan perangkat jaringan diproduksi oleh negara-negara maju, sehingga mereka memiliki *bargaining position* lebih dalam ekosistem siber dunia.

Kedelapan, menghadapi serangan siber dalam situasi dan kondisi pertahanan yang lemah hanya dapat dihadapi dengan kekuatan yang dibangun melalui kolaborasi berbagai komponen yang ada dalam sebuah negara – sebagaimana layaknya sebuah perang. Kolaborasi merupakan hal yang sangat mahal karena harus menghancurkan ego-ego atau silo-silo sektoral yang kerap dimiliki oleh berbagai institusi formal maupun informal. Namun dengan impian dan kepentingan bersama, kolaborasi dapat diusahakan dengan baik.

Kesembilan, negara hanya dapat bertahan apabila dikelola dengan baik, berbasis pada *good governance*. Kolaborasi antar semua pihak akan terlaksana dalam sebuah ekosistem tata kelola yang efektif dan efisien. Tata kelola pertahanan dan keamanan siber adalah kunci dari kekuatan sebuah negara moderen.



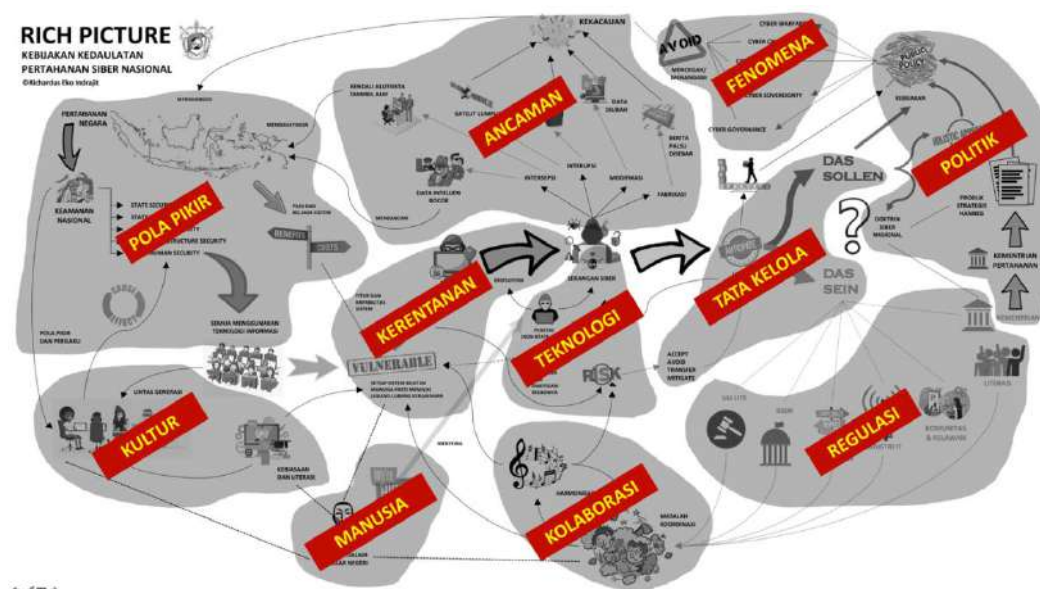
Gambar 4. 60 Klasterisasi Rich Picture Seputar  
Pertahanan Siber Nasional

Sumber : Klasterisasi Rich Picture Seputar Pertahanan Siber Nasional  
(hasil pengolahan oleh data peneliti)

Kesepuluh, tata kelola dan kolaborasi hanya dapat dijalankan apabila menjadi regulasi atau kebijakan yang harus ditaati segenap warganegara. Dalam konteks ini, perlu dikembangkan strategi yang tepat dalam menyusun regulasi, mengingat bahwa perkembangan teknologi bergerak jauh lebih cepat dari peraturan yang dibuat untuk memanfaatkan atau mengantisipasi keberadaannya.

Kesebelas, *political will* atau keinginan politik pada akhirnya akan berpengaruh dalam pembentukan ekosistem negara yang mampu membangun pertahanan dan kemanan siber yang kuat. Tidak ada regulasi, tata kelola, maupun kolaborasi yang dapat berjalan dengan baik tanpa adanya agenda politik yang didukung oleh sebanyak mungkin pihak di suatu negara. Oleh karena itulah maka komponen ini perlu mendapatkan perhatian pula dalam konteks dimaksud.

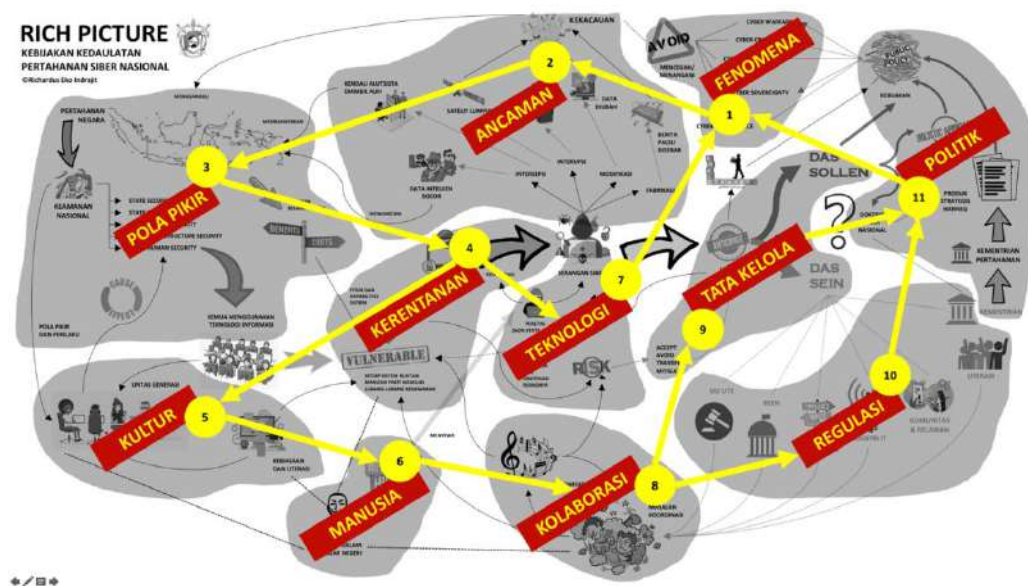
Gambar terkait memperlihatkan tema dari kesebelas domain di atas. Analisa lebih mendalam terhadapnya memperlihatkan bahwa pada dasarnya terdapat hubungan antar kesebelas domain komponen di atas. Hubungan yang bersifat siklus ini memperlihatkan bahwa isu pertahanan dan keamanan siber harus dilihat sebagai sebuah sistem yang dinamis. Melihat bahwa ada hubungan keterkaitan yang erat antar domain, maka pendekatan sistem secara holistik dan komprehensif harus dipergunakan dalam mengembangkan strategi yang tepat dalam membangun sistem pertahanan kedaulatan siber yang kokoh.



Gambar 4. 61 Domain Komponen Utama pada Ekosistem Pertahanan Siber Nasional

Sumber : Domain Komponen Utama pada Ekosistem Pertahanan Siber Nasional

(hasil pengolahan data oleh peneliti)



Gambar 4. 62 Relasi Keterkaitan antar Komponen pada Ekosistem Pertahanan Siber Nasional

Sumber : Relasi Keterkaitan antar Komponen pada Ekosistem Pertahanan Siber Nasional (hasil pengolahan oleh data peneliti)

Data yang diperoleh pertama-tama diolah menggunakan analisa CATWOE, yang merupakan singkatan dari *Customers, Actors, Transformation, Weltanschauung, Owner*, dan *Environmental Constraints*. Hasil olahannya adalah sebagai berikut.

### Customers

Pihak utama yang paling berkepentingan terhadap keberadaan strategi kebijakan pertahanan siber nasional adalah negara, yang merupakan representasi kolektif dari segenap masyarakat Indonesia. Merekalah yang mengharapkan *output* serta *outcomes* dari adanya kebijakan pertahanan siber yang kuat dan efektif, sehingga masyarakat Indonesia akan merasa aman dari berbagai ancaman yang mengintainya sehari-hari.

### Actors

Aktor yang paling bertanggung jawab dalam keberadaan dan pengembangan strategi kebijakan pertahanan siber nasional adalah pemerintah Indonesia, yang dalam manifestasinya meliputi trias politika, yaitu lembaga legislatif, eksekutif, dan yudikatif. Dalam konteks pertahanan siber, pihak yang paling banyak disebut adalah Badan Siber dan Sandi Negara, Kementerian Pertahanan, serta Kementerian Komunikasi dan Informatika.

### Transformation

Dalam konteks penelitian ini, transformasi yang dimaksud adalah menguraikan benang kusut tata kelola siber yang dimiliki menuju pada kondisi ideal, yaitu keberadaan strategi kebijakan yang efektif dalam pembentukan pertahanan siber yang kuat dan berdaulat penuh. Transformasi kebijakan dirasakan perlu karena adanya paradigma baru dalam menghadapi ancaman siber dewasa ini.

### Weltanschauung

Berbeda dengan dunia fisik, arena siber memiliki karakteristik khusus yang atributnya kebanyakan bertolak belakang dengannya. Hal ini



mengakibatkan perlunya cara pandang berbeda dalam mengembangkan kebijakan terkait dengannya. Perspektif ini mutlak diperlukan karena penyebab utama tidak efektifnya kebijakan yang disusun selama ini adalah akibat penyusunnya salah menggunakan kacamata analisa.

### Owner

Indonesia sebagai sebuah negara berdaulat, adalah pemilik dari aktivitas transformasi dan kebijakan yang dikembangkan. Sebagai “pemilik”-nya, Indonesia sangat berkepentingan menciptakan suasana aman bagi masyarakatnya, agar pembangunan nasional dapat dilaksanakan demi tercapainya tujuan negara. Oleh karena itulah maka pemerintah harus berinvestasi mengembangkan strategi kebijakan pertahanan siber yang berdaulat penuh, jauh dari intervensi pihak-pihak asing yang berpotensi merugikan bangsa.

### Environmental Constraints

Tantangan dan hambatan terbesar yang dihadapi adalah karena pada kenyataannya Indonesia masih jauh dari berdaulat dalam konteks pertahanan sibernya. Selain belum berkembangnya industri teknologi dan informasi nasional, rendahnya literasi masyarakat membuat sulitnya menyusun kebijakan yang mampu berhadapan dengan lingkungan strategis yang penuh dengan fenomena VUCA (*Volatile, Uncertain, Complex, dan Ambiguous*).





Gambar 4. 63 Pemetaan CATWOE pada Ekosistem  
Pertahanan Siber Nasional

Sumber : Pemetaan CATWOE pada Ekosistem Pertahanan Siber Nasional (hasil  
pengolahan oleh data peneliti)

Berbasis pada analisa CATWOE di atas, melalui metoda klasterisasi terhadap berbagai isu termutakhir yang dihadapi, dapat ditemukan sejumlah potensi akar permasalahan yang perlu dipelajari. Paling tidak terdapat sebelas aspek dimaksud, yaitu terkait dengan:

1. Aspek Doktrin Pertahanan dan Kedaulatan Siber Negara
2. Aspek Prinsip, Paradigma, dan Kerangka Kebijakan
3. Aspek Ekosistem Pertahanan Siber Nasional
4. Aspek Jaringan Infrastruktur Telekomunikasi dan Internet
5. Aspek Suprastruktur Pertahanan Siber
6. Aspek Sistem Peraturan dan Perundang-Undangan
7. Aspek Struktur Kelembagaan dan Otoritas Kolektif
8. Aspek Industri Teknologi dan Informasi Nasional
9. Kooperasi Nasional dan Internasional

10. Standar Pertahanan dan Keamanan Siber
11. Sumber Daya Manusia dan Pasukan Siber

#### Hasil Analisis Kualitatif dan Kuantitatif

Adapun pendekatan analisis yang dipergunakan dalam mengelola data kualitatif dengan dibantu oleh aplikasi NVivo adalah berbasis pada konsep Spradley, sebagaimana diklasifikasikan berikut ini.

#### Analisis Domain

Analisis domain adalah upaya untuk memperoleh gambaran umum dan menyeluruh dari objek atau isu sosial yang diteliti. Ketika mencari gambaran umum dari suatu objek atau isu, peneliti akan menemukan berbagai domain atau kategori. Kemudian peneliti menetapkan domain tertentu sebagai pijakan tahap penelitian yang selanjutnya. Tentunya semakin banyak domain yang dipilih, maka akan semakin banyak waktu yang diperlukan untuk penelitian.

#### Analisis Taksonomi

Domain-domain yang telah dipilih selanjutnya dijabarkan menjadi lebih rinci, untuk mengetahui struktur internalnya. Caranya adalah dengan melakukan observasi terfokus pada masing-masing domain. Intinya pada tahap ini masing-masing domain yang telah dipilih dibedah dan dikaji secara detail untuk diketahui apa saja unsur-unsur yang membangunnya.

### Analisis Komponensial

Mencari ciri spesifik pada setiap struktur internal dengan cara mengontraskan antar unsur atau elemen yang telah diketahui dari analisis taksonomi. Hal ini dilakukan melalui observasi dan jika perlu wawancara terseleksi dengan pertanyaan yang mengontraskan (menjelaskan perbedaan utama dari masing-masing unsur).

### Analisis Tema Kultural

Mencari hubungan di antara domain, dan bagaimana hubungannya dengan keseluruhan, dan selanjutnya dinyatakan ke dalam tema/judul penelitian.

Keempat model analisis Spradley ini dipilih karena sesuai dengan tujuan, karakteristik, dan permasalahan penelitian yang dilakukan. Pendekatan ini sangat cocok dan relevan jika dipergunakan dalam penelitian yang membutuhkan pemahaman akan ekosistem secara utuh, holistik, komprehensif dan berbasis sistem.

### Potensi Ancaman Serangan Siber terhadap Pertahanan Negara

Kesembilan potensi ancaman siber yang mengambil bentuk atau modus delapan buah jenis serangan pada dasarnya merupakan sebuah aktivitas yang tidak berada di ruang hampa. Hampir semua serangan siber yang terjadi didahului dengan sejumlah peristiwa di masa lalu. Analisis dan investigasi secara mendalam terhadap berbagai serangan siber yang pernah terjadi di tanah air dapat dijadikan sebagai dasar dalam menentukan apa penyebab dari ancaman dimaksud.

### Penyerangan terhadap Infrastruktur Kritis Nasional

Setiap negara memiliki infrastruktur yang menguasai hajat hidup orang banyak. Sebuah infrastruktur dikategorikan sebagai *critical infrastructure* apabila

**Universitas Pertahanan RI**

memiliki peran dan fungsi sangat strategis bagi keberlangsungan hidup berbangsa, bernegara, dan bermasyarakat. Infrastruktur dimaksud antara lain seperti infrastruktur, jaringan, dan instalasi listrik, telekomunikasi, air minum, transportasi publik, perbankan/ keuangan, militer, energi (minyak dan gas bumi), distribusi logistik, dan lain sebagainya. Intinya adalah jika terjadi gangguan terhadap infrastruktur kritis atau vital ini, akan terjadi gejala serius dalam kehidupan bermasyarakat (Hurst et al., 2014; The National Institute of Standards and Technology, 2013).

Sesuai kemajuan dan perkembangan teknologi, berbagai sarana dan prasarana infrastruktur tersebut dikendalikan dengan peralatan elektronik atau digital. Bahkan untuk generasi terbaru, sistem yang dimiliki telah terhubung ke internet atau dunia siber. Dihubungkannya sistem infrastruktur kritis melalui internet memberikan banyak keuntungan bagi negara, karena dapat melayani masyarakat di manapun mereka berada karena keterjangkauannya (Bhardwaj et al., 2016). Namun di sisi lain membuka kemungkinan terjadinya serangan siber yang dapat melumpuhkan kinerja atau operasional infrastruktur kritis dimaksud.

Kerusuhan yang terjadi di Estonia ketika sistem jaringan distribusi listriknya diretas memperlihatkan besarnya dampak atau magnitude yang ditimbulkan (Boeke, 2018). Pemadaman listrik oleh pihak kriminal berakibat terganggunya jaringan perbankan dan sistem keuangan negara, sehingga masyarakat melakukan kerusuhan karena tidak dapat membeli kebutuhan pokok melalui transaksi elektronik. Dimasukinya virus Stuxnet oleh hacker pada sistem kendali nuklir Iran jika tidak diantisipasi dapat berakibat fatal (Farwell & Rohozinski, 2011). Peristiwa katastrofi Chernobyl dapat terjadi yang berdampak musnahnya peradaban manusia dalam beberapa generasi.

Pernahkah terbayangkan apabila peretas atau kriminal siber melakukan serangan terhadap sistem radar pesawat, jaringan ATM nasional, infrastruktur perkeratopian, lumbung logistik makanan pokok, pengolahan minyak bumi, dan lain sebagainya? Serangan terhadap infrastruktur kritis nasional dapat memporak-porandakan sendi-sendi kehidupan masyarakat yang berpotensi menimbulkan gejala dan kekacauan sosial yang membahayakan keutuhan dan kedaulatan negara (Gisladdottir et al., 2017; Weed, 2017).

### Penyadapan Sistem Komunikasi Pertahanan Negara

Masyarakat moderen menggunakan berbagai media komunikasi digital dalam melakukan kegiatannya sehari-hari. Para pemangku kepentingan dalam sektor pemerintahan maupun pertahanan, memanfaatkan berbagai media komunikasi berbasis digital dan elektronik (Kovaité et al., 2020)k. Pemanfaatan teknologi seperti telepon genggam, tablet, dan gawai yang mudah dibawa ke mana-mana memberikan keleluasaan pada setiap manusia untuk melakukan komunikasi via email, *group messangers*, *chatting*, *teleconference*, dan berbagai model komunikasi lainnya. Pada sektor militer misalnya, para perwira tinggi dalam kesehari-hariannya menggunakan gawai elektronik untuk berkomunikasi, berkolaborasi, berinteraksi, dan berkoordinasi. Sementara pada tataran di bawahnya, para pegawai pemerintahan aktif menggunakan komputer dan *notebook* dalam menjalankan proses dan aktivitas operasional sehari-hari (Abrams & Merchant, 2013). Pada saat yang sama, Presiden beserta kabinet dan petinggi pemerintahan melakukan komunikasi aktif dan interaksi via teknologi serupa.

Komunikasi berbasis digital sangat rawan diserang oleh penjahat siber (Landwehr, 2001). Salah satu modus yang paling disenangi kriminal atau musuh adalah melakukan penyadapan atau interception. Proses mendengar pembicaraan atau percakapan secara lisan maupun tulisan dapat dilakukan dengan cara melakukan *man-in-the-middle attack* atau melakukan intersepsi terhadap medium komunikasi (Yannakogeorgos, 2012). Dengan melakukan berbagai cara tapping, media transmisi baik melalui darat (fiber optic), laut (kabel laut), dan udara (wireless atau via satelit) dapat dilakukan dengan mudah. Walaupun teknologi terkini telah menerapkan protokol komunikasi termutakhir yang handal, ditambah kekuatan sistem kriptografi yang diterapkan, proses penyadapan dapat berhasil dilakukan dengan menggunakan pendekatan serangan *social engineering* – yaitu memanipulasi manusia atau user yang menggunakannya (Mouton et al., 2016; Salahdine & Kaabouch, 2019).

Berbeda dengan penyadapan konvensional yang berjalan di atas teknologi analog atau elektronik, penyadapan digital sangat sulit untuk dideteksi – karena pihak yang disadap akan sangat sulit mengetahui keberadaan pihak lain yang melakukan intersepsi terhadap komunikasi yang dilakukan. Dapat dibayangkan betapa bahayanya kondisi kedaulatan bangsa apabila musuh dengan leluasa mengetahui berbagai percakapan yang terjadi antara pimpinan pemerintahan seperti menteri dan kepala institusi negara yang terjadi setiap harinya (Wagner et al., 2019). Belum lagi dampak negatif yang membayangi apabila pihak lawan berhasil menyadap sentra-sentra komunikasi penting sebuah negara, seperti pusat intelijen, instalasi militer, sentra telekomunikasi, dan lain sebagainya.

#### Pengambilalihan Kendali Alutsista Digital

Salah satu pilar pertahanan negara terletak pada kekuatan angkatan bersenjata. Kemampuan militer dalam menghadapi berbagai ancaman dari dalam maupun luar negara diperkuat dengan sumber daya dan konfigurasi persenjataan yang dimiliki. Persenjataan militer yang disebut sebagai alutsista, memiliki sejumlah kapabilitas dan kemampuan dalam usahanya untuk menjaga dan menghadapi lawan – baik yang mencoba menguasai negara dari wilayah darat, laut, dan udara (Lasiello, 2015). Secara periodik dan berkala, persenjataan yang dimiliki oleh instansi militer diperbaharui dan dimutakhirkan agar sesuai dengan tuntutan jaman, yang diwarnai dengan berbagai perubahan postur ancaman terhadap kedaulatan negara.

Senjata militer moderen memiliki sebuah ciri khas, yaitu dilibatkannya teknologi informasi, komunikasi, dan siber di dalamnya. Ditanamkannya sejumlah chip berbasis mikroprosesor pada sebagian komponen atau sub-sistem senjata memberikan berbagai kehandalan dan fitur baru yang tidak dikenal sebelumnya. Pertama, chip yang dikoneksi dengan sensor dapat meningkatkan kinerja penginderaan senjata sehingga memiliki kemampuan mendeteksi berbagai aktivitas dari jarak jauh (Eszter Katalin, 2018). Kedua, kecepatan pemrosesan data berlipat ganda sehingga fungsi akurasi pengambilan keputusan dalam

medan perang menjadi sangat cepat (Hare, 2019). Ketiga, penempatan aktuator pada sejumlah sendi-sendi komponen berbasis IOT (Internet-Of-Things) memungkinkan persenjataan untuk dikendalikan dari jarak jauh (*remote access*) (Cha et al., 2018). Keempat, kombinasi teknologi digital menghasilkan persenjataan yang dapat beroperasi secara mandiri seperti yang diperlihatkan pada unmanned aerial vehicle (Cho & Kim, 2015; Yaacoub et al., 2020).

Sejalan dengan kemajuan teknologi yang memberikan dampak positif pada perkembangan alutsista tersebut, membayangi pula risiko yang menyertainya. Dapat dibayangkan apa yang akan terjadi seandainya pihak lawan berhasil meretas UAV yang dimiliki militer Indonesia, sehingga dapat disalahgunakan untuk memata-matai kondisi negara. Atau penjahat siber berhasil mengambil alih kendali senjata-senjata dari jarak jauh, sehingga disalahgunakan untuk menghancurkan diri sendiri. Belum lagi pengambilalihan kendali terhadap sensor-sensor yang melekat pada alutsista yang dapat menjadi kunci bagi pihak lawan dalam melakukan proses intelijen. Pengambilalihan kendali terhadap alutsista berbasis digital merupakan ancaman yang sangat serius karena dapat menimbulkan dampak katastrofi yang sangat dahsyat.

#### Penyabotan Pusat Komando dan Kendali Militer

Pertahanan negara dapat dijaga oleh pihak militer apabila yang bersangkutan mampu melakukan koordinasi dan kolaborasi efektif antar komponen-komponen yang tersebar di seluruh wilayah tanah air. Indonesia sebagai negara maritim memiliki tantangan tersendiri dalam menjaga kedaulatannya karena luasnya sebaran geografis yang dimiliki. Oleh karena itulah maka berbagai pihak yang bertugas memastikan terselenggaranya proses komunikasi, kolaborasi, kooperasi, dan koordinasi yang efektif membangun fasilitas bernama Pusat Komando dan Kendali (Puskodal) – sebagaimana lumrah dilakukan di kalangan militer.

*Command Center* ini merupakan sebuah fasilitas pusat konsentrasi pengelolaan dan pengendalian seluruh aset dan sumber daya militer yang keberadaannya tersebar di seluruh wilayah nusantara. Melalui fasilitas ini, dapat

dilakukan hal-hal seperti: pemantauan seluruh kondisi negara secara utuh, pemberian komando pimpinan militer terhadap seluruh jajarannya, pengendalian berbagai aset dan sumber daya militer, pengawasan pergerakan komponen strategis pertahanan negara, pendayagunaan kekuatan militer untuk berbagai keperluan pertahanan, dan lain sebagainya. Dengan adanya fasilitas dan sarana prasarana yang lengkap, seorang *commander* dapat mengambil keputusan strategis secara cepat, tepat, dan berkualitas.

Semenjak komputer diperkenalkan, berbagai pusat komando dan kendali militer dibangun sarat dengan teknologi informasi dan komunikasi. Sensor-sensor yang ditanam di seluruh wilayah negara dapat diakses dari pusat kendali ini. Demikian juga berbagai piranti, komponen, dan alutsista pertahanan negara dapat dikendalikan secara jarak jauh dari puskodal ini. Kemampuan lainnya adalah melakukan kegiatan intelijen dari lokasi yang sama, melalui berbagai kemampuan di bidang serangan siber. Kapabilitas lainnya adalah melakukan koordinasi, komunikasi, kolaborasi, dan interaksi rahasia antar berbagai pihak secara aman dan rahasia. Hanya mereka yang punya level of clearance tinggi yang dapat masuk secara fisik ke dalam sebuah *command center*.

Puskodal berbasis teknologi digital yang serba canggih tersebut selain memberikan banyak sekali kemampuan dan kehandalan juga mendatangkan permasalahan tersendiri. Dapat dibayangkan apabila penjahat, kriminal, atau peretas berhasil mengakses fasilitas tersebut – baik secara fisik maupun via dunia siber. Tentu saja hal ini merupakan ancaman serius bagi pertahanan dan kedaulatan negara. Oleh karena itulah maka *command center* yang dimiliki berbagai pihak – terutama militer – harus benar-benar dijaga keamanannya agar terhindar dari serangan siber yang sangat membahayakan negara.

#### Pencurian Data dan Informasi Rahasia

Data dan informasi adalah aset tak ternilai harganya yang harus dijaga kemanan, integritas, dan aksesabilitasnya. Dalam konteks kehidupan bernegara, terutama dalam menjaga kedaulatan dan pertahanan negara, begitu banyak data



dan informasi rahasia yang harus dijaga keberadaannya agar tidak jatuh ke tangan orang lain (Osho & Onoja, 2015). Berbagai upaya dilakukan pihak-pihak untuk memastikan tidak bocornya rahasia negara ini ke tangan pihak-pihak dalam maupun luar negeri yang tidak berhak mengaksesnya.

Seperti diketahui bersama, pada abad ke-21 ini hampir seluruh data dan informasi disimpan dalam bentuk berkas elektronik atau yang biasa disebut sebagai file. Jenis, bentuk, dan format datanya pun dapat beragam, seperti: teks/dokumen, suara/audio, citra/gambar, filem/video, atau kombinasi di antaranya (multimedia). Keseluruhan files ini disimpan pula dalam media elektronik seperti *flash disk*, memory card, external hard drive, internal hard disk, storage, dan lain sebagainya (Andone & Vasiu, 1998; Samaras et al., 2006). Sementara seluruh media penyimpan tersebut biasanya diletakkan secara fisik *menjadi bagian dari sebuah sistem komputer, gawai, server atau data center*. Sebagaimana layaknya sebuah data rahasia, manajemen pengelolaannya pun dibuat khusus sedemikian rupa agar keamanannya terjaga.

Para peretas dan penjahat siber paham sekali mengenai situasi ini, sehingga mereka mengembangkan berbagai strategi dan skenario untuk mendapatkan akses (mencuri) terhadap sistem dimaksud. Berbagai jenis serangan langsung maupun tidak langsung dapat diluncurkan oleh peretas untuk mencuri data dan informasi rahasia yang tersimpan dalam berbagai sistem komputasi ini (Domingo & Parmar, 2019). Bahaya besar dihadapi negara apabila data dan informasi penting seperti kekuatan pertahanan negara, strategi dan operasional pertahanan, daftar nama intelijen berbagai negara, dan lain-lain jatuh ke tangan pihak-pihak tak bertanggung jawab. Peristiwa Wikileaks memperlihatkan bagaimana kebocoran informasi penting dan rahasia dapat menyebabkan terjadinya berbagai ketegangan antar negara-negara di dunia (Barnard-Wills, 2011).

#### Pelumpuhan Sistem Militer dan Pertahanan Negara

Sistem militer dan pertahanan terdiri dari begitu banyak sub-sistem yang saling terkait satu dan lainnya. Negara maju seperti Amerika Serikat

misalnya, memiliki lima sub-sistem besar pertahanan sesuai dengan angkatan persenjataan yang dimiliki, yaitu: Angkatan Darat, Angkatan Laut, Angkatan Udara, Angkatan Antariksa, dan Angkatan Siber (Campbell, 2018). Masing-masing sub-sistem militer dan pertahanan tersebut melibatkan begitu banyak teknologi persenjataan, yang dalam era moderen ini pasti dilengkapi dengan komponen berbasis elektronik dan digital – atau yang dikenal sebagai teknologi informasi dan komunikasi. Dalam kondisi perang, kehandalan sistem militer ini menjadi kunci kemenangan. Sementara dalam kondisi damai, keberadaannya menjadi bagian tak terpisahkan dari penciptaan efek gentar yang efektif (Beidleman, 2009; Wilner, 2020).

Melihat kenyataan seperti ini, kinerja operasional sistem militer sangatlah menentukan berhasil tidaknya sebuah negara menjaga pertahanannya. Sedikit gangguan pada satu komponen atau sub-sistem berpotensi mempengaruhi kehandalan keseluruhan sistem. Fenomena perang siber yang terjadi belakangan ini memperlihatkan adanya berbagai usaha lawan untuk mencoba melumpuhkan sistem pertahanan yang dimiliki. Cara melumpuhkannya pun bermacam-macam, seperti mengirimkan jutaan paket data secara masif ke sejumlah sumber daya komputasi (serangan botnet). Metoda lain yang kerap dipergunakan adalah dengan memasukkan *malware* atau virus komputer ke dalam *server* utama sehingga sistem berhenti bekerja (*halting* atau *shut down*) atau melalui teknik penetrasi yang memungkinkan peretas mengakses aplikasi penting yang ada dalam sistem pertahanan dimaksud (Beidleman, 2009).

Tujuan dari lawan atau peretas melakukan kegiatan tersebut adalah untuk membuat sistem pertahanan negara tidak berfungsi apabila dibutuhkan. Pada saat sistem tersebut lumpuh, biasanya lawan akan meluncurkan serangannya (“Cybersecurity Risks: Are They Inflated?,” 2016). Bisa dibayangkan situasi dan kondisi yang akan menimpa negara ketika sistem teknologi militer dan pertahanannya berhasil dilumpuhkan oleh pihak lawan.

#### Penyesatan Fakta dan Informasi

Salah satu modus perang konvensional yang dibawa ke dalam dunia siber adalah berbasis propaganda. Sejumlah praktisi menyebutnya sebagai perang *mindset*. Fenomena *hoax* yang belakangan ini mengemuka di berbagai negara merupakan salah satu bentuk manifestasi dari serangan dengan mengirimkan pesan-pesan penyesatan yang bermuara pada perpecahan antar sejumlah komunitas masyarakat (Jones, 2013; Nastiti et al., 2018). Model adu domba ini merupakan salah satu upaya musuh dalam menanamkan benih-benih perpecahan terutama pada negara yang masyarakatnya masih tidak merata latar belakang pendidikannya.

Pada dasarnya ada dua istilah yang banyak dikenal dengan modus pengubahan informasi yang ingin disampaikan, dikenal sebagai misinformasi, disinformasi, dan malinformasi. Misinformasi adalah informasi atau berita palsu yang beredar, namun pihak yang membaginya tidak menyadari bahwa itu salah atau menyesatkan (Norri–Sederholm et al., 2020). Sementara disinformasi adalah informasi yang sengaja dirancang (dimanipulasi) agar menyebabkan kerugian (Fraga-Lamas & Fernández-Caramés, 2019). Dan malinformasi adalah informasi yang asli, namun penyajiannya dikemas sedemikian rupa untuk mendapatkan persepsi yang merugikan sejumlah pihak (McGarr, 2021). Konsep inilah yang banyak dipakai oleh para penggiat media sosial dalam menciptakan kekacauan sosial seperti terjadi di Tunisia dan Mesir.

Negara berkembang seperti Indonesia banyak sekali mengalami berbagai jenis serangan berbasis pengelabuan informasi. Lawan memilih jenis penyerangan ini karena sejumlah alasan. Alasan pertama adalah berkembangnya platform media sosial yang sangat digemari masyarakat. Dengan menggunakan aplikasi ini, penyebaran berita bohong dan menyesatkan, dengan niat mengadu-domba atau membentuk persepsi keliru, dapat dilakukan secara cepat, murah, dan masif. Alasan kedua adalah mudahnya membuat berita sensasi yang sanggup membuat orang percaya akan terjadinya sebuah peristiwa. Perkembangan teknologi grafis dan multimedia semakin membantu pihak lawan dalam mengatur narasi yang sanggup menghipnotis pembacanya. Dan alasan ketiga adalah karena literasi informasi masyarakat Indonesia yang masih relatif rendah. Kenyataan ini menyebabkan mudahnya seseorang percaya

pada berita bohong dan palsu, serta tidak ragu-ragu menyebarkan dan meyakinkan pihak lain akan kebenarannya.

Jenis serangan yang menyerang langsung ke pusat kesadaran manusia atau otak ini sangat sulit untuk diantisipasi karena sifatnya yang subyektif dan masif (Canan & Akil, 2020; Murphy & Keane, 2019). Dalam konteks peperangan, serangan terhadap pola pikir masyarakat dapat berasal dari luar maupun dalam negeri. Serangan dari luar negeri diluncurkan melalui berita-berita dari sumber internasional berbagai negara. Sementara serangan serupa dari dalam negeri biasanya diluncurkan oleh pihak-pihak yang anti pemerintah atau tidak setuju dengan kebijakan yang diberlakukan oleh negara terhadap mereka.

#### Perusakan Sistem dan Instalasi Teknologi Informasi

Arena siber terbentuk melalui relasi keterhubungan antara berbagai sumber daya komputasi melalui ekosistem jejaring elektronik. Sebagai pengguna siber atau internet, dibutuhkan sejumlah komponen teknologi untuk dapat terhubung ke jaringan interkoneksi raksasa tersebut. Contohnya adalah keberadaan fasilitas atau instalasi data center yang di dalamnya terdapat ratusan bahkan ribuan *server* atau media komputasi lainnya. *Command center* yang merupakan pusat pengendalian operasional berbagai aktivitas kenegaraan adalah contoh lain dari instalasi sistem teknologi informasi dimaksud. Berbagai sistem instalasi teknologi informasi yang banyak dibangun dan dikembangkan dalam sektor pertahanan antara lain adalah: *cyber operation center*, *security operation center*, *war simulation center*, *cyber intelligence agency*, dan lain sebagainya (Carvalho, 2015; Theohary & Harrington, 2015; Zhong et al., 2018).

Pada dasarnya keseluruhan fasilitas dan instalasi teknologi informasi tersebut merupakan sumber daya strategis yang harus dijaga kerahasiaan dan keamanan operasionalnya. Tidak semua pihak dapat mengakses secara fisik maupun virtual sebagian atau keseluruhan sistem komputasi yang ada di dalamnya. Sementara bagi mereka yang berhak, harus melalui sejumlah prosedur baku untuk dapat mengaksesnya. Terminologi *clearance level* adalah

salah satu sistem klasifikasi hak akses yang kerap diberlakukan dalam sektor pertahanan negara (Olofsson & Lindberg, 2012; Z. Zhang et al., 2020).

Fenomena yang terjadi di masa lalu terkait dengan ancaman terhadap instalasi strategis ini adalah dilakukannya perusakan secara fisik agar fasilitas tidak dapat menjalankan fungsi operasionalnya. Perusakan fisik dapat dilakukan dengan berbagai cara, seperti: penghancuran data center dengan bahan peledak, pemutusan *fiber optic* yang menjadi tulang punggung media transmisi data, pencurian server aplikasi utama, perusakan media penyimpan *hard disk*, dan lain sebagainya. Selain perusakan fisik, dapat juga dilakukan “perusakan virtual” melalui berbagai cara, seperti: *demagnetizing hard disk*, *malware* yang merusak *firmware*, *remote memory clean-up*, dan lain-lain (Bhardwaj et al., 2016; Gunduz & Das, 2020; Lendvay, 2016). Dengan rusaknya sebagian atau keseluruhan sub-sistem maupun sistem yang ada, akan ada kelumpuhan operasional yang berdampak serius pada kondisi pertahanan negara.

#### Penyusupan ke Dalam Ekosistem Pertahanan Negara

Terminologi penyusupan mulai diperkenalkan ketika mengemuka sejumlah kasus penyerangan dimensi keterlibatan orang dalam atau pihak internal yang bekerjasama dengan pihak eksternal yang merupakan lawan atau musuh. Ada beberapa modus yang dikenal dalam konteks penyusupan terhadap ekosistem pertahanan negara dimaksud – dimana intinya adalah mencoba mengakses sistem yang berhubungan dengan sejumlah data atau informasi rahasia.

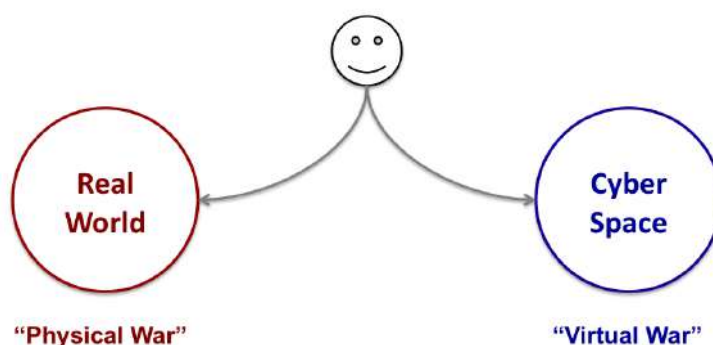
Pertama adalah menyusup melalui proses penyamaran secara fisik ke dalam sistem rahasia. Penyamaran secara fisik dilakukan biasanya setelah pihak lawan melakukan analisa terhadap kebiasaan prosedur operasional sehari-hari di dalam perimeter (Kumar et al., 2015). Kemudian hasil pembelajaran terhadap pola aktivitas tersebut dicari titik lemahnya, dan dimanfaatkan dengan menggunakan teknik *social engineering*. Kedua adalah dengan mengikuti rekrutmen pegawai dan kemudian secara formal menjadi bagian dari organisasi dimaksud. Ketika saatnya tiba (bisa bertahun-tahun setelah yang bersangkutan

bergabung agar tidak dicurigai dan telah mendapatkan kepercayaan dari organisasi), maka yang bersangkutan akan masuk menyusup ke tempat-tempat tertentu karena sudah dikenal oleh sejawatnya (Gawthorpe, 2016). Ketiga adalah melalui modus kerjasama antar lembaga atau institusi. Dalam konteks kerjasama tersebut, banyak hal yang dapat dilakukan secara bersama-sama, dimana pada suatu titik tertentu terjadi kelengahan yang dimanfaatkan pihak lawan untuk menyusup (Edwards et al., 2017). Keempat adalah melalui kemitraan vendor – baik dalam maupun luar negeri – dimana jika tidak sungguh-sungguh dilakukan kontrak yang transparan dan akuntabilitas, pihak ketiga tersebut dapat menyusup ke dalam perimeter rahasia karena alasan memperbaiki atau memutakhirkan sistem (Van Horenbeeck, 2018). Dan yang kelima adalah melalui skenario “pengkhianatan” orang dalam atau internal yang mendapatkan keuntungan pribadi dari pihak lawan atau musuh. Modus yang terakhir ini sangat sulit untuk dideteksi karena karakteristiknya (Bhardwaj et al., 2016; Zaytsev et al., 2017).

Berhasil masuk atau menyusup ke perimeter keamanan rahasia pertahanan negara memberikan keuntungan besar bagi lawan atau musuh. Mereka dapat dengan leluasa mengakses berbagai data, informasi, catatan, dan pengetahuan terkait dengan pertahanan negara. Disamping itu keberhasilan mereka masuk ke fasilitas strategis berpotensi dapat memporakporandakan sistem pertahanan negara karena kemampuan mereka untuk mengontrol dan mengendalikan berbagai fasilitas teknologi yang saling terhubung satu dan lainnya via internet. Berbeda dengan model kejahatan konvensional, modus penyusupan hanya membutuhkan satu kali usaha efektif untuk dapat mengacaukan sistem teknologi informasi pertahanan negara.

Ada suatu hal yang menarik dalam dunia keamanan informasi dan internet yang patut untuk dicermati dan dipelajari lebih lanjut. Hal ini berdasarkan riset dan pengamatan ID-SIRTII terhadap pola kejadian potensi serangan internet yang ada di Indonesia. Melalui studi tersebut, ada sebuah hipotesa yang dikembangkan dan dicoba untuk dibuktikan, yaitu: terdapat suatu hubungan yang signifikan antara kejadian di dunia nyata dengan peristiwa serangan di dunia maya (baca: internet) dan sebaliknya.

Pada awal mulanya lahir dan dimanfaatkannya internet, terkenal suatu istilah semacam *virtual world* atau *cyber world* untuk menggambarkan. Dunia maya ini dianggap sebagai sebuah arena interaksi antara mereka yang memiliki “hak eksklusif” penggunaan sistem komputer yang terhubung dalam sebuah jejaring raksasa. Peristiwa historis tersebut secara tidak langsung mewarnai pola pikir manusia di masa-masa awal perkembangan internet, yang mendikotomikan antara dunia nyata dengan dunia maya.



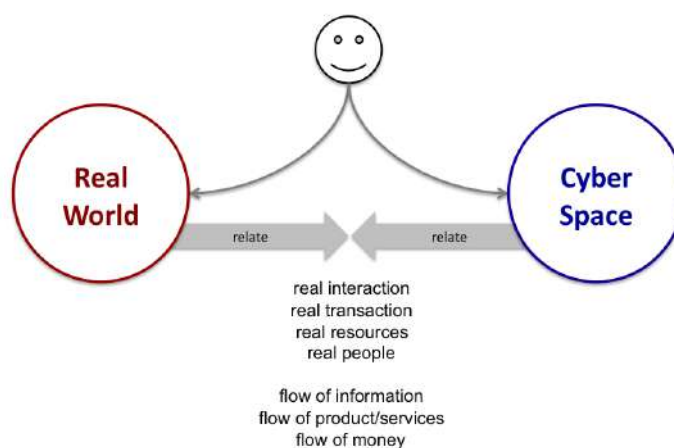
Gambar 4. 64 Dua Dunia dalam Kehidupan Manusia Moderen

Sumber : Dua Dunia dalam Kehidupan Manusia Moderen (Indrajit, 2010)

Dalam konteks dikotomi inilah kemudian terbentuk suatu opini bahwa tidak adanya hubungan yang jelas dan tegas antara dua dunia ini. Masing-masing berdiri sendiri dan tidak saling mempengaruhi. Contohnya adalah pendapat yang mengatakan bahwa peperangan yang terjadi di dunia nyata, tidak akan berpengaruh di dunia maya, dan sebaliknya. Bahkan pengguna atau *user* atau individu terkadang memiliki “dua kepribadian” yang berbeda ketika berinteraksi dengan dua dunia ini. Ketika di dunia nyata, yang bersangkutan memiliki data, perilaku, dan profil seperti apa adanya; namun ketika masuk ke dunia maya, yang bersangkutan dapat “menyamar” menjadi orang lain karena keleluasaan dan kemungkinan-kemungkinan yang ditawarkan.

Lambat laun, sesuai dengan perkembangan internet dan teknologi informasi yang sedemikian cepat, yang tadinya internet hanya dipergunakan untuk riset dan pendidikan, mulai berkembang ke industri serta aspek kehidupan lainnya. Transaksi bisnis mulai terjadi, interaksi sosial antar individu semakin menggejala, penyebaran budaya terjadi secara intensif, keterbukaan politik dan kebebasan media mendominasi kehidupan sehari-hari, dan lain sebagainya. Beberapa pusat riset dunia bahkan mensinyalir, telah terjadi penurunan secara cukup signifikan jumlah transaksi ekonomi yang biasanya terjadi di dunia nyata – karena berpindah ke dunia maya yang memberikan sejumlah manfaat semacam efisiensi dan optimalitas. Misalnya adalah dalam hal kecenderungan membeli barang yang beralih dari uang tunai menjadi model pembayaran berbasis elektronik (seperti kartu kredit, kartu debit, pulsa telepon, dan lain sebagainya).

Fenomena tersebut mengandung arti bahwa apa yang terjadi di dunia maya, tidak dapat dilepaskan begitu saja dengan kenyataan di dunia nyata, mengingat terjadinya kecenderungan keberhimpitan kedua dunia tersebut yang menampakkan irisan semakin lama semakin bertambah besar.



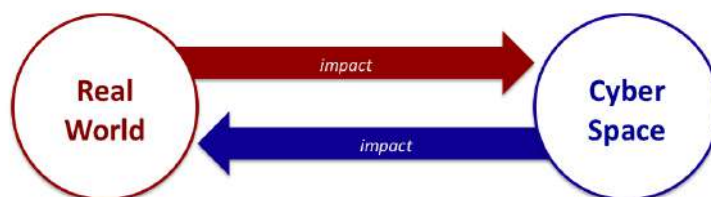
Gambar 4. 65 Hubungan Keterkaitan antar Dua Dunia

Sumber : Hubungan Keterkaitan antar Dua Dunia (Indrajit, 2010)



Hal ini semakin diperjelas dengan kenyataan yang memperlihatkan bahwa yang berinteraksi di dunia maya adalah benar-benar individu manusia, dengan menggunakan alat pembayaran uang yang sah, dan melibatkan sejumlah dokumen perjanjian yang legal. Dengan berhimpitnya dua dunia tersebut, maka jelas akan terjadi hubungan keterkaitan yang cukup erat antara satu dunia dengan dunia lainnya. Apa yang terjadi di dunia maya akan sangat mempengaruhi mereka yang ada di dunia nyata, dan berlaku pula sebaliknya. Bahkan di masa mendatang, ketika seluruh individu telah terhubung dan dapat mengakses internet, maka kedua dunia tersebut akan menyatu secara identik.

Terkait dengan isu keamanan internet yang menjadi pembicaraan banyak orang dewasa ini, terbersit pula sejumlah praduga alias “hipotesa” tidak tertulis yang memperkirakan bahwa hal-hal yang terjadi di dunia nyata dapat berpengaruh di dunia maya dan sebaliknya – terutama hal-hal yang terkait dengan berbagai peristiwa (baca: *incident*) kejahatan internet.



Gambar 4. 66 Pengaruh Tak Terpisahkan antar Dua Dunia

Sumber : Pengaruh Tak Terpisahkan antar Dua Dunia (Indrajit, 2010)

Dari berbagai hasil pemantauan sejumlah praktisi keamanan informasi dan internet, terdapat sejumlah kejadian di dunia nyata yang secara langsung maupun tidak langsung berpengaruh terhadap berbagai peristiwa yang

berlangsung dalam dunia maya. Berikut adalah beberapa jenis pemicu terjadinya sejumlah peristiwa tersebut.

Pertama adalah dipicu oleh kejadian bernuansa politis. Contohnya adalah ketika Indonesia dan Malaysia “berhadapan” secara politis dalam kasus perebutan wilayah Ambalat, maka sekonyong-konyong terjadi “perang” *web defacement* atau “permak tampilan situs” antara *hacker underground* Indonesia dan Malaysia. Berbagai situs dengan domain .id dicoba di-*hack* oleh pihak Malaysia, demikian juga dengan situs berakhiran .my yang coba diserang oleh pihak Indonesia. Tidak tanggung-tanggung berbagai pihak di Indonesia maupun Malaysia berusaha “menenangkan” para pihak yang terbakar emosinya ini di dunia maya. Hal yang sama berlangsung pula antara Indonesia dan Australia misalnya setiap kali ada satu atau dua buah berita politik yang mendatangkan ketegangan hubungan bilateral antara dua buah negara terkait. Yang menarik adalah bahwa tidak jarang terjadi peristiwa dimana negara-negara simpatisan atau sekutu juga turut serta “meramaikan dunia persilatan” jika dipandang perlu. Tengoklah apa yang terjadi di dunia maya ketika terjadi perseteruan antara China dan Tibet, Malaysia dan Singapura, Rusia dan Georgia, dan lain sebagainya.



Gambar 4. 67 Pengaruh Dunia Nyata terhadap Dunia Siber

Sumber : Pengaruh Dunia Nyata terhadap Dunia Siber (Indrajit, 2010)

Kedua adalah peristiwa-peristiwa yang dipicu oleh terselenggaranya berbagai *event* atau kegiatan berskala internasional, semacam Olimpiade, Sea Games, Asian Games, World Cup, dan lain sebagainya. Hal-hal menarik yang terjadi di dalam momen-momen olah raga tersebut adalah persaingan ketat antara sejumlah negara maupun peristiwa-peristiwa tertentu yang menodai rasa keadilan. Lihatlah contohnya ketika terjadi final piala sepakbola antara dua negara, maka tidak jarang di dunia maya pun terjadi peristiwa “serang-serangan” ide, gagasan, maupun situs-situs terkait. Kejadian dipukulinya wasit karateka Indonesia oleh sejumlah atlet Malaysia juga memicu serangan besar-besaran di dunia maya yang sulit dikendalikan. Perlu dicatat bahwa tidak hanya *event* olah raga saja, namun pertemuan-pertemuan akbar seperti PBB, G8, OPEC, dan lain-lain juga sering menjadi pemicu serangan yang terjadi di dunia maya.

Ketiga merupakan hasil kajian yang sungguh menarik dari sejumlah pihak terkait. Ternyata trend jenis-jenis serangan di dunia maya – seperti *SQL Injection*, *Web Defacement*, *Botnet*, *DOS/DDOS Attack*, dan lain sebagainya – sangat berkaitan erat dengan buku-buku publikasi terkait dengan proses *hacking* yang dijual bebas di pasaran. Alasannya cukup sederhana. Biasanya buku-buku berbahasa Indonesia maupun Inggris tersebut dalam memberikan penjelasannya disertai dengan contoh kasus atau latihan-latihan yang melibatkan situs-situs tertentu. Dengan sedikit kreativitas pembaca, maka yang bersangkutan dapat mencoba teknik terkait ke sejumlah situs atau website atau sistem komputer atau jaringan yang ada di tanah air.

Keempat yang merupakan fenomena serupa tapi tak sama adalah trend kejadian “penyerangan” di dunia maya dengan modus operandi seperti yang sering dicontohkan lembaga-lembaga penyelenggara pelatihan *internet security*

atau *ethical hacker*. Sesuai yang dicontohkan oleh instruktur pengajarnya maupun yang ditulis dalam buku materi pelatihan yang diberikan ke peserta. Hal ini dapatlah dimengerti mengingat sejumlah alasan. Misalnya adalah sangat sulit memahami teori keamanan internet tanpa memberikan dan melakukan sejumlah contoh-contoh analisa kerawanan (baca: *vulnerabilities*), atau aktivitas uji coba keamanan (baca: *penetration test*), atau tindakan eksploitasi kerawanan. Alasan lain yang berpegang pada prinsip untuk menjadi seorang “*defenser*” yang baik, maka harus mengerti cara-cara kerja “*offenser*” – alias untuk dapat menjadi polisi yang baik, harus tahu persis bagaimana orang jahat atau kriminal berpikir dan bekerja. Sangat sulit melakukan contoh-contoh yang kontekstual tanpa melibatkan jaringan yang riil.

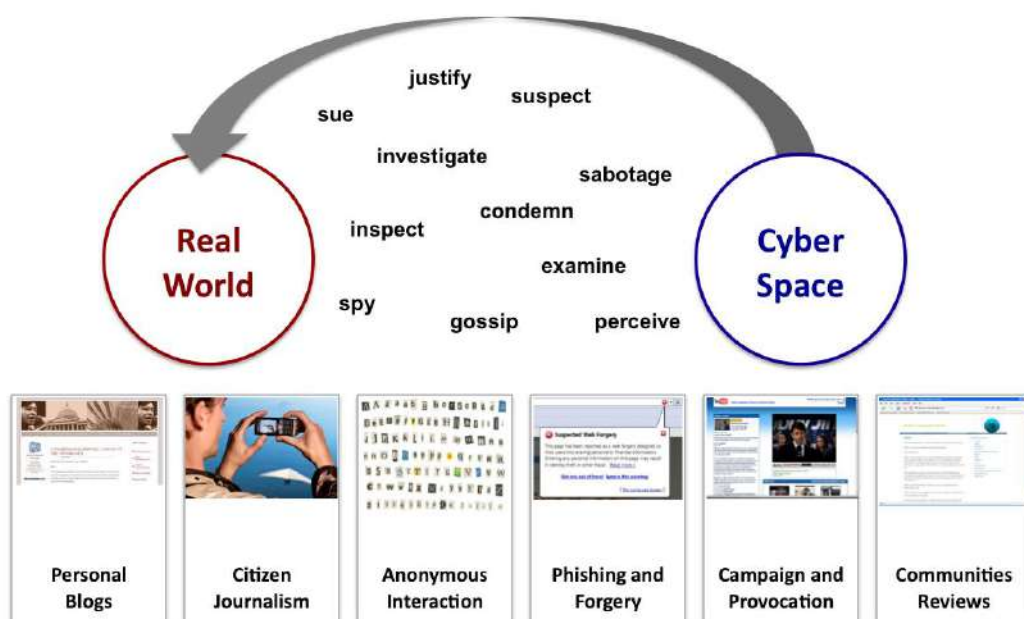
Kelima adalah disebabkan karena begitu banyaknya di pasaran piranti lunak atau *tools* untuk melakukan *hacking* yang diperjualbelikan secara gratis – yang kebanyakan merupakan *software* bajakan. Program-program yang dijual bebas dengan harga murah ini tidak saja memberikan keleluasaan kepada penggunaanya untuk melakukan berbagai jenis serangan di dunia maya, namun dari hari ke hari menawarkan pula kemudahan-kemudahan dalam menggunakannya (baca: semakin *user friendly*). Bagi mereka yang memiliki hobi menekuni dunia keamanan internet, perangkat-perangkat lunak penunjang ini sangatlah berguna karena memberikan berbagai trik, fasilitas, fitur, dan kapabilitas yang sangat beragam.

Keenam yang kerap memicu terjadinya tindakan maupun peristiwa di dunia maya adalah dimulai dari sejumlah pertemuan *community of interest* baik secara terbuka maupun tertutup (baca: *underground*) yang membahas berbagai fenomena yang terjadi di dunia maya. Tidak jarang hasil dari diskusi, tukar pikiran, lokakarya, seminar, maupun pertemuan ini bermuara pada uji coba atau tindakan penetrasi terhadap situs atau jaringan tertentu yang menjadi bahan pembicaraan khalayak atau komunitas sejenis ini.

Relasi antara dua dunia tersebut berlaku pula sebaliknya. Tidak jarang terjadi suatu sengketa serius di dunia nyata, yang pada awal mulanya sebenarnya terjadi di dunia maya. Hal ini semakin lama semakin banyak terjadi seiring dengan semakin berkembangnya komunitas pengguna internet, dan mulai

diperkenalkannya *cyber law* di Indonesia melalui UU ITE No.11 tahun 2008. Berikut adalah sejumlah fenomena kejadian di dunia maya yang memicu terjadinya peristiwa menarik di dunia nyata.

Pertama, yang paling banyak terjadi dan menggejala belakangan ini adalah dimulai dari penulisan *blog* oleh seseorang. Sering kali isinya *blog* lebih merupakan suatu pengalaman dan pandangan pribadi terhadap individu maupun peristiwa atau kejadian tertentu yang didasarkan pada perasaan, persepsi, sangkaan, maupun asumsi tertentu dari si pengarang atau penulis. Tidak jarang ditemui dalam *blog* tersebut disebutkan secara jelas dan tegas nama-nama individu pelaku yang terkait dengan isi cerita yang ada.



Gambar 4. 68 Pengaruh Dunia Siber terhadap Dunia Nyata

Sumber : Pengaruh Dunia Siber terhadap Dunia Nyata (Indrajit, 2010)

Dalam konteks ini ternyata tidak semua individu dalam dunia nyata telah siap berhadapan dengan alam “demokrasi mengemukakan pendapat” semacam itu, sehingga cukup banyak yang berlanjut dengan adanya tuntutan “pencemaran nama baik” dari mereka yang namanya disebutkan dalam sejumlah blog-blog pribadi yang menjamur di dunia maya. Dengan menggunakan berbagai jenis pasal dalam UU ITE, yang bersangkutan berusaha mempidanakan si penulis blog.

Kedua merupakan fenomena yang dipicu dengan berkembangnya komunitas *citizen journalism*. Dengan menggunakan berbagai *electronic gadget* seperti kamera digital, telepon genggam, *personal digital assistant*, dan lain sebagainya – seorang awam dapat menjadi wartawan karena kemampuannya dalam meliput berita dimana saja yang bersangkutan beraktivitas. Lihatlah bagaimana dibukanya jalur-jalur komunikasi antara televisi dan radio dengan para individu tersebut seperti yang dilakukan oleh kantor berita terkemuka di dunia CNN maupun YouTube. Tidak jarang seorang individu dalam melakukan aktivitasnya sehari-hari berjumpa dengan peristiwa menarik seperti: anggota parlemen yang sedang memarahi pelayan rumah makan, atau mantan pejabat yang sedang memaki-maki satpam, atau artis yang sedang mencak-mencak kesal dengan penjual, atau tokoh masyarakat yang sedang bersua dengan konglomerat hitam, dan lain sebagainya. Kejadian tersebut dengan mudahnya direkam dan diliput dengan menggunakan telepon genggam atau piranti digital yang dibawa untuk selanjutnya di-*upload* ke internet untuk dapat diakses dan dinikmati oleh publik. Tentu saja yang bersangkutan dengan berbagai dalih menyangkal dirinya yang berada dalam rekaman tersebut dan berbalik bersengketa serta menuntut si “wartawan amatir” tersebut.

Ketiga adalah banyaknya beredar email-email gelap alias “email kaleng” yang isinya berupa ancaman, tuduhan, diskriminasi, maupun hal-hal lain yang bersifat menakut-nakuti maupun mendeskreditkan seseorang atau lembaga

di dunia maya. Walaupun tidak jelas identitas pengirimnya (baca: *anonymous*), namun jika isi ancaman terkait dengan terorisme misalnya, atau mereka yang diancam adalah tokoh-tokoh penting seperti para pejabat pemerintahan, terlepas dari benar atau tidaknya konten ancaman tersebut, keberadaannya patutlah ditanggapi secara serius. Misalnya adalah kasus beredarnya surat wasiat pelaku bom Bali yang mengancam keselamatan Presiden Republik Indonesia yang langsung mendapatkan tanggapan serius dari polisi, intelijen, dan segenap penegak hukum beserta praktisi keamanan internet yang ada di tanah air.

Keempat adalah terjadinya berbagai jenis kejahatan atau *forgery* yang bersifat melakukan penipuan identitas atau *phishing* terhadap para pelanggan perusahaan tertentu, terutama bank. Modul operandi yang paling banyak dipergunakan adalah menggunakan media email dan SMS. Dengan berkedok seolah-olah yang bersangkutan merupakan pihak yang sah, para pelanggan diminta untuk melakukan tindakan pengiriman uang maupun pemberitahuan kata kunci (baca: *password*) tertentu yang bermuara pada raibnya harta finansial milik si korban tersebut. Kejadian di dunia maya ini benar-benar berdampak pada dunia nyata karena si pelaku tahu persis kelemahan atau keterbatasan pengetahuan dari para calon korbannya.

Kelima merupakan suatu tindakan di dunia nyata yang bermula dari diskursus yang terjadi di dunia nyata melalui email, situs, *mailing list*, *newsgroup*, *social networking application*, *chatting room*, dan lain sebagainya yang bernuansa kampanye atau persuasif untuk melakukan tindakan tertentu – baik yang bersifat positif maupun negatif. Misalnya adalah sebuah email yang menceritakan suatu peristiwa yang berbau SARA. Terlepas dari benar atau tidak, keberadaan email berantai ini telah memicu kemarahan pihak-pihak yang merasa tersinggung dan berniat untuk melakukan demo besar-besaran di dunia nyata. Atau sebuah *mailing list* yang menyarankan agar para anggotanya untuk melakukan hal tertentu, seperti: tidak berpartisipasi dalam pemilu alias menjadi golput, memboikot produk-produk asing, memusuhi organisasi tertentu, dan lain sebagainya. Tentu saja segala bentuk himbauan di dunia maya ini sedikit banyak berpengaruh pada kehidupan sehari-hari.

Keenam adalah kejadian di dunia nyata akibat berbagai penilaian yang dilakukan oleh sejumlah individu atau komunitas terhadap suatu hal tertentu – barang, jasa, produk, individu, organisasi, dan lain sebagainya - yang memberikan dampak cukup luas di dunia nyata. Lihatlah bagaimana seorang pelanggan yang kecewa dengan kualitasnya produk yang dibelinya kemudian membeberkan seluruh kegundahannya di dunia maya. Atau seorang wisatawan yang mengalami pengalaman buruk ketika sedang berada di suatu daerah wisata tertentu yang menyarankan orang lain untuk tidak pergi ke sana. Atau bagaimana sekelompok orang yang pernah merasa dirugikan oleh pelayanan bank tertentu menceritakan pengalaman pribadi masing-masing mereka yang dapat berakibat terjadinya *rush* dari para pelanggan yang masih menjadi nasabah aktif di bank yang bersangkutan, dan lain sebagainya. Jika pada jaman dahulu pengalaman-pengalaman semacam ini dapat terisolasi beritanya, maka dengan adanya internet, publik dapat turut mengetahuinya dalam waktu sangat singkat.

Keseluruhan fenomena di atas menyiratkan perlu dilakukannya usaha yang terus menerus dan tidak berkesudahan untuk mengedukasi dan meningkatkan wawasan masyarakat dan komunitas terkait dengan pentingnya berhati-hati serta memperhatikan etika ketika berinteraksi di dunia nyata maupun di dunia maya. Jika terjadi peristiwa yang tidak diinginkan terjadi di dunia nyata, seluruh pihak harus bersiap-siap jika hal tersebut akan dan pasti menular ke dunia maya – sehingga seluruh aset data maupun informasi yang ada di internet haruslah dijaga keamanannya. Demikian pula mereka yang berfikir dapat berkomunikasi secara bebas tak terbatas di internet patut pula berhati-hati karena jika yang bersangkutan melakukan perbuatan tertentu yang dapat merugikan orang lain dan telah diatur mekanismenya dalam undang-undang yang berlaku, maka hukuman perdata maupun pidana di dunia nyata dapat ditimpakan kepadanya.

Komunitas internet dunia sadar akan seluruh hal ini, dan mereka semua pun paham akan kompleksitas penanganannya mengingat internet merupakan sebuah jejaring raksasa yang bersifat lintas bidang dan geografis. Beberapa pertanyaan mendasar sering terbersit oleh komunitas keamanan internet.



Berbagai pertanyaan yang terkait dengan strategi serta prosedur mengamankan internet antara lain:

1. Perlukah ada lembaga yang mengawasi dunia maya seperti halnya pemerintahan dan penegakan hukum di dunia nyata?
2. Haruskah ada suatu cara atau mekanisme atau prosedur yang menghubungkan kedua dunia tersebut?
3. Perlukah ada sebuah konvensi internasional yang harus diratifikasi oleh seluruh pihak yang paham akan perlunya kolaborasi dalam mengamankan internet?
4. Apakah perlu dilakukan berbagai kerjasama bilateral atau multilateral antar negara terkait dengan pemanfaatan internet?
5. Perlukah lembaga seperti interpol dibentuk di internet? Atau CERTs dan CSIRTs saja sudah cukup membantu untuk melakukan mitigasi keamanan internet?
6. Apakah lembaga semacam PBB, ITU, ASEAN, dan lain sebagainya perlu membentuk kelompok kerja khusus untuk mengamankan internet? ... dan lain sebagainya.

Tentu saja keseluruhan ide maupun inisiatif yang ada akan memberikan sedikit banyak kontribusi terhadap keamanan internet. Namun berpegang pada prinsip bahwa kekuatan sebuah rantai sangat ditentukan oleh mata rantai terlemah, jelas tersirat bahwa pada akhirnya faktor manusia lah yang akan menentukan kualitas keamanan dari internet. Dengan berpegang pada kenyataan bahwa di dunia ini lebih banyak jumlah orang baiknya dibandingkan dengan yang jahat, maka mudah-mudahan di dunia maya situasi yang sama dapat terjadi, sehingga keberadaan internet lebih dirasakan manfaatnya daripada kerugiannya.

Berdasarkan seluruh kajian kualitatif maupun kuantitatif yang ada, dapat diambil kesimpulan terkait dengan pertanyaan penelitian sebagaimana diperlihatkan pada tabel berikut ini.

Tabel 4. 49 Triangulasi Hasil Penelitian terhadap Pertanyaan Pertama

| No | Jenis Analisa                           | Kesimpulan                                                                                                                                                                                                                                             |
|----|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Kualitatif, <i>Text Analysis</i>        | Studi terhadap 30 (tiga puluh) publikasi yang membahas mengenai puluhan kasus serangan siber yang menimpa sektor pertahanan negara memperlihatkan adanya 9 (sembilan) kategori ancaman serangan.                                                       |
| 2  | Kualitatif, <i>Research Result</i>      | Hasil kajian ENISA dan beragam lembaga kajian siber terkemuka memperlihatkan adanya 15 (lima belas) modus serangan siber yang akan menjadi tren dalam 5-10 tahun ke depan.                                                                             |
| 3  | Kualitatif, <i>Risk Mapping</i>         | Sejumlah kajian yang dinyatakan dalam beragam publikasi memperlihatkan adanya hubungan yang erat antara sembilan kategori ancaman serangan hasil penelitian dengan kelimabelas modus serangan siber yang diprediksi akan mendominasi aktivitas global. |
| 4  | Kuantitatif, <i>Risk Assessment</i>     | Perhitungan asesmen risiko yang melibatkan sejumlah pakar dalam penelitian ini berkesimpulan bahwa terdapat delapan modus serangan yang memiliki probabilitas keterjadian tinggi dengan eksposur dampak yang membahayakan bagi pertahanan negara.      |
| 5  | Kuantitatif, <i>Traffick Monitoring</i> | Kedelapan modus serangan tersebut terdeteksi dalam berbagai institusi pemantau nasional maupun internasional, terutama yang mentargetkan IP Indonesia sebagai tujuan serangan.                                                                         |
| 6  | Kualitatif, <i>Case Studies</i>         | Seluruh kejadian serangan siber di masa lalu yang menimpa beragam negara dapat dipetakan terhadap kesembilan jenis kategori yang dihasilkan dalam penelitian.                                                                                          |

Sumber: Hasil Pengolahan Data Peneliti

#### Dampak Serangan Siber terhadap Kedaulatan Negara

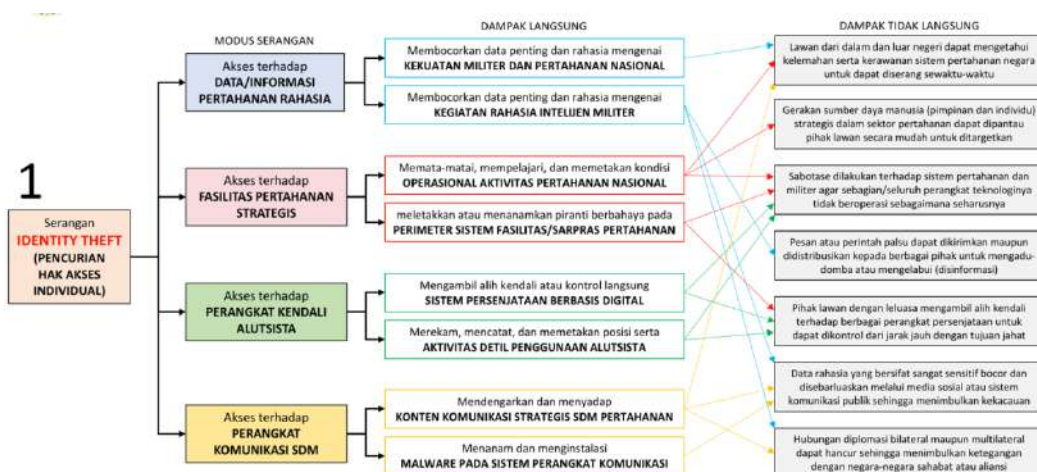
Analisis lebih lanjut berdasarkan data yang telah diolah sebelumnya memperlihatkan bagaimana setiap masing-masing ancaman serangan dapat

memberikan dampak secara langsung maupun tidak langsung terhadap kedaulatan dan pertahanan negara, keselamatan masyarakat, maupun keamanan nasional. Berikut adalah hasil analisis lebih lanjut dengan menggunakan metoda pendekatan sebab-akibat.

### Ancaman dan Dampak Identity Theft

*Identity Theft* adalah serangan dengan cara melakukan pencurian identitas seseorang untuk mendapatkan data atau informasi terkait dengan hak akses (misalnya: *passwords* dan *biometrics*) yang bersangkutan. Dengan memiliki *privilege* tersebut, maka pihak lawan atau musuh dapat memiliki:

1. Hak akses terhadap data/informasi penting yang berhubungan dengan pertahanan negara;
2. Hak akses terhadap fasilitas pertahanan strategis seperti *data center*, *control room*, *command center*, dan lain sebagainya;
3. Hak akses terhadap perangkat kendali alutsista yang ditanamkan pada aset seperti kendaraan tempur, senjata, pesawat udara, kapal laut, dan lain sebagainya; dan
4. Hak akses terhadap perangkat komunikasi dan koordinasi seperti telepon genggam, gawai, tablet, dan piranti komunikasi lainnya.



Gambar 4. 69 Dampak Serangan *Identity Theft*

Sumber : Dampak Serangan Identity Theft (hasil pengolahan data oleh peneliti)

Dampak langsung yang dapat terjadi apabila serangan *identity theft* tersebut berakhir sangat bervariasi, dimana yang paling membahayakan adalah ketika pihak musuh atau lawan melakukan hal-hal sebagai berikut:

1. Membocorkan data penting dan rahasia mengenai kekuatan militer yang dimiliki Indonesia dan berbagai informasi rahasia lain terkait dengan situasi maupun kondisi pertahanan nasional;
2. Membocorkan data penting dan rahasia terkait dengan informasi yang berhasil dikumpulkan oleh intelijen dari berbagai institusi terkait;
3. Memata-matai, mempelajari, dan memetakan kondisi operasional aktivitas pertahanan dan keamanan negara yang sedang maupun akan dilakukan oleh berbagai pihak di tanah air;
4. Meletakkan atau menanam piranti keras maupun lunak berbahaya (*malware*) dalam perimeter sistem fasilitas teknologi informasi di lingkungan sektor pertahanan negara;
5. Mengambil alih kendali atau kontrol langsung terhadap sistem alutsista maupun persenjataan lainnya yang berbasis digital;

6. Merekam, mencatat, dan memetakan posisi serta aktivitas detail seluruh aset militer maupun sumber daya pertahanan yang tersebar di seluruh wilayah NKRI;
7. Menyadap dan mendengarkan seluruh isi percakapan komunikasi maupun interaksi antar pihak-pihak strategis yang menggunakan perangkat digital seperti komputer, telepon genggam, tablet, dan gawai lainnya; dan
8. Menanam aplikasi mata-mata khusus atau *spyware* yang dapat mendengarkan seluruh pembicaraan maupun aktivitas yang dilakukan individu ketika menggunakan perangkat teknologinya untuk berkomunikasi dan berinteraksi.

### Ancaman dan Dampak Data Breach

*Data Breach* adalah suatu fenomena dimana terjadi kesengajaan atau ketidaksengajaan “membocorkan” data atau informasi rahasia ke pihak-pihak yang tidak berhak. Empat modus serangan yang paling banyak terjadi adalah sebagai berikut:

1. Pencurian data yang berisi dokumen rahasia mengenai berbagai hal terkait dengan pertahanan negara;
2. Modifikasi data yang ada pada dokumen atau informasi rahasia untuk menciptakan fenomena disinformasi, misinformasi, dan malinformasi;
3. Penghapusan data penting dan rahasia sehingga negara kehilangan catatan fakta penting yang dimiliki; dan
4. Penyadapan terhadap piranti yang dipergunakan dalam menyusun, menorgnisasikan, dan mengelola dokumen rahasia di lingkungan berbagai institusi terkait dengan pertahanan negara.



Gambar 4. 70 Dampak Serangan *Data Breach*

Sumber : Dampak Serangan Data Breach (hasil pengolahan data oleh peneliti)

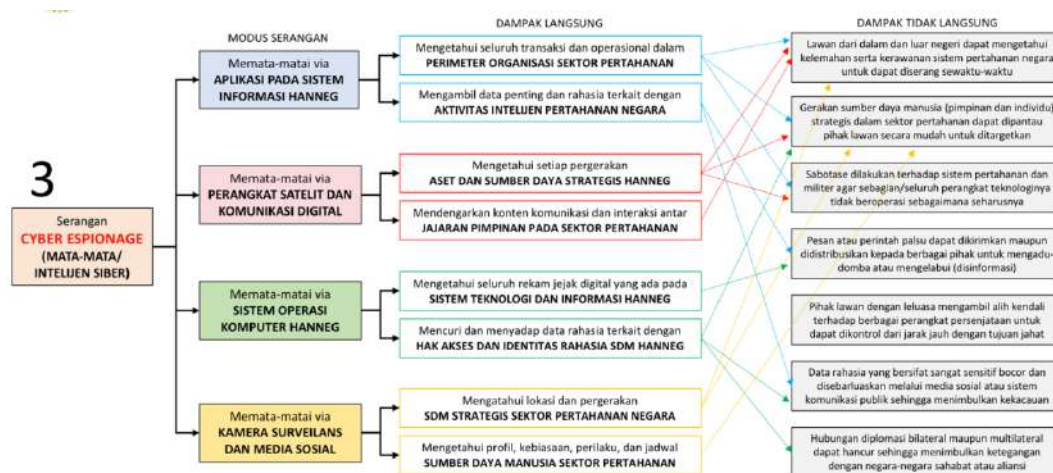
Sejumlah dampak langsung yang dapat terjadi berbasis modus di atas adalah kemampuan musuh atau lawan dalam:

1. Menjualbelikan data rahasia yang berhasil diperoleh ke pihak lain yang bersedia membayarnya, terutama terkait dengan informasi mengenai kekuatan militer dan pertahanan negara;
2. Menggunakan data sebagai salah satu sumber rahasia intelijen militer dan negara untuk melakukan aktivitas *counter intelligence*;
3. Mengubah fakta yang sebenarnya terjadi mengenai catatan operasional aktivitas pertahanan negara yang terjadi di masa lalu;
4. Menambahkurangi data atau konten penting mengenai catatan kegiatan dalam perimeter lingkungan pertahanan negara;

5. Menghilangkan sebagian atau seluruh catatan fakta, bukti, atau peristiwa penting yang pernah terjadi di masa lalu (arsip atau rekam jejak digital);
6. Menghilangkan data dan dokumen penting terkait dengan profil, situasi, dan kondisi mengenai kekuatan militer dan pertahanan negara;
7. Mendengarkan dan menyimak berbagai rencana strategis serta taktikal yang sedang dibicarakan oleh para pimpinan pertahanan negara; dan
8. Memahami dan mengetahui informasi terkait dengan kekuatan serta kelemahan pertahanan negara.

#### Ancaman dan Dampak *Cyber-Espionage*

*Cyber-Espionage* adalah kegiatan mata-mata dalam dunia siber dengan memanfaatkan berbagai *tools* dan teknologi digital. Dalam prakteknya, terdapat empat modus pemanfaatan teknologi untuk melakukan proses mata-mata, yaitu:



Gambar 4. 71 Dampak Serangan *Cyber-Espionage*

Sumber : Dampak Serangan Cyber-Espionage (hasil pengolahan data oleh peneliti)

1. Memata-matai via aplikasi pada sistem informasi pertahanan negara, karena sistem ini paling banyak dipergunakan oleh *users* dan pemangku kepentingan di lingkungan pertahanan dan keamanan;
2. Memata-matai via perangkat satelit dan komunikasi digital, karena melalui satelit tidak ada lagi hal yang dapat disembunyikan, sementara perangkat komunikasi digital seperti telepon genggam dan gawai dipergunakan banyak individu di lingkungan pertahanan;



3. Memata-matai via sistem operasi yang paling banyak dipergunakan oleh komputer dalam lingkungan pertahanan negara, karena melalui level penyadapan ini dapat diperoleh atau diakses berbagai konten yang ada di dalam jaringan; dan
4. Memata-matai via kamera surveilans dan/atau media sosial, karena kedua entitas tersebut merupakan bagian tak terpisahkan dari kehidupan publik secara luas.

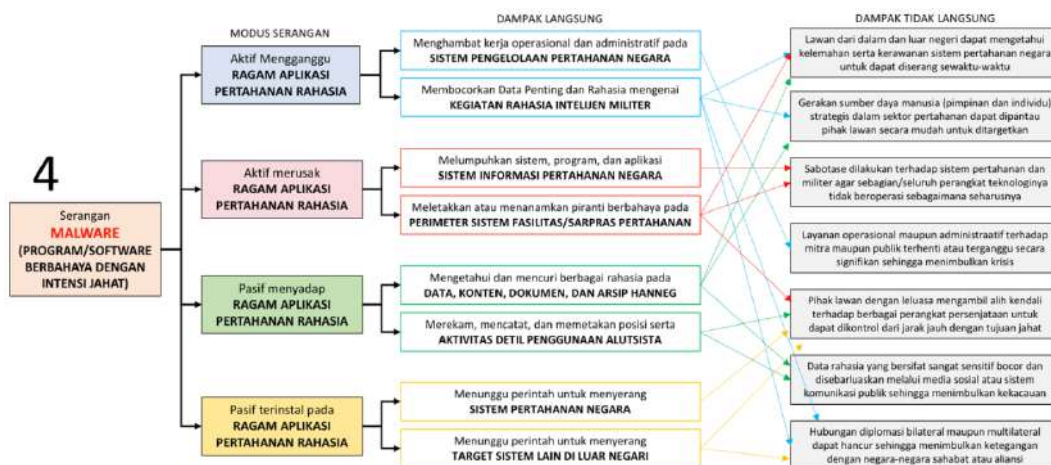
Jika modus serangan tersebut sukses, maka akan banyak kerugian yang akan menimpa negara, karena musuh atau lawan dapat melakukan hal-hal destruktif sebagai berikut:

1. Mengetahui seluruh interaksi, komunikasi, kolaborasi, dan transaksi yang terjadi dalam perimeter organisasi sekitar pertahanan dan keamanan negara;
2. Mengakses dan mengambil data penting terkait dengan hasil intelijen negara yang dilakukan oleh berbagai institusi;
3. Mengetahui setiap pergerakan ases maupun sumber daya pertahanan negara yang bergerak atau dimobiliasi oleh pengambil keputusan;
4. Mendengarkan konten komunikasi dan interaksi antar pihak yang saling berhubungan secara khusus maupun rahasia;
5. Mengetahui seluruh rekam jejak digital yang pernah tercatat di lingkungan perimeter pertahanan negara;
6. Mencuri dan menyadap data, konten, maupun informasi penting tanpa diketahui oleh pihak yang memilikinya secara sah;
7. Mengetahui, melacak, dan mengikuti pergerakan individu, kelompok, maupun pimpinan penting dalam lingkungan sektor pertahanan negara; dan

8. Memetakan profil kebiasaan yang dilakukan oleh berbagai pihak dalam melakukan pengelolaan terhadap pengelolaan negara.

### Ancaman dan Dampak Malware

*Malware* adalah aplikasi atau *software* berintensitas jahat yang ditanamkan pada sistem tanpa sepengetahuan pemiliknya untuk melakukan sejumlah aktivitas berbahaya atau melawan hukum. Modus serangan *malware* dilihat dari perspektif tujuan dari aplikasi tersebut dibuat, yaitu perangkat *software* yang:



Gambar 4. 72 Dampak Serangan *Malware*

Sumber : Dampak Serangan *Malware* (hasil pengolahan data oleh peneliti)

1. Aktif mengganggu ragam sistem dan/atau pertahanan negara agar tidak beroperasi normal sebagaimana seharusnya terjadi;

2. Aktif merusak ragam sistem dan/atau aplikasi pertahanan negara agar sumber daya tersebut lumpuh dan tidak dapat beroperasi sama sekali;
3. Pasif menyadap ragam sistem dan/atau aplikasi pertahanan negara agar berbagai data, konten, atau informasi berharga dapat diperoleh lawan secara ilegal; dan
4. Pasif terinstal pada ragam sistem dan/atau aplikasi pertahanan negara agar sewaktu-waktu dapat digerakkan untuk melakukan tugas tertentu yang membahayakan.

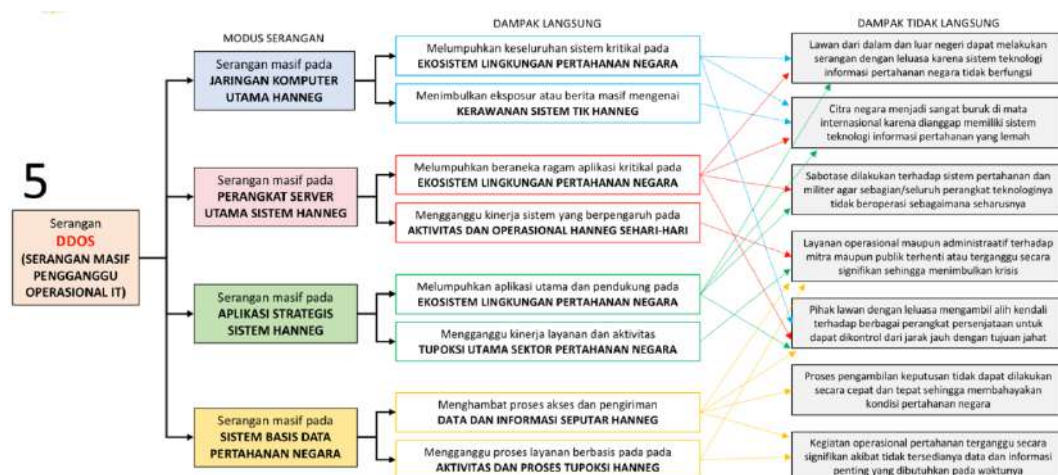
Keberhasilan lawan dalam mengeksploitasi kelemahan yang ada dengan memanfaatkan *malware* akan berakibat fatal karena musuh dapat memiliki kapabilitas dalam melakukan hal-hal ofensif sebagai berikut:

1. Menghambat kerja operasional dan administratif organisasi maupun institusi yang berkaitan dengan pertahanan negara karena sistem aplikasinya terganggu;
2. Membocorkan data penting dan rahasia mengenai kegiatan rahasia intelijen negara;
3. Melumpuhkan program, aplikasi, dan sistem informasi dalam lingkungan pertahanan negara;
4. Menanamkan program dengan intensi berbahaya di sekitar aset dan sumber daya militer maupun fasilitas lain yang terkait dengan pertahanan negara;
5. Mengetahui berbagai pergerakan yang sedang dan akan dilakukan oleh para pimpinan negara dalam usahanya untuk menjaga kedaulatan, keutuhan, dan keselamatan bangsa;
6. Merekam, mencatat, dan mengetahui seluruh posisi aset maupun sumber daya strategis pertahanan negara, baik yang utama maupun cadangan sebagai pendukungnya;

7. Memobilisasi *malware* yang tertanam di berbagai lokasi strategis untuk aktif menjalankan algoritma jahat yang telah diprogramkan; dan
8. Memerintahkan *malware* yang tertanam untuk menyerang berbagai target di dalam dan di luar negeri.

#### Ancaman dan Dampak DDOS

DDOS (*Distributed Denial of Services*) adalah serangan yang bertujuan melumpuhkan sebuah sistem melalui pengiriman jutaan paket data ke satu atau sejumlah titik sasaran. Agar efektif, biasanya modus serangannya diarahkan pada satu titik *server* yang merupakan pusat kendali jejaring komputer, sehingga dalam perimeter pertahanan akan berpotensi terjadi:



Gambar 4. 73 Dampak Serangan DDOS

Sumber : Dampak Serangan DDOS (hasil pengolahan data oleh peneliti)

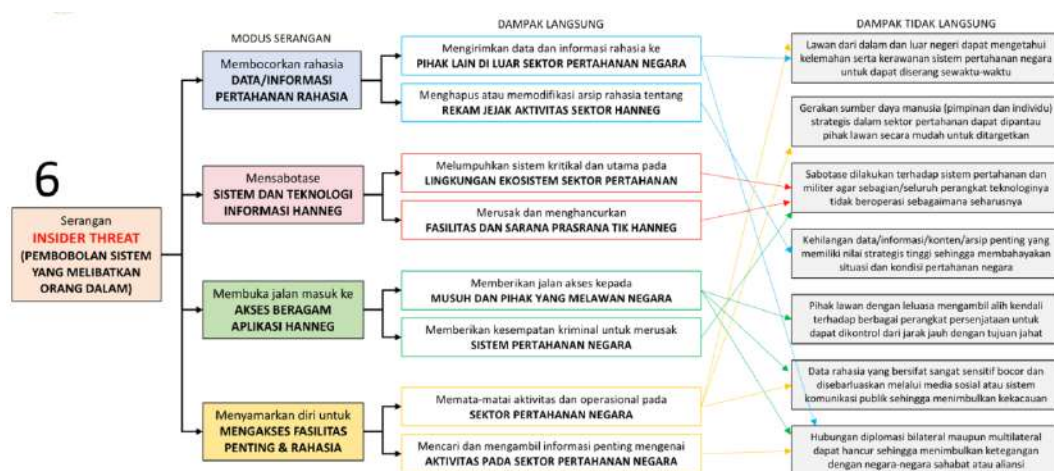
1. Serangan masif pada jaringan komputer utama pertahanan negara yang terhubung dengan berbagai sistem eksternal antar kementerian, institusi, dan lembaga negara;
2. Serangan masif pada perangkat server utama sistem pertahanan negara tempat diinstalasinya berbagai aplikasi penting dalam lingkungan pertahanan negara;
3. Serangan masif pada aplikasi strategis yang ada di dalam sistem pertahanan negara, seperti aplikasi terkait dengan personal militer, persenjataan, aset dan sumber daya, keuangan pertahanan, dan lain-lain; dan
4. Serangan masif pada sistem basis data pertahanan negara, terutama yang menyimpan data, konten, maupun informasi rahasia.

Serangan DDOS dalam implementasinya memberikan dampak langsung maupun tak langsung yang signifikan, karena pihak lawan berpotensi:

1. Melumpuhkan sebagian besar atau bahkan keseluruhan sistem kritikal dalam lingkungan sektor pertahanan negara, yang akan sangat membahayakan situasi bangsa;
2. Memperlihatkan kepada dunia luas betapa rawannya sistem informasi pertahanan Indonesia sehingga selain merangsang hadirnya pihak lain untuk melakukan serangan, namun meruntuhkan reputasi pemerintahan, bangsa, dan negara;
3. Mengganggu sistem aplikasi utama yang ada dalam lingkungan pertahanan negara, sehingga aktivitas operasional sehari-hari mengalami kendala untuk diselenggarakan;
4. Menyebabkan kinerja institusi dan organisasi dalam lingkungan pertahanan negara turun secara signifikan karena banyaknya gangguan yang signifikan terhadap sistem dan teknologi informasi yang dimiliki;
5. Mengganggu sistem aplikasi pendukung pada sejumlah unit atau divisi tertentu sehingga terjadi gangguan pelaksanaan proses atau aktivitas secara sebagian atau menyeluruh;
6. Mempengaruhi kualitas layanan institusi atau lembaga pertahanan negara yang diharapkan oleh para mitra dan organisasi eksternal yang bekerjasama secara erat;
7. Menghambat proses akses atau distribusi data, konten, maupun informasi penting ke berbagai titik-titik unit organisasi di dalam maupun ke luar organisasi; dan
8. Memperlambat aktivitas pengambilan keputusan karena tidak tersedianya data, informasi, maupun konten pada waktu yang dibutuhkan.

### Ancaman dan Dampak Insider Threat

*Insider Threat* adalah serangan yang berasal atau melibatkan individu yang berada di dalam lingkungan organisasi atau institusi yang ingin dilindungi. Serangan ini adalah yang paling sulit untuk dimitigasi karena melibatkan orang-orang yang selama ini dipercaya. Modus yang dilakukan musuh atau lawan dari dalam organisasi adalah:



Gambar 4. 74 Dampak Serangan *Insider Threat*

Sumber : Dampak Serangan Insider Threat (hasil pengolahan data oleh peneliti)

1. Membocorkan rahasia negara yang data maupun informasinya berasal dari dalam organisasi atau lembaga terkait dengan pertahanan negara;

2. Mensabotase sistem dan teknologi informasi pertahanan negara dari dalam sehingga terganggu atau lumpuh secara operasional;
3. Memberikan jalan masuk bagi pihak tak berhak untuk mengakses berbagai sumber daya komputasi maupun sistem aplikasi yang dimiliki pertahanan negara; dan
4. Menyamarkan diri untuk memperoleh akses berbagai fasilitas dan sarana prasarana penting serta sangat rahasia dalam ekosistem pertahanan negara.

Musuh yang berhasil menyamarkan diri atau memperdaya orang lain dalam organisasi untuk meluncurkan serangan dari dalam memiliki kapabilitas:

1. Mengirimkan data atau informasi rahasia yang dimiliki negara ke pihak lain, termasuk lawan atau musuh yang membutuhkannya;
2. Menghapus atau menghilangkan arsip rahasia tertentu yang terkait dengan individu maupun rekam jejak digital seputar kejadian yang berkaitan dengan pertahanan negara;
3. Melumpuhkan sistem dan teknologi kritikal bagi sektor pertahanan negara sehingga tidak beroperasi sebagaimana seharusnya;
4. Merusak dan menghapuskan fasilitas teknologi pertahanan yang telah dibangun dengan berbagai cara destruktif;
5. Memberikan jalan akses kepada pihak lawan atau musuh untuk mengambil alih kendali pertahanan negara melalui akses pada sistem informasi rahasia;
6. Memberikan kesempatan kepada kriminal global untuk menghancurkan sistem teknologi pertahanan negara berbasis digital;

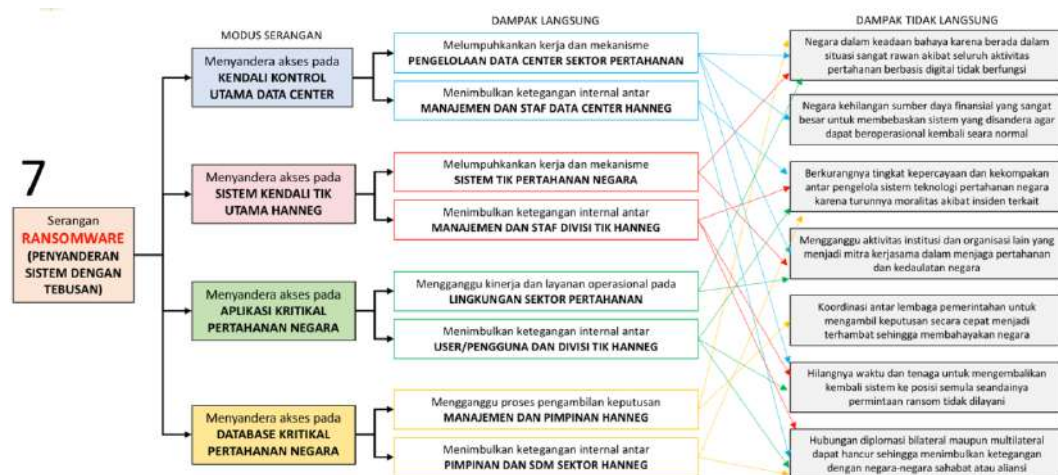


7. Melakukan aktivitas mata-mata intelijen di berbagai unit strategis untuk memperoleh data dan informasi penting maupun krusial; dan
8. Mencari, memodifikasi, dan mendistribusikan informasi bohong, salah, atau keliru untuk berbagai tujuan yang membahayakan pertahanan negara.

#### Ancaman dan Dampak *Ransomware*

*Ransomware* adalah jenis serangan dengan menggunakan pendekatan penyanderaan terhadap sistem oleh pihak lawan atau musuh, sehingga sang pemilik tidak dapat menggunakan sistem, aplikasi, aset, atau sumber daya komputasi terkait. Modus yang biasa dilakukan oleh pihak lawan atau musuh adalah:

1. Menyandera akses pada kendali kontrol utama yang ada di *data center* sehingga seluruh sistem yang aplikasi maupun *database*-nya diletakkan atau di-*host* pada fasilitas terkait tidak bisa diakses atau dioperasikan;
2. Menyandera akses pada sistem informasi utama dalam lingkungan pertahanan keamanan, sehingga seluruh proses atau aktivitas yang berhubungan dengan aplikasi maupun *database* kritikal tidak dapat dipergunakan;
3. Menyandera aplikasi utama atau *core application* dalam lingkungan pertahanan sehingga berbagai aktivitas atau proses rutin yang seharusnya terjadi sehari-hari terganggu keberadaannya; dan
4. Menyandera akses pada sistem *database* kritikal yang menyimpan data maupun informasi penting yang dibutuhkan para pemangku kepentingan dalam lingkungan pertahanan negara setiap harinya.



Gambar 4. 75 Dampak Serangan Ransomware

Sumber : Dampak Serangan Ransomware (hasil pengolahan data oleh peneliti)

Sistem yang diserang oleh *ransomware* akan sulit dikembalikan ke fungsi asalnya kecuali pemilik sistem bersedia memenuhi permintaan apapun yang diajukan oleh sang penyerang – dimana sebagian besar memaksa untuk melakukan pembayaran dalam jumlah sangat besar. Musuh dan lawan yang berhasil meluncurkan serangan ini berhasil:

1. Melumpuhkan kerja dan mekanisme pengelolaan *data center* yang menjadi pusat pengendalian berbagai sistem informasi dan aplikasi dalam lingkungan pertahanan;

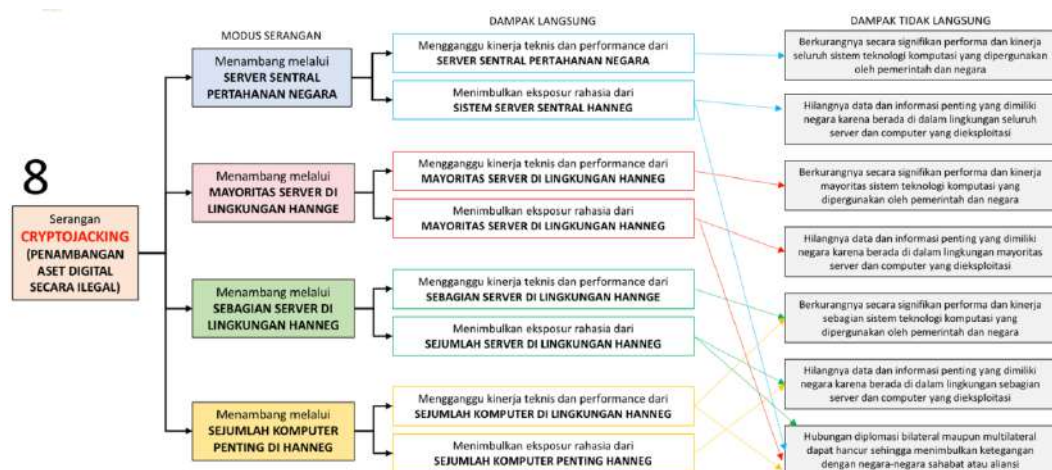
2. Menimbulkan ketegangan internal antara pimpinan dan manajemen *data center* karena tersanderanya sistem tanpa dapat berbuat apapun;
3. Melumpuhkan kerja dan mekanisme sistem teknologi informasi pertahanan negara karena disanderanya aplikasi utama yang berkaitan dengannya;
4. Menimbulkan konflik internal antara pihak-pihak yang bertanggung jawab dalam hal pengelolaan sistem informasi utama pertahanan negara;
5. Mengganggu kinerja dan layanan operasional pada lingkungan pertahanan negara karena tidak dapat diaksesnya sejumlah aplikasi terkait;
6. Menimbulkan pertentangan internal antara divisi teknologi informasi dan pengguna karena mereka tidak dapat menjalankan aktivitas sehari-hari yang berkaitan dengan pengelolaan pertahanan negara;
7. Mengganggu proses pengambilan keputusan pimpinan maupun sejumlah pemangku kepentingan karena seluruh data dan informasi yang dibutuhkan tidak dapat diakses sebagaimana mestinya; dan
8. Meningkatnya ketegangan dan konflik antar *users* dalam lingkungan sektor pertahanan negara karena mereka tidak dapat melaksanakan tugas sehari-hari.

#### Ancaman dan Dampak *Cryptojacking*

*Cryptojacking* adalah penggunaan atau pemanfaatan sumber daya komputasi (*server* atau komputer) untuk melakukan penambangan *crypto-currency* tanpa diketahui oleh sang pemilik. Seperti diketahui bersama, salah satu cara untuk memperoleh *crypto-currency* adalah melalui aktivitas

penambangan yang membutuhkan sumber daya komputasi ekstra besar. Mengingat besarnya biaya yang perlu dikeluarkan untuk membangun fasilitas penambangan dimaksud, maka lawan atau musuh memilih menggunakan aset sumber daya komputasi pihak lain untuk melakukannya. Modus yang biasa dilakukan para musuh dan lawan adalah:

1. Menambang melalui *server* sentral yang terletak pada *data center* utama sektor pertahanan – mengingat begitu banyak sumber daya yang dioperasikan pada fasilitas ini;
2. Menambang melalui mayoritas *server* yang tersebar di berbagai unit organisasi atau instansi terkait dengan sektor pertahanan;
3. Menambang melalui sebagian *server* yang terletak pada satu unit atau divisi organisasi atau lembaga yang berada di dalam perimeter lingkungan pertahanan; dan
4. Menambang melalui sejumlah komputer penting *user* karena teknologi yang dipergunakan adalah termutakhir.



Gambar 4. 76 Dampak Serangan *Cryptojacking*

Sumber : Dampak Serangan *Cryptojacking* (hasil pengolahan data oleh peneliti)

Pihak musuh atau lawan yang berhasil meluncurkan serangan *cryptojacking* akan memiliki kemampuan atau kapabilitas secara langsung maupun tak langsung dalam:

1. Mengganggu kinerja teknis dan *performance* dari *server* sentral sehingga terjadi kelambatan atau gangguan pada aktivitas pengelolaan pertahanan negara;
2. Merusak citra atau reputasi pengelolaan pertahanan negara yang dianggap lemah karena dipergunakannya aset dan fasilitas negara oleh pihak yang tidak berhak memanfaatkannya;
3. Mengganggu kinerja sebagian atau keseluruhan unit dalam lingkungan sektor pertahanan karena sebagian besar komputer yang dipergunakan sering mengalami *error* atau kelambatan proses yang signifikan;
4. Menimbulkan ketegangan dan konflik antara sejumlah pemangku kepentingan karena divisi teknologi informasi tidak dapat memberikan jaminan kinerja sistem yang optimal;
5. Mengganggu kinerja berbagai institusi dan lembaga negara yang terhubung secara *network* dengan sistem pada sektor pertahanan, karena aset pihak lain tersebut berpotensi diserang dengan cara yang sama;
6. Melakukan aktivitas penyadapan, pengambilalihan, dan pengaksesan terhadap aplikasi dan data rahasia yang berada di dalam sumber daya komputas yang dipergunakan untuk menambang;

7. Mengganggu kinerja berbagai *user* individu yang mesin komputernya dipergunakan untuk menambang; dan
8. Mengambil-alih akses komputer individu yang di dalamnya berpotensi terdapat data atau informasi rahasia yang tidak boleh diketahui banyak orang.

Berdasarkan seluruh kajian kualitatif maupun kuantitatif yang ada, dapat diambil kesimpulan terkait dengan pertanyaan penelitian sebagaimana diperlihatkan pada tabel berikut ini.

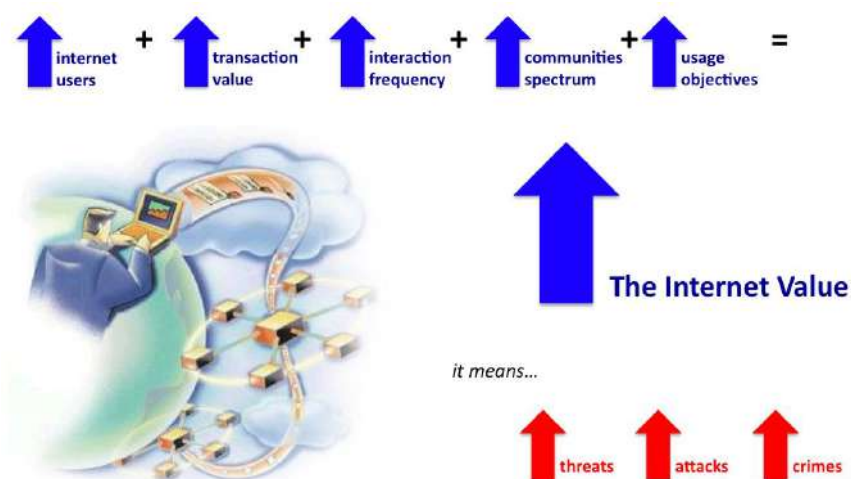
Tabel 4. 50 Triangulasi Hasil Penelitian terhadap Pertanyaan Kedua

| No | Jenis Analisa                            | Kesimpulan                                                                                                                                                                                                                                                             |
|----|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Kualitatif, <i>Cause-Effect Analysis</i> | Studi yang diwarnai dengan diskusi dengan para pakar dan pemangku kepentingan menghasilkan dampak langsung dan tidak langsung dari setiap jenis serangan siber yang berpotensi mengganggu pertahanan nasional.                                                         |
| 2  | Kualitatif, <i>Case Studies</i>          | Keseluruhan dampak langsung maupun tidak langsung tersebut telah terjadi dalam berbagai peristiwa serangan siber di masa lalu baik yang terjadi di Indonesia maupun negara lain di dunia.                                                                              |
| 3  | Kualitatif, <i>Case Studies</i>          | Beragam modus serangan pada masing-masing jenis ancaman serangan merupakan kategori yang diklasifikasikan oleh peneliti berdasarkan berbagai kejadian riil yang telah terjadi di masa lalu.                                                                            |
| 4  | Kuantitatif, <i>Public Discourse</i>     | Keseluruhan dampak langsung maupun tidak langsung yang diidentifikasi pada penelitian kerap disampaikan dalam berbagai konferensi, seminar, lokakarya, maupun forum diskusi karena tingkat kepentingannya untuk mendapatkan perhatian publik dan penyelenggara negara. |

Sumber: Hasil Pengolahan Data Peneliti

## Tingkat Kerawanan Pertahanan Siber di Indonesia

Seperti yang telah diketahui bersama, fakta dan statistik memperlihatkan terjadinya sejumlah kecenderungan yang meningkat di dalam dunia maya, seperti: jumlah pengguna dan pelanggan yang semakin bertambah, nilai transaksi perdagangan yang meningkat nilainya, frekuensi transaksi yang meningkat tajam, tumbuh beranekaragamnya komunitas baru, dan lain sebagainya. Karena semakin banyak orang yang memanfaatkan internet, maka “nilai” atau *value* dari dunia maya ini semakin meningkat. Akibatnya, semakin banyak pihak yang merasa berkepentingan dengan keberadaan internet, dari mereka yang ingin memanfaatkan berbagai peluang yang ada, hingga para kriminal yang ingin memperoleh keuntungan melalui perbuatan-perbuatan yang tidak baik.



Gambar 4. 77 Tren Serangan dan Kejahatan Siber

Sumber : Tren Serangan dan Kejahatan Siber (Indrajit, 2010)

Untuk dapat mengurangi atau memitigasi meningkatnya jumlah kejadian kejahatan (kriminal) di dunia maya, perlu diperhatikan akar penyebabnya terlebih dahulu. Dari berbagai pendapat dan pendekatan yang ada, terlihat adanya tiga jenis aspek usaha mengatasinya, yaitu masing-masing dipandang dari sisi teknis, bisnis, dan sosial.

Aspek teknis digunakan sebagai pendekatan karena menimbang bahwa pada tataran infrastruktur, internet tidak lain terbentuk dari gabungan sejumlah komponen teknis – seperti komputer, *router*, *hub*, modem, database, aplikasi, *printer*, *website*, *firewalls*, dan lain-lain – yang membentuk sebuah jejaring raksasa, dimana secara bebas data dan informasi dapat dipertukarkan untuk beragam keputusan. Berdasarkan konteks ini maka terlihat jelas adanya langkah-langkah secara teknis yang harus dilakukan untuk dapat mengawasi keberlangsungan operasional infrastruktur jejaring internet. Sementara itu dipandang dari perspektif bisnis, internet dianggap sebagai suatu medium atau alat atau sarana berbagai pemangku kepentingan dalam usahanya untuk melakukan kegiatan pertukaran barang dan/atau jasa (baca: bisnis). Tanpa adanya konteks kebutuhan, maka tidak terjadi peristiwa bisnis.





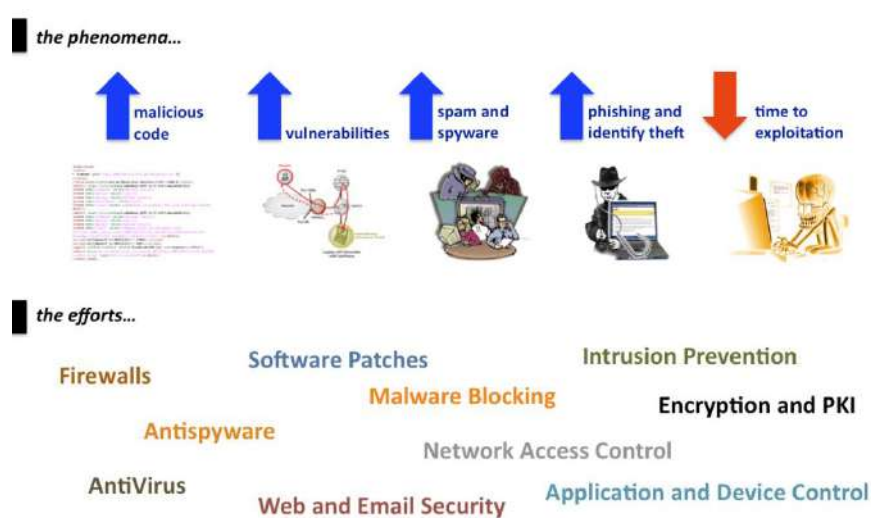
Gambar 4. 78 Tiga Domain Keamanan Siber

Sumber : Tiga Domain Keamanan Siber (Indrajit, 2010)

Di satu sisi ada perusahaan yang jika internetnya tidak jalan akan menimbulkan kerugian yang luar biasa, sementara di pihak lain ada organisasi yang tanpa internet masih dapat berjalan dengan baik. Sehingga kebutuhan untuk mengamankan internet harus dipandang dari sisi ini. Sementara itu aspek sosial menekankan bahwa walau bagaimanapun juga, yang berinteraksi dalam internet adalah manusia – bukan robot atau mesin, sehingga harus diperhatikan pula aspek psikologis dan perilaku mereka sebagai individu yang berakal budi. Marilah satu-satu aspek terkait dibedah untuk melihat bagaimana usaha yang telah dilakukan untuk mempromosikan keamanan dalam berinternet. Perlu diingat bahwa dalam implementasinya, ketiga aspek ini biasanya dilihat sebagai sebuah kesatuan holistik – dalam arti kata bahwa untuk mendapatkan pengamanan yang maksimal, ketiga aspek tersebut harus dilihat dan dipelajari secara lebih mendalam.

Dilihat dari perspektif teknis, terjadi trend dimana jumlah dan variasi *malicious software* bertambah dari masa ke masa. Hal yang sama terjadi pula dengan total kasus *vulnerabilities* yang ditemui dalam berbagai produk perangkat keras maupun perangkat lunak teknologi informasi. Dari segi ancaman atau serangan, data memperlihatkan adanya peningkatan tajam pula terhadap pertumbuhan *spam* maupun *spyware*. Begitu pula halnya dengan kecenderungan terjadinya peningkatan yang berarti terhadap tindakan kriminal seperti *phishing* maupun *identity theft*, yang telah mengakibatkan terjadinya kerugian ekonomis maupun politis. Yang menarik untuk dicermati adalah, terlepas dari adanya trend peningkatan dari seluruh komponen atau entitas di atas, waktu bagi seorang kriminal untuk mengeksploitasi berbagai kelemahan sistem komputer atau jaringan semakin sedikit – alias proses untuk membobol

sebuah jaringan komputer menjadi semakin cepat dari hari ke hari. Tentu saja kenyataan menakutkan ini harus diwaspadai secara serius bagi mereka yang keberlangsungan hidup bisnisnya sangat ditentukan oleh kinerja teknologi informasi yang dimilikinya.



Gambar 4. 79 Strategi Penanganan Domain Teknis

Sumber : Strategi Penanganan Domain Teknis (Indrajit, 2010)

Secara teknis, cara untuk menanggulangi ancaman tersebut, adalah melalui instalasi berbagai produk pengamanan internet maupun komputer untuk mencegah kemungkinan dieksploitasinya berbagai kelemahan yang dimiliki oleh sebuah sistem. Misalnya adalah instalasi *firewalls* untuk melindungi jaringan

internal perusahaan dari akses pihak yang berada pada jejaring eksternal (baca: internet), atau dilibatkannya program *anti-virus* dan *anti-spyware* untuk mencegah berbagai program jahat masuk ke dalam sistem komputer, atau pemasangan *software patches* untuk menambal lubang-lubang kerawanan yang ada pada sistem aplikasi, atau melakukan proses *encryption* untuk mencegah pihak yang tidak berwenang mengerti isi dari suatu pesan atau informasi rahasia. Keseluruhan usaha yang bertujuan untuk mengurangi probabilitas terjadinya eksploitasi terhadap kerawanan sistem ini (baca: mitigasi) dilakukan pada level teknis operasional, dalam arti kata dikembangkan dengan cara mengadakan sejumlah piranti lunak/keras yang kemudian dipasang atau diinstalasi pada sistem komputer atau jaringan yang ingin dilindungi.



Gambar 4. 80 Strategi Penanganan Domain Bisnis

Sumber : Strategi Penanganan Domain Bisnis (Indrajit, 2010)

Dalam perspektif bisnis, tindakan pengamanan terhadap internet dari sebuah organisasi komersial semacam perusahaan dapat dilihat dari berbagai sudut.

Yang pertama adalah memandang isu keamanan internet dari sisi manajemen resiko. Jika sebuah perusahaan sangat tergantung bisnisnya dengan kinerja sistem aplikasi yang terhubung dengan internet, sementara berdasarkan kajian/analisa resiko terdapat sejumlah potensi gangguan yang probabilitas terjadinya tinggi dan dapat mengakibatkan dampak yang signifikan jika sampai terjadi, maka perlu dilakukan tindakan pengamanan secara serius untuk mencegah terjadinya gangguan atau *un-intended event* tersebut. Konteks yang kedua adalah dengan mempertimbangkan tindakan pengamanan yang dimaksud berdasarkan analisa *cost benefit*. Sejauh manfaat yang diperoleh dengan mengamankan sebuah sistem jauh lebih besar dibandingkan dengan biaya yang dikeluarkan, maka tindakan pengamanan tersebut perlu dilakukan. Sementara pendekatan ketiga adalah pemenuhan aspek pengamanan sistem komputer atau internet karena mengacu pada peraturan internal maupun eksternal yang berlaku – misalnya yang telah dikeluarkan oleh pemerintah atau pun pihak otoritas lain berdasarkan standar baku mutu (inter-) nasional. Konteks berikutnya adalah pemenuhan kebutuhan modul pengamanan karena merupakan bagian tak terpisahkan dari tuntutan aspek tata kelola (baca: *governance*) yang baik, seperti transparansi, akuntabilitas, responsibilitas, dan independensi. Perspektif lain yang belakangan ini juga mengemuka adalah alasan pelaksanaan pengamanan yang disebabkan karena tingginya nilai sejumlah aset data dan/atau informasi yang dimiliki oleh perusahaan, sehingga untuk melindunginya, dilakukan sejumlah usaha pengamanan. Misalnya adalah keberadaan data pelanggan yang harus dilindungi, atau informasi intelijen yang bersifat rahasia, atau rumusan/formula paten tertentu, dan lain sebagainya. Dan yang terakhir, kegiatan pengamanan dilakukan oleh segenap pemangku kepentingan karena telah menjadi bagian tak terpisahkan dari manajemen pengelolaan organisasi atau korporasi yang dimaksud (baca: SOP=*Standard Operating Procedure*). Biasanya hal ini dilakukan oleh sebuah perusahaan multi-nasional yang membuka cabangnya di beberapa

negara. Agar seluruh manajemen dan karyawan patuh serta tertib dalam menjaga keamanan informasinya, maka dibuatlah SOP yang harus ditaati dalam kegiatan operasional sehari-hari.



Gambar 4. 81 Strategi Penanganan Domain Sosial

Sumber : Strategi Penanganan Domain Sosial (Indrajit, 2010)

Sifat dan karakteristik manusia sangat dipengaruhi oleh keadaan lingkungan di sekitarnya. Dalam jaman moderen ini, dimana teknologi informasi dan komunikasi telah merasuki seluruh aspek kegiatan dan kehidupan manusia, para generasi muda semakin akrab dengan keberadaan teknologi ini. Sifat *“technology savvy”* tersebut sangat kental melekat pada komunitas kota-kota besar maupun daerah-daerah keramaian lainnya. Kenyataan ini didukung dengan data semakin pesatnya penggunaan telepon genggam dan piranti-piranti digital lainnya (baca: *digital gadgets*) oleh masyarakat luas. Didukung oleh arusnya deras globalisasi dalam dunia perdagangan maupun politis, para

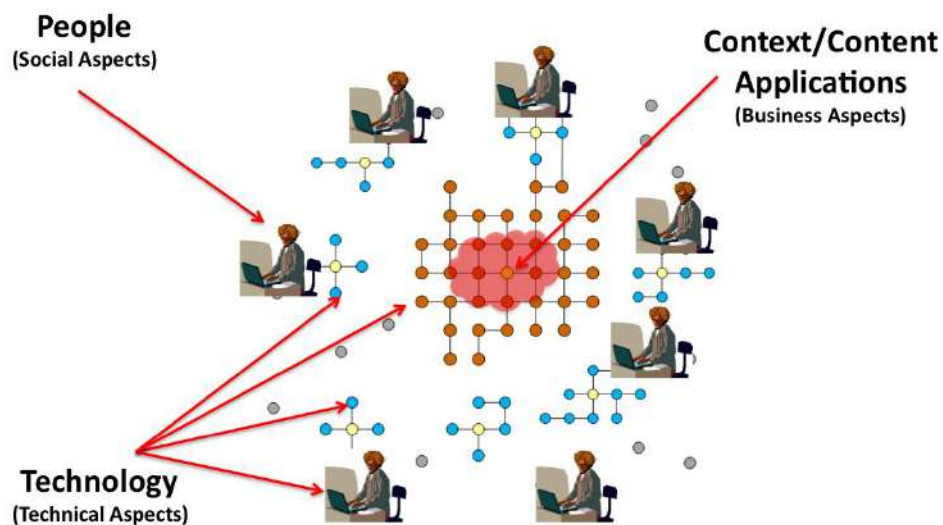
generasi muda ini sudah menganggap dunia maya atau internet menjadi bagian dari kehidupannya sehari-hari. Aplikasi semacam *email*, *chatting*, *mailing list*, *blogging*, *newsgroup*, dan lain-lain sudah merupakan santapan sehari-hari yang tiada henti dimanfaatkan. Namun kenyataan membuktikan bahwa komunitas digital ini terlampau “disilaukan” oleh manfaat internet dan agak lupa atau lalai dalam memandang sisi negatifnya yang dapat merugikan seandainya tidak dikelola dan diperhatikan secara sungguh-sungguh. Jika hal keamanan informasi ini diabaikan, isu-isu seperti pornografi, pelanggaran hak-hak pribadi (baca: *privacy*), kriminalitas, penyadapan, pencurian informasi, dan lain sebagainya dengan leluasa dapat terjadi.

Untuk membiasakan diri peduli dengan keamanan informasi, memang harus dilakukan sejumlah usaha seperti sosialisasi dan pelatihan. Namun terlepas dari hal itu, banyak hal yang dapat dilakukan agar tindakan preventif maupun korektif terkait dapat secara efektif diterapkan. Belajar dan berkaca dari pengalaman organisasi yang berhasil membudayakan kebiasaan mengamankan informasi, berikut adalah ragam “pasangan” pendekatan yang bisa dipergunakan:

1. Antara menerapkan kebijakan dengan mengembangkan desain teknis yang mendukung keamanan (baca: *policy vs. design*). Contohnya kebijakan adalah dengan mengeluarkan surat keputusan berisi butir-butir prosedur yang harus ditaati oleh seluruh karyawan dalam hal mengoperasikan komputer di lingkungan organisasi terkait. Sementara melalui desain teknis adalah dengan mengkondisikan terjadinya suatu status aplikasi yang memaksa pengguna atau *user* taat untuk melakukan tindakan tertentu. Misalnya adalah “paksaan” dari sebuah sistem agar setiap tiga bulan sekali setiap pengguna harus mengganti *password*-nya. Jika tak dilakukan, maka yang bersangkutan tidak dapat mengoperasikan sistem aplikasinya. Contoh lainnya adalah keharusan melakukan proses enkripsi terhadap setiap email yang ingin dikirimkan ke mitra bisnis, tanpa dilakukan proses enkripsi yang benar, maka surat elektronik yang dibuat tidak dapat dikirimkan karena ditolak oleh sistem;

2. Antara menerapkan sistem bonus dengan hukuman penalti (baca: *reward vs. punishment*) terhadap seluruh staf dan karyawan yang berperan sebagai pengguna sistem. Melalui pendekatan bonus, sejumlah “hadiah” atau insentif tertentu diberikan oleh perusahaan kepada karyawannya yang melalui rekam jejak yang dipelajari terbukti selalu patuh dan peduli dengan mekanisme pengamanan informasi yang diberlakukan oleh perusahaan – terutama dalam mencegah terjadinya hal-hal yang tidak diinginkan (usaha preventif). Sementara untuk setiap kasus kebocoran informasi yang terjadi, baik disengaja maupun tidak, sejumlah hukuman secara individu maupun kolektif telah siap dibebankan kepada mereka yang terbukti lalai mengabaikan aspek keamanan informasi tersebut;
3. Antara memberikan “tekanan” atau *pressure* terhadap seluruh karyawan untuk mendapatkan hasil yang cepat dengan memilih pendekatan edukatif yang lebih lambat namun akan jauh lebih efektif;
4. Antara pendekatan “*top down*” dimana setiap pimpinan akan memberikan instruksi kepada bawahannya secara berkala untuk peduli dan menjalankan prosedur keamanan, dengan pendekatan “*bottom up*” dimana terjadi proses sosialisasi mekanisme pengamanan informasi dari level staf maupun karyawan yang sehari-harinya berhadapan langsung dengan permasalahan operasional ke pihak manajemen dengan menggunakan bahasa dan kasus yang kontekstual; dan lain sebagainya.

Intinya adalah jika ketiga aspek tersebut dicoba untuk dihubungkan satu dengan lainnya, maka akan terlihat secara jelas relasi di antaranya, yaitu:



Gambar 4. 82 Jejaring Keterkaitan antar Komponen Siber

Sumber : Jejaring Keterkaitan antar Komponen Siber (Indrajit, 2010)

1. Internet merupakan suatu jejaring raksasa yang mempertemukan berbagai jaringan komputer yang ada di muka bumi ini. Jejaring raksasa tersebut terjadi dengan cara menghubungkan beraneka ragam pusat-pusat penyimpanan data dan informasi yang tersebar lokasinya di seluruh dunia dengan memanfaatkan teknologi informasi dan komunikasi. Berbagai peralatan teknis dan piranti teknologi ini merupakan kunci terciptanya sebuah jaringan raksasa yang tumbuh secara eksponensial dari waktu ke waktu.
2. Jejaring raksasa ini pada dasarnya merupakan sebuah infrastruktur komunikasi yang di atasnya dapat diimplementasikan berbagai aplikasi untuk memenuhi sejumlah kebutuhan hidup manusia, seperti: keperluan pendidikan, interaksi sosial, transaksi bisnis, pengembangan pribadi, dan lain sebagainya. Konteks



pertukaran barang dan jasa tersebut (baca: bisnis) kerap mendominasi pemanfaatan infrastruktur internet ini.

3. Pada akhirnya, sang pengguna berbagai aplikasi yang berjalan di atas internet ini adalah para individu atau komunitas yang berkepentingan, mulai dari anak-anak, orang tua, karyawan, pengusaha, seniman, politikus, pendidik, wiraswastawan, dan lain sebagainya.

Melihat adanya keterhubungan yang jelas baik secara fisik maupun virtual antara ketiga komponen ini, maka dapat disimpulkan bahwa kunci sukses tidaknya atau tinggi rendahnya tingkat keamanan internet sangat ditentukan oleh setiap perangkat teknis, setiap aplikasi, dan setiap individu yang mempergunakannya

Dengan mengibaratkan jejaring raksasa ini sebagaimana halnya sebuah rantai, maka berlaku prinsip yang menyatakan bahwa “kekuatan sebuah rantai sangat ditentukan oleh mata rantai yang terlemah”. Dalam perspektif inilah maka prinsip keamanan “your security is my security” menemukan konteksnya. Tidak ada gunanya atau kecil perannya sebuah *firewalls* dalam sebuah organisasi tanpa diiringi dengan perilaku/budaya pengamanan oleh seluruh pengguna sistem maupun kualitas keamanan seluruh aplikasi yang dipergunakan.

Berdasarkan seluruh kajian kualitatif maupun kuantitatif yang ada, dapat diambil kesimpulan terkait dengan pertanyaan penelitian sebagaimana diperlihatkan pada tabel berikut ini.

Tabel 4. 51 Triangulasi Hasil Penelitian terhadap Pertanyaan Ketiga

| No | Jenis Analisa                        | Kesimpulan                                                                                                                                                                                                                                       |
|----|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Kuantitatif,<br><i>National Rank</i> | Peringkat rendah Indonesia dalam berbagai hal terkait dengan profil, postur, karakteristik, dan kinerja siber yang dinilai oleh sejumlah lembaga terkemuka memperlihatkan masih lemah dan rentannya pertahanan dan keamanan siber yang dimiliki. |

- |   |                                           |                                                                                                                                                                                                                                                                   |
|---|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2 | Kuantitatif, <i>Survey</i>                | Hasil survei dengan responden pengguna komputer di kalangan sektor pertahanan dan militer memperlihatkan masih sangat rendahnya literasi terhadap keamanan informasi dan internet yang bermuara pada rentannya sistem pertahanan dan keamanan siber di Indonesia. |
| 3 | Kuantitatif, <i>Penetration Test</i>      | Uji coba penetrasi terhadap berbagai situs di sektor pertahanan dan militer memperlihatkan bahwa mayoritas situs yang dimiliki mudah ditembus dan dieksploitasi oleh para peretas.                                                                                |
| 4 | Kualitatif, <i>Case Studies</i>           | Sangat banyak kejadian pembobolan sistem teknologi informasi yang menimpa lembaga-lembaga penting negara, termasuk dalam lingkungan pertahanan dan militer.                                                                                                       |
| 5 | Kualitatif, <i>Intelligent Analysis</i>   | Para peretas dan dunia bawah tanah ( <i>dark web</i> ) banyak berbicara mengenai kondisi pertahanan dan keamanan siber Indonesia yang sangat rentan terhadap serangan dan eksploitasi.                                                                            |
| 6 | Kualitatif, <i>Forum Group Discussion</i> | Sebagian besar para pemangku kepentingan pada sektor pertahanan dan militer tidak menerapkan ISO27001 pada institusi penting tempat mereka bekerja dan berkarya.                                                                                                  |
| 7 | Kuantitatif, <i>Traffic Monitoring</i>    | Institusi pemantau internet Indonesia masih melihat kecenderungan jenis serangan yang serupa ke situs-situs di tanah air dengan tingkat keberhasilan yang cukup tinggi, akibat tidak adanya perbaikan terhadap sistem yang dimiliki.                              |

Sumber: Hasil Pengolahan Data Peneliti

#### Efektivitas Kebijakan Kedaulatan Pertahanan Siber di Indonesia

Efektivitas oleh William N. Dunn (1998:429) diartikan apakah suatu alternatif tidak mencapai hasil (akibat) yang diharapkan, atau mencapai tujuan dari dilaksanakannya suatu tindakan, berkenaan aspek rasionalitas teknis, dan selalu diukur dari unit produk atau layanan. Dalam pelaksanaan kebijakan publik, efektifitas diukur dari keberhasilan pencapaian tujuan dan sasaran yang telah ditetapkan pada kebijakan publik. Evaluasi efektivitas merupakan salah satu tipe evaluasi kebijakan yang menilai apakah hasil dan dampak suatu program

kebijakan sesuai yang diharapkan, apakah tujuan yang ingin dicapai dapat terwujud, dan apakah dampak yang diharapkan sebanding dengan usaha yang telah dilakukan (Badjuri, Abdulkahar dan Yuwono, 2002:135). Konseptualisasi efektivitas adalah adanya korelasi antara tujuan kebijakan dan hasil yang dicapai, dimana kerangka penilaian efektivitas mencakup 3 hal (Oberthür & Groen, 2015:1320), yaitu: 1. Input (masukan): kualitas tujuan kebijakan; 2. Proses: terkait dengan tata kelola (keterlibatan, komunikasi, kesesuaian posisi dalam konstelasi kekuasaan dan kepentingan); 3. Outcomes (hasil akhir): Pencapaian tujuan sebagaimana ditetapkan.

Secara input, kualitas tujuan kebijakan sangat jelas, karena berkaitan langsung dengan keberadaan atau eksistensi negara. Beragam kebijakan di bidang pertahanan dan keamanan siber yang telah diundangkan selama ini tidak lain dan tidak bukan bertujuan untuk memastikan terlindunginya masyarakat serta seluruh tumpah darah Indonesia dari berbagai ancaman nyata yang membayangi. Dalam konteks doktrin pertahanan negara, berbagai kebijakan yang telah diberlakukan adalah jawaban terhadap besarnya serangan siber yang merupakan bagian tak terpisahkan dari ancaman non militer. Aspek yang perlu dikritisi terkait dengan komponen input ini adalah ruang lingkup pertahanan dan keamanan yang kerap dipisahkan karena keputusan politik – walaupun dalam dunia siber keduanya saling berhubungan erat dan tak dapat dipisahkan satu dan lainnya.

Secara proses, terdapat banyak isu yang mengemuka terkait dengan efektivitas kebijakan seputar pertahanan dan keamanan siber. Pertama berkaitan dengan *leading sector* atau pihak yang bertanggung jawab terhadapnya. Berbeda dengan negara-negara lain, Indonesia memisahkan antara ruang lingkup pertahanan siber yang menjadi tanggung jawab Kementerian Pertahanan dan keamanan siber yang menjadi akuntabilitas BSSN. Memisahkan kedua domain tersebut sangat berlawanan dengan karakteristik siber yang bebas ruang dan waktu (*borderless*) – sehingga akan sangat menyulitkan dalam proses penetapan peran, tugas, wewenang, dan tanggung jawab masing-masing institusi. Kedua berhubungan dengan cara melakukan tata kelola siber yang cenderung formal, eksklusif, dan birokratis. Sifat-sifat tersebut sangat

bertentangan dengan mekanisme kerja siber yang cenderung egaliter, inklusif, dan non-birokratis. Pendekatan yang tidak kompatibel tersebut membuat sulitnya melaksanakan pertahanan dan keamanan siber yang efektif. Ketiga berkaitan dengan tidak adanya *political will* yang cukup untuk membuat isu pertahanan dan keamanan siber menjadi sebuah permasalahan yang bersifat penting dan genting. Kuantitas dan kualitas peraturan yang sangat rendah di bidang *cyber law* adalah bukti bahwa para regulator belum merasa perlu menaruh perhatian pada aspek pertahanan dan keamanan siber yang di luar negeri telah menjadi sebuah prioritas negara. Keempat berhubungan dengan lemahnya koordinasi antar berbagai pihak dan institusi dalam konteks menjaga pertahanan dan keamanan siber. Masih bekerjanya organisasi birokrasi secara silos tidak saja mempersulit kerjasama antar mereka, namun justru melahirkan kerentanan tersendiri terhadap pertahanan dan keamanan siber negara. Kelima berkaitan dengan pola pikir eksekutif, legislatif, dan yudikatif yang menganggap isu pertahanan dan keamanan siber hanya diperuntukkan bagi negara-negara maju dan besar semata. Mereka lupa bahwa salah satu penyebab terpecahnya komponen masyarakat belakangan ini karena adanya serangan siber berbasis *hoax* pada media sosial. Keenam berhubungan dengan kesiapan masyarakat luas sebagai salah satu komponen penting dalam pertahanan dan keamanan siber yang harus dibekali dengan literasi tinggi. Prinsip bahwa penyerang dan penjahat siber akan selalu mencari *the weakest link* adalah alasan mengapa rakyat dan warga negara Indonesia perlu memiliki kompetensi dan keahlian paling tidak dalam mengamankan dirinya dari berbagai ancaman siber. Dan ketujuh berkaitan dengan ekosistem pertahanan dan keamanan siber yang belum terbentuk secara institusional. Ekosistem dimaksud seharusnya terdiri dari berbagai komponen dan pemangku kepentingan yang saling bekerjasama satu dan lainnya untuk memastikan pertahanan dan keamanan siber nasional.

Secara *outcome*, jelas terlihat bahwa tujuan yang ingin dicapai masih jauh dari kenyataan. Tingginya frekuensi serangan ke situs-situs penting Indonesia, meningkatnya kejahatan siber yang memakan korban, kultur pengguna komputer di sektor pertahanan dan militer yang tidak memperhatikan keamanan informasi, rendahnya literasi mayoritas penduduk Indonesia, dan tidak kompaknya lembaga-lembaga negara dalam bekerjasama hanyalah sejumlah

simtom yang membuktikan belum efektifnya kebijakan yang disusun dan diimplementasikan.

Berdasarkan seluruh kajian kualitatif maupun kuantitatif yang ada, dapat diambil kesimpulan terkait dengan pertanyaan penelitian sebagaimana diperlihatkan pada tabel berikut ini.

Tabel 4. 52 Triangulasi Hasil Penelitian terhadap Pertanyaan Keempat

| No | Jenis Analisa                       | Kesimpulan                                                                                                                                                                                                                                                                                        |
|----|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Kualitatif, <i>Archives Studies</i> | Studi memperlihatkan bahwa regulasi dan/atau kebijakan yang dimiliki Indonesia terkait dengan pertahanan dan keamanan siber sangatlah kurang, baik dari segi kuantitatif maupun kualitatif.                                                                                                       |
| 2  | Kuantitatif, <i>Survey</i>          | Hasil survei dengan responden para pelaku kebijakan sepakat beranggapan bahwa kebijakan yang telah disusun dan diberlakukan selama ini terkait dengan pertahanan dan keamanan siber masih jauh dari efektif.                                                                                      |
| 3  | Kualitatif, <i>Case Studies</i>     | Beraneka ragam peristiwa maupun fenomena serangan di dunia siber yang frekuensinya meningkat dari masa ke masa memperlihatkan masih belum efektifnya kebijakan siber yang ada di tanah air.                                                                                                       |
| 4  | Kualitatif, <i>Group Discussion</i> | Beragam seminar, konferensi, lokakarya, dan forum diskusi kerap menyampaikan pesan akan pentingnya diperkuat faktor kebijakan siber di Indonesia, karena dinilai kurang memadai dan sangat tertinggal dari negara lain yang senantiasa bersifat antisipatif terhadap cepatnya kemajuan teknologi. |

Sumber: Hasil Pengolahan Data Peneliti

Model Pertahanan Siber Ideal yang Holistik dan Komprehensif

ISO (the International Organization for Standardization) dan IEC (the International Electrotechnical Commission) membentuk sistem khusus untuk standarisasi universal. Badan-badan nasional anggota ISO dan IEC berpartisipasi dalam pengembangan standarisasi internasional melalui panitia teknis yang disepakati oleh organisasi-organisasi yang terpercaya keahliannya dalam aktivitas-aktivitas teknis. Panitia Teknis ISO dan IEC berkolaborasi dengan prinsip saling menguntungkan. Organisasi-organisasi internasional lainnya, baik pemerintah maupun non-pemerintah, bekerja sama dengan ISO dan IEC, juga ambil bagian dalam kegiatan tersebut.

Di bidang teknologi informasi, ISO dan IEC telah menetapkan suatu Panitia Teknis Gabungan (ISO/IEC JTC 1). Rancangan standar internasional yang diadopsi oleh panitia teknis gabungan diedarkan kepada seluruh badan-badan nasional untuk diambil suara (*voting*). Penentuan sebagai satu sebuah standar internasional memerlukan persetujuan minimal 75% dari badan-badan nasional yang memberikan suara (pilihan).

Perlu diperhatikan terhadap kemungkinan bahwa beberapa elemen dari standar internasional ini, masih menjadi subyek bahasan hak-hak paten. Dalam hal ini, ISO dan IEC tidak bertanggung jawab untuk mengidentifikasi bagian manapun tentang hak-hak paten tersebut. Standar internasional ISO/IEC 17799 dipersiapkan oleh Institut Standar Inggris (dikenal sebagai BS 7799) dan diadopsi di bawah “prosedur jalur cepat” khusus oleh Panitia Teknis Gabungan ISO/IEC JTC 1, Teknologi Informasi, secara bersamaan dengan persetujuan dari badan-badan nasional ISO dan IEC).

Informasi merupakan aset yang sangat berharga bagi sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha. Oleh karena itu maka perlindungan terhadap informasi (keamanan informasi) merupakan hal yang mutlak harus diperhatikan secara sungguh-sungguh oleh segenap jajaran pemilik, manajemen, dan karyawan organisasi yang bersangkutan. Keamanan informasi yang dimaksud menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman terhadapnya sehingga daapt menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup organisasi.

Informasi dikumpulkan, disimpan, diorganisasikan, dan disebarluaskan dalam berbagai bentuk – baik dokumen berbasis kertas hingga berkas elektronik. Apapun bentuk maupun cara penyimpanannya, harus selalu ada upaya dan untuk melindungi keamanannya sebaik mungkin. Keamanan yang dimaksud harus memperhatikan sejumlah aspek, yaitu:

1. Kerahasiaan – memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya;
2. Integritas – melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif; dan
3. Ketersediaan – memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

Jaminan kewanitaan informasi dapat dicapai melalui aktivitas penerapan sejumlah kontrol yang sesuai. Kontrol yang dimaksud meliputi penerapan berbagai kebijakan, prosedur, struktur, praktek, dan fungsi-fungsi tertentu. Keseluruhan kontrol tersebut harus diterapkan oleh organisasi agar seluruh sasaran keamanan yang dimaksud dapat tercapai.

Menjaga keamanan informasi berarti pula perlunya usaha dalam memperhatikan faktor-faktor keamanan dari keseluruhan piranti pendukung, jaringan, dan fasilitas lain yang terkait langsung maupun tidak langsung dengan proses pengolahan informasi. Dengan amannya keseluruhan lingkungan tempat informasi tersebut berada, maka kerahasiaan, integritas, dan ketersediaan informasi akan dapat secara efektif berperan dalam meningkatkan keunggulan, keuntungan, nilai komersial, dan citra organisasi yang memiliki aset penting tersebut.

Adalah merupakan suatu kenyataan bahwa pada abad globalisasi ini, berbagai organisasi dihadapkan pada sejumlah ancaman-ancaman keamanan informasi dari berbagai sumber, seperti yang diperlihatkan dengan keberadaan sejumlah kasus kejahatan komputer secara sengaja, seperti: pencurian data, aktivitas spionase, percobaan *hacking*, tindakan vandalisme, dan lain-lain,

maupun ancaman yang disebabkan karena kejadian-kejadian lain seperti bencana alam, misalnya: banjir, gempa bumi, tsunami, dan kebakaran. Bergantungnya kinerja organisasi pada sistem informasi mengandung arti bahwa keseluruhan ancaman terhadap keamanan tersebut merupakan portofolio resiko yang dihadapi oleh organisasi yang bersangkutan.

Perencanaan dan pengembangan sistem keamanan informasi yang baik semakin mendapatkan tantangan dengan adanya interkoneksi antara berbagai jaringan publik dan privat, terutama terkait dengan proses pemakaian bersama sejumlah sumber daya informasi untuk meningkatkan optimalisasi akses. Manfaat yang didapatkan melalui pendistribusian komputasi ini disaat yang sama melemahkan efektivitas kontrol secara terpusat, yang berarti pula menciptakan suatu kelemahan-kelemahan baru pada sistem tersebut. Kenyataan memperlihatkan bahwa sebagian besar sistem informasi yang dirancang dan dibangun dewasa ini kurang begitu memperhatikan faktor-faktor keamanan tersebut. Padahal untuk membangun sistem keamanan informasi yang baik, perlu dilakukan sejumlah langkah-langkah metodologis tertentu.

Keamanan informasi yang baik dapat dicapai melalui penerapan sejumlah upaya-upaya teknis (operasional) yang didukung oleh berbagai kebijakan dan prosedur manajemen yang sesuai. Proses tersebut dimulai dari pengidentifikasian sejumlah kontrol yang relevan untuk diterapkan dalam organisasi, yang tentu saja harus berdasarkan pada analisa kebutuhan aspek keamanan informasi seperti apa yang harus dimiliki perusahaan. Setelah kebijakan, prosedur, dan panduan teknis operasional mengenai kontrol-kontrol yang harus diterapkan dalam organisasi disusun, langkah berikutnya adalah sosialisasi keseluruhan piranti tersebut ke segenap lapisan manajemen dan karyawan organisasi untuk mendapatkan dukungan dan komitmen. Selanjutnya, para pihak berkepentingan lain yang berada di luar organisasi – seperti pemasok, pelanggan, mitra kerja, dan pemegang saham – harus pula dilibatkan dalam proses sosialisasi tersebut karena mereka merupakan bagian tidak terpisahkan dari sistem keamanan informasi yang dibangun. Keterlibatan sejumlah pakar maupun ahli dari luar organisasi kerap kali dibutuhkan untuk membantu organisasi dalam menerapkan langkah-langkah di tersebut. Dengan



adanya pengetahuan yang mereka miliki, terutama dalam membantu organisasi menyusun kebutuhan dan mengidentifikasi kontrol-kontrol yang dibutuhkan, niscaya sistem keamanan informasi yang dibangun dapat lebih efektif dan ekonomis.

Dari penjabaran sebelumnya jelas terlihat bahwa semua pihak di dalam organisasi (manajemen dan karyawan) maupun di luar organisasi (pemasok, pelanggan, mitra kerja, dan pemegang saham) bertanggung jawab secara penuh dalam proses keamanan informasi. Hal tersebut disebabkan karena mereka semua terlibat secara langsung maupun tidak langsung dalam proses penyediaan, penyimpanan, pemanfaatan, dan penyebarluasan informasi dalam organisasi. Untuk menjamin adanya kesadaran, kemauan, dan komitmen untuk melakukan hal tersebut, maka perlu adanya pihak yang memiliki tugas dan kewajiban khusus untuk memantau efektivitas keamanan informasi tersebut. Keberadaan pihak tersebut mutlak dibutuhkan oleh organisasi dalam berbagai bentuknya, seperti: perusahaan komersial, institusi pemerintah, organisasi publik, lembaga nirlaba, dan lain sebagainya.

Pemahaman dan kesadaran mengenai pentingnya memperhatikan aspek-aspek keamanan informasi harus ditanamkan sedini mungkin oleh setiap organisasi terhadap seluruh jajaran manajemen dan karyawannya. Setiap individu yang berada di dalam organisasi memiliki tanggung jawab untuk melindungi keamanan informasi yang dimilikinya, sebagaimana layaknya memperlakukan hal yang sama terhadap aset-aset berharga lainnya. Dalam kaitan dengan hal ini, harus terdapat kebijakan menyangkut pemberian sanksi bagi mereka yang lalai memperhatikan hal ini maupun penghargaan bagi mereka yang berprestasi mempromosikan dan menerapkan keamanan informasi di organisasi terkait.

Tentunya proses keamanan informasi harus dimulai dari menjaga tempat-tempat atau fasilitas fisik dimana informasi beserta piranti/peralatan pendukungnya disimpan. Mengingat bahwa hampir seluruh fungsi dalam organisasi memiliki tanggung jawab dalam mengelola informasinya masing-masing, maka setiap individu dalam berbagai fungsi-fungsi tersebut harus secara aktif menjaga keamanan informasi. Dengan berkembangnya teknologi akses

informasi dari jarak jauh melalui pemanfaatan jaringan komputer, maka ruang lingkup keamanan menjadi semakin besar dan kompleks, karena sudah tidak dibatasi lagi oleh sekat-sekat lingkungan fisik tertentu. Perkembangan internet yang telah membentuk sebuah dunia maya tempat berbagai individu maupun komunitas berinteraksi (tukar menukar informasi) secara elektronik memperlihatkan bagaimana kompleksnya keamanan area baik secara fisik maupun virtual – yang tentu saja akan sangat berpengaruh terhadap manajemen kontrol yang akan dipilih dan diterapkan.

Untuk dapat membangun dan menerapkan sistem keamanan informasi yang baik, sebaiknya organisasi memulainya dari upaya melakukan kajian atau telaah terhadap resiko-resiko keamanan yang mungkin timbul. Kajian yang dimaksud dapat diterapkan dalam tingkatan organisasi, maupun pada tataran sub bagian atau fungsi organisasi tertentu, seperti sistem informasi, komponen, layanan, dan lain sebagainya – sesuai dengan skala prioritas yang ada. Kajian resiko yang dimaksud merupakan suatu pendekatan sistematis dari proses:

1. Identifikasi terhadap kejadian-kejadian apa saja yang dapat mengancam keamanan informasi perusahaan dan potensi dampak kerugian yang ditimbulkan jika tidak terdapat kontrol yang memadai; dan
2. Analisa tingkat kemungkinan (probabilitas) terjadinya hal-hal yang tidak diinginkan tersebut akibat adanya sejumlah kelemahan pada sistem yang tidak dilindungi dengan kontrol tertentu.

Hasil dari kajian tersebut akan menghasilkan arahan yang jelas bagi manajemen dalam menentukan prioritas dan mengambil sejumlah tindakan terkait dengan resiko keamanan informasi yang dihadapi. Dengan adanya prioritas yang jelas maka akan dapat didefinisikan kontrol-kontrol mana saja yang perlu diterapkan. Perlu diperhatikan bahwa langkah-langkah tersebut harus dilakukan secara kontinyu dan periodik, mengingat dinamika perubahan organisasi dan lingkungan eksternal yang sedemikian cepat. Langkah-langkah interaktif yang dimaksud meliputi:

1. Menganalisa perubahan kebutuhan dan prioritas organisasi yang baru sesuai dengan pertumbuhannya;
2. Mempelajari ancaman-ancaman atau kelemahan-kelemahan baru apa yang terjadi akibat perubahan yang ada tersebut; dan
3. Memastikan bahwa kendali-kendali yang dimiliki tetap efektif dalam menghadapi ancaman-ancaman kejadian terkait.

Perlu dicatat bahwa peninjauan berkala tersebut harus dilakukan pada bagian organisasi dengan tingkat kedalaman tertentu sesuai dengan hasil analisa risiko yang telah dilakukan sebelumnya. Karena keberadaan kontrol ini akan sangat berpengaruh terhadap kinerja sebuah organisasi, maka proses telaah risiko harus dimulai dari tingkat, agar mereka yang berwenang dapat menilainya berdasarkan tingkat kepentingan tertinggi (pendekatan *top down*).

Keberadaan dan kepatuhan terhadap standar merupakan hal mutlak yang harus dimiliki oleh pihak manapun yang ingin menerapkan sistem keamanan informasi secara efektif. Sejumlah alasan utama mengapa standar diperlukan adalah untuk menjamin agar:

1. Seluruh pihak yang terlibat dalam proses keamanan informasi memiliki kesamaan pengertian, istilah, dan metodologi dalam melakukan upaya-upaya yang berkaitan dengan keamanan data;
2. Tidak terdapat aspek-aspek keamanan informasi yang terlupakan karena standar yang baik telah mencakup keseluruhan spektrum keamanan informasi yang disusun melalui pendekatan komprehensif dan holistik (utuh dan menyeluruh);
3. Upaya-upaya untuk membangun sistem keamanan informasi dilakukan secara efektif dan efisien dengan tingkat optimalisasi yang tinggi, karena telah memperhatikan faktor-faktor perkembangan teknologi serta situasi kondisi yang berpengaruh terhadap organisasi;

4. Tingkat keberhasilan dalam menghasilkan sistem keamanan informasi yang berkualitas menjadi tinggi, karena dipergunakan standar yang sudah teruji keandalannya.

Seperti yang telah dijelaskan sebelumnya, proses awal yang harus dilakukan setiap organisasi adalah melakukan kajian awal untuk mengidentifikasi kebutuhan keamanan, mengingat setiap organisasi memiliki sifat uniknya masing-masing. Berdasarkan hasil tersebut, pilihlah kontrol-kontrol sesuai yang dapat diambil dalam dokumen standar ini, maupun dari sumber-sumber lain untuk melengkapinya manakala dibutuhkan. Setelah itu susunlah perencanaan program penerapan kontrol-kontrol yang dimaksud dengan melibatkan pihak internal maupun eksternal organisasi sesuai dengan kebutuhan. Perlu diperhatikan bahwa sejumlah kontrol sifatnya mutlak harus dimiliki oleh sebuah organisasi, sementara berbagai kontrol lainnya hakekatnya ditentukan oleh situasi dan kondisi organisasi yang bersangkutan. Disamping itu terdapat pula sejumlah kontrol yang harus diperhatikan secara sungguh-sungguh karena memiliki implikasi besar karena menyangkut kepentingan publik atau kontinuitas keberadaan organisasi.

Berikut adalah penjabaran ringkas dari sepuluh domain atau aspek yang harus diperhatikan terkait dengan isu keamanan informasi dalam sebuah organisasi atau institusi.

1. **Kebijakan Keamanan:** untuk memberikan arahan dan dukungan manajemen keamanan informasi. Manajemen harus menetapkan arah kebijakan yang jelas dan menunjukkan dukungan, serta komitmen terhadap keamanan informasi melalui penerapan dan pemeliharaan suatu kebijakan keamanan informasi di seluruh tataran organisasi;
2. **Pengorganisasian Keamanan:** untuk mengelola keamanan informasi dalam suatu organisasi. Satu kerangka kerja manajemen harus ditetapkan untuk memulai dan mengontrol penerapan keamanan informasi di dalam organisasi. Untuk manajemen

dengan kepemimpinan yang kondusif harus dibangun untuk menyetujui kebijakan keamanan informasi, menetapkan peran keamanan dan mengkoordinir penerapan keamanan di seluruh tataran organisasi. Jika diperlukan, pendapat pakar keamanan informasi harus dipersiapkan dan tersedia dalam organisasi. Hubungan dengan pakar keamanan eksternal harus dibangun untuk mengikuti perkembangan industri, memonitor standar dan metoda penilaian serta menyediakan penghubung yang tepat, ketika berurusan dengan insiden keamanan. Pendekatan multi-disiplin terhadap keamanan informasi harus dikembangkan, misalnya dengan melibatkan kerjasama dan kolaborasi di antara manajer, pengguna, administrator, perancang aplikasi, pemeriksa dan staf keamanan, serta keahlian di bidang asuransi dan manajemen resiko;

3. **Klasifikasi dan Kontrol Aset:** untuk memelihara perlindungan yang tepat bagi pengorganisasian aset. Semua aset informasi penting harus diperhitungkan keberadaannya dan ditentukan kepemilikannya. Akuntabilitas terhadap aset akan menjamin terdapatnya perlindungan yang tepat. Pemilik semua aset penting harus diidentifikasi dan ditetapkan tanggung jawabnya untuk memelihara sistem kontrol tersebut. Tanggungjawab penerapan sistem kontrol dapat didelegasikan. Akuntabilitas harus tetap berada pada pemilik aset;
4. **Pengamanan Personil:** untuk mengurangi resiko kesalahan manusia, pencurian, penipuan atau penyalahgunaan fasilitas. Tanggung jawab keamanan harus diperhatikan pada tahap penerimaan pegawai, dicakup dalam kontrak dan dipantau selama masa kerja pegawai. Penelitian khusus harus dilakukan terhadap calon pegawai khususnya di bidang tugas yang rahasia. Seluruh pegawai dan pengguna pihak ketiga yang menggunakan fasilitas pemrosesan informasi harus menanda-tangani perjanjian kerahasiaan (*non-disclosure*);

5. **Keamanan Fisik dan Lingkungan:** untuk mencegah akses tanpa otorisasi, kerusakan, dan gangguan terhadap tempat dan informasi bisnis. Fasilitas pemrosesan informasi bisnis yang kritis dan sensitif harus berada di wilayah aman, terlindung dalam perimeter keamanan, dengan rintangan sistem pengamanan dan kontrol masuk yang memadai. Fasilitas tersebut harus dilindungi secara fisik dari akses tanpa izin, kerusakan dan gangguan. Perlindungan harus disesuaikan dengan identifikasi risiko. Disarankan penerapan kebijakan *clear desk* dan *clear screen* untuk mengurangi risiko akses tanpa izin atau kerusakan terhadap kertas, media dan fasilitas pemrosesan informasi.
6. **Komunikasi dan Manajemen Operasi:** untuk menjamin bahwa fasilitas pemrosesan informasi berjalan dengan benar dan aman. Harus ditetapkan tanggungjawab dan prosedur untuk manajemen dan operasi seluruh fasilitas pemrosesan informasi. Hal ini mencakup pengembangan instruksi operasi yang tepat dan prosedur penanganan insiden. Dimana mungkin harus ditetapkan pemisahan tugas, untuk mengurangi resiko penyalahgunaan sistem karena kecerobohan atau kesengajaan;
7. **Pengontrolan Akses:** untuk mencegah akses tanpa izin terhadap sistem informasi. Prosedur formal harus diberlakukan untuk mengontrol alokasi akses, dari pendaftaran awal dari pengguna baru sampai pencabutan hak pengguna yang sudah tidak membutuhkan lagi akses ke sistem informasi dan layanan. Perhatian khusus harus diberikan, jika diperlukan, yang dibutuhkan untuk mengontrol alokasi hak akses istimewa, yang memperbolehkan pengguna untuk menembus sistem kontrol;
8. **Pengembangan dan Pemeliharaan Sistem:** untuk memastikan bahwa keamanan dibangun dalam sistem informasi. Persyaratan Keamanan sistem mencakup infrastruktur, aplikasi bisnis dan aplikasi yang dikembangkan pengguna. Disain dan implementasi proses bisnis yang mendukung aplikasi atau layanan sangat

menentukan bagi keamanan. Persyaratan keamanan harus diidentifikasi dan disetujui sebelum pengembangan sistem informasi. Semua persyaratan keamanan sistem informasi, termasuk kebutuhan pengaturan darurat, harus diidentifikasi pada fase persyaratan suatu proyek, dan diputuskan, disetujui serta didokumentasikan sebagai bagian dari keseluruhan kasus bisnis sebuah sistem informasi;

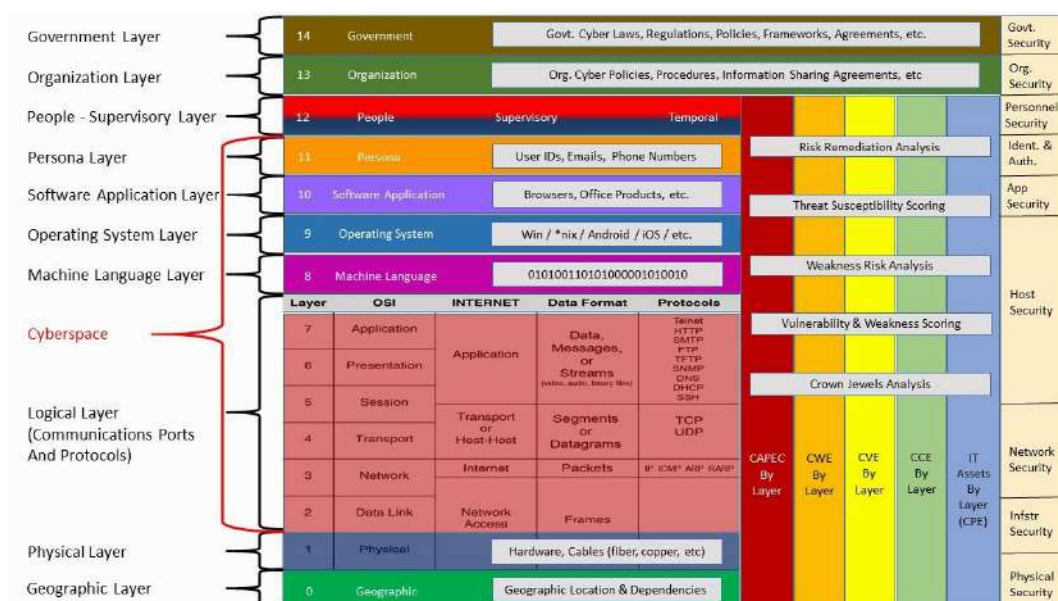
9. **Manajemen Kelangsungan Bisnis:** Untuk menghadapi kemungkinan penghentian kegiatan usaha dan melindungi proses usaha yang kritis dari akibat kegagalan atau bencana besar. Proses manajemen kelangsungan usaha harus diterapkan untuk mengurangi kerusakan akibat bencana atau kegagalan sistem keamanan (yang mungkin dihasilkan dari, sebagai contoh, bencana alam, kecelakaan, kegagalan alat dan keterlambatan) sampai ke tingkat yang dapat ditolerir melalui kombinasi pencegahan dan pemulihan kontrol. Konsekuensi dari bencana alam, kegagalan sistem keamanan dan kehilangan layanan harus dianalisa. Rencana darurat harus dikembangkan dan diterapkan untuk memastikan proses usaha dapat disimpan ulang dalam skala waktu yang dibutuhkan. Rencana semacam itu harus dijaga dan dipraktekkan untuk menjadi bagian integral keseluruhan proses manajemen. Manajemen kelangsungan bisnis harus mencakup kontrol untuk mengidentifikasi dan mengurangi risiko, membatasi konsekuensi kesalahan yang merusak, dan memastikan penyimpulan tahapan operasional yang penting; dan
10. **Kesesuaian:** Untuk menghindari pelanggaran terhadap hukum pidana maupun hukum perdata, perundangan, peraturan atau kewajiban kontrak serta ketentuan keamanan lainnya. Desain, operasional, penggunaan dan manajemen sistem informasi adalah subyek dari perundangan, peraturan, dan perjanjian kebutuhan keamanan. Saran untuk kebutuhan legalitas yang bersifat khusus harus dicari dari penasihat hukum organisasi, atau

praktisi hukum yang berkualitas. Kebutuhan legalitas bervariasi dari negara ke negara dan bagi informasi yang dihasilkan dalam satu negara yang didistribusikan ke negara lain (contohnya arus data lintas batas).

Ruang siber terbentuk akibat adanya interkoneksi antar sumber daya komputasi dan perangkat dukung lainnya. Hal ini mengandung arti bahwa keberadaan entitas virtual tersebut adalah akibat dari dihubungkannya beragam aset fisik dalam sebuah rancangan tertentu. Dengan kata lain, eksistensi ruang siber dapat “dikendalikan” dengan cara mengontrol sumber daya komputasi yang membentuknya. Pengertian ini sungguh penting mengingat ada banyaknya diskursus seputar dapat atau tidaknya ruang siber itu didefinisikan dan dikenladikan keberadaannya.

Adapun sumber daya fisik dimaksud membutuhkan tempat untuk meletakkan dan menginstalasinya. Pilihannya pertama adalah di darat, yaitu menempati lokasi pada sebidang tanah atau bangunan yang berdiri di atasnya. Pilihan kedua adalah di laut, dimana dapat diletakkan di atas instalasi bangunan atau kapal yang bergerak di atasnya. Dan pilihan ketiga adalah di udara, baik dalam ketinggian rendah hingga menembus stratosfir (antarksa) sebagaimana sebuah satelit. Intinya adalah bahwa aset digital tersebut perlu menempati spasi geografis.





Gambar 4. 83 Cyber Terrain (Riley, 2014) – US Department of Defense

Sumber : US Department of Defense (Riley, 2014)

Setelah berbagai piranti keras dan lunak diinstalasi ke dalam sumber daya komputasi, maka terbentuklah ruang siber. Berbeda dengan dua domain sebelumnya yang menempati wilayah atau entitas fisik, yaitu *layer* geografis dan *layer* fisikal, *layer* di atasnya merupakan entitas yang bersifat abstrak sehingga kerap disebut sebagai *layer* logika. Dikatakan sebagai *layer* logika karena cara kerjanya berdasarkan algoritma logis yang didasarkan pada bilangan dasar dua atau *binary*. Ada enam *layer* dalam *layer* logika ini yaitu *data link*, *network*, *transport*, *session*, *presentation*, dan *application*. Kemudian ada empat *layer* abstrak lagi di dalam domain siber, yaitu *layer* bahasa mesin, sistem operasi, *software* aplikasi, dan *persona*.

Sebagai pengguna ruang siber, manusia merupakan *layer* yang ada di atasnya. Berbagai hal dilakukan antar individu melalui beragam aktivitas interaksi, transaksi, kolaborasi, kooperasi, dan komunikasi. *Layer* pengguna atau *users* ini adalah mereka yang aktif sehari-harinya mengakses ruang siber seperti internet. Manusia dalam kehidupan sosialnya membentuk berbagai kelompok atau

komunitas, baik yang bersifat formal maupun informal. Jika mereka berkumpul dalam satu kelompok guna mencapai tujuan tertentu, maka terbentuklah sebuah organisasi. Pada tataran organisasi ini dibuatlah aturan, prosedur, mekanisme, proses, dan hal-hal lain untuk mengelola data, informasi, dan berbagai aset digital lainnya. Seluruh organisasi dalam masyarakat perlu dikelola keberadaannya agar dapat berfungsi secara harmoni. Di sinilah *layer* berikutnya terbentuk, yaitu pemerintah. Untuk memastikan seluruh organisasi berjalan dengan baik, termasuk interaksi yang terjadi di antaranya, disusunlah regulasi, peraturan, standar, kerangka, dan lain sebagainya.

Setiap *layer* pada dasarnya memiliki risiko untuk diserang, karena memiliki kerentanannya masing-masing. Tabel berikut memperlihatkan berbagai jenis ancaman serangan yang membayangi setiap *layer*.

Tabel 4. 53 Ancaman Serangan berbasis Lapisan Teknologi

| Layer | Nama             | Ancaman Serangan                                                                                                                                                                                                                                                                                                             |
|-------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0     | Geographic Layer | <ol style="list-style-type: none"> <li>1. Social Information Gathering via Dumpster Diving</li> <li>2. Social Information Gathering via Pretexting</li> <li>3. Physical Theft</li> <li>4. Bypassing Physical Locks</li> </ol>                                                                                                |
| 1     | Physical Layer   | <ol style="list-style-type: none"> <li>1. Physical Theft</li> <li>2. Bypassing Physical Locks</li> <li>3. Cloning Magnetic Strip Cards</li> <li>4. Physical Destruction of Device or Component</li> <li>5. Malicious Logic Insertion via Counterfeit Hardware</li> <li>6. Malicious Logic Insertion via Inclusion</li> </ol> |

- of Counterfeit Hardware Components
- 2-7 Logical Layers
7. Harvesting Usernames or UserIDs via Application API Event Monitoring (Application Layer)
  8. Traceroute Route Enumeration (Network Layer & Transport Layer)
  9. Network Topology Mapping (Network Layer, Transport Layer, & Application Layer)
  10. OS Fingerprinting (Network Layer, Transport Layer, & Application Layer)
  11. ICMP Fingerprinting Probes (Network Layer)
  12. Scanning for Vulnerable Software (Network Layer, Transport Layer, & Application Layer)
  13. TCP/IP Fingerprinting Probes (Network Layer, Transport Layer, & Application Layer)
  14. Active OS Fingerprinting (Network Layer)
  15. DNS Zone Transfers (Application Layer)
  16. TCP RPC Scan (Transport Layer)
- 8 Machine Language
17. Lifting Data Embedded in Client Distributions
  18. Reverse Engineer an Executable to Expose Assumed Hidden Functionality or Content
  19. Lifting Credential Key Material Embedded in Client Distributions
- 9 Operating System
20. Buffer Overflow in Local Command-Line Utilities

21. Buffer Overflow via Symbolic Links
22. Buffer Overflow in an API Call
23. Client-side Injection-induced Buffer Overflow
24. Gather Information
25. Audit Log Manipulation
26. Modification of Registry Run Keys
27. Accessing, Modifying or Executing Executable Files
- 10 Software Application
28. Target Programs with Elevated Privileges
29. Gather Information
30. Manipulating Input to File System Calls
31. Leverage Executable Code in Non-Executable Files
32. Browser Fingerprinting
33. Subverting Environmental Values
34. Overflow Variables and Tags
- 11 Persona
35. Social Information Gathering Attacks
36. Harvesting Usernames or UserIDs via Application API Event Monitoring
37. Deceptive Interactions
38. Identity Spoofing
39. Phishing
40. Spear Phishing
41. Mobile Phishing

|    |                             |     |                                                |
|----|-----------------------------|-----|------------------------------------------------|
| 12 | People/Supervisory/Temporal | 42. | Social Information Gathering Attacks           |
|    |                             | 43. | Information Elicitation via Social Engineering |
|    |                             | 44. | Target Influence via Social Engineering        |
|    |                             | 45. | Manipulate System Users                        |
|    |                             | 46. | Deceptive Interactions                         |
|    |                             | 47. | Phishing                                       |
|    |                             | 48. | Spear Phishing                                 |
|    |                             | 49. | Mobile Phishing                                |
|    |                             | 50. | Social Engineering                             |
| 13 | Organization                | 51. | Social Engineering                             |
| 14 | Government                  |     |                                                |

Sumber : Klasifikasi oleh Mitrrre Attack, 2018 (hasil pengolahan data oleh peneliti)

Berdasarkan seluruh kajian kualitatif maupun kuantitatif yang ada, dapat diambil kesimpulan terkait dengan pertanyaan penelitian sebagaimana diperlihatkan pada tabel berikut ini.

Tabel 4. 54 Triangulasi Hasil Penelitian terhadap Pertanyaan Kelima

| No | Jenis Analisa                       | Kesimpulan                                                                                                                                                                                                |
|----|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Kualitatif, <i>Benchmarking</i>     | Hasil studi perbandingan terhadap berbagai negara di dunia memperlihatkan adanya sebelas komponen penting yang harus ada pada ekosistem pertahanan siber negara.                                          |
| 2  | Kualitatif, <i>Group Discussion</i> | Sementara di Indonesia para pakar menyimpulkan pula adanya sejumlah komponen penting yang harus ada dalam ekosistem pertahanan siber nasional – walaupun tidak semua terminologinya sama, namun kesebelas |

aspek dimaksud merupakan komponen inti dari ekosistem terkait.

- |   |                                                |                                                                                                                                                                                                                 |
|---|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | Kualitatif, <i>Expert Justification</i>        | Sejumlah pakar sepakat akan adanya sejumlah komponen yang harus ada pada ekosistem, yang episentrumnya terletak pada keberadaan regulasi dan kebijakan yang efektif.                                            |
| 4 | Kuantitatif, <i>Benchmarking</i>               | Penelitian yang membandingkan komponen-komponen pada ekosistem pertahanan siber berbagai negara memperlihatkan adanya sejumlah aspek yang menjadi kunci sukses ( <i>critical success factors</i> ).             |
| 5 | Kualitatif, <i>Gap Analysis</i>                | Kajian gap antara kondisi ideal dengan yang dimiliki Indonesia memperlihatkan masih belum diperhatikannya sejumlah aspek atau komponen kunci dalam pembentukan ekosistem pertahanan siber yang kuat dan handal. |
| 6 | Kuantitatif, <i>Analytic Hierarchy Process</i> | Analisa AHP menghasilkan sejumlah komponen penting dalam ekosistem pertahanan siber, yaitu: kebijakan, sumber daya manusia, dan peran komunitas.                                                                |

Sumber: Hasil Pengolahan Data Peneliti

#### Strategi Pengembangan Kebijakan Pertahanan Siber Nasional

Pada dasarnya strategi adalah pendekatan mencapai tujuan dengan keterbatasan sumber daya yang dimiliki. Hasil analisis terhadap strategi yang perlu dimiliki Indonesia berdasarkan kajian komparasi dengan negara lain dan kondisi yang dijalankan sekarang melahirkan sejumlah gap atau kesenjangan. Gap ini perlu digambarkan sebagai dasar dalam membuat kebijakan ke depan yang jauh lebih efektif. Berikut adalah sejumlah gap per masing-masing domain yang merupakan hasil analisis lebih mendalam terkait dengan kondisi yang ada.

#### Gap 1: Doktrin Pertahanan dan Kedaulatan Siber Negara

Aspek ini berkaitan dengan keberadaan dan posisi siber dalam ruang lingkup doktrin negara dan keterkaitannya dengan pertahanan serta kedaulatan negara.

Tabel 4. 55 Gap pada Doktrin Pertahanan dan Kedaulatan Siber Negara

| No | Aspek    | Kondisi AS-IS                                                                                                           | Target TO-BE                                                                                                                                                                                                               |
|----|----------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Definisi | Siber tidak didefinisikan secara eksplisit sebagai salah satu ruang kehidupan bernegara yang harus dijaga kedaulatannya | Siber dinyatakan sebagai arena yang sangat berpengaruh terhadap kehidupan berbangsa dan bernegara                                                                                                                          |
| 2  | Konteks  | Ancaman siber merupakan salah satu bagian kecil dari ancaman non militer                                                | Ancaman siber merupakan peristiwa besar dan serius karena sifatnya yang masif serta dampak eksposur yang sangat membahayakan keutuhan bangsa dan negara                                                                    |
| 3  | Posisi   | Ancaman siber menjadi bagian dari doktrin pertahanan negara                                                             | Ancaman siber merupakan bagian dari doktrin bernegara, dimana pertahanan merupakan salah satu aspek penting disamping domain lainnya seperti keamanan nasional, ketangguhan negara, daya saing bangsa, dan lain sebagainya |
| 4  | Spektrum | Pertahanan siber dipandang dari sisi potensi ancaman yang ditimbulkan padanya dan posisinya pada pertahanan negara      | Selain pertahanan siber, kedaulatan siber dianggap sebagai kunci dari pertahanan siber sebuah negara                                                                                                                       |

Sumber : Gap pada Doktrin Pertahanan dan Kedaulatan Siber Negara (hasil pengolahan data oleh peneliti)

### Gap 2: Prinsip, Paradigma, dan Kerangka Kebijakan

Aspek ini berkaitan dengan keberadaan prinsip, paradigma, dan kerangka kebijakan terkait dengan pertahanan dan kedaulatan siber dalam perspektif wilayah Negara Kesatuan Republik Indonesia.

Tabel 4. 56 Gap pada Prinsip, Paradigma, dan Kerangka Kebijakan

| No | Aspek      | Kondisi AS-IS                                                                                                                                                   | Target TO-BE                                                                                                                                                   |
|----|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Prinsip    | Pemahaman akan posisi siber sebagai sebuah arena strategis masih berada di bawah matra darat, laut, dan udara                                                   | Posisi siber dalam konteks pertahanan dan kedaulatan negara relatif sejajar dengan matra darat, laut, dan udara – disamping matra antariksa atau ruang angkasa |
| 2  | Paradigma  | Ancaman siber masih dipandang sebagai bentuk ancaman periferi atau tambahan, yang memicu terjadinya perang asimetri atau perang proksi                          | Siber adalah ruang baru yang dipergunakan sejumlah negara dalam meningkatkan daya saing dan nilai tawar politik kekuatan pertahananannya                       |
| 3  | Kebijakan  | Kebijakan masih bersifat sporadis atau kompartemental, belum dirancang secara utuh ( <i>bottom up approach</i> )                                                | Kebijakan bersifat holistik dan komprehensif, yang dirancang dengan menggunakan pendekatan <i>top down</i>                                                     |
| 4  | Episentrum | Pertahanan siber diposisikan sebagai konsekuensi adanya perang siber atau <i>cyberwar</i> – sehingga menjadi urusan Kementerian Pertahanan dan instansi militer | Pertahanan siber adalah bagian tak terpisahkan dari kedaulatan negara dan keselamatan masyarakatnya – sehingga seluruh pihak bertanggung jawab terhadapnya     |



Sumber : Gap pada Prinsip, Paradigma, dan Kerangka Kebijakan (hasil pengolahan data oleh peneliti)

### Gap 3: Ekosistem Pertahanan Siber Nasional

Aspek ini berkaitan dengan keberadaan ekosistem secara *de jure* dan *de facto* dalam lingkungan Negara Kesatuan Republik Indonesia. Ekosistem dimaksud adalah kerangka keterhubungan antara berbagai sistem, sub-sistem, dan komponen yang terkait dengan terbentuknya pertahanan dan kedaulatan siber yang kuat.

Tabel 4. 57 Gap pada Ekosistem Pertahanan Siber Nasional

| No | Aspek               | Kondisi AS-IS                                                                                                                                                                                 | Target TO-BE                                                                                                                                                                 |
|----|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Postur              | Ekosistem pertahanan siber nasional masih dibatasi pada sektor pertahanan negara, yang berpusat pada Kementerian Pertahanan dan instansi militer                                              | Ekosistem pertahanan siber nasional melibatkan berbagai domain kehidupan bernegara (pentahelix), seperti: pemerintah, industri, masyarakat, media, dan akademisi             |
| 2  | Kerangka            | Sejumlah konsep atau kerangka ekosistem yang dikembangkan masih sporadis, disusun oleh berbagai institusi atau <i>stakeholder</i> terkait                                                     | Adanya kerangka ekosistem pertahanan dan kedaulatan siber nasional yang menjadi acuan bagi seluruh komponen bangsa dan negara                                                |
| 3  | Relasi dan Komponen | Hubungan antara komponen satu dan lainnya masih belum terintegrasi secara terpadu, karena kerangka yang berbasis institusi lebih mengutamakan keterkaitannya dengan tupoksi yang bersangkutan | Relasi antar komponen dalam ekosistem tergambar dengan jelas, sehingga peran masing-masing pihak terkait dengan menjaga pertahanan dan kedaulatan siber menjadi sangat jelas |

Sumber : Gap pada Ekosistem Pertahanan Siber Nasional (hasil pengolahan data oleh peneliti)

#### Gap 4: Jaringan Infrastruktur Telekomunikasi dan Internet

Aspek ini berkaitan dengan ketersediaan, kepemilikan, kapabilitas, dan kinerja jaringan infrastruktur telekomunikasi dan internet yang menghubungkan seluruh entitas dan individu dalam kehidupan berbangsa dan bernegara, terutama dalam hal pertahanan dan keamanan.

Tabel 4. 58 Gap pada Jaringan Infrastruktur Telekomunikasi dan Internet

| No | Aspek                   | Kondisi AS-IS                                                                                                                                                              | Target TO-BE                                                                                                                                                |
|----|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Penyedia                | Sebagian jaringan infrastruktur telekomunikasi dan internet dikendalikan oleh pihak swasta yang dimiliki berbagai perusahaan milik asing yang tunduk pada aturan korporasi | Keseluruhan jaringan infrastruktur telekomunikasi dan internet dikendalikan secara penuh oleh negara walaupun dimiliki berbagai perusahaan asing            |
| 2  | Keamanan                | Tidak semua jaringan infrastruktur dan koneksi terhadap infrastruktur kritis nasional diproteksi dengan sistem keamanan siber yang prima                                   | Seluruh jaringan infrastruktur dan koneksi terutama yang berkaitan dengan infrastruktur kritis nasional dilindungi dengan sistem keamanan siber yang handal |
| 3  | Pengawasan              | Tidak semua jaringan infrastruktur dapat diawasi oleh negara utlisasinya, terutama yang berkaitan dengan infrastruktur kritis nasional                                     | Seluruh jaringan infrastruktur terutama yang berkaitan dengan infrastruktur kritis nasional wajib diawasi negara agar tidak disalahgunakan                  |
| 4  | Topologi dan Arsitektur | Sebagian besar sub-sistem jaringan atau infrastruktur tidak dibuat secara redundan, sehingga berisiko tinggi jika terjadi sesuatu dengannya                                | Seluruh sub-sistem jaringan atau infrastruktur yang penting dibuat secara redundan untuk mencegah terjadinya serangan fisik terhadapnya                     |

Sumber : Gap pada Jaringan Infrastruktur Telekomunikasi dan Internet (hasil pengolahan data oleh peneliti)

#### Gap 5: Suprastruktur Pertahanan Siber

Aspek ini berkaitan dengan aspek suprastruktur yang dimiliki Indonesia dalam mengelola pertahanan siber, terutama berkaitan dengan sumber daya

**Universitas Pertahanan RI**

manusia Indonesia dalam konteks literasi, struktur, dan kultur masyarakat - baik dalam perspektif hubungan sosial maupun bernegara.

Tabel 4. 59 Gap pada Suprastruktur Pertahanan Siber

| No | Aspek    | Kondisi AS-IS                                                                                                                                                                    | Target TO-BE                                                                                                                                                        |
|----|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Literasi | Sebagian besar pimpinan maupun masyarakat Indonesia masih relatif rendah literasi terhadap keamanan data dan informasi                                                           | Seluruh pimpinan dan mayoritas masyarakat harus memiliki literasi yang relatif tinggi terhadap keamanan data dan informasi                                          |
| 2  | Struktur | Pengetahuan dan keterampilan terkait dengan keamanan data dan informasi belum menjadi persyaratan bagi mereka yang bertanggung jawab terhadap pos-pos penting pengelolaan negara | Pengetahuan dan keterampilan terkait keamanan data dan informasi menjadi syarat penting bagi mereka yang diberikan tugas mengelola pos-pos penting institusi negara |
| 3  | Kultur   | Budaya dan semangat berbagai data serta informasi pribadi telah mengakar dalam kehidupan sosial masyarakat                                                                       | Budaya dan semangat tidak berbagi data serta informasi pribadi harus menjadi gaya hidup kehidupan sosial masyarakat                                                 |

Sumber : Gap pada Suprastruktur Pertahanan Siber (hasil pengolahan data oleh peneliti)

#### Gap 6: Sistem Peraturan dan Perundang-Undangan

Aspek ini berkaitan dengan keberadaan dan penerapan berbagai peraturan, kebijakan, dan peraturan perundang-undangan yang secara langsung maupun tidak langsung berkaitan dengan dunia siber dan digital.

Tabel 4. 60 Gap pada Sistem Peraturan dan Perundang-Undangan

| No | Aspek      | Kondisi AS-IS                                       | Target TO-BE                                          |
|----|------------|-----------------------------------------------------|-------------------------------------------------------|
| 1  | Eksistensi | Sangat sedikit peraturan, kebijakan, dan perundang- | <i>Cyberlaw</i> yang terdiri dari sejumlah peraturan, |

|   |                     |                                                                                                                                         |                                                                                                                                                       |
|---|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |                     | undangan yang mengatur masalah yang berhubungan secara langsung maupun tidak langsung dengan isu siber ( <i>cyberlaw</i> )              | kebijakan, dan perundang-undangan secara dinamis disusun dan diberlakukan sesuai dengan kemajuan jaman yang sangat dinamis                            |
| 2 | Integrasi           | Cukup banyak peraturan dan kebijakan saling tumpang tindih sehingga mengurangi efektivitas implementasinya di lapangan                  | Kerangka komprehensif dan holistik dipergunakan sebagai panduan dalam mengembangkan berbagai peraturan dan kebijakan di bidang siber                  |
| 3 | Intensi dan Urgensi | Pengelolaan terhadap berbagai hal yang berkaitan dengan siber dan digital belum dianggap sebagai sebuah fokus yang harus diprioritaskan | Pengelolaan terhadap siber merupakan prioritas utama dalam menghadapi dinamika perubahan jaman yang dipicu oleh Revolusi Industri 4.0 dan Society 5.0 |

Sumber : Gap pada Sistem Peraturan dan Perundang-Undangan (hasil pengolahan data oleh peneliti)

#### Gap 7: Struktur Kelembagaan dan Otoritas Kolektif

Aspek ini berkaitan dengan keberadaan, dukungan, dan efektivitas berbagai institusi di Indonesia yang memiliki tanggung jawab yang berkaitan dengan pertahanan dan keamanan siber.

Tabel 4. 61 Gap pada Struktur Kelembagaan dan otoritas Kolektif

| No | Aspek         | Kondisi AS-IS                                                                       | Target TO-BE                                                                   |
|----|---------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 1  | Akuntabilitas | Pada saat ini akuntabilitas tertinggi berada di tangan Badan Siber dan Sandi Negara | Akuntabilitas tertinggi berada di tangan Kepala Negara dan Kepala Pemerintahan |
| 2  | Wewenang      | BSSN dan lembaga terkait                                                            | <i>Leading sector</i> perlu                                                    |

|   |        |                                                                                                        |                                                                                                                 |
|---|--------|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
|   |        | lainnya memiliki kewenangan kolektif yang tidak lengkap dan utuh                                       | diberikan wewenang mutlak dalam mengelola pertahanan dan keamanan siber nasional                                |
| 3 | Posisi | Posisi BSSN dan sejumlah pemangku kepentingan saling setara sesuai dengan tata kenegaraan yang berlaku | Posisi <i>leading sector</i> dalam hal pengelolaan dan pertahanan siber harus lebih tinggi dari lembaga lainnya |

Sumber : Gap pada Struktur Kelembagaan dan otoritas Kolektif (hasil pengolahan data oleh peneliti)

#### Gap 8: Industri Teknologi dan Informasi Nasional

Aspek ini berkaitan dengan keberadaan dan perkembangan industri nasional terkait dengan teknologi dan informasi.

Tabel 4. 62 Gap pada Industri Teknologi dan Informasi Nasional

| No | Aspek        | Kondisi AS-IS                                                                                                                                                             | Target TO-BE                                                                                                                                                         |
|----|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Produksi     | Mayoritas jika tidak dapat dikatakan seluruh perangkat dan teknologi yang dipergunakan merupakan buatan dari negara luar                                                  | Mayoritas atau seluruh perangkat dan teknologi jaringan yang dipergunakan merupakan buatan dalam negeri dan negara sekutu                                            |
| 2  | Keamanan     | Tidak semua peralatan impor teknologi buatan luar negeri harus diinspeksi keamanannya, terutama yang dipergunakan sebagai komponen jaringan infrastruktur kritis nasional | Semua peralatan import teknologi buatan luar negeri harus diinspeksi keamanannya, terutama yang dipergunakan sebagai komponen jaringan infrastruktur kritis nasional |
| 3  | Keperpihakan | Sangat sedikit produk teknologi buatan anak bangsa yang diakui, dibeli, dan diterapkan dalam berbagai sistem pertahanan                                                   | Adanya keberpihakan terhadap industri dalam negeri melalui pemanfaatan hasil karya dalam negeri di bidang                                                            |

dan keamanan siber di tanah teknologi informasi dan  
air komunikasi

Sumber : Gap pada Industri Teknologi dan Informasi Nasional (hasil pengolahan data oleh peneliti)

#### Gap 9: Kooperasi Nasional dan Internasional

Aspek ini berkaitan dengan kerjasama antar lembaga dan pemangku kepentingan di tanah air maupun antar Indonesia dengan negara lain di dunia.

Tabel 4. 63 Gap pada Kooperasi Nasional dan Internasional

| No | Aspek        | Kondisi AS-IS                                                                                                                             | Target TO-BE                                                                                                                                                                |
|----|--------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Aliansi      | Indonesia aktif menjadi anggota sejumlah asosiasi maupun perhimpunan di dunia, namun antar pihak yang mewakili tidak saling berkoordinasi | Koordinasi nasional harus dilakukan untuk membagi tugas keterwakilan Indonesia dalam berbagai asosiasi dan perhimpunan di dunia                                             |
| 2  | Kepemimpinan | Kebanyakan peran Indonesia masih sebagai anggota dalam berpartisipasi pada asosiasi, fora, maupun perhimpunan internasional               | Indonesia harus berani memimpin dan membentuk beragam komunitas aliansi di bidang pertahanan dan keamanan siber                                                             |
| 3  | Aktivitas    | Aktivitas yang dilakukan cenderung bersifat seremonial, tidak banyak yang secara substantif melakukan kerjasama kolaboratif dan teknis    | Kerjasama yang dijalin tidak saja bersifat strategis, namun juga merambah pada aktivitas teknis dan operasional – yang dilandasi pada <i>trust</i> dan saling menguntungkan |

Sumber : Gap pada Kooperasi Nasional dan Internasional (hasil pengolahan data oleh peneliti)



### Gap 10: Standar Pertahanan dan Keamanan Siber

Aspek ini berkaitan dengan adopsi, pemberlakuan, dan kepatuhan terhadap standar di bidang pertahanan maupun keamanan siber.

Tabel 4. 64 Gap pada Standar Pertahanan dan Keamanan Siber

| No | Aspek         | Kondisi AS-IS                                                                                                                                 | Target TO-BE                                                                                                                                                              |
|----|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Referensi     | Kebanyakan standar yang ada dipergunakan sebatas referensi atau panduan dalam mengembangkan kebijakan maupun peraturan                        | Standar harus dijadikan sebagai acuan yang diadopsi oleh segenap entitas yang ada dalam ekosistem pertahanan siber                                                        |
| 2  | Kepatuhan     | Walaupun diberlakukan, tidak ada <i>law enforcement</i> yang efektif untuk memaksa sejumlah entitas menerapkan standar sebagaimana seharusnya | Kepatuhan kepada standar yang diadopsi adalah suatu kewajiban ( <i>mandatory</i> ) – dimana perlu diterapkan konsep <i>reward and punishment</i> yang efektif terhadapnya |
| 3  | Ruang Lingkup | Standar yang dipergunakan dan diadopsi sangatlah terbatas, dan dipergunakan secara umum ( <i>one size for all</i> )                           | Setiap konteks pertahanan dan keamanan siber memiliki standarnya masing-masing yang harus diadopsi dan dilaksanakan secara konsisten serta berkesinambungan               |

Sumber : Gap pada Standar Pertahanan dan Keamanan Siber (hasil pengolahan data oleh peneliti)

### Gap 11: Sumber Daya Manusia dan Pasukan Siber

Aspek ini berkaitan dengan kebutuhan akan SDM yang secara resmi maupun tak resmi menjalankan tugas untuk menjaga pertahanan kedaulatan siber di tanah air.

Tabel 4. 65 Gap pada Sumber Daya Manusia dan Pasukan Siber

| No | Aspek      | Kondisi AS-IS                                                                                                                       | Target TO-BE                                                                                                                              |
|----|------------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Potensi    | Indonesia memiliki lumayan banyak individu yang ahli di bidang pertahanan dan keamanan siber, namun belum diasah secara profesional | Negara memiliki program khusus untuk menciptakan sebanyak mungkin sumber daya manusia dengan kualitas dan kuantitas yang dibutuhkan       |
| 2  | Kerjasama  | Bentuk kolaborasi antara pihak formal dan komunitas informasi masih berbasis <i>case-by-case</i>                                    | Kolaborasi antar berbagai pihak dalam sebuah negara bersifat terintegrasi dan terpadu                                                     |
| 3  | Formalitas | Secara <i>de jure</i> , Indonesia belum memiliki tentara siber untuk menjaga pertahanan dan kedaulatan negara di ranah maya         | Indonesia perlu memiliki tentara siber secara <i>de facto</i> dan <i>de jure</i> yang bertugas menjaga kedaulatan negara di ranah virtual |

Sumber : Gap pada Sumber Daya Manusia dan Pasukan Siber (hasil pengolahan data oleh peneliti)

Berdasarkan seluruh kajian kualitatif maupun kuantitatif yang ada, dapat diambil kesimpulan terkait dengan pertanyaan penelitian sebagaimana diperlihatkan pada tabel berikut ini.

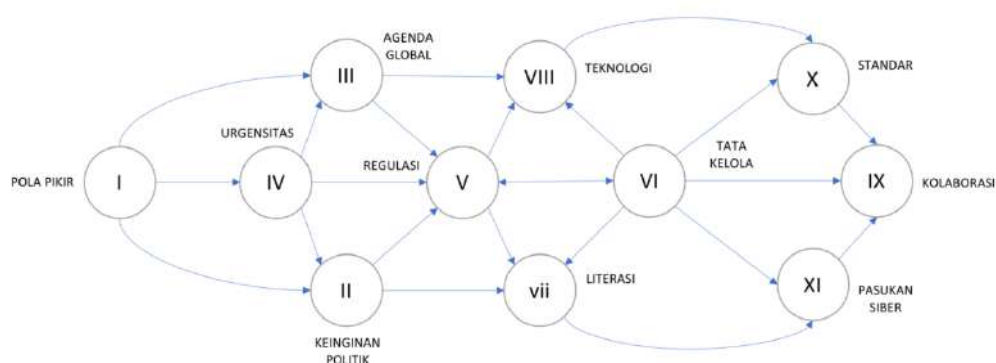
Tabel 4. 66 Triangulasi Hasil Penelitian terhadap Pertanyaan Keenam

| No | Jenis Analisa                                    | Kesimpulan                                                                                                                                                                                       |
|----|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Kualitatif, <i>Policy Benchmarking</i>           | Kebijakan pada sektor pertahanan siber harus mencakup sejumlah hal penting, baik yang bersifat utama ( <i>core</i> ) maupun pendukung ( <i>support</i> ).                                        |
| 2  | Kualitatif, <i>Group Discussion</i>              | Sejumlah diskusi menyarankan agar Indonesia memutakhirkan regulasi dan kebijakan sibernya agar sesuai dengan lingkungan strategis yang menciptakan berbagai ancaman teknologi (siber) yang baru. |
| 3  | Kualitatif, <i>Expert Justification</i>          | Sejumlah pakar sepakat akan perlunya dikembangkan model kebijakan pertahanan siber yang <i>agile</i> , agar dapat selalu beradaptasi dengan kecepatan perkembangan teknologi.                    |
| 4  | Kualitatif, <i>Observation</i>                   | Berbagai institusi pertahanan siber di Indonesia fokus pada pembentukan kapabilitas dalam memproteksi/melindungi, bertahan, dan menyerang – yang didukung oleh sejumlah kebijakan sektoral.      |
| 5  | Kuantitatif, <i>Analytical Hierarchy Process</i> | Analisa AHP memperlihatkan urutan pengembangan kebijakan berdasarkan prioritas, yaitu kemampuan: perlindungan/proteksi, bertahan, menyerang, dan berperang.                                      |

Sumber: Hasil Pengolahan Data Peneliti

### Interpretasi Data

Berbagai data kualitatif hasil wawancara dengan berbagai pihak tersebut memperlihatkan bahwa pada dasarnya terdapat sebelas akar permasalahan yang perlu diperhatikan secara sungguh-sungguh.



Gambar 4. 84 Hubungan Keterkaitan antar Akar Masalah Pertahanan Siber

Sumber : Hubungan Keterkaitan antar Akar Masalah Pertahanan Siber  
(hasil pengolahan data oleh peneliti)

Untuk mempermudah pemahaman secara menyeluruh, kedelapan akar masalah tersebut dapat diringkas menjadi: (i) pola pikir; (ii) keinginan politik; (iii) agenda global; (iv) urgensi; (v) regulasi; (vi) tata kelola; (vii) literasi; (viii) teknologi; (ix) kolaborasi; (x) standar; dan (xi) pasukan siber. Hasil diskusi dengan para pakar maupun nara sumber, serta berdasarkan studi terhadap sejumlah literatur, dapat digambarkan hubungan keterkaitan antar akar permasalahan sebagaimana terlihat pada Gambar. Kesebelas akar permasalahan tersebut memiliki hubungan erat dengan keenam pertanyaan penelitian yang menjadi fokus dalam kajian sebagaimana terlihat berikut ini.

Tabel 4. 67 Pemetaan Akar Permasalahan ke dalam Konteks Pertanyaan Penelitian

| Pertanyaan Penelitian | Pola Pikir | Keinginan Politik | Agenda Global | Urgensi | Regulasi | Tata Kelola |
|-----------------------|------------|-------------------|---------------|---------|----------|-------------|
| 1                     | X          |                   | X             | X       |          |             |
| 2                     | X          |                   |               | X       |          |             |

|   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|
| 3 | X | X |   | X |   | X |
| 4 | X | X |   |   | X | X |
| 5 | X |   | X |   | X | X |
| 6 | X |   | X |   | X | X |

| Pertanyaan Penelitian | Literasi | Teknologi | Kolaborasi | Standar | Pasukan Siber |
|-----------------------|----------|-----------|------------|---------|---------------|
| 1                     | X        | X         |            |         | X             |
| 2                     | X        | X         |            |         |               |
| 3                     | X        |           | X          | X       |               |
| 4                     | X        |           | X          | X       |               |
| 5                     |          | X         | X          | X       | X             |
| 6                     |          | X         | X          | X       | X             |

Sumber: Hasil Pengolahan Penelitian

### Ancaman terhadap Kedaulatan Negara di Era Digital

Hasil pengolahan data memperlihatkan bahwa serangan siber terhadap sektor pertahanan adalah nyata, dan bukan merupakan rekaan yang bersifat hipotetikal. Kumpulan dari data, informasi, dan konten yang dikumpulkan selama penelitian dapat diinterpretasikan sebagai berikut.

Pertama, keseriusan sebuah negara dalam menghadapi dan menanggapi ancaman serangan siber berbeda-beda. Walaupun fenomena ini telah dibahas dan diperdebatkan oleh berbagai negara maju semenjak internet ditemukan, peristiwa serangan ke negara Estonia-lah yang menjadi titik balik bagi berbagai negara untuk memperhatikan hal tersebut secara serius. Sebagai sebuah *wake-up call*, negara-negara yang pertama kali bersikap terhadap

peristiwa yang hampir melumpuhkan negara Estonia ini adalah para anggota NATO, yaitu: *Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom*, dan *United States*. Kesadaran mereka dilandasi pada kenyataan bahwa seluruh negara NATO tersebut telah saling terhubung jejaring pertahanan sibernya, dan Estonia sebagai salah satu anggotanya telah berhasil dilumpuhkan oleh para peretas. Oleh karena itulah maka tingkat kepentingan dan urgensi negara-negara anggota NATO meningkat pesat dalam membangun pertahanan sibernya. Setiap negara berusaha keras mengembangkan strateginya masing-masing, termasuk mereka bersepakat untuk bekerjasama erat melalui inisiatif NATO Cyber Defense. Berbagai usaha dilakukan secara kolektif untuk menghindari berbagai serangan termutakhir, seperti: *cyber espionage, identity theft, malware, ransomware, phishing, distributed-denial-of-services, cryptojacking*, dan lain sebagainya. Indonesia dapat belajar dengan cara membangun pertahanan siber kolektif dengan negara-negara ASEAN atau G-20 misalnya, karena merupakan anggota dari konsorsium negara tersebut.

Kedua, serangan yang terjadi merupakan faktor eksternal yang tidak dapat dikendalikan, dimana keberadaannya semakin meningkat volume maupun frekuensinya dari hari ke hari. Selamanya sebuah negara yang tidak memiliki kemandirian industri digital dan teknologi informasinya akan berada pada posisi lemah, mengingat mayoritas komponen pembentuk ruang siber berasal dari teknologi buatan negara maju. Kenyataan inilah yang mendasari China memutuskan untuk membangun ruang sibernya sendiri, yang “terlepas” dari dominasi asing negara-negara barat. Mereka mengaggap bahwa serangan siber tidak akan pernah bisa dihentikan sejauh ketergantungan terhadap teknologi barat masih tinggi. Kemajuan perusahaan raksasa yang pesat seperti Huawei selain membuat gerah industri IT Amerika Serikat, juga berhasil membuat pendulum kekuatan siber dunia bergeser ke Asia. Indonesia harus berusaha keras membangun industri teknologi informasinya agar dapat memproduksi berbagai teknologi *hardware* maupun *software* untuk kebutuhan dalam negeri. Selain meningkatkan kemandirian dan kedaulatan negara, Indonesia dapat mulai

meningkatkan kinerja pertahanan sibernya secara perlahan namun pasti. Selain kedua komponen penting tersebut, Indonesia perlu pula mengembangkan berbagai aset *tangible* dan *intangible* lainnya seperti algoritma enkripsi/dekripsi, sumber daya manusia siber yang kompeten, standar pertahanan dan keamanan, dan lain sebagainya.

Ketiga, setiap negara memiliki postur ancaman portofolio serangan yang beragam dan berbeda-beda. Ragam serangan ini sangat tergantung pada karakteristik negara beserta lingkungan strategis di sekitarnya. Amerika Serikat yang memiliki banyak musuh akan selalu berhadapai dengan serangan siber dari berbagai negara-negara yang pernah memiliki sejarah suram dengannya. China akan senantiasa berhadapan dengan gempuran negara-negara barat, terutama para peretas dari Amerika Serikat. Sementara negara-negara Timur Tengah kerap saling melakukan penyerangan karena perbedaan posisi mereka dalam konstelasi politik global. Sementara negara berkembang lainnya di wilayah Asia dan Afrika kebanyakan menghadapi banyak serangan dari internal negaranya akibat kondisi politik, ekonomi, dan sosial budaya yang kerap bergejolak. Artinya adalah Indonesia harus memahami benar kondisi internal dan eksternal yang berpengaruh padanya, karena pada dasarnya serangan siber tidak berada di ruang hampa, melainkan sangat tergantung dengan situasi, kondisi, dan konteks multi-dimensi yang ada di sekelilingnya – baik yang bernuansa politik, ekonomi, sosial, budaya, ideologi, dan lain sebagainya.

Pada tataran kebijakan, posisi strategis serangan siber ini harus dibahas secara serius dalam doktrin pertahanan negara yang dianut dan diadopsi. Doktrin pertahanan sebuah negara sangat menentukan langkah-langkah kebijakan strategis dan operasional yang diambil dan diimplementasikan. Pada dasarnya, doktrin ini menjadi pegangan utama dalam menjalankan beragam aksi siber di lapangan. Setiap negara maju di dunia memiliki pandangan sendiri mengenai doktrin siber yang disusun dan diadopsinya. Doktrin pertahanan siber yang kuat terlihat apabila berada pada level negara atau nasional, dan secara eksplisit menyebutkan kata “siber” di dalamnya. Sementara doktrin pertahanan siber yang lemah tidak secara tersurat terlihat dalam doktrin nasional maupun doktrin pertahanan negara terkait, karena

menjadi bagian kecil dari domain tertentu, seperti: ancaman, serangan, fenomena, tren, teknologi, dan lain sebagainya. Di antara dua ekstrim tersebut terlihat beragam variasi posisi doktrin pertahanan dan kedaulatan siber yang dirancang sesuai dengan filosofi negara yang menganutnya. Indonesia sebagai sebuah negara berdaulat perlu memikirkan keberadaan dan posisi doktrin pertahanan serta kedaulatan siber ini dalam pola pikir dan struktur ketatanegaraan yang dimiliki. Dengan berpegang pada efektivitas kebijakan negara yang top down, maka dapat dikatakan bahwa keberadaan doktrin pertahanan dan kedaulatan siber negara bersifat wajib dimiliki. Hanya kesadaran dan kemauan politik yang kuat dapat mengembangkan doktrin yang paling tepat untuk negara maritim seperti Indonesia. Berbasis pada doktrin yang ada, maka ditetapkanlah prinsip-prinsip utama yang harus dipegang teguh dalam kehidupan bernegara dalam kaitannya dengan pertahanan dan kedaulatan siber. Paling tidak ada tiga hal yang harus didefinisikan dan ditetapkan. Pertama adalah prinsip, yang merupakan nilai-nilai yang akan dipegang teguh sebagai panduan dalam berfikir, bersikap, dan berperilaku. Kedua adalah paradigma, yang menggambarkan pola pikir yang sesuai dengan karakteristik dan postur pertahanan siber. Ketiga adalah kerangka kebijakan, menyangkut konseptualisasi terhadap kebijakan yang perlu disusun dan dikembangkan dalam ranah pertahanan dan kedaulatan siber. Keseluruhan aspek ini saling terkait satu dan lainnya yang diturunkan berdasarkan doktrin yang telah ditetapkan.

#### Dampak Serangan Siber terhadap Kedaulatan Negara

Hasil pengolahan data berbasis diagram *cause and effect* memperlihatkan bahwa dampak serangan siber yang berhasil sungguhlah sangat membahayakan kedaulatan dan ketahanan negara. Melalui dampak langsung maupun tidak langsung dari kedelapan serangan siber dengan tren tertinggi di Indonesia dapat diinterpretasikan sebagai berikut.

Pertama, motivasi dan target utama penyerang sektor pertahanan adalah untuk mendapatkan data dan informasi rahasia mengenai negara



tersebut, terutama dalam hal kekuatan dan aktivitas militer yang dilakukannya. Dengan menguasai data dan informasi *confidential* tersebut, maka para peretas dapat melakukan berbagai kegiatan yang diinginkannya, mulai dari menjual belikan informasi tersebut ke pasar gelap, mengirimkan konten rahasia yang berhasil diperoleh ke negara tetangga (yang menganggap Indonesia adalah ancaman serius bagi kedaulatan mereka), mendistribusikannya ke industri pertahanan global, dan lain sebagainya. Apakah motivasi di belakangnya bersifat politis atau ekonomis, kedaulatan negara terancam ketika ada pihak luar yang mendapatkan akses ke informasi rahasia pertahanan dan militer.

Kedua, selain keinginan untuk memperoleh data dan informasi rahasia sebagaimana kerap dibutuhkan oleh intelijen, motivasi lain yang dapat berdampak serius pada pertahanan dan kedaulatan negara adalah keinginan pihak lawan dalam mengendalikan berbagai sistem teknologi pertahanan negara. Alutsista yang berada dalam armada pertahanan Indonesia hampir seluruhnya buatan luar negeri, dari berbagai negara seperti Rusia, Korea, Amerika, Spanyol, Italia, dan lain sebagainya. Khusus bagi perangkat persenjataan moderen, kebanyakan telah dilengkapi dengan instrumen digital yang dapat dihubungkan secara nirkabel. Tentu saja negara pembuat persenjataan dapat dengan mudah mengetahui gerakan berbagai persenjataan tersebut ke manapun yang bersangkutan dimobilisasi. Artinya secara tidak langsung adalah pihak lain mengetahui posisi, kondisi, dan status persenjataan moderen yang dimiliki Tentara Nasional Indonesia – terlepas dari pengakuan mereka sebagai produsen yang mengatakan bahwa tidak ada satu pun pihak yang dapat mengendalikan alutsista moderen yang dibeli. Dampak dari serangan berbasis pengendalian ini sangatlah membahayakan pertahanan negara, karena senjata berat untuk berperang tidak boleh dikontrol oleh pihak lain selain yang memiliki otoritas.

Ketiga, banyaknya serangan yang mengarah pada pelaksanaan perang asimetri dan perang proksi, dimana aset komputasi Indonesia dipergunakan sebagai komponen perang yang tak terdeteksi. Akibatnya adalah jika pihak yang berperang mengetahui skenario ini dapat berakibat pada anggapan mereka bahwa Indonesia terlibat sebagai salah satu pihak yang

melakukan penyerangan. Hubungan diplomasi antara Indonesia selaku negara non-blok dengan negara-negara lain dapat memburuk bahkan memanas.

Indonesia dalam kurun satu windu belakangan ini merasakan benar dampak “kerusakan” yang terjadi akibat fenomena membanjirnya *hoax* yang mampu memporakporandakan sendi-sendi kehidupan masyarakat melalui teknik adu domba. Serangan terhadap *mindset* ini secara skala belum apa-apa jika dibandingkan dengan keberhasilan serangan yang ditujukan pada sektor pertahanan, kedaulatan, dan keamanan negara. Dapat dibayangkan kekacauan yang dapat terjadi apabila infrastruktur vital nasional dilumpuhkan, senjata berat militer diambil alih pihak lawan, radar-radar pesawat tidak berfungsi, atau data detil masyarakat Indonesia bocor ke seluruh dunia akibat beragam serangan siber yang diluncurkan. Lihatlah bagaimana negara semacam Estonia, Georgia, Ukraina, atau bahkan Belgia sempat hampir lumpuh karena dampak yang disebabkan serangan siber.

#### Kerentanan dalam Ruang Siber Nasional

Data yang berhasil dikumpulkan dari berbagai sumber jelas memperlihatkan betapa lemah dan rentannya ruang siber Indonesia dalam berbagai segi. Semakin banyaknya kasus serangan yang berhasil mengeksploitasi kerawanan situs-situs siber di tanah air, rendahnya peringkat kinerja dan pengelolaan siber yang merupakan hasil kajian institusi terkemuka global, dan bocornya berbagai data masyarakat menunjukkan lebahnya sistem siber dimaksud. Sejumlah interpretasi dapat dikembangkan berdasarkan hasil pengolahan data pada penelitian ini.

Pertama, ruang siber tidak dapat dikelola secara sporadis, silo-silo, terkotak-kotak, atau sepotong-sepotong. Pendekatan yang harus diambil dalam membangun pertahanan siber yang kuat adalah holistik dan komprehensif. Memahami ekosistem terbentuknya ruang siber adalah hal mutlak yang harus dilakukan agar dapat melihat isu yang dihadapi secara utuh. Ada adagium berbunyi “kekuatan sebuah rantai tergantung dari mata rantai terlemah” yang sangat cocok dipergunakan dalam memahami isu kerentanan pada ruang siber.

Adagium ini mengandung arti bahwa kekuatan sebuah sistem siber adalah sama dengan kekuatan dari komponen terlemah yang ada di dalamnya. Oleh karena itulah maka pendekatan yang perlu diambil oleh pemerintah Indonesia dalam membangun pertahanan siber yang kuat apabila menggunakan metoda *system dinamic*.

Kedua, kekuatan atau kelemahan sebuah sistem siber bukanlah sekedar merupakan isu teknis, melainkan mengandung permasalahan yang bersifat multi-dimensi. Aspek manusia, manajemen, bisnis, sosial, ideologi, politik, ekonomi, maupun proses hanyalah sejumlah entitas yang berpengaruh terhadapnya. Karakteristiknya yang *borderless* dan virtual menambah kompleksitas penanganan maupun pengelolaannya. Melihat kenyataan ini maka perlu dilakukan asesmen menyeluruh terhadap berbagai komponen yang membentuk ruang siber pertahanan nasional agar terhindar dari adanya lubang-lubang kerawanan yang mudah dieksploitasi pihak lawan. Adapun komponen yang perlu diperkuat dapat dilihat dari hasil asesmen lembaga terkemuka dunia terhadap kualitas dan kinerja infrastruktur maupun suprastruktur internet Indonesia.

Ketiga, proses pengelolaan siber harus terjadi secara *end-to-end* atau menyeluruh. Yang dimaksud *end-to-end* adalah menyangkut serangkain proses berkelanjutan, yaitu: perencanaan, pengorganisasian, perancangan, pembangunan, pengujian, penerapan, pengendalian, penilaian, pengembangan, dan pengawasan. Tidak dilakukannya aktivitas rancang bangun secara baik akan berpotensi menghasilkan sejumlah kerentanan dalam ekosistem yang dibangun. Karena keberadaannya yang menyangkut hajat hidup orang banyak, pemerintah harus benar-benar memiliki kendali terhadap ruang siber yang dipergunakan serta dimanfaatkan masyarakat Indonesia.

Mata dunia mulai terbuka ketika melihat bagaimana ngototnya negara China dalam membuat ekosistem internetnya sendiri secara tertutup (*great wall of China*). Awalan ini pada mulanya ditertawakan oleh banyak pihak karena selain dinilai mustahil, juga dianggap lebih banyak ruginya dibandingkan manfaat. Namun belakangan ini perhatian dunia justru melihat ke China karena keberhasilan mereka melakukan proyek mercu suar tersebut. Semenjak awal

China melihat bahwa dominasi teknologi digital yang menciptakan arena siber sepenuhnya ada di tangan Amerika Serikat dan negara-negara Barat lainnya. Jika hal ini dibiarkan, maka negara-negara adidaya tersebutlah yang akan menguasai dunia.

Paling tidak saat ini terlihat dengan jelas tingginya ketergantungan negara berkembang seperti Indonesia akan internet dan berbagai teknologi informasi maupun digital yang diproduksi oleh negara Barat. Bedanya dengan beragam dominasi teknologi terdahulu, yang menjadi kekhawatiran adalah terjadinya perebutan terhadap sumber daya paling berharga di abad ini yaitu data dan informasi. Menguasai teknologi informasi dan komunikasi pada saat yang sama berarti menguasai data dan informasi yang mengalir di seluruh belahan dunia. Data dan informasi tersebut adalah sumber pengetahuan atau aset tak ternilai harganya yang dapat memberikan keuntungan kompetitif bagi bangsa yang menguasainya. Perang moderen mengambil bentuk virtual dalam bentuk pertempuran berbasis informasi. Lihatlah bagaimana fenomena perang proksi, perang iregular, perang pola pikir, perang hibrid, dan jenis-jenis perang lainnya menjadi bagian tak terpisahkan dari *cyber war* yang sudah, telah, dan akan terus terjadi.

#### Kesiapan Regulasi dalam Konteks Pertahanan Siber

Penyusunan dan pengembangan kebijakan siber di Indonesia termasuk yang paling lambat dibandingkan dengan negara-negara ASEAN lainnya seperti Singapura, Malaysia, dan Thailand. Hingga hari ini baru satu undang-undang yaitu UU ITE yang paling banyak dipergunakan dalam mengelola berbagai aktivitas di dunia siber. Sementara Permenhan mengenai Panduan Pertahanan Siber tahun 2014 adalah satu-satunya acuan dalam sektor pertahanan dalam mengelola ruang sibernya. Memang belakangan ini sudah mulai banyak kementerian maupun lembaga di bawah presiden yang menyusun dan memberlakukan aturan seputar siber, namun sifatnya masih sangat sektoral – sehingga tidak berkontribusi signifikan terhadap kemandirian dan kedaulatan siber nasional. Interpretasi yang dapat disimpulkan dari hasil pengolahan data terkait dengan regulasi yang ada saat ini adalah sebagai berikut.

Pertama, negara dalam hal ini pemerintah dan masyarakatnya baru akan menaruh perhatian terhadap suatu hal apabila dianggap sebagai sesuatu yang penting dan genting (*important and urgent*). Aspek “penting dan genting” ini biasanya baru disematkan pada entitas, kejadian, atau peristiwa yang jarang terjadi, seperti: perang, kerusuhan, pemberontakan, dan lain sebagainya. Bagi negara yang memahami bagaimana strategisnya posisi siber dalam dunia moderen, pimpinannya mengambil sejumlah langkah strategis. Contoh langkah strategis dimaksud misalnya adalah membentuk lembaga otoritas pertahanan dan keamanan siber di bawah kepala negara, menyusun serangkaian regulasi dan konstitusi yang melibatkan siber di dalamnya, memutakhirkan doktrin pertahanan siber negara, membantuk pasukan resmi atau tentara siber, mengalokasikan anggaran yang memadai untuk pengelolaan siber, penerapan standar keamanan informasi pada sektor penting negara, dan lain sebagainya. Semua hal yang terkait dengan siber dianggap sebagai sesuatu yang “penting dan genting” karena setiap hari terjadi perang informasi yang tak terlihat oleh mata manusia. Situasi “kegentingan yang memaksa” ini haruslah menjadi sebuah rutinitas keseharian sehingga perlu dibangun ekosistem pertahanan dan keamanan siber yang kokoh. Tentu saja dalam konteks kenegaraan, pendekatan *top-down* harus dilaksanakan agar efektif. Peran dan kerjasama serta dukungan seluruh lembaga eksekutif, legislatif, dan yudikatif adalah sebuah keniscayaan. Kolaborasi antar lembaga formal, non-formal, dan informal juga harus dibangun mengingat siber adalah dunia tak terbatas oleh ruang dan waktu.

Kedua, ekosistem pertahanan dan kedaulatan siber nasional baru akan berjalan dengan baik apabila dalam konteks ketatanegaraan, penyelenggaraannya diatur melalui sejumlah peraturan, kebijakan, dan perundang-undangan. Berdasarkan Undang-undang Nomor 12 Tahun 2011, definisi Peraturan Perundang-undangan adalah peraturan tertulis yang memuat norma hukum yang mengikat secara umum. Sistem regulasi di Indonesia yang dimaksud adalah sesuai dengan tata urutannya, yaitu: Undang-Undang Dasar Negara Republik Indonesia tahun 1945, Ketetapan Majelis Permusyawaratan Rakyat, Undang-Undang atau Peraturan Pemerintah Pengganti Undang-Undang, Peraturan Pemerintah, Peraturan Presiden, dan Peraturan Daerah. Disamping itu terdapat pula peraturan perundang-undanganyang dimaksud mencakup

peraturan yang ditetapkan oleh: Majelis Permusyawaratan Rakyat, Dewan Perwakilan Rakyat, Dewan Perwakilan Daerah, Mahkamah Agung, Mahkamah Konstitusi, Badan Pemeriksa Keuangan, Komisi Yudisial, Bank Indonesia, Menteri (termasuk badan, lembaga, atau komisi yang setingkat – dibentuk dengan undang-undang atau pemerintah atas perintah undang-undang), Dewan Perwakilan Daerah Provinsi, Gubernur, DPRD Kabupaten atau Kota, Bupati atau Walikota, dan Kepala Desa atau yang setingkat. Sebagai informasi, UU No. 12 tahun 2011 tersebut menggantikan UU No. 10 Tahun 2004. Dalam UU. No. 10 Tahun 2004, tata urutan peraturan perundang-undangan adalah sebagai berikut: (i) UUD 1945; (ii) UU atau Perpu; (iii) Peraturan Pemerintah; (iv) Peraturan Presiden; dan (v) Peraturan Daerah, meliputi: Peraturan Daerah Provinsi, Peraturan Daerah Kabupaten atau Kota, dan Peraturan Desa atau peraturan yang setingkat.

Ketiga, menyusun dan membuat peraturan seputar siber memiliki tantangan tersendiri. Tantangan dari dalam negeri biasanya akan berada pada seputar perimbangan antara kendali negara dengan kebebasan masyarakat. Sementara tantangan dari luar negara berkaitan erat dengan isu seputar perdangan, politik, dan pertahanan. Lamanya UU ITE disusun, dipersiapkan, dirancang, dan diundangkan dapat menjadi pelajaran bagaimana sulitnya membuat regulasi seputar dunia yang tak kasat mata seperti siber atau internet ini. Dibutuhkan koordinasi, kolaborasi, dan rasa saling percaya yang tinggi antara para pemangku kepentingan di Indonesia agar dapat secara bersama-sama mempersiapkan regulasi yang dibutuhkan demi terbangunnya ruang pertahanan siber yang kuat, kokoh, berdaulat, dan mandiri.

Pada intinya, keberadaan regulasi berkaitan sangat erat dengan dinamika politik. Sementara dinamika politik akan sangat dipengaruhi oleh partai yang berkuasa. Oleh karena itulah maka Indonesia perlu memikirkan cara agar isu pertahanan siber ini tidak tergantung dari rezim yang berkuasa karena akan menempatkan negara dalam kondisi yang rentan dan tak menentu.

Ekosistem Ideal Pertahanan Siber Negara

Indonesia perlu belajar banyak dari negara maju lainnya yang telah lebih dahulu berhasil mengembangkan pertahanan sibernya. Sejumlah hasil studi komparasi dan *benchmarking* yang dilakukan selama penelitian memberikan sejumlah gambaran penting yang harus diperhatikan. Berikut adalah interpretasi peneliti terhadap hasil pengolahan data pada tahap sebelumnya.

Pertama, sebagaimana disampaikan sebelumnya, setiap negara memiliki ekosistem pertahanan sibernya masing-masing. Ekosistem ini perlu digambarkan dan ditetapkan agar negara dan masyarakatnya mengetahui secara pasti komponen-komponen apa saja yang ada di dalamnya, dan bagaimana antar satu komponen dengan lainnya saling berelasi dan berinteraksi. Biasanya yang terjadi adalah bahwa komponen-komponen dimaksud pada dasarnya telah dimiliki oleh Indonesia. Hanya saja hubungan dan relasi di antaranya masih bersifat sporadis, dan beberapa cenderung informal. Ekosistem yang utuh, holistik, dan komprehensif harus digambarkan secara skematik dan ditetapkan oleh pemerintah – agar secara kolektif seluruh komponen yang terlibat dapat bahu-membahu dalam mengembangkannya. Disamping itu keberadaan ekosistem dimaksud akan mencegah terjadinya redudansi atau tumpang tindih peran, sekaligus mencegah kosongnya komponen yang belum tersentuh hingga saat ini. Agar ekosistem pertahanan siber nasional ini menjadi “milik bersama”, maka diusulkan agar pengembangannya melibatkan sebanyak mungkin *stakeholders* dalam sebuah *round-table discussion* (masing-masing pihak memiliki posisi dan peran yang setara dalam diskusi penyusunan kerangka ekosistem pertahanan siber nasional).

Kedua, disamping infrastruktur, sub-sistem penting lainnya adalah suprastruktur. Pada sub-sistem ini terdapat berbagai komponen seperti peraturan dan kebijakan, sumber daya manusia, organisasi penyelenggara, komunitas industri, pemerintah, dan lain sebagainya. Aspek suprastruktur ini pada dasarnya merupakan pihak yang akan merencanakan, mengatur, menyelenggarakan, mengawasi, dan mengendalikan dunia siber di Indonesia maupun dunia. Sebagai subset dari suprastruktur dunia, para pemangku kepentingan ini selain harus mematuhi aturan pengelolaan internet global, perlu pula memiliki strategi yang ampuh agar di satu pihak dunia siber memberikan keuntungan maksimum

kepada masyarakat, namun di pihak lain kedaulatan siber nasional tetap terjaga dengan baik.

Ketiga, pengembangan model pertahanan siber yang utuh dan holistik hanya dapat dilakukan apabila dipergunakan pendekatan *top-down* dalam implementasinya. Negara melalui pimpinan, pemerintah, dan instrumennya harus memiliki pandangan yang sama mengenai pentingnya melakukan tata kelola dan manajemen pertahanan siber yang baik. Tanpanya yang akan terjadi tidak lebih dari tambah sulam kebijakan dan usaha pengembangan tanpa arah yang jelas dan nyata.

Membangun ekosistem pertahanan siber tidak semudah membalikkan telapak tangan. Diperlukan proses evolusi yang memakan waktu, tenaga, perhatian, dan biaya yang tidak sedikit. Aktivitas edukasi, sosialisasi, dan *lobbying* perlu dilakukan secara intens dan berkesinambungan. Selain itu dibutuhkan pula keterlibatan sejumlah pakar terbaik bangsa yang memiliki keahlian dalam membangun arsitektur pertahanan siber yang kuat. Pengalaman memperlihatkan bahwa modal yang paling sulit dimiliki adalah keinginan untuk saling bekerjasama, berkoordinasi, dan berkolaborasi demi tujuan yang lebih besar. Berfikir secara komparatemenal atau sektoral merupakan penghalang terbesar bagi negara yang ingin membangun pertahanannya dengan baik.

#### Strategi Pengembangan Kebijakan Pertahanan Siber

Kesebelas gap yang merupakan hasil pengolahan data terkait dengan ekosistem pertahanan siber memperlihatkan begitu banyaknya inisiatif yang harus dijalankan oleh negara. Untuk menjalankannya dibutuhkan sejumlah prasyarat yang harus dimiliki secara kolektif oleh segenap pemangku kepentingan. Interpretasi dari hasil pengolahan data yang disarikan dalam tabel gap analisis adalah sebagai berikut.

Pertama, keinginan dengan kemampuan adalah dua hal berbeda. Jika keinginan dinyatakan dalam *political will*, maka kemampuan berkaitan dengan literasi. Pimpinan dan penyelenggara negara harus memiliki tingkat literasi yang cukup terkait dengan peran, posisi, dan karakteristik siber dalam kehidupan



bernegara. Memahami bahwa siber hanyalah merupakan teknologi atau *tools* pendukung kegiatan manusia tidaklah cukup. Mereka harus tahu persis bagaimana kemajuan teknologi digital dan internet telah membawa perubahan mendasar dalam kehidupan berbangsa dan bernegara. Bahkan dalam konteks kehidupan moderen, keberadaan teknologi telah menjadi faktor penyebab disrupsi dan transformasi. Pemimpin dan penyelenggara negara tidak boleh enggan untuk belajar teknologi siber dari negara lain tidak pada tataran strategis dan kulitnya belaka, namun harus lebih mendalam terkait dengan penerapannya dalam kehidupan umat manusia. Sementara untuk masyarakat Indonesia, perlu dipastikan bahwa kompetensi dan keterampilan minimum di bidang literasi digital telah dikuasai secara masif. Edukasi dan sosialisasi secara menyeluruh perlu dilakukan secara terus menerus dan berkesinambungan – baik yang diprakarsai oleh pemerintah maupun yang didadani industri swasta. Literasi digital yang perlu dimiliki masyarakat Indonesia mencakup delapan aspek *digital quotient*, yaitu: (i) *digital identity*; (ii) *digital use*; (iii) *digital safety*; (iv) *digital security*; (v) *digital emotional intelligence*; (vi) *digital communication*; (vii) *digital literacy*; dan (viii) *digital right*.

Kedua, secara esensial, ekosistem yang dibangun terbagi menjadi dua domain – yang bersifat fisik (*tangible*) dan non-fisik (*intangible*). Sub-sistem fisik didominasi oleh jaringan infrastruktur digital beserta perangkat jaringan dan piranti kerasnya. Infrastruktur ini adalah tulang punggung dari internet karena melalui keberadaannya adalah arena siber terbentuk secara riil maupun konseptual. Isu terkait dengan jaringan infrastruktur telekomunikasi dan internet sangatlah krusial dalam konteks pertahanan dan kedaulatan negara. Telah diketahui bersama bahwa siber dianggap sebagai arena yang borderless karena secara fisik dan logis terbangun dari jejaring raksasa yang menyatukan beragam jaringan negara-negara di dunia. Keberadaannya yang lintas negara dengan topologi dan protokol komunikasi yang sangat kompleks membuatnya sangat sulit kalau tidak bisa dikatakan mustahil untuk memilah-milahnya per region negara. Masalah kedaulatan mengemuka ketika berbagai perangkat maupun standar yang dipergunakan dimonopoli produksinya maupun operasionalnya oleh sejumlah negara besar. Konsep internet governance yang dirancang dan diterapkan

negara-negara besar dunia ini membuat Indonesia harus memutar otak dalam menyusun strategi kedaulatan sibernya.

Ketiga, kedaulatan penuh terhadap pertahanan siber Indonesia akan diperoleh apabila industri teknologi dan informasi nasional berkembang dengan baik. Sebagaimana negara-negara berkembang lainnya, Indonesia perlu sadar dan berusaha untuk turut berpartisipasi dalam penciptaan produk-produk siber yang dapat dipergunakan oleh dunia. Perlu diperhatikan bahwa produk dimaksud tidak semuanya membutuhkan teknologi tinggi, namun banyak yang dapat dikembangkan secara kompetitif oleh berbagai pendatang baru, terutama yang berkaitan dengan software atau aplikasi. Pada saat ini telah terdapat cukup banyak produk-produk piranti keras dan piranti lunak buatan anak bangsa yang terbukti efektif dalam memenuhi kebutuhan pertahanan dan keamanan siber negara. Sudah saatnya negara memperlihatkan keberpihakannya terhadap industri dalam negeri ini sebagai salah satu jalan untuk meningkatkan kualitas pertahanan dan kedaulatan siber nasional.

Keempat, peraturan dan kebijakan yang disusun serta diberlakukan akan menugaskan berbagai lembaga otoritas negara maupun swasta untuk menjalankan perannya masing-masing. Entitas institusi atau organisasi tersebut dibentuk dan ditugaskan sesuai dengan peranannya dalam kerangka ekosistem pertahanan dan kedaulatan siber yang telah ditetapkan oleh negara. Perlu dipahami dan diperhatikan bahwa hal yang paling sulit dalam mengelola siber adalah kerjasama dan koordinasi seluruh lembaga-lembaga yang secara langsung maupun tidak langsung diberikan otoritas sesuai dengan peran, tugas, dan fungsinya. Pengalaman masa lampau di berbagai negara memperlihatkan bahwa terlepas dari adanya struktur kelembangaan dan otoritas kolektif yang bertanggung jawab terhadap pengelolaan siber, kunci suksesnya terletak pada kredibilitas dan trust antar lembaga-lembaga dimaksud. *Trust* atau rasa percaya ini sangatlah dibutuhkan karena cepatnya dinamika dan situasi dalam dunia siber yang selalu jauh lebih cepat perkembangannya dibandingkan dengan peraturan yang dirancang dan berlaku.

Kelima, siber merupakan arena yang tidak mengenal batasan negara atau *borderless*. Namun demikian, siber terbentuk karena kolaborasi antar

negara yang bersepakat untuk mengembangkan protokol komunikasi yang disepekat bersama. Oleh karena itulah maka dalam hal apapun terkait dengan siber, kolaborasi dan kooperasi antar berbagai institusi di dalam maupun antar negara merupakan suatu keniscayaan. Menghadapi kejahatan siber hanya dapat dilakukan apabila berbagai negara dan institusi beragam negara saling menjalin hubungan kerjasama, baik secara formal maupun informal. Indonesia yang merupakan negara non-blok harus memperhatikan hal ini karena kemitraan dengan negara lain berpengaruh secara langsung dalam penciptaan kedaulatan pertahanan siber yang kuat.

Keenam, standar adalah minimum kriteria yang harus dipenuhi oleh sebuah entitas agar memiliki kualitas kinerja yang diinginkan. Dalam konteks pertahanan dan keamanan siber, terdapat sejumlah standar yang telah dikembangkan lama – baik yang bersifat umum maupun spesifik. Sejumlah aspek penting yang berkaitan dengan pertahanan dan keamanan siber dikembangkan kriteria kualitasnya, sebagai patokan dasar dalam mengembangkan berbagai proses dan sistem yang diperlukan. Perlu diketahui bahwa Indonesia telah menetapkan beraneka ragam standar selama ini. Sebagian besar dilakukan melalui adopsi standar internasional yang telah disusun dan dikembangkan berbagai negara. Sementara beberapa standar dibuat secara mandiri dengan tetap berpegang pada sejumlah *good practices* yang dikenal dan diterapkan dalam industri. Standar Nasional Indonesia ini telah menjadi referensi dari berbagai regulasi dan kebijakan yang diberlakukan, walaupun dalam kenyataannya masih sangat kurang terlihat *law enforcement*-nya.

Ketujuh, sejumlah negara maju merasakan perlu untuk memiliki sekumpulan individu khusus yang memiliki kemampuan dan tugas khusus di bidang pertahanan dan keamanan siber. Amerika Serikat sendiri sebagai negara adidaya bahkan membentuk Angkatan Siber sebagai matra kelimanya setelah Angkatan Darat, Angkatan Laut, Angkatan Udara, dan Angkatan Antariksa (Ruang Angkasa). Sementara negara-negara besar lainnya di Eropa Barat tidak mau kalah dengan membentuk pasukan siber khususnya. Indonesia dikenal dengan para “pasukan gerilya siber” yang disegani dunia, dimana para anak-

anak muda berbakat dari berbagai komunitas mengasah dirinya dengan kemampuan kelas dunia di bidang pertahanan dan keamanan siber. Bahkan cukup banyak yang berhasil memiliki sertifikat kompetensi maupun profisiensi terkait dengannya.

Menjembatani berbagai gap tersebut merupakan sebuah perjalanan transformasi yang panjang. Sifatnya yang multi-dimensi dan lintas sektoral membutuhkan kesungguhan negara dalam membangun pertahanan siber secara konsisten dan berkesinambungan. Berbagai regulasi perlu dikembangkan sebagai pijakan hukum bagi mereka yang diberikan tanggung jawab untuk membangun dan mengembangkannya. Dinamika perkembangan teknologi yang sedemikian cepat memberikan tantangan tersendiri bagi pengembangan regulasi dimaksud. Indonesia harus memiliki sistem penyusunan dan pengembangan kebijakan yang *agile*, agar dapat senantiasa beradaptasi dengan perubahan jaman. Tanpanya kumpulan regulasi yang dimiliki tidak akan mampu menjawab kebutuhan pembangunan dan pengembangan sistem pertahanan siber yang kokoh.

## Pembahasan

### Indonesia dalam Pusaran Ancaman Serangan Siber

Semenjak kejadian diretasnya Sistem Pemilihan Umum tahun 2004, era serangan siber di wilayah Indonesia dimulai. Kejadian pada saat itu merupakan *wake up call* bagi pemerintah dan masyarakat terkait dengan bagaimana dampak sebuah serangan digital berpotensi membahayakan negara. Pandangan bahwa serangan siber hanya akan terjadi di ruang maya atau internet terpatahkan ketika dampak yang dirasakan oleh masyarakat terlihat begitu nyata dalam kasus tersebut. Ketegangan antar para politikus mengemuka yang jika tidak dikelola dengan baik berpotensi menimbulkan gesekan horisontal antar berbagai kelompok komunitas dalam masyarakat. Kejadian itu bermuara pada satu diskursus serius di antara penyelenggara negara terkait dengan pertanyaan: “Siapakah yang seyogyanya harus bertanggung jawab

mengantisipasi dan mengelola serangan yang terjadi?”. Berbagai diskusi dilakukan untuk mendapatkan jawaban terhadap pertanyaan ini.

Bambang Permantoro mengatakan bahwa ketika itu terjadi sejumlah pertemuan antar pemangku kepentingan untuk membahas isu penyerangan yang berdampak serius tersebut (komunikasi personal, 14 Juli 2021). Sementara Heru Nugroho beranggapan bahwa perlu dibentuk semacam *task force* atau tim kerja khusus untuk mengatasi berbagai situasi berskala nasional yang disebabkan serangan siber seperti yang terjadi pada sistem pemilu tersebut (komunikasi personal, 11 Juni 2021). Pada akhirnya Kementerian Komunikasi dan Informatika berinisiatif menyelenggarakan *forum group discussion* yang dihadiri oleh sejumlah pemangku kepentingan (Ismail, komunikasi personal, 10 May 2021). Hasil serangkaian diskusi dan pertemuan akhirnya melahirkan sebuah lembaga pengawas internet Indonesia yang diberi nama ID-SIRTII atau Indonesia Security Incident Response Team on Internet Infrastructure (Indrajit & Idsirtii, 2011).

Salah satu tugas pertama ID-SIRTII adalah memantau trafik internet Indonesia. Disinyalir bahwa pada sekitar tahun 2005-2010, terjadi rata-rata serangan sekitar 1,5 juta *event* per harinya (Salahuddien, komunikasi personal, 11 April 2021). Bisyron Wahyudi mengatakan bahwa serangan yang paling banyak terjadi ketika itu adalah *web defacement* dan *phising* (komunikasi personal, 11 April 2021). Setelah kurang lebih sepuluh tahun berjalan, data terakhir dari BSSN memperlihatkan bahwa rata-rata serangan siber yang dideteksi pada tahun 2019 dan 2020 berkisar antara 2,5 hingga 3 juta serangan per harinya (Siburian, komunikasi personal, 1 Juli 2021). Artinya adalah bahwa dari tahun ke tahun terjadi pertumbuhan jumlah serangan per hari yang sangat signifikan. Muhammad Salahuddien secara eksplisit menceritakan sebuah fenomena menarik yang terjadi pada saat beroperasinya ID-SIRTII sepuluh tahun yang lalu sebelum institusi ini melebur ke dalam Badan Siber dan Sandi Negara:

*“Yang menarik untuk dicermati adalah kenyataan bahwa cukup banyak serangan siber yang justru berasal dari dalam negeri, dibandingkan yang berasal dari negara luar. Hal ini perlu dipelajari karena sangat berkaitan dengan menentukan strategi mengantisipasi*

*serangan yang tepat.*” (Salahuddien, komunikasi personal, 2 Agustus 2021)

Pernyataan tersebut hingga saat ini masih relevan kebenarannya karena rekam jejak digital dari hasil pemantauan Satuan Siber TNI memperlihatkan kecenderungan serupa (Yanu, komunikasi personal, 15 Mei 2021). Kenyataan terkait mempertegas pendapat yang mengatakan bahwa ancaman serangan siber dapat berasal dari dalam maupun luar negeri (Indrajit, 2012).

Hal mengkhawatirkan lainnya dapat dilihat dari hasil pemantauan dunia mengenai tingginya frekuensi serangan siber yang menempatkan Indonesia sebagai target. Hasil analisa data peneliti selama setahun terakhir terhadap berbagai lembaga dan institusi terkemuka yang melakukan *live threat monitoring* memperlihatkan bagaimana Indonesia selalu berada dalam sepuluh besar target penyerangan setiap harinya. Sistem *monitoring* berbasis *realtime* dapat dilihat dalam berbagai situs internet, seperti:

1. Arbor Networks DDoS Attack Map yang didedikasikan khusus untuk melacak serangan berbasis *Distributed Denial of Services* dimana rekam jejak penyerangan tersebut beserta jenis dan modusnya terekam per detikanya secara detil ([www.digitalattackmap.com](http://www.digitalattackmap.com), 2021);
2. Kaspersky Cyber Malware and DDoS Real-Time Map yang khusus fokus pada deteksi virus maupun *malware* dengan laporan statistik yang sangat detil per masing-masing negara ([www.cybermap.kaspersky.com](http://www.cybermap.kaspersky.com), 2021);
3. ThreatCoud Live Cyber Attack Threat Map yang fokus melihat serangan berbasis *malware*, *phising*, *worm*, dan *exploit* dari satu negara ke negara lain dan melakukan analisis target serangan terbanyak berdasarkan negara dan industri ([www.threatmap.checkpoint.com](http://www.threatmap.checkpoint.com), 2021);
4. Fortinet Threat Map yang secara khusus melakukan analisis terhadap adanya anomali pada trafik antar negara serta

melaporkan jenis kerentanan *software* yang menjadi titik eksploitasi ([www.fortiguard.com](http://www.fortiguard.com), 2021);

5. LookingGlass Phishing/Malicious URL Map yang memberikan hasil kajian berdasarkan konsep *threat intelligence* yang dipetakan terhadap sejumlah negara target serangan *botnet* ([www.lookingglasscyber.com](http://www.lookingglasscyber.com), 2021);
6. Threat Butt Hacking Attack Map yang memperlihatkan *attribution map* berupa tampilan menarik untuk memperlihatkan terjadinya *tribution map* berupa tampilan menarik untuk memperlihatkan terjadinya peristiwa *cyber crime* antar negara ([www.ghreatbutt.com](http://www.ghreatbutt.com), 2021);
7. Talos Spam and Malware Map yang secara jelas memperlihatkan informasi negara produsen *spam* dan *malware* terbesar setiap harinya beserta asal *internet service providers* yang dipergunakan ([www.talosintelligence.com](http://www.talosintelligence.com), 2021);
8. Sophos Threat Tracking Map yang memilih fokus pada ancaman terhadap *web attacks* dan *email phishing* untuk membantu negara mengantisipasi kemungkinan buruk yang berpotensi merusak sumber daya digital yang dimiliki ([www.sophos.com](http://www.sophos.com), 2021);
9. FireEye Cyber Threat Map yang memperlihatkan fenomena serangan selama tiga puluh hari terakhir dengan tampilan grafik menarik dan menampilkan lima besar industri yang menjadi sasaran serangan siber ([www.fireeye.com](http://www.fireeye.com), 2021);
10. Deteque Botnet Threat Map yang menggambarkan secara grafis 10 serangan terburuk berbasis botnet per negara dan per *internet service providers* yang memberikan jasanya dari berbagai belahan dunia ([www.spamhaustech.com](http://www.spamhaustech.com), 2021);
11. Bitdefender Live Cyber Threat Map yang memberikan informasi mengenai jenis serangan yang terjadi dan tingkat bahayanya bagi

negara target dengan tampilan grafis yang menarik ([www.threatmap.bitdefender.com](http://www.threatmap.bitdefender.com), 2021);

12. SonicWall Live Cyber Attacks Map yang fokus melakukan pemantauan terhadap kejadian pada ruang siber dalam 24 jam terakhir yang dilengkapi dengan analisis statistics dan berita kerentanan yang relatif lengkap ([www.securitycenter.sonicwall.com](http://www.securitycenter.sonicwall.com), 2021); dan
13. NETSCOUT Cyber Threat Horizon yang merupakan situs khusus untuk melakukan analisis berbasis *threat intelligence* guna membantu negara dalam memenangkan peperangan siber ([www.netscout.com](http://www.netscout.com), 2021).

Situs *underground* Zone-H memperlihatkan betapa rentannya *website* kalangan militer yang ada di Indonesia, dimana sewaktu-waktu peretas dan pihak lawan dapat melakukan serangan serta perusahkan terhadapnya (Atmodjo, komunikasi personal, 20 Juli 2021).



www.zone-h.org/archive

90%

zone-h  
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login

search...

NOTIFIER: DOMAIN mil.id

Special defacements only ☐ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☐

Date: ALL Apply filter

Total notifications: 545 of which 208 single ip and 337 mass defacements

Legend:  
 H - Homepage defacement  
 M - Mass defacement (click to view all defacements of this IP)  
 R - Redefacement (click to view all defacements of this site)  
 L - IP address location  
 ★ - Special defacement (special defacements are important websites)

| Date       | Notifier                    | H | M | R | L | Domain                            | OS       | View   |
|------------|-----------------------------|---|---|---|---|-----------------------------------|----------|--------|
| 2021/07/15 | Moroccan Revolution         | H | R |   |   | lantamal11-koarmada3.trial.mil... | Win 2016 | mirror |
| 2021/07/15 | Moroccan Revolution         | H | R |   |   | lantamal10-koarmada3.trial.mil... | Win 2016 | mirror |
| 2021/07/06 | Moroccan Revolution         |   | R |   |   | lantamal9-koarmada3.trial.mil...  | Linux    | mirror |
| 2021/06/28 | Moroccan Revolution         |   | R |   |   | pusjanmar-seskoal.trial.mil.i...  | Unknown  | mirror |
| 2021/06/28 | Moroccan Revolution         | H | R |   |   | jurnalmaritim.trial.mil.id/pub... | Unknown  | mirror |
| 2021/06/05 | SABUNNANDI CYBER TEAM       | H | R |   |   | www.pussenkav.mil.id/sabun.html   | Unknown  | mirror |
| 2021/03/26 | /Rayzky...                  |   | R |   |   | dithub-triad.mil.id/pentest.html  | Linux    | mirror |
| 2021/02/25 | Electronic Team Thunderbolt |   | R |   |   | koinleml.trial.mil.id/inject...   | Linux    | mirror |
| 2021/02/25 | Electronic Team Thunderbolt | H | R |   |   | lantamal12-koarmada1.trial.mil... | Linux    | mirror |
| 2021/02/25 | Electronic Team Thunderbolt | H | R |   |   | jalsenastr.trial.mil.id/inje...   | Linux    | mirror |
| 2021/02/25 | Electronic Team Thunderbolt | H | R |   |   | lantamal13-koarmada1.trial.mil... | Linux    | mirror |
| 2021/02/24 | Moroccan Revolution         |   | R |   |   | lantamal1-koarmada1.trial.mil...  | Linux    | mirror |
| 2021/01/31 | /Tikus_Hakor                | H |   |   |   | dittop-triad.mil.id               | Linux    | mirror |
| 2021/01/19 | Moroccan Revolution         |   | R |   |   | perpustakaan-seskoal.trial.mil... | Win 2016 | mirror |
| 2021/01/12 | U - Serpi                   | H |   |   |   | akadem-trial.mil.id               | Linux    | mirror |
| 2021/01/03 | aDriv4                      |   | R |   |   | kodam17enderawasih-triad.mil...   | Linux    | mirror |
| 2020/12/16 | ADIT HACKER CILACAP         | H | H | R |   | www.kodam0399elok.mil.id          | Linux    | mirror |
| 2020/10/31 | Moroccan Revolution         |   | R |   |   | kodikat-triad.mil.id/vz.txt       | Linux    | mirror |
| 2020/09/02 | aDriv4                      |   | R |   |   | kasuar18-triad.mil.id/vz.txt      | Linux    | mirror |
| 2020/08/19 | Moroccan Revolution         |   | R |   |   | ditbekangad.mil.id/asset/maga...  | Linux    | mirror |
| 2020/08/06 | /Sn00py                     | H | R |   |   | amanudsa16.kodam-wirabuana.mil... | Linux    | mirror |
| 2020/08/06 | /Sn00py                     | H |   |   |   | babinmivteccaddam.kodam-wirabu... | Linux    | mirror |
| 2020/08/06 | /Sn00py                     | H |   |   |   | bekangdam.kodam-wirabuana.mil...  | Linux    | mirror |
| 2020/08/06 | /Sn00py                     | H |   |   |   | bekang.kodam-wirabuana.mil.id/... | Linux    | mirror |
| 2020/08/06 | /Sn00py                     | H |   |   |   | brigi22.kodam-wirabuana.mil.i...  | Linux    | mirror |

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

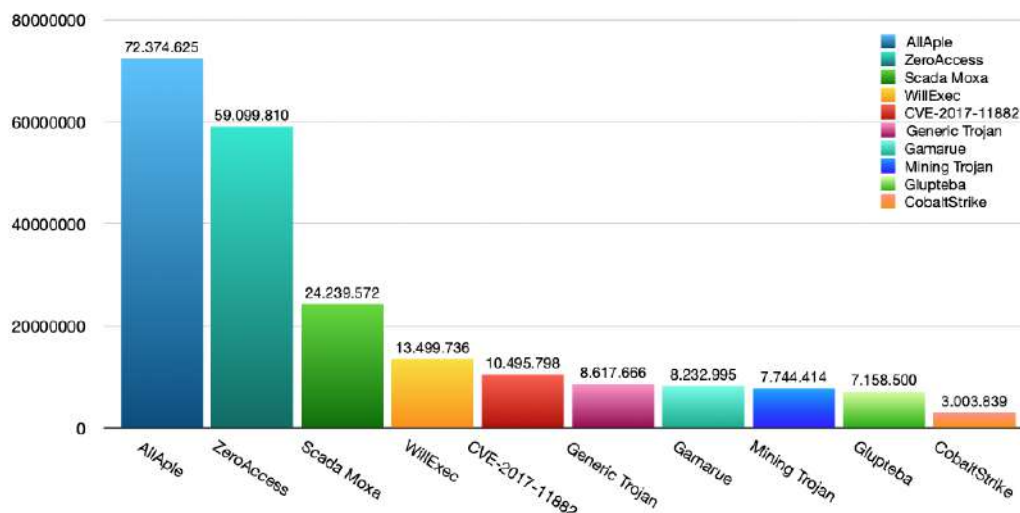
Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

Gambar 4. 85 Profil Serangan terhadap Situs Militer Indonesia

Sumber : <http://zone-h.org>, 2021

Pantauan terhadap situs ini memperlihatkan bagaimana berbagai peretas dari dalam maupun luar negeri mencoba merusak situs institusi militer di Indonesia melalui serangan berbasis *homepage defacement*, *mass defacement*, dan *redefacement*. Fenomena ini selaras dengan pantauan Pusat Pertahanan Siber Kementerian Pertahanan yang memantau begitu banyaknya percobaan serangan ke pusat-pusat komputasi Kementerian Pertahanan maupun lembaga institusi militer di tanah air (Sarwono, komunikasi personal, 15 Juni 2021).



Gambar 4. 86 Grafik 10 Anomali Trafik Selama Tahun 2020

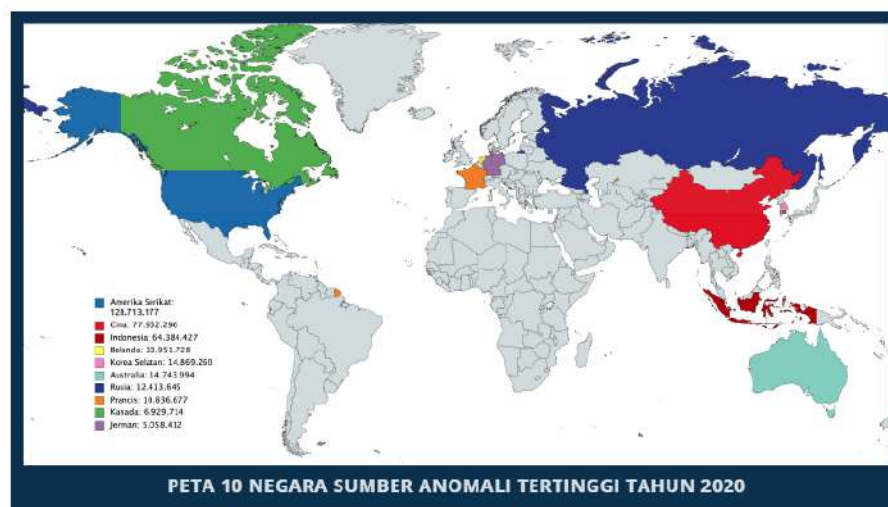
Sumber : Badan Siber dan Sandi Negara (Pusopskamsinas, 2021)

Studi ENISA yang memperlihatkan adanya 15 (limabelas) tren modus serangan untuk 5-10 tahun ke depan menegaskan bahwa tidak ada negara yang terbebas dari serangan siber. Hasil penelitian memperlihatkan bahwa berdasarkan asesmen risiko yang dilakukan oleh lima pakar pertahanan siber di Indonesia, 8 (delapan) modus besar nampak selaras dengan hasil kajian ENISA. Data lebih detail diperlihatkan oleh Badan Siber dan Sandi Negara melalui laporan tahunannya. Hasil *monitoring* pada tahun 2020 memperlihatkan informasi sebagai berikut (BSSN, 2021):

1. Pusopskamsinas BSSN melihat adanya anomali trafik terhadap ruang siber Indonesia, dengan jumlah yang cukup fantastis yaitu 495,337,292 event;
2. Sumber anomali trafik terbesar yang menyerang Indonesia adalah negara Amerika Serikat dan China – dan yang menarik adalah bahwa serangan ketiga terbesar berasal dari negara Indonesia sendiri; dan

3. Hal menarik lainnya untuk diperhatikan adalah kenyataan yang memperlihatkan bahwa tujuan serangan dari pihak Indonesia justru ke situs-situs dalam negeri, atau dengan kata lain terjadi banyak sekali serangan yang berasal dari peretas Indonesia itu sendiri.

Pada dasarnya serangan-serangan di lingkungan siber tidak berada dalam ruang hampa. Setiap serangan pada dasarnya dilatarbelakangi motivasi tertentu. Rudi Luhmanto mengatakan bahwa kebanyakan serangan dilatarbelakangi oleh tujuan ekonomis atau politis (komunikasi personal, 1 Juli 2021), sementara Bisyrn Wahyudi mensinyalir bahwa setiap serangan pasti dipicu sebuah kejadian dalam dunia nyata (komunikasi personal, 6 Juli 2021). Kedua pernyataan ini diperkuat dengan fenomena yang memperlihatkan bahwa setiap kali ada kejadian perseteruan fisik antar dua atau lebih pihak (terutama negara), selalu diikuti dengan serang menyerang dalam ruang siber (Edwards et al., 2017). Atau justru kebalikannya, dimana cara mempengaruhi apa yang terjadi dalam dunia nyata dimulai dengan aksi dalam dunia maya (Nastiti et al., 2018) – mengingat keduanya memiliki hubungan keterkaitan yang sangat tinggi.



| TOP 10 SOURCE COUNTRY                                                               |                                   | TOP 10 DESTINATION COUNTRY                                                          |                            |
|-------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------|----------------------------|
|   | 1. Amerika Serikat<br>128.713.177 |   | 8. Australia<br>14.743.994 |
|  | 2. Cina<br>77.932.296             |  | 7. Rusia<br>12.413.645     |
|  | 3. Indonesia<br>64.383.427        |  | 8. Prancis<br>10.836.667   |
|  | 4. Belanda<br>33.951.728          |  | 9. Kanada<br>6.929.714     |
|  | 5. Korea Selatan<br>14.869.260    |  | 10. Jerman<br>5.058.412    |

Selain itu, hasil monitoring Pusopskamsinas BSSN juga mampu memetakan negara mana saja yang menjadi tujuan dari anomali yang berasal dari Indonesia (dengan alamat IP Indonesia). Berikut merupakan urutan daftar 10 negara dengan jumlah serangan tertinggi dari Indonesia selama tahun 2020:

|                    |                  |
|--------------------|------------------|
| 1. Indonesia       | 6. Belanda       |
| 2. Amerika Serikat | 7. Korea Selatan |
| 3. Cina            | 8. Hong Kong     |
| 4. Jerman          | 9. Prancis       |
| 5. Argentina       | 10. Rusia        |

Gambar 4. 87 Negara-Negara Sumber dan Destinasi Anomali Trafik Siber

Sumber : Badan Siber dan Sandi Negara (Pusopskamsinas, 2021)

Gildas Deograt dalam beberapa kesempatan mengatakan bagaimana terbuka dan “telanjang”-nya lalu lintas komunikasi dan interaksi digital di Indonesia karena kurang perdulinya banyak pihak terhadap keamanan informasi (komunikasi personal, 11 Januari 2021). Charles Liem melihat masih rendahnya literasi masyarakat Indonesia sebagai penyebab belum mampunya mereka

memahami dan mengamankan komunikasi digitalnya (komunikasi personal, 15 Februari 2021). Memang kenyataan memperlihatkan bahwa literasi keamanan informasi masih belum dianggap penting oleh sebagian besar masyarakat di tanah air dan dunia (Literacy & Literacy, n.d.). Kerentanan ini sangat dipahami oleh berbagai pihak sehingga menyebabkan semakin tingginya frekuensi dan volume serangan di dunia siber Indonesia dari masa ke masa (BSSN, 2020).

Sebagaimana di negara-negara maju dan berkembang lainnya, selain lembaga atau industri keuangan, sektor pertahanan dan menjadi sasaran utama dari para peretas lintas negara (Gawthorpe, 2016). BSSN dalam laporannya memperlihatkan bagaimana terjadi sejumlah serangan di berbagai sektor termasuk pertahanan dan militer, seperti: *ransomware*, *border gateway protocol*, *remote code execution*, *arbitrary code execution*, dan lain sebagainya. Bahkan mereka yang sehari-harinya banyak menggunakan sistem operasi Windows dari Microsoft kerap kali mendapatkan serangan dari para peretas. Sejumlah sumber yang tidak mau disebutkan namanya menyebutkan betapa seringnya yang bersangkutan dipanggil oleh sektor pertahanan, militer, dan kepolisian untuk menginvestigasi serangan siber yang terjadi serta menimpa sejumlah infrastruktur vital (*anonymous*, komunikasi personal, 24 Januari 2021). Bahkan dalam beberapa kasus telah terbukti berhasil dikendalikannya sumber daya militer dari jarak jauh yang berakibat bocornya berbagai data penting dan rahasia yang dimiliki negara. Fenomena ini terjadi hampir di seluruh sektor pertahanan dan militer di dunia karena dianggap sebagai salah satu titik lemah negara yang dapat dimanfaatkan oleh pihak lawan dalam peperangan siber (Rid, 2013; "The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case," 2013).

Konteks pertahanan siber kerap dibahas ketika membicarakan konsep perang siber atau *cyber warfare*. Definisi mengenai istilah *cyber warfare* pun masih sangat beragam karena berbedanya perspektif dan pola pandang masing-masing manusia. RAND Cooperation mengatakan bahwa:

*"Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."* (www.rand.org, 4 Agustus 2021)

Definisi ini diperkuat dengan Fortinet yang melihat perang siber sebagai berikut:

*“Cyber warfare consists of attacks on computer systems of countries or institutions with the intention of disrupting, damaging, or destroying infrastructure.”* (www.fortinet.com, 11 Agustus 2021)

Kedua definisi di atas mirip dengan yang diajukan oleh Tampubolon (2019) sebagai berikut:

*“Cyber warfare dapat diartikan sebagai perang di dalam cyberspace, namun di dalam cyber warfare terdapat penyerangan yang berbeda dengan penyerangan dalam perang konvensional atau perang fisik lainnya. Media utama yang digunakan di dalam cyber warfare adalah komputer dan internet. Objek yang diserang dalam cyber warfare bukan merupakan wilayah fisik, wilayah teritorial ataupun wilayah geografis, namun objek dalam cyberspace yang dikuasai oleh suatu negara.”* (Tampubolon, 2019)

Definisi yang cukup banyak diadopsi oleh berbagai kalangan adalah yang dibuat oleh UNTERM (organisasi organ dari Persekutuan Bangsa-Bangsa), yaitu:

*“The offensive and defensive use of information and informations system to deny, exploit, corrupt or destroy an adversary’s computer based network while protecting one’s own. Such actions are designed to achieve advantages over military or business adversaries.”* (UNTERM, 2018)

Sementara UNICJRI yang juga merupakan organ dari Persekutuan Bangsa-Bangsa secara ringkas mengatakan bahwa *cyber warfare* pada dasarnya merupakan:

*“Any action by a nation-state to penetrate another nation’s computer networks for the purpose of causing some sort of damage.”* (UICJRI, 2015)

Berbagai definisi yang dipergunakan untuk menggambarkan *cyber warfare* bermuara pada satu pemahaman yang mengatakan bahwa pada dasarnya perang siber adalah “perang yang dilakukan di ruang siber dengan berbekal senjata siber dan memiliki karakteristik perebutan atau penguasaan wilayah maya yang berkesesuaian dengan sistem siber” sebagaimana termaktub dalam *Tallin*

*Manual Rule No.41* (Andress & Winterfield, 2014). Pemahaman dan studi mendalam mengenai perang siber mulai dilakukan semenjak serangan terhadap Estonia di tahun 2007.

Studi dan penelitian ini berhasil menemukan sembilan jenis serangan siber yang khusus terjadi dalam perimeter sektor pertahanan dan militer. Taksonomi serangan ini diperoleh dan dibangun berdasarkan tujuan, obyektif, atau motivasi sang penyerang atau pihak yang melakukan aneksasi maupun penetrasi ofensif. Kesembilan klasifikasi serangan terhadap sektor pertahanan dan militer dimaksud dipaparkan sebagai berikut.

Pertama adalah serangan terhadap infrastruktur kritis nasional atau yang dikenal sebagai *national critical infrastrcuture*. Tujuannya jelas yaitu untuk menyebabkan terjadinya kekacauan nasional, mengingat infrastruktur vital ini menguasai hajat hidup orang banyak (Gawthorpe, 2016; The National Institute of Standards and Technology, 2013). Kejadiannya matinya listrik atau yang dikenal sebagai *blackout* karena pasokannya terganggu akibat serangan siber adalah salah satu modus yang paling disukai peretas (Geers, 2010). Terganggunya pasokan listrik PLN pada bulan Agustus 2019 menyisakan tanda tanya besar dan mengundang perhatian cukup banyak pemangku kepentingan (“Hacker Ancaman Nyata Pembangkit Listrik, Siapkah PLN?”, [www.cyberthreat.id](http://www.cyberthreat.id), 5 Agustus 2019). Bahkan lembaga intelijen dan pakar praktisi keamanan siber pun turut serta mengkaji serta menganalisis kejadian dimaksud untuk memastikan ada tidaknya sistem distribusi listrik yang berhasil dikuasai *hacker* atau peretas (“Peneliti Intelijen: Listrik Padam, PLN Harus Waspada Siber Terorisme”, [www.tribunnews.com](http://www.tribunnews.com), 5 Agustus 2019). Sektor industri *utility* yang paling banyak dikuasai oleh Badan Usaha Milik Negara (BUMN) harus berhati-hati terhadap kemungkinan serangan ini. Karena serangan masif terhadap mereka akan berpengaruh terhadap keselamatan masyarakat dan keamanan nasional – karena potensi dampaknya yang dapat menyebabkan suasana *chaos*. Sistem yang paling banyak dipergunakan oleh perusahaan dalam sektor industri vital adalah SCADA (Supervisory Control And Data Acquisition), yang dalam era moderen ini diperlengkapi atau dimutakhirkan dengan sistem berbasis IOT (*Internet-Of-Things*) dengan beragam variasinya (Weed, 2017).

Kedua adalah serangan dengan cara menyadap sistem komunikasi para pemangku kepentingan atau *stakeholders* di lingkungan pertahanan negara. Mereka yang dimaksud adalah para pimpinan dan karyawan dalam perimeter Kementerian Pertahanan, dan para petinggi maupun pasukan militer (tentara) dalam ekosistem Angkatan Darat, Angkatan Laut, dan Angkatan Udara (Dwicahyo, 2019; Hemanidhi & Chimmanee, 2017). Fenomena penyadapan semakin marak sejalan dengan diperjualbelikannya alat-alat sadap dengan beragam teknologi secara bebas kepada masyarakat (“Penyadap Canggih Sekelas NSA Kini Dijual Bebas”, [www.tempo.co](http://www.tempo.co), 20 November 2013). Tentu saja hal ini sangat membahayakan. Dapat dibayangkan apa yang akan terjadi apabila alat komunikasi militer yang dipegang para perwira tinggi dapat diintersepsi oleh pihak lawan atau kriminal. Selain situasi tersebut membahayakan pertahanan negara, hal tersebut dapat menyebabkan terjadinya insiden lain yang dapat menimbulkan efek domino yang lebih dahsyat (Prakasa & Noviandi Nur, 2019). Lihatlah akibat yang terjadi ketika terjadi penyadapan dalam kasus yang menimpa Timor Timur di tahun 1999 (“Australia Sadap Operasi Militer Indonesia di Timor Timur”, [www.merdeka.com](http://www.merdeka.com), 27 November 2013) atau yang menyebabkan presiden Indonesia Susilo Bambang Yudhoyono memberhentikan kerjasama militer dengan Australia (“Australia Menyadap, SBY: Kerjasama Militer Dihentikan Dulu, 20 November 2013). Muhammad Salahuddien mengingatkan bahwa modus penyadapan ada beraneka ragam, mulai dari yang bersifat pasif hingga aktif (komunikasi personal, 24 Februari 2021). Pada penyadapan pasif, tertanam *software* jahat atau *malware* dalam alat komunikasi seperti *handphone* atau telepon genggam. Sementara pada penyadapan aktif, terjadi aktivitas intersepsi sinyal digital selama proses komunikasi dilakukan.

Ketiga adalah serangan berupa usaha untuk mengambil alih alutsista yang merupakan peralatan persenjataan utama yang dimiliki militer sebagai alat untuk meningkatkan kemampuan tentara dalam melaksanakan tugas pokok TNI. Peralatan dan senjata perang moderen kebanyakan telah dilengkapi dengan teknologi komputer maupun digital (“Panglima TNI menargetkan Alutsista Berbasis Digital”, [www.antaraneews.com](http://www.antaraneews.com), 17 Agustus 2018). Kelebihannya terletak pada semakin handal dan akuratnya sistem persenjataan tersebut ketika dipergunakan dalam berperang atau dipakai guna melumpuhkan lawan (Siroli,



2018). Namun pada saat yang sama keberadaannya mendatangkan risiko tersendiri berupa serangan siber atau aktivitas eksploitasi kerawanan digital yang ada di dalamnya (Turunen & Kari, 2020). Pengambilalihan kontrol alutsista secara jarak jauh melalui peretasan digital (*remote hacking*) menyebabkan sang empunya tidak dapat mengendalikan senjata yang dimilikinya. Peretas atau pihak lawan dapat dengan mudah melakukan apa saja yang diinginkan, termasuk mengarahkan dan menembakkan peluru ke pemilik alutsista dimaksud. Kenyataan tersebut tentu saja sangat membahayakan dalam konteks peperangan. Bahkan dalam konteks perang assimetri, mereka yang hanya memiliki kemampuan dalam meretas sistem dapat menghancurkan bala tentara dengan kekuatan persenjataan moderen berbasis digital dan komputer (Kenway, 2019). Rudi Luhmanto mengatakan bahwa dalam peperangan moderen, kerap dikirim mata-mata yang ditugaskan untuk menanamkan *malware* ke dalam sistem persenjataan moderen berbasis digital tersebut, agar dapat dikendalikan oleh pihak lawan dari jarak jauh (komunikasi personal, 11 Maret 2021). Karena sifatnya yang *eksklusif*, tidak banyak aplikasi atau pihak yang memiliki kesempatan untuk membantu pihak militer untuk mendeteksi atau mengidentifikasi ada tidaknya aplikasi jahat yang tertanam di dalam sistem persenjataan TNI.

Keempat adalah serangan yang diarahkan pada titik pusat pertahanan dan militer, yaitu pusat komando atau *command center*. Puskodal moderen dibangun dengan memanfaatkan berbagai teknologi digital secara terintegrasi dan terpadu. Sebagaimana namanya, sebuah pusat komando biasanya terhubung dengan seluruh titik-titik unit koordinasi yang perlu dikendalikan, sehingga serangan terhadap puskodal berarti memberikan kesempatan kepada peretas untuk dapat melakukan penetrasi akses ke mana saja (Krueger & Banderet, 2007). Dalam kesempatan wawancara, Muhammad Salahuddien menyatakan:

*“Hampir semua perencanaan dan pengembangan command center di sektor pertahanan dan militer menggunakan pihak luar, yaitu vendor system integration. Dan sudah merupakan rahasia umum bahwa cukup banyak puskodal berbasis teknologi informasi yang melibatkan pihak eksternal untuk mengendalikan sekaligus mengoperasikannya.*

*Hal ini selain membuat adanya ketergantungan tinggi kepada pihak ketiga, keberadaan mereka dalam perimeter aset strategis pertahanan dan militer dapat berpotensi menjadi ancaman tersendiri yang disebut sebagai insider threat.” (Salahuddien, komunikasi personal, 23 Januari 2020)*

Serangan terhadap puskodal pada dasarnya telah menjadi pertimbangan serius kalangan militer di Indonesia. Sejumlah seminar dan diskursus telah mengemuka dengan cara paling efektif dalam mengatasi isu kerentanan yang ditemukan tersebut (“Asops Panglima TNI: Fenomena Global dan Ancaman Kontemporer Sulit Diantisipasi”, [www.ppido.tni.mil.id](http://www.ppido.tni.mil.id), 5 Maret 2020). Salah satu cara yang dapat mulai dirintis adalah dengan meningkatkan kualitas dan kompetensi SDM pertahanan maupun militer yang mengoperasikan puskodal (Hausken, 2020). Serangan siber yang pernah terjadi di masa lalu di berbagai negara terhadap puskodal dilakukan melalui teknik berbasis *insider threat*, yaitu dengan menyelundupkan individu dengan niat jahat (Wong et al., 2019). Pengambilalihan *command center* ini dapat pula dilakukan secara jarak jauh dengan cara melakukan penetrasi digital ke dalamnya. Tentu saja bantuan pihak dalam secara sadar maupun tidak sadar akan semakin mempercepat peretas dalam menjalankan aksinya (Maasberg et al., 2020).

Kelima adalah serangan dengan motivasi mengumpulkan informasi rahasia dengan cara mencurinya. Ada cukup banyak cara yang dapat dilakukan sebagai modus pencurian. Cara yang paling banyak dilakukan adalah via penyadapan digital, yaitu dengan cara menanamkan *malware* atau *software* jahat ke dalam sistem dimaksud. Charles Liem dalam kesempatan wawancara mengatakan:

*“Server-server di Indonesia dikenal sebagai tempat paling banyak menyimpan malware dengan berbagai tujuan dan motivasi dari penanamnya. Ada yang menanamkan malware bersifat zombie, yang pada saatnya nanti akan dibangun dan dimobilisasi pada saat serangan DDOS dilakukan. Namun ada pula yang bertugas untuk menjadi mata-mata dengan mengirimkan data maupun informasi rahasia ke pihak lawan.” (Liem, komunikasi personal, 5 Januari 2020)*

Berkaca pada pencurian data dan informasi rahasia yang dilakukan oleh Korea Utara terhadap Korea Selatan (Edwards et al., 2017), dan China terhadap

Amerika (Shen, 2016), dunia militer Indonesia telah memasang kuda-kuda terhadap kemungkinan terjadinya peristiwa serupa menimpa sektor pertahanan dan militer di tanah air ("Waspada! Kebocoran Informasi Rahasia", [www.tni.mil.id](http://www.tni.mil.id), 27 Desember 2010). Modul lain yang juga banyak dipergunakan adalah dengan menggunakan serangan dengan istilah *man-in-the-middle attack (MTM)*, dimana diletakkan semacam alat atau diskenariokan terjadinya pihak ketiga yang mampu mengetahui isi atau konten dari aliran data maupun informasi rahasia yang dikirimkan dalam sebuah lingkungan perimeter tertentu (Bajoghli, 2019). Intelijen biasa menggunakan teknik ini dalam mengumpulkan informasi rahasia dari berbagai sumber. Keberadaan vendor atau mitra pengembang yang tidak terkendali dengan baik dapat pula menjadi potensi pelaku serangan MTM. Untuk itulah maka pihak militer harus berhati-hati dan menerapkan standar yang ketat dalam bekerjasama dengan pihak ketiga atau eksternal untuk menghindari diri dari serangan MTM. Teknik lain yang kerap dipakai adalah *social engineering*, yaitu dengan menjadi pihak ketiga (perantara) yang mencuri data dengan mengelabui pihak manusia melalui interaksi berbasis sosial (Greavu-Serban & Serban, 2014). Bisyrn Wahyudi mengatakan bahwa hampir setiap kejahatan besar melibatkan aktivitas *social engineering* di dalamnya, terutama di Indonesia yang literasi keamanan informasi masyarakatnya relatif rendah (B. Wahyudi, komunikasi personal, 13 Mei 2020). Sekuat dan secanggih apapun sistem teknologi yang dimiliki, dengan *social engineering* serangan dapat berhasil karena yang menjadi sasaran perantara adalah manusia (Ross, 2019).

Keenam adalah serangan guna melumpuhkan sistem dan teknologi informasi yang dipergunakan sehari-hari oleh institusi pertahanan dan militer dalam menjalankan aktivitasnya. Contohnya adalah Sistem Informasi Pertahanan Negara atau Sisfohaneg yang dikelola oleh Kementerian Pertahanan dimana di dalamnya terdiri dari berbagai fitur dan informasi penting untuk menunjang kegiatan strategis maupun operasional militer sehari-hari. Seluruh pengelolaan dan manajemen aset serta sumber daya pertahanan dilakukan dan dicatat secara digital oleh sistem ini. Ribuan pengguna aktif maupun pasif setiap harinya memanfaatkan sistem informasi haneg yang telah dikembangkan serta dioperasikan cukup lama tersebut. Dominggus Pakel mengatakan:

*“Tidak dapat dibayangkan apa yang akan terjadi seandainya data pada Sisfohanneg ini jatuh ke tangan orang lain atau sistem ini diretas sehingga tidak berfungsi sebagaimana seharusnya atau malfungsi.”*  
(Pakel, komunikasi personal, 11 November 2019)

Penyerangan terhadap sistem informasi terintegrasi milik institusi pertahanan maupun militer adalah salah satu sasaran utama para peretas global karena fungsinya yang sangat strategis (Skyttner, 2005). Alasannya adalah karena sistem informasi hanneg merupakan jantung aktivitas strategis maupun operasional dari institusi pertahanan dan militer. Jika sistem ataupun sub-sistem utama dapat dilumpuhkan, maka dapat dipastikan terjadinya gangguan serius terhadap sistem pertahanan negara terkait. Perlu diingat bahwa hampir semua negara menempatkan sistem informasi militer sebagai infrastruktur kritis yang harus menjadi prioritas penjagaan keamanannya. Artinya adalah bahwa aplikasi utama yang dipergunakan dalam mengelola sistem pertahanan negara dan militer harus mendapatkan perlindungan tingkat tinggi agar terhindar dari serangan siber (Barnes, 2018).

Ketujuh adalah serangan berbasis propaganda melalui penyesatan fakta atau informasi berbasis digital. Jenis ancaman dan serangan ini adalah yang paling banyak mewarnai kehidupan dunia moderen karena maraknya pemanfaatan media sosial oleh masyarakat dunia (Awan, 2017). Melalui fenomena disinformasi dan misinformasi, masyarakat dibanjiri fakta atau informasi palsu guna mengadudomba satu komunitas dan lainnya (Sirajuddin et al., 2017). Dalam konteks peperangan siber, propaganda disampaikan melalui berbagai cara dan memanfaatkan beragam media. Pemanfaatan media sosial dianggap yang paling cepat, murah, masif, dan efektif. Alasannya adalah karena lebih dari setengah penduduk dunia telah terhubung dengan dunia siber melalui akun media sosial yang dimilikinya. Cara lain adalah dengan mengambil alih berbagai sistem pada beragam stasiun berita resmi dan menyiarkan kabar bohong yang dapat menciptakan katastrofi berbasis pemberontakan, pembangkangan, separatisme, revolusi berdarah, dan gerakan-gerakan politik lainnya (Fagan, 2013). Lihatlah bagaimana *hoax* pasca pemilihan presiden di Indonesia berhasil membelah masyarakat menjadi dua kutub yang saling serang hingga hari ini (“Hoaks dan Propaganda Memecah Belah Bangsa”,

www.medcom.id, 16 Desember 2020. Perang dengan modus menjadikan pikiran sebagai target serangan kerap diistilahkan sebagai perang *mindset* (“Menhan Ingatkan Bahaya Perang Mindset yang Ancam Pancasila”, www.news.detik.com, 8 Mei 2019). Salah satu modus yang banyak digemari adalah melalui proses pengubahan atau modifikasi data terkait dengan fakta yang sebenarnya, sehingga menyesatkan para pimpinan atau penyelenggara negara maupun petinggi militer dalam membuat berbagai keputusan strategis. Perang berbasis propaganda ini hanya dapat dilawan dengan melancarkan propaganda pula, agar terjadi keseimbangan kuantitas informasi yang mengalir di dunia maya.

Kedelapan adalah serangan yang bersifat fisik, yaitu merusak fasilitas atau instalasi teknologi dalam lingkungan pertahanan negara. Seperti diketahui bersama bahwa arena siber terbentuk karena adanya interkoneksi antar berbagai sumber daya komputasi melalui medium transmisi. Jika salah satu atau sebagian aset digital tersebut terganggu secara fisik, jelas akan berpengaruh terhadap ruang siber yang terbentuk darinya. Masih lekat dalam ingatan masyarakat Indonesia, terlepas dari peristiwa tersebut disengaja atau tidak, insiden putusnya koneksi kabel laut dapat mengganggu kinerja internet di berbagai daerah (“Kabel Bawah Laut Telkom Putus, Jaringan Internet di Jayapura Terganggu”, www.tekno.kompas.com, 1 mei 2021). Demikian pula jika jaringan *fiber optic* yang dibentang mengalami gangguan “Jaringan Fiber Optik Indonesia-Singapura Putus, Internet Jadi Lambat. Serangan lain yang kerap terjadi adalah merusakkan atau pencurian komputer server utama yang ada di dalam *data center*. Sabotase semacam ini kerap terjadi dalam sejumlah *data center* yang ada dalam lingkungan Kementerian Pertahanan dan militer di Indonesia (*anonymous*, personal komunikasi, 11 Juli 2020). Richard Kartawijaya dalam suatu kesempatan mengatakan:

*“Mayoritas server room atau mini data center yang ada di Indonesia tidak dijaga dengan baik kemanan fisik maupun logisnya. Orang-orang yang tidak berkepentingan dapat dengan mudah masuk ke dalamnya, dan tidak diawasi aktivitasnya ketika yang bersangkutan berada di dalam data center.”* (Kartawijaya, komunikasi personal, 1 Agustus 2020)

Dapat dibayangkan apabila terjadi sabotase yang dilakukan di dalam *data center* akibatnya sangat fatal dan serius bagi seluruh sistem informasi pertahanan dan militer di Indonesia. Perang fisik dalam dunia moderen menempatkan *data center* sebagai salah satu sasaran yang harus dirusak sesegera mungkin (Barde, 2020). Indonesia sudah berkali-kali mendapatkan serangan langsung ke *data center* yang dimilikinya (“Lebih dari 6 Juta Serangan Siber Menyerang Data Center Jawa Barat”, [www.cloudcomputing.id](http://www.cloudcomputing.id), 21 Desember 2020). CEO Data Center Indonesia mengkonfirmasi adanya ribuan serangan per harinya ke berbagai *data center* di Indonesia (Sugiri, komunikasi personal, 2019).

Kesembilan adalah serangan dengan cara melakukan penyusupan ke dalam instalasi rahasia negara. Perimeter yang kerap dianggap sebagai *restricted area* di antaranya adalah: instalasi militer, pusat intelijen, kementerian pertahanan, fasilitas pembangkit energi, dan lain sebagainya. Penyusupan dilakukan oleh pihak yang tidak memiliki otoritas guna melakukan aksi jahat dengan melakukan berbagai sabotase terhadap sistem teknologi dan digital yang ada di dalamnya (Süzen, 2020). Aktivitas ilegal ini dapat terjadi karena dipergunakannya pendekatan *social engineering* oleh penyerang dengan memanfaatkan rendahnya literasi mereka yang bekerja di tempat-tempat vital tersebut (Avery, 2000). Rudi Luhmanto mengatakan dalam wawancara bahwa:

*“Indonesia yang memiliki kultur timur sangat rentan terhadap serangan social engineering. Keramahaman dan kemudahpercayaan masyarakat sering dimanfaatkan oleh penjahat siber dalam melakukan aktivitas penipuan dengan cara memperdaya mereka dengan berbagai modus serangan yang terbukti efektif dalam pelaksanaannya.”* (Luhmanto, komunikasi personal, 2 Agustus 2020)

Cara lain adalah dengan “menanam orang” atau “mata-mata” ke dalam sistem melalui proses rekrutmen karyawan atau pihak ketiga. Pada saatnya, setelah bertahun-tahun bekerja dan mendapatkan posisi penting, barulah yang bersangkutan melakukan aktivitas perusakan. Pada era Revolusi Industri 4.0, begitu banyak cara baru yang dapat dilakukan untuk melakukan berbagai penyusupan dimaksud. Misalnya adalah pemanfaatan teknologi *drone* untuk memata-matai kegiatan yang terjadi di dalam perimeter rahasia, penanaman *device* berbasis *IOT* (*Internet-Of-Things*) dengan variasi sensor yang dapat

mengambil konten penting dalam sebuah instalasi tertutup, *autonomous vehicle* yang dapat berjalan tanpa dikendalikan manusia, robot berbasis *hardware* maupun *software* yang dapat bekerja secara mandiri, dan lain sebagainya (Riola et al., 2020).

Keseluruhan situasi yang dipaparkan beserta sembilan jenis ancaman maupun serangan terhadap sistem pertahanan dan militer di Indonesia merupakan bukti bahwa NKRI sedang dalam pusaran serangan siber dari dalam maupun luar negeri. Serangan siber ini tidak akan pernah berhenti karena secara paradoksial hadir akibat perkembangan dan penggunaan teknologi informasi serta komunikasi oleh seluruh umat manusia ("Cybersecurity Risks: Are They Inflated?," 2016; Theohary & Harrington, 2015). Oleh karena itulah tidak berlebihan jika berbagai negara berkeputusan untuk meningkatkan anggaran pertahanan sibernya sejalan dengan meningkatkan pemanfaatan teknologi digital di kalangan pengguna pada sektor pertahanan dan militer (Sargent, 2018). Kesembilan klasifikasi serangan siber ini diluncurkan dengan menggunakan 8 (delapan) cara atau modus serangan, masing-masing adalah: (i) *identity theft*; (ii) *data breach*; (iii) *cyber espionage*; (iv) *malware plantation*; (v) *DDOS attack*; (vi) *insider threat*; (vii) *ransomware*; dan (viii) *cryptojacking*. Setiap modus serangan ini menghasilkan dampak yang sangat berbahaya bagi kelangsungan sebuah negara apabila target serangannya adalah sektor pertahanan dan militer.

#### Dampak Serangan Siber terhadap Pertahanan NKRI

Setiap modus serangan memiliki karakteristiknya masing-masing. Karakteristik dimaksud berkaitan dengan sejumlah aspek, seperti: tingkat kesulitan, modus operandi, jenis sasaran, target kerentanan, model eksploitasi, kompleksitas serangan, pilihan skenario, dan dampak kerusakan (Sepúlveda Estay et al., 2020). Dari segi risiko, penyerangan terhadap aset digital apapun dalam teritori sektor pertahanan dan militer dipersepsikan berakibat serius bagi keberlangsungan hidup berbangsa dan bernegara. Pemikiran ini berkembang berdasarkan prinsip yang mengatakan bahwa keberlangsungan hidup sebuah negara dapat terjadi karena adanya tentara militer yang menjaganya. Ketika

institusi tersebut diganggu aktivitas kesehariannya, secara otomatis merupakan ancaman serius bagi sebuah negara (Hare, 2019; Theohary & Harrington, 2015). Sektor pertahanan dan militer di Indonesia harus paham benar kedelapan modus serangan yang diprediksi akan terjadi alam 5-10 tahun ke depan agar dapat melakukan tindakan antisipasi ataupun mitigasi sedini mungkin.

Pertama, *identity theft* berkaitan dengan modus serangan dimana peretas atau pihak lawan berusaha keras untuk mencuri identitas data seseorang demi mendapatkan hak akses rahasia yang melekat padanya. Seperti diketahui bersama bahwa *password* adalah pintu gerbang untuk memasuki sebuah sistem berbasis digital. Proteksi berbasis kata kunci tersebut telah mengalami pemutakhiran dengan diperkenalkannya konsep *biometrics* yang jauh lebih aman dan nyaman (Michael, 2010). Namun demikian, sekuat apapun model proteksi identitas seseorang, faktor literasi yang rendah akan meniadakan kelebihan tersebut (Tintin, komunikasi personal, 3 Juli 2020). Marsudi Kisworo mengatakan dalam wawancara:

*“Banyak filem yang mengajarkan bagaimana caranya mengambil identitas biometrik seseorang seperti sidik jari, suara, retina mata, dan lain sebagainya. Teknik social engineering yang diperlihatkan juga menjadi ide bagi peretas dan penjahat siber untuk menerapkannya dalam kehidupan sehari-hari.”* (Kisworo, komunikasi personal, 5 Agustus 2020)

Ada sejumlah kultur di Indonesia yang dipandang dari keamanan siber relatif memiliki risiko. Sebut saja bagaimana kebiasaan meninggalkan kartu identitas diri (KTP atau SIM) kepada pihak lain. Padahal data yang berada padanya dapat dipergunakan sebagai cara melakukan *social engineering* maupun melakukan penipuan biometrik (C. Liem, komunikasi personal, 3 September 2020). Banyak pihak lupa bahwa SIM Indonesia menampakkan sidik jari di dalamnya, dan KTP Indonesia dapat dibaca dengan menggunakan *digital reader* via telepon genggam. Risiko lainnya adalah data yang ada di dalam kartu identitas tersebut yang kerap dijadikan sebagai alat untuk mendapatkan inspirasi dalam menentukan *password* atau kata kunci (Salahdine & Kaabouch, 2019). Dapat dibayangkan apabila kebiasaan ini dilakukan oleh seluruh masyarakat termasuk di dalamnya adapah para petinggi yang berada di sektor pertahanan maupun



militer. Dengan mudahnya penjahat siber dapat memiliki identitas aset strategis negara ini untuk dimanfaatkan sebagai instrumen melakukan tindakan kejahatannya. Kemajuan dunia e-commerce yang memberikan keleluasan kepada setiap individu untuk menjadi pelanggan dengan memberikan data pribadi detilnya juga memiliki risiko tinggi bagi dunia pertahanan dan militer. Dapat dibayangkan apa yang terjadi seandainya data diri tersebut bocor atau berhasil diretas oleh pihak ketiga. Setidaknya dua *unicorn* besar di Indonesia telah mengalami kejadian dimaksud (“Bukalapak Akui 13 Juta Data yang Dijual Hacker adalah Peretasan di Maret 2019”, [www.kumparan.com](http://www.kumparan.com), 6 Mei 2020; “Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual”, [www.cnnindonesia.com](http://www.cnnindonesia.com), 3 Mei 2020). Bayangkan jika akun yang berhasil diretas adalah Tiket.com atau Traveloka.com, dimana masyarakat Indonesia terbiasa membeli tiket perjalanan atau transportasi via *online*. Hal ini mengandung risiko terbukanya data dan informasi pergerakan para petinggi militer yang merupakan sumber daya strategis pertahanan Indonesia dari masa ke masa. Indonesia dinilai belum memiliki protokol khusus guna mengamankan pergerakan pihak-pihak penting di dalam negara (*VIP=Very Important Person*) – kecuali bagi Kepala Negara dan/atau Kepala Pemerintahan (Hasibuan, komunikasi personal, 11 Februari 2021). Pencurian identitas adalah sasaran antara dari para peretas, dimana tujuan utamanya adalah memperoleh data diri atau *password* pemegang otoritas tertinggi agar penjahat kriminal atau teroris siber dapat masuk ke dalam sistem dalam lingkungan pertahanan maupun militer.

Kedua, *data breach* berkaitan dengan modus serangan dengan tujuan membocorkan atau mencuri data maupun informasi rahasia untuk diakses atau disalurkan ke mereka yang tidak memiliki otoritas terhadapnya. Membocorkan data secara digital dapat dilakukan melalui berbagai cara, baik langsung maupun tidak langsung. Kasus yang menimpa Bukalapak maupun Tokopedia juga menimpa perusahaan-perusahaan dunia seperti Yahoo, Facebook, Alibaba, LinkedIn, dan lain sebagainya (“The 15 Biggest Data Breaches of the 21<sup>st</sup> Century”, [www.csonline.com](http://www.csonline.com), 16 Juli 2021). Kebocoran data dalam sektor pertahanan maupun militer kerap kali tidak disadari oleh pengguna karena dalam dunia digital, tidak terlihat adanya bukti fisik entitas yang hilang (Joseph, 2018). Ada sejumlah risiko yang berpotensi membuat kebocoran pada sektor

pertahanan dan militer di tanah air. Risiko pertama adalah karena arsitektur sistem teknologi informasi yang buruk, dimana faktor keamanan data tidak diperhitungkan di dalamnya. Penelusuran peneliti pada situs Zone-H memperlihatkan bagaimana rentannya berbagai *website* yang dimiliki institusi pertahanan maupun militer Indonesia. Jika sistem dalam perimeter sektor pertahanan maupun militer dirancang-bangun dengan arsitektur yang buruk, maka melalui peretasan berbasis *website* data rahasia dan penting dapat dicuri oleh pihak lawan (Atmodjo, komunikasi personal, 2 Januari 2021).

www.zone-h.org/archive 90% ☆

Home News Events Archive Archive ★ Onhold Notify Stats Register Login search...

NOTIFIER  DOMAIN mil.id

Special defacements only ☐ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☐

Date: ALL Apply filter

Total notifications: 545 of which 208 single ip and 337 mass defacements

Legend:  
H - Homepage defacement  
M - Mass defacement (click to view all defacements of this IP)  
R - Redefacement (click to view all defacements of this site)  
L - IP address location  
★ - Special defacement (special defacements are important websites)

| Date       | Notifier              | H | M | R | L | Domain                             | OS       | View   |
|------------|-----------------------|---|---|---|---|------------------------------------|----------|--------|
| 2021/07/15 | Moroccan Revolution   | M | R |   |   | lanterna11-koarmada3.tnial.mil...  | Win 2016 | mirror |
| 2021/07/15 | Moroccan Revolution   | M | R |   |   | lanterna10-koarmada3.tnial.mil...  | Win 2016 | mirror |
| 2021/07/06 | Moroccan Revolution   | R |   |   |   | lanterna9-koarmada3.tnial.mil...   | Linux    | mirror |
| 2021/06/28 | Moroccan Revolution   | R |   |   |   | pustakamar-seskoal.tnial.mil.i...  | Unknown  | mirror |
| 2021/06/28 | Moroccan Revolution   | M | R |   |   | jurnalmaritim.tnial.mil.id/pub...  | Unknown  | mirror |
| 2021/06/05 | SABUNMANDI CYBER TEAM | M | R |   |   | www.pussenkav.mil.id/sabun.html    | Unknown  | mirror |
| 2021/03/26 | /Raysky...            |   |   | R |   | dithub-tniad.mil.id/pentest.html   | Linux    | mirror |
| 2021/02/25 | Electronic Team       |   |   | R |   | kolimleml.tnial.mil.id/inject...   | Linux    | mirror |
| 2021/02/25 | Electronic Team       | M | R |   |   | lanterna12-koarmada1.tnial.mil...  | Linux    | mirror |
| 2021/02/25 | Electronic Team       | M | R |   |   | jalasenastr.tnial.mil.id/inje...   | Linux    | mirror |
| 2021/02/25 | Electronic Team       | M | R |   |   | lanterna13-koarmada1.tnial.mil...  | Linux    | mirror |
| 2021/02/24 | Moroccan Revolution   |   |   | R |   | lanterna11-koarmada1.tnial.mil...  | Linux    | mirror |
| 2021/01/31 | ./Tikus_HaXoR         | H |   |   |   | dittop-tniad.mil.id                | Linux    | mirror |
| 2021/01/19 | Moroccan Revolution   |   |   | R |   | perustakaan-seskoal.tnial.mil...   | Win 2016 | mirror |
| 2021/01/12 | U ~ Senpai            | H |   |   |   | akademi-tni.mil.id                 | Linux    | mirror |
| 2021/01/03 | aDriv4                |   |   | R |   | kodam127cenderawasih-tniad.mil...  | Linux    | mirror |
| 2020/12/16 | ADIT HACKER CILACAP   | H | M | R |   | www.kodim0309selok.mil.id          | Linux    | mirror |
| 2020/10/31 | Moroccan Revolution   |   |   | R |   | kodikat-tniad.mil.id/d.html        | Linux    | mirror |
| 2020/09/02 | aDriv4                |   |   | R |   | kasuari18-tniad.mil.id/vz.txt      | Linux    | mirror |
| 2020/08/19 | Moroccan Revolution   |   |   | R |   | ditbekangad.mil.id/asset/image...  | Linux    | mirror |
| 2020/08/06 | ./Sn00py              | M | R |   |   | erhanudse16.kodam-wirabuana.mil... | Linux    | mirror |
| 2020/08/06 | ./Sn00py              | M |   |   |   | babinminvettoddam.kodam-wirabu...  | Linux    | mirror |
| 2020/08/06 | ./Sn00py              | M |   |   |   | bekangdam.kodam-wirabuana.mil...   | Linux    | mirror |
| 2020/08/06 | ./Sn00py              | M |   |   |   | bekang.kodam-wirabuana.mil.id/...  | Linux    | mirror |
| 2020/08/06 | ./Sn00py              | M |   |   |   | brngif22.kodam-wirabuana.mil.i...  | Linux    | mirror |

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

Gambar 4. 88 Hasil Penetrasi Zone-H terhadap Situs Militer di Indonesia

Sumber : <http://zone-h.org> , 2021)

Risiko lain yang timbul disebabkan karena banyaknya proyek perencanaan dan pengembangan yang pemeliharaan serta operasionalnya pasca pekerjaan berakhir diserahkan kepada pihak eksternal melalui mekanisme *outsourcing* maupun *insourcing* (Dwicahyono, komunikasi personal, 2 Agustus 2021). Kebanyakan kerjasama ini dilandasi pada perjanjian “tahu sama tahu” dibandingkan membuat kontrak kerja yang detil dengan memperhatikan prinsip-prinsip keamanan data – terutama yang berkaitan dengan hak maupun kewajiban masing-masing pihak yang bekerjasama (*anonymous*, komunikasi personal, 3 Oktober 2020). Masalah kontrak perjanjian dengan pihak pengembang sistem informasi memang menjadi tantangan tersendiri dalam dunia informatika (Kuehn, 2018).

Ketiga, *cyber espionage* berkaitan dengan modus serangan melalui cara melakukan mata-mata dengan memanfaatkan teknologi digital agar dapat mengetahui segala gerakan lawan (Zotti, 2011). Kegiatan mata-mata siber di era moderen sudah dilakukan secara canggih dengan metoda yang semakin kompleks agar tidak mudah dideteksi. Penggunaan alat sadap digital yang tidak kasat mata akibat perkembangan teknologi yang sedemikian pesat merupakan salah satu instrumen yang paling banyak digunakan untuk memata-matai pihak lawan (Prakasa & Noviandi Nur, 2019). Gildas Deograt mengatakan:

*“Silahkan membuka situs-situs e-commerce di Indonesia dimana siapa saja dapat dengan leluasa membeli alat sadap dengan rupa beraneka ragam, seperti:acamata, pulpen, gantungan kunci, bahkan kancing baju. Siapa saja dapat melakukan mata-mata terhadap siapapun.”* (Deograt, komunikasi personal, 1 Agustus 2020)

Sektor pertahanan dan militer di Indonesia disinyalir belum memberlakukan protokol rapat rahasia yang dihadiri oleh berbagai pihak untuk memastikan tidak bocornya isi atau konten dari pertemuan tersebut (Wahyudi, komunikasi personal, 4 Agustus 2021). Beberapa industri strategis telah mulai mengembangkan aturan ketat ketika melakukan rapat direksi yang dipandang penting dan rahasia, seperti: melarang membawa telepon genggam (seluruh

*handphone* peserta rapat diamankan dalam brankas), mengaktifkan *signal jammer*, menandatangani *non-disclosure agreement*, dan lain sebagainya (Soares, 2020). Pendekatan lainnya adalah dengan melakukan analisis dengan menggunakan teknik *big data* yang melibatkan *data science*. Berbasis pada pengumpulan data secara masif dari berbagai tempat, baik yang dilakukan secara legal maupun ilegal, dilakukan proses inferensi (pengambilan kesimpulan) mengenai suatu peristiwa yang sekilas nampak tidak berhubungan sama sekali (“Mewaspada Media Sosial sebagai ‘Mata-Mata’ di Era Digital”, [www.merdeka.com](http://www.merdeka.com), 18 September 2019). Pendekatan ini dikenal cukup kompleks tapi efektif, terutama jika sang peretas memiliki kemampuan untuk mengakses *dark net* (Persson & Rigas, 2014). Bambang Permantoro mengatakan bahwa jaman dahulu hanya orang-orang dengan kemampuan intelijen tertentu saja yang dapat melakukan aktivitas mata-mata, namun sekarang siapapun dapat melakukannya dengan mudah via siber (komunikasi personal, 2 November 2020). Dapat dibayangkan betapa bahayanya kondisi pertahanan dan keamanan negara apabila ketika mata-mata siber bertebaran di berbagai titik-titik institusi pertahanan maupun militer vital yang ada dalam wilayah NKRI. Model lainnya adalah dengan menggunakan alat canggih untuk mengambil alih sensor-sensor penting yang tersebar di mana-mana, seperti: kamera pada telepon genggam, CCTV di tempat publik, *microphone* pada komputer, dan lain sebagainya. Semoga teknologi berbasis sensor dapat dengan mudah diambil alih oleh peretas digital (Bambenek, 2017).

Keempat, *malware plantation* berkaitan dengan modus serangan berbasis penanaman virus atau *software* jahat (*malware*) yang berfungsi melakukan berbagai aktivitas ilegal sesuai dengan maksud pemrogramnya. Seperti diketahui bahwa *malware* dapat melakukan berbagai aktivitas mulai dari yang tidak berbahaya hingga yang dapat menciptakan katastrofi (Lindsay, 2013; Maathuis et al., 2017). *Malware* yang tidak berbahaya adalah yang ditanam pada sebuah sistem untuk melakukan aktivitas seperti pencurian data atau pengiriman data tanpa diketahui pemiliknya. Sementara yang dapat menimbulkan hal serius ketika entitas tersebut menyebabkan rusaknya atau hilangnya data digital yang penting. Adapun *malware* yang sangat berbahaya apabila sudah pada tahapan mampu mengambil alih kendali atau mengubah cara kerja fasilitas vital seperti

instalasi militer, pembangkit nuklir, sistem radar penerbangan, kendali transportasi kereta api, jaringan listrik, dan lain sebagainya (Farwell & Rohozinski, 2011). Hasil penelitian memperlihatkan bagaimana rawannya *server* dan komputer di sektor pertahanan dan militer Indonesia terkena serangan *malware* ini. Contohnya adalah kebiasaan *user* mengklik *link* atau tautan yang tidak jelas asal usulnya ketika dikirimkan melalui media *email* atau pesan pada media sosial maupun *whatsapp*. Penyebaran *malware* atau yang dulu dikenal sebagai virus ataupun bertipe *worms* dapat pula terjadi melalui *flasdisk* – atau media penyimpan *portable* yang banyak dipergunakan *user* komputer (Song et al., 2008). Perang *malware* adalah sebuah fenomena umum di era perang siber pada saat ini. Bahkan beberapa *malware* yang diluncurkan merupakan buatan dari pasukan militer dari berbagai negara di dunia (“Militer Jepang Bikin Senjata Siber Malware, Ini Kemampuannya”, [www.infokomputer.grid.id](http://www.infokomputer.grid.id), 9 Mei 2019). Terlibatnya pasukan militer dalam mengembangkan *malware* akibat dipergunakannya modus serangan ini dalam berbagai perang siber moderen. Milliter Indonesia sebenarnya memiliki kemampuan untuk melakukan hal yang sama mengingat cukup banyak fasilitas penelitian dan pengembangan yang bisa dimanfaatkan seperti yang dimiliki oleh Pusat Pertahanan Siber Nasional Kementerian Pertahanan Republik Indonesia (*anonymous*, komunikasi personal, 1 Juli 2019).

Kelima, *DDOS attack* berkaitan dengan modus serangan masif berupa pengiriman data dengan frekuensi tinggi dan/atau volume besar dari berbagai titik yang telah dipersiapkan dengan baik sebelumnya (melalui penanaman *zombie malware*). Rangkaian serangan ini dimulai dengan menanamkan program kecil secara tak terlihat pada berbagai komputer di seluruh dunia yang dapat dikendalikan dari jarak jauh oleh pembuatnya (peretas).



Gambar 4. 89 Contoh Modus Serangan DDOS berupa Pemusatan ke Satu Destinasi

Sumber : Arbor Networks DdoA Attack Map, 2021

Serangan DDOS berskala nasional yang sangat fenomenal adalah peristiwa Estonia di tahun 2007 yang mengakibatkan *chaos* di ibukotanya yaitu Tallin (McGuinness, 2017). Menariknya adalah bahwa hasil investigasi forensik digital memperlihatkan bahwa jumlah program *zombie* yang menyerang secara masif banyak berasal dari komputer-komputer di Indonesia (Czosseck et al., 2011). Rudi Luhmanto menyatakan bahwa kondisi tersebut dapat dipahami mengingat masih rendahnya kepedulian masyarakat Indonesia terhadap keamanan komputer, sehingga mereka tidak tahu ketika perangkat yang dipergunakannya telah terjangkiti program jahat (komunikasi personal, 7 Januari 2021). Tujuan akhir dari serangan DDOS adalah pelumpuhan sistem atau layanan teknologi informasi. Indonesia sering sekali diserang dengan menggunakan teknik DDOS, termasuk dalam dua tahun belakangan ini dimana bencana pandemi Covid-19 melanda dunia ("Mengenal DDOS yang Serang Situs Virus Corona DKI ala Anies", [www.cnnindonesia.com](http://www.cnnindonesia.com), 13 Maret 2020). Pada peperangan siber, DDOS banyak ditujukan ke titik-titik penting yang dapat melumpuhkan sistem

pertahanan dan militer, misalnya pada: puskodal (*command center*), *data center*, server utama, pusat pengendali alutsista, sistem logistik perang, dan lain sebagainya. Rasional di belakangnya adalah jika fasilitas ini lumpuh, maka akan menghantam sistem pertahanan negara bersangkutan (Bawany et al., 2017).

Keenam, *insider threat* berkaitan dengan modus serangan dari dalam organisasi yang biasanya dilakukan oleh individu yang diselundupkan atau pengkhianat yang dibayar oleh musuh (Zaytsev et al., 2017). Orang dalam yang dimaksud misalnya adalah pegawai aktif, mantan karyawan, kontraktor, vendor, mitra bisnis, atau pihak eksternal lainnya. Serangan yang dilakukan bervariasi seperti pencurian data, penanaman *malware*, perusakan fasilitas, sabotase sistem, pembocoran informasi, dan lain sebagainya. Wikipedia membagi sumber ancaman ini menjadi tiga jenis ("Insider Threat", [www.en.wikipedia.org](http://www.en.wikipedia.org), 14 Agustus 2021). Pertama adalah *malicious insiders* yaitu anggota organisasi yang memanfaatkan otoritas yang dimilikinya untuk merusak sistem digital atau komputer institusi tempatnya bekerja. Kedua adalah *negligent insiders* yaitu anggota organisasi yang ceroboh atau lalai dalam menjalankan aktivitas wajib untuk menjaga keamanan data dan informasi institusi. Dan ketiga adalah *infiltrators*, yaitu pihak luar yang memiliki keleluasan untuk berada dalam teritori atau perimeter organisasi namun tidak berhak atas sejumlah otoritas tertentu. Pihak terakhir ini yang dalam konteks sektor pertahanan dan militer Indonesia dikenal sebagai vendor, pengembang, atau mitra bisnis (kontraktor). Hubungan antara institusi pertahanan dan militer dengan pihak pengembang memang kerap dilematis. Di satu pihak pengembang dibutuhkan untuk membangun, mengembangkan, dan mengendalikan operasional sistem teknologi informasi yang dibutuhkan; sementara di pihak lain keberadaannya di dalam perimeter institusi pertahanan dan militer mengandung risiko tersendiri yang tidak kecil (Van Horenbeeck, 2018). Untuk menghadapi serangan ini dibutuhkan pendekatan terintegrasi yang mengkonvergensi tiga jenis kontrol atau kendali sekaligus, yaitu: *people*, *process*, dan *technology* ("An Analysis of Identity Theft: Motives, Related Frauds, Techniques and Prevention," 2012).

Ketujuh, *ransomware* berkaitan dengan modus serangan dengan cara menyandera sistem guna mendapatkan uang tebusan. Serangan ini

dikategorikan sebagai “mematikan” karena tidak banyak yang dapat dilakukan oleh korban kecuali memanfaatkan data *backup* jika memiliki. Hampir semua penjahat pelaku *ransomware* berorientasi pada finansial (Y. Connolly & Wall, 2019). Indonesia pernah menjadi sasaran empuk jenis serangan tipe ini di tahun 2018 dengan nama serangan WannaCry atau WannaCrypt. Bahkan Indonesia menjadi negara kedua terbesar di dunia yang berhasil diporakporandakan oleh serangan yang ditujukan kepada organisasi atau institusi pengguna aplikasi Microsoft (“Serangan WannaCry di Indonesia Terbesar Kedua di Dunia”, [www.inet.detik.com](http://www.inet.detik.com), 6 Mei 2018). Masalah sebenarnya adalah terletak pada kenyataan, dimana walaupun sistem yang disandera akan dilepas setelah uang tebusan dibayarkan, tidak ada yang tahu apakah hal serupa akan terjadi lagi di masa mendatang, mengingat sang peretas telah mengetahui kelemahan sistem institusi yang diserangnya (Paquet-Clouston et al., 2019). Kebanyakan sang peretas meninggalkan *malware* ketika yang bersangkutan berhasil melakukan serangan *ransomware* ke dalamnya, sehingga di kemudian hari yang bersangkutan dapat mengulangi perbuatan jahatnya. Awal May 2021 serangan *ransomware* kembali melanda dunia dimana Indonesia kembali menjadi salah satu target utama dari kelompok peretas global (“Riset Sebut Indonesia Rawan Serangan Ransomware”, [www.republika.co.id](http://www.republika.co.id), 17 Juni 2021). Salah satu aspek lain yang menyebabkan serangan ini dianggap sangat berbahaya adalah karena para peretas berhasil masuk ke dalam jantung sistem informasi institusi, karena keberhasilannya mengunci aplikasi dan data yang dipergunakan. Artinya adalah bahwa tidak ada yang dapat mengetahui apakah selama proses penyanderaan berlangsung, sang penyerang tidak mengambil data dan informasi penting yang dimiliki institusi. Sehingga kerap kali serangan ini dianggap sebagai *double jeopardy* (Or-Meir et al., 2019; Y. Connolly & Wall, 2019).

Kedelapan, *cryptojacking* berkaitan dengan modus penggunaan atau pengambilalihan sumber daya komputasi (*server*) untuk melakukan proses *mining*. Serangan jenis ini mengemuka sejalan dengan maraknya penggunaan *crypto currency* sebagai alat pembayaran dan investasi – terutama di ruang siber. Ada berbagai cara untuk mendapatkan mata uang kripto ini, dimana salah satunya adalah melalui penambangan atau *mining*. Untuk melakukan penambangan, dibutuhkan sumber daya komputasi ekstra besar yang



membutuhkan biaya tidak sedikit untuk mengadakannya (Mansor et al., 2020). Didasari oleh kenyataan inilah maka para penjahat siber menggagas sebuah serangan baru dengan cara memanfaatkan komputer-komputer yang tersebar di seluruh dunia sebagai sumber daya komputasi untuk keperluan *mining* mereka (Tuttle, 2018). Dalam sebuah diskusi, Muhammad Salahuddien dan Bisyron Wahyudi menyatakan bahwa maraknya generasi muda melakukan *crypto mining* karena dapat dipergunakan untuk berbagai keperluan di dunia siber, terutama yang berkaitan dengan *games* (Salahuddien & Wahyudi, komunikasi personal, 25 Januari 2020). Bahkan belakangan ini Indonesia disinyalir sebagai negara ketiga terbesar di dunia yang komputernya dipergunakan oleh para penjahat *cryptojacker* ("Indonesia Berada di Tiga Besar Negara dengan Upaya CryptoJacking terhadap UKM Terbanyak, [www.akurat.co](http://www.akurat.co), 6 Juni 2020). Tidak heran bahwa komputer-komputer milik UKM yang paling banyak menjadi korban karena rentannya keamanan yang dimiliki dan rendahnya literasi SDM yang ada. Sektor pertahanan dan militer disinyalir akan menjadi target selanjutnya karena dinilai memiliki *server* berkinerja tinggi (*high performance computer*) yang sangat efektif untuk dipergunakan dalam proses *mining* (Carlin et al., 2020). Kejahatan *cryptojacking* berpengaruh signifikan terhadap kinerja komputer korban karena sebagian besar sumber daya komputasinya dipergunakan untuk menambang ("Cryptojacking Diprediksi Jadi Tren Serangan Siber Berikutnya, [www.cnnindonesia.com](http://www.cnnindonesia.com), 20 Juni 2019).

Jika diperhatikan dampak kolektif dari berbagai modus serangan sebagaimana dipaparkan, dapat diambil kesimpulan betapa berbahayanya keberadaan ancaman tersebut bagi Indonesia. Menyerang sektor pertahanan dan militer berarti mencoba untuk mengganggu, melumpuhkan, bahkan memporakporandakan sistem koordinasi pertahanan negara – yang jika hal ini dibiarkan akan mengancam kedaulatan negara, keselamatan bangsa, keamanan nasional, dan keutuhan NKRI. Oleh karena itulah maka negara harus hadir secara aktif dalam membangun pertahanan siber yang kuat, kokoh, mandiri, dan berdaulat; karena tanpanya maka gangguan serangan siber ini akan menjadi ancaman serius bagi Indonesia yang berusaha menggapai tujuan negaranya.

## Kerentanan dan Kelemahan Sistem Pertahanan Siber Nasional

Adagium yang berlaku dalam dunia siber menyatakan bahwa kekuatan sistem pertahanan siber sebuah negara sangat bergantung pada titik terlemah yang dimilikinya. Prinsip ini dianut berdasarkan postur dan karakteristik siber yang tercipta karena terhubungnya titik-titik komputasi dan koneksi dalam sebuah jejaring raksasa. Peretas atau penjahat siber akan senantiasa berusaha mencari “the weakest link” sebagai pintu gerbang masuk ke dalam sebuah sistem atau sub-sistem siber (Geers, 2012; Rosner, 2017). Oleh karena itulah maka literasi masyarakat di bidang keamanan siber dianggap sebagai hal yang serius karena darinya dapat dilihat kekuatan dari “the weakest link” dimaksud.

Penelitian ini menggunakan sejumlah pendekatan untuk meninjau seberapa rentan dan lemah pertahanan siber Indonesia, terutama ketika berhadapan dengan kedelapan modus serangan sebagaimana dibahas sebelumnya. Pendekatan pertama adalah dengan melihat secara langsung seberapa banyak serangan ke sistem pertahanan siber nasional yang berhasil mengganggu aktivitas operasional institusi pertahanan dan militer. Pendekatan berikutnya adalah melalui survei perilaku *user* di lingkungan sektor pertahanan dan militer dalam menjalankan aktivitas kesehariannya di ruang siber. Pendekatan lainnya adalah melalui kegiatan *penetration test* maupun *vulnerability analysis* terhadap sistem yang ada di lingkungan pertahanan siber dan militer. Dan yang terakhir melalui hasil pemeringkatan lembaga dalam dan luar negeri terhadap situasi, kondisi, dan kinerja sistem pertahanan siber Indonesia.

Seluruh lembaga *monitoring* nasional seperti yang dimiliki BSSN, Kemkominfo, Polri, PT Telkom, APJII, IIX, dan lain sebagainya memperlihatkan terjadinya kenaikan akan jumlah serangan setiap tahunnya (Salahuddien, komunikasi personal, 2020). Demikian juga laporan dari masyarakat industri maupun komunitas mengenai insiden yang dialami meningkat secara pesat sejalan dengan pertumbuhan teknologi itu sendiri (“Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi”, [www.tekno.kompas.com](http://www.tekno.kompas.com), 12 Oktober 2020). Sistem *monitoring* Polri memperlihatkan bahwa Indonesia di tahun 2018 yang lalu disematkan sebagai negara dengan kejahatan siber tertinggi kedua di dunia

(“Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia”, [www.kominfo.go.id](http://www.kominfo.go.id), 18 Juli 2018). Perusahaan *unicorn* Indonesia, yang masuk dalam sepuluh besar di ASEAN, yaitu Tokopedia dan Bukalapak, berhasil diretas jutaan data pelanggannya. Belum lagi terhitung ratusan web pemerintah Indonesia yang berhasil diretas setiap tahunnya (“Kerugian Serangan Siber Tahun 2021 Diprediksi Rp84.000 Triliun”, [www.tekno.sindonews.com](http://www.tekno.sindonews.com), 30 Desember 2020). Jika perusahaan besar sekelas Tokopedia dan Bukalapak dapat dengan mudah diretas, dapat dibayangkan betapa rentannya perusahaan-perusahaan maupun beragam institusi lain di tanah air. Pada sektor infrastuktur kritis nasional, tercatat sejumlah peristiwa nasional, seperti:

1. Peretas dengan identitas RansomEXX telah membobol sistem komputer milik PT Pertamina EP, dimana yang bersangkutan telah mengantongi dan membocorkan data internal milik perusahaan di situs *dark web* (“Data Internal Pertamina Bocor Dibobol Hacker”, [www.merdeka.com](http://www.merdeka.com), 29 Maret 2021);
2. Padamnya listrik total separuh Jawa pada tahun 2019 disinyalir tidak saja karena disebabkan adanya pohon tunbang di jalur transmisi Ungaran-Pemalang, namun dimungkinkan ada penyebab lainnya – dimana serangan siber menjadi salah satu kemungkinan yang terjadi sehingga dilakukan investigasi khusus terhadapnya (“Kabar Terbaru, PLN Tak Memungkiri Kemungkinan Terkena Serangan Siber”, [www.industri.kontan.co.id](http://www.industri.kontan.co.id), 8 Agustus 2019);
3. Kebocoran data jutaan nasabah BRI Life yang disinyalir dilakukan oleh kelompok yang terafiliasi dengan perangkat mata-mata Pegasus milik NSO Group Israel; dan
4. Kementerian Pertahanan turut mengusut dugaan kebocoran data data BPJS Kesehatan karena di dalamnya terdapat begitu banyak data prajurit TNI serta pegawai Kemhan yang pada dasarnya merupakan rahasia negara (“Ada Data Prajurit TNI, Kemhan Ikut

Usut, Dugaan Data BPJS Kesehatan Bocor”, [www.news.detik.com](http://www.news.detik.com), 25 Mei 2021).

Mencermati lemah dan rentannya kondisi pertahanan siber Indonesia, dalam diskusi yang dihadiri Rudiantara (Menkominfo 2014-2019) dan pakar intelijen Andi Wijayanto, disimpulkan oleh Anis Matta bahwa Indonesia perlu merumuskan sistem dan strategi pertahanan yang baru, serta independen dalam teknologi (“Anis Matta: Perlu Sistem dan Strategi Pertahanan Baru agar Kasus Kebocoran Data Tak Terjadi Lagi”, [www.tribunnews.com](http://www.tribunnews.com), 30 Mei 2021). Keseluruhan kejadian di atas disebabkan karena buruknya manajemen proses dan teknologi terkait dengan pertahanan maupun keamanan siber di Indonesia.

Disamping kerentanan pada aspek proses dan teknologi, hasil survei yang dilakukan selama penelitian memperlihatkan lemahnya pula komponen manusia atau pengguna teknologi informasi di lingkungan pertahanan dan militer yang dapat menjadi pintu masuk empuk bagi serangan siber. Kerentanan dimaksud diperlihatkan pada perilaku atau budaya sebagai berikut:

1. Keenganan mengganti *password* secara berkala mempermudah peretas dan penjahat siber dalam menjalankan aksinya. Dengan memanfaatkan teknik *brute force*, peretas akan dapat dengan mudah membobol *password* seseorang yang tidak pernah diganti (Indrajit, 2012a; Williams & Joinson, 2020).
2. Kebiasaan meminjamkan *flashdisk* ke orang lain, atau menggunakan *flashdisk* milik orang lain memperbesar potensi risiko tertanamnya virus atau *malware* ke dalam sistem komputer pengguna (Kalash et al., 2018; Wangen, 2015). Banyak *user* belum tahu atau paham mengenai risiko ini, sehingga yang terjadi adalah kebiasaan saling *sharing files* dengan tukar menukar *flashdisk*.
3. Kesenangan mengunduh atau *men-download file* dari internet, terutama yang berformat multimedia (gambar, suara, dan video) dan bersifat gratis (*freeware*). Penjahat siber mengetahui betul

*hobby* kebanyakan masyarakat ini sehingga yang bersangkutan menggunakan kebiasaan tersebut menjadi jebakan atau *phising* (Soo Hoo, 2000; Williams & Joinson, 2020).

4. Kemalasan dalam mem-*backup file* penting adalah risiko besar bagi sebuah institusi jika yang bersangkutan terkena serangan *ransomware*, karena *backup files* inilah adalah satu-satunya harapan atau cara melawan serangan “mematikan” ini (Y. Connolly & Wall, 2019). Prosedur pencadangan konten digital harus menjadi aktivitas standar yang dilakukan organisasi secara berkala untuk menghadapi serangan *ransomware*.
5. Ketidakhati-hatian dalam memindahkan data antar perangkat, seperti dari satu *handphone* ke *handphone* yang lain, atau dari satu komputer ke komputer lain, atau mungkin dari *handphone* ke komputer. Bahkan seringkali *user* mempercayakan pihak eksternal untuk memindahkannya (teman kantor, gerai toko, penyedia jasa, dan lain sebagainya). Pencurian data digital banyak terjadi dalam proses pemindahan atau sinkronisasi dimaksud (Hoofnagle, 2007).
6. Kepercayaan bahwa semua kiriman pesan elektronik itu baik adanya (berfikir positif) menjadi sumber masalah begitu banyaknya terjadi serangan *phishing* yang berhasil di Indonesia. Tanpa memeriksa atau mengecek apakah sebuah tautan atau *link* itu aman atau tidak, begitu banyak *user* yang mengklik-nya karena adanya tawaran yang menggurukan. Dengan sedikit teknik *social engineering*, maka *malware* atau virus dapat dengan mudah masuk ke dalam sistem komputer yang penggunanya tidak berhati-hati (Mouton et al., 2016).
7. Keinginan untuk selalu terhubung ke internet menjadikan individu untuk selalu mencari koneksi di manapun mereka berada. Ketika yang bersangkutan berada di arena publik yang terdiri dari berbagai pihak yang menyediakan wifi gratis, tanpa pikir panjang

biasanya individu tersebut langsung berusaha keras untuk mengkoneksikan gawai atau perangkat digitalnya. Bahkan dalam sejumlah konteks para individu tersebut tidak segan-segan menyerahkan data dirinya untuk memperoleh layanan tersebut. Kebiasaan ini merupakan risiko tersendiri mengingat tidak semua penyedia sambungan wifi gratis memiliki niat baik (Damodaran & Mittal, 2017).

8. Ketidaktahuan menggunakan biometrik untuk meningkatkan level keamanan pribadi maupun institusi. Kebanyakan masih menggunakan *password* konvensional (berbasis kata kunci), sehingga sangat rentan terhadap serangan siber. Walaupun secara sistem kunci biometrik tersedia, namun fitur tersebut tidak dimanfaatkan secara optimal (H. Saini, 2016).

Hasil penelitian memperlihatkan heterogenitas atau variasi perilaku dan budaya dalam berinteraksi di internet. Situasi dan kondisi ini membuat lemahnya aspek keamanan karena peretas menemukan begitu banyak “the weakest link” yang dapat dieksploitasi via *user* yang tidak peduli atau rendah literasi keamanannya. Gildas Deograt dalam sejumlah kesempatan mengatakan:

*“Literasi pengguna komputer baik level pimpinan maupun staf di lingkungan sektor pertahanan maupun militer di Indonesia relatif rendah, terutama dalam menggunakan berbagai aplikasi yang berhubungan dengan internet (dunia siber). Banyak sekali perilaku atau kultur yang membahayakan keamanan institusi karena memberikan peluang peretas untuk melakukan eksploitasi.”* (Deograt, komunikasi personal, 2 Agustus 2020)

*Penetration test* maupun *vulnerability analysis* adalah dua teknik yang biasa dipergunakan untuk mengetahui ketahanan keamanan sebuah sistem. Data dan hasil analisis Zone-H seperti yang telah diperlihatkan sebelumnya memperlihatkan bagaimana setiap hari terdapat situs militer Indonesia (ditandai dengan domain sufiks .mil.id) yang situsnya diserang oleh peretas, karena begitu lemahnya sistem keamanan yang dimiliki. Seandainya *website* ini dibangun dengan arsitektur yang buruk, maka data penting yang ada pada organisasi

dapat dengan mudah diambil dan dicuri. Contoh hasil analisis lain terhadap situs-situs utama di kalangan militer dan Kementerian Pertahanan dapat dilihat pada hasil sebagai berikut:

1. Sucuri.net menganalisis dan menilai bahwa situs resmi Angkatan Laut <https://tnial.mil.id> berada pada tingkatan kerawanan “medium risk”;
2. Quttera.com menyatakan bahwa situs resmi Angkatan Darat <https://tniad.mil.id/> diberi peringkat atau nilai “F” (skor 20 dari maksimum 100) terkait dengan aspek HTTP Observatory; dan
3. Shyk.io memberikan nilai “B” untuk situs resmi Angkatan Udara (<https://tni-au.mil.id/>) yang seharusnya untuk institusi penting ini memperoleh nilai “A+”;
4. Pentest-tools.com menyatakan bahwa situs Kementerian Pertahanan RI dengan alamat <https://www.kemhan.go.id/> memiliki tingkatan risiko “high” karena banyaknya kerentanan yang ditemukan pada *server*-nya.

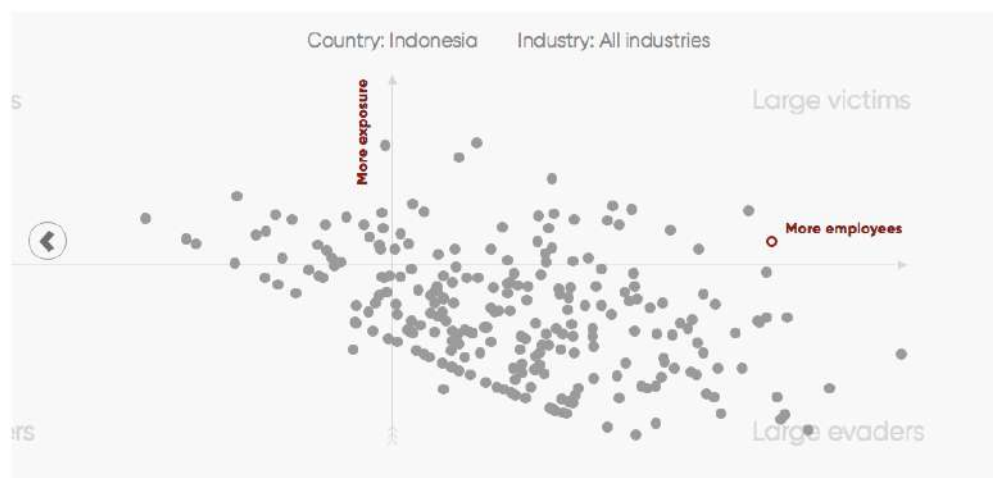
Perlu dipahami bahwa pada tataran kenegaraan, institusi-institusi militer dan pertahanan seharusnya memiliki proteksi tingkat tinggi karena keberadaannya sangat vital bagi pertahanan dan keamanan negara. Situasi dan kondisi ini seharusnya menjadi sebuah *wake-up call* bagi penyelenggara negara untuk lebih memperhatikan isu pertahanan dan keamanan siber di lingkungan strategis dimaksud.

Keseluruhan fenomena dan temuan yang telah disampaikan sebelumnya menguatkan hasil pemeringkatan yang dilakukan oleh lembaga-lembaga independen dan terkemuka dunia, terhadap Indonesia, seperti:

1. National Cyber Security Index yang menempatkan Indonesia di peringkat 77 dengan nilai 38.96 dari skala 100;

2. The Global Economy.com yang menempatkan Indonesia di peringkat 76 dengan nilai 5.80 dari skala 10;
3. The ICT Development Index yang menempatkan Indonesia pada peringkat 111 dunia;
4. The Network Readiness Index yang menempatkan Indonesia pada peringkat 73 dengan nilai 38.38/100 untuk pilar *technology*, 50.20/100 untuk pilar *impact*, 43.26/100 untuk pilar *people*, dan 54.99/100 untuk pilar *goverance*;
5. NordVPN menempatkan Indonesia pada peringkat 47 dalam konteks Cyber Risk Index; dan
6. The International Technology Union yang menempatkan Global Cybersecurity Index Indonesia di urutan 24 (naik pesat setelah BSSN terbentuk).





| Nº | Company                                | Country   | Industry                   | Exposure Score |
|----|----------------------------------------|-----------|----------------------------|----------------|
| 01 | PT. Toba Pulp Lestari, Tbk             | Indonesia | Materials                  | 300+           |
| 02 | PT Trimegah Sekuritas Indonesia Tbk    | Indonesia | Financials                 | 300+           |
| 03 | PT Buana Finance Tbk.                  | Indonesia | Financials                 | 300+           |
| 04 | PT Wijaya Karya (Persero) Tbk          | Indonesia | Industrials                | 300+           |
| 05 | PT. Minna Padi Investama Sekuritas Tbk | Indonesia | Financials                 | 300+           |
| 06 | PT Energi Mega Persada Tbk             | Indonesia | Energy                     | 300+           |
| 07 | PT Erseval Putera Megatrading Tbk      | Indonesia | Health Care                | 300+           |
| 08 | PT BFI Finance Indonesia Tbk           | Indonesia | Financials                 | 300+           |
| 09 | PT Telekomunikasi Indonesia Tbk        | Indonesia | Telecommunication Services | 300+           |
| 10 | PT Asuransi Bina Dana Arta Tbk         | Indonesia | Financials                 | 300+           |

Gambar 4. 90 Cyber Exposure Index Indonesia

Sumber : <https://cyberexposureindex.com>

Tentu saja semua indeks yang dikembangkan dengan melihat dari berbagai perspektif berbeda ini memiliki dampak langsung maupun tidak langsung kepada situasi siber nasional karena karakteristik internet yang merupakan jejaring raksasa dan saling mempengaruhi (Bytheway, 2014; Mueller, 2019). Kecuali Global Cybersecurity Index, peringkat Indonesia dari tahun ke tahun cenderung statis bahkan menurun relatif terhadap negara-negara lain yang perkembangannya jauh lebih cepat. Sebuah ukuran baru sedang dikembangkan

yang bernama Cyber Exposure Index, untuk melihat seberapa besar eksposur keamanan data di berbagai perusahaan di Indonesia dalam dunia siber. Data yang diambil dan dikumpulkan tidak semata-mata dari internet, tapi diambil juga dari komunitas bawah tanah “the dark web. Kondisi termutakhir memperlihatkan bahwa Indonesia berada pada kuadran “Large Victims” dan “Large Evaders”.

#### Efektivitas dan Kualitas Kebijakan Pertahanan Siber di Indonesia

Sejarah perkembangan penyusunan kebijakan dalam bidang siber di Indonesia mengalami sejumlah dinamika. Jika dilihat secara sempit, maka semenjak Indonesia merdeka hanya ditemukan satu kebijakan yang secara eksplisit menggunakan frase “pertahanan siber”, yaitu Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber. Peraturan pada level kementerian ini bersifat sebagai pedoman, sehingga dari segi pengertian bebas dianggap sebagai dokumen atau referensi pemandu – yang tidak memiliki unsur kewajiban kuat untuk dipatuhi di dalamnya (tidak terdapat pasal atau klausul terkait dengan sanksi jika tidak mengikuti pedoman). Connie Bakrie mengatakan dalam sebuah webinar dan wawancara mengenai pentingnya isu pertahanan negara di bawa ke level yang lebih tinggi yaitu negara (Bakrie, komunikasi personal, 4 Juli 2021). Hal ini sejalan dengan sejumlah pemikiran dari tokoh pertahanan siber, sebagaimana disampaikan dalam berbagai kesempatan:

*“Hal yang pertama dan utama untuk dilakukan guna membentuk ekosistem pertahanan siber yang kuat adalah menyusun regulasi pada tingkat undang-undang. Keberadaan peraturan pada level tertinggi ini dibutuhkan karena isu pertahanan siber membutuhkan partisipasi dari seluruh komponen masyarakat dan negara.”* (Wahyudi, komunikasi personal, 4 Agustus 2020)

*“Adalah merupakan sebuah kenyataan bahwa sistem birokrasi di Indonesia baru akan bergerak apabila ada peraturan perundang-undang yang mengamanatkannya. Demikian pula keberadaan*

*aktivitas kolaborasi dan koordinasi yang intensif antar institusi dan lembaga negara hanya dapat dipicu apabila terdapat peraturan yang menyuruhnya.” (Ramli, komunikasi personal, 21 Agustus 2021)*

*“Komunitas non-formal dan informasi sudah terbiasa berjalan tanpa regulasi. Namun untuk institusi resmi negara perlu memiliki payung hukum yang kuat untuk dapat saling bekerjasama.” (Harris, komunikasi personal, 16 Agustus 2021)*

Negara-negara yang maju pertahanan sibernya memiliki regulasi yang sangat lengkap dan berada pada seluruh domain atau spektrum dalam sistem peringkat perundang-undangnya. Artinya adalah untuk dapat membentuk dan mengembangkan ekosistem pertahanan siber yang kuat, regulasi terkait dengannya harus berada pada seluruh tata urutan peraturan perundang-undangan di Indonesia, yaitu paling tidak pada domain undang-undang, peraturan pemerintah, keputusan presiden, dan peraturan atau instruksi menteri. Artinya adalah bahwa saat ini Indonesia baru memiliki satu kebijakan terkait dengan pertahanan siber yang berada pada tingkat peraturan menteri. Adapun pada tingkatan regulasi lain yang lebih tinggi masih bergantung pada kebijakan umum di bidang siber – bukan spesifik berada dalam domain pertahanan siber.

Kebijakan lain yang dimaksud dimulai dengan diberlakukannya Undang-Undang Republik Indonesia nomor 36 tahun 1999 tentang Telekomunikasi – yang hingga saat ini belum mengalami pemutakhiran. Muhammad Salahuddien mengatakan bahwa walaupun ruang siber terbentuk karena adanya jejaring telekomunikasi, namun pada undang-undang ini sama sekali tidak disebut terminologi “internet” maupun “siber” (komunikasi personal, 2 Agustus 2020). Artinya adalah bahwa undang-undang ini hanya murni mengatur masalah infrastruktur telekomunikasi, terutama yang berbasis elektronik (tidak sepenuhnya menyentuh konsep digital). Sebagaimana disampaikan oleh Heru Nugroho, mantan Ketua Asosiasi Penyelenggara Jasa Internet Indonesia:

*“Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi sudah tidak relevan lagi dipergunakan pada masa sekarang. Jika tidak segera dimutakhirkan, justru akan mendatangkan masalah*

*besar bagi keberlangsungan internet di Indonesia.”* (Nugroho, komunikasi personal, 1 Agustus 2020)

Pendapat ini didukung oleh berbagai pihak, baik praktisi, pengamat, pelaku, maupun akademisi di tanah air, sebagai berikut:

*“Indonesia harus memiliki sejumlah undang-undang di bidang siber. Telekomunikasi hanya merupakan komponen kecil dari ekosistem siber, sehingga undang-undang telekomunikasi yang selama ini dikenal hanya dapat dimanfaatkan untuk mengelola infrastruktur jaringan telekomunikasi, bukan seluruh sistem siber.”* (Kisworo, komunikasi personal, 1 Juni 2020)

*“Perkembangan komputer dan digital sudah terjadi sedemikian pesatnya. Undang-Undang Telekomunikasi yang diberlakukan semenjak tahun 1999 tidak dapat mengatasi permasalahan yang ditimbulkan oleh berbagai fenomena baru, seperti: cloud computing, sharing resources, public-private partnerships, dan lain sebagainya.”* (Kisworo, komunikasi personal, 6 Maret 2020)

*“Ketika Undang-Undang Telekomunikasi disusun, para pemangku kepentingan yang merancanginya belum mengantisipasi tren perkembangan teknologi yang sedemikian cepat di masa mendatang. Peraturan ini pada dasarnya hanya mengatur layer terendah dalam ekosistem siber, yaitu media transmisi.”* (Saragih, komunikasi personal, 2 Februari 2020)

Kebijakan berikutnya yang diperkenalkan pada tataran tinggi sistem perundang-undangan di Indonesia adalah ketika disusun dan diberlakukannya Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). UU ITE ini dalam perkembangannya telah mengalami beberapa kali perubahan (adendum) sebagai jawaban terhadap dinamika perubahan jaman. Permasalahannya adalah bahwa kebijakan ini hanya mengatur masalah seputar informasi dan transaksi elektronik, yang berada pada domain ancaman *cyber crime* – bukan *cyber defense*. Bahkan dalam perjalanannya, UU ITE kerap memicu sejumlah kontroversial karena dianggap mengandung berbagai “pasal karet” yang dapat disalahgunakan implementasinya oleh masyarakat hukum. Berbagai kasus di tanah air menggambarkan bagaimana fenomena *false positive* maupun *false negative* terjadi dalam implementasinya. *False positive* berkaitan

dengan dipergunakannya UU ITE untuk konteks permasalahan yang keliru (dibandingkan dengan peruntukannya); sementara *false negative* berhubungan dengan tidak mampunya UU ITE menindak kejahatan yang sesungguhnya terjadi.

Cara penelitian ini mengetahui seberapa besar efektivitas kebijakan pertahanan siber atau regulasi lain di sekitarnya adalah melalui sejumlah pendekatan. Pendekatan pertama adalah dengan mempelajari seluruh kebijakan yang berkaitan langsung maupun tidak langsung dengan pertahanan siber untuk dilihat kinerjanya. Kedua adalah dengan mencermati sejumlah studi kasus yang terjadi di tanah air berkaitan dengan pertahanan siber dan bagaimana menanganinya. Dan pendekatan ketiga adalah melalui survei yang ditujukan kepada para responden yang memiliki pemahaman dan pengetahuan luas mengenai kebijakan siber di Indonesia. Sejumlah peraturan dan kebijakan seputar siber dan internet dipelajari sebagai masukan. Demikian pula berbagai pedoman, panduan, maupun referensi yang kerap dijadikan sebagai pegangan bagi pemerintah maupun penyelenggara siber negara dalam membangun ekosistemnya – terutama berkaitan secara langsung maupun tidak langsung dengan pertahanan siber. Data lain diperoleh melalui “aktivitas intelijen” dengan bertemu dan berdiskusi dengan mereka yang berada “di bawah tanah” atau para aktivis *dark web* guna memperoleh pandangan dan pengalaman praktis yang bersangkutan. Jacob et al. (2020) dalam karyanya “Approach to Assessment of Policy Effectiveness” menawarkan tiga belas kriteria dalam mengevaluasi efektivitas sebuah kebijakan sebagai berikut:

1. *Goal achievement* – berkaitan dengan dampak langsung maupun tidak langsung dengan kekuatan pertahanan siber negara;
2. *Unintended effects* – berkaitan dengan hal-hal yang tidak diinginkan akibat diberlakukannya kebijakan pertahanan siber selama ini;
3. *Baseline* – berkaitan dengan ada tidaknya rancangan (naskah akademik) yang berkualitas ketika kebijakan pertahanan siber dikembangkan;

4. *Coherence/convergence/synergy* – berkaitan dengan keselarasan antara kebijakan seputar pertahanan siber dengan regulasi lainnya yang diberlakukan dan diundangkan dalam wilayah NKRI;
5. *Co-benefits* – berkaitan dengan adanya manfaat yang diperoleh dari institusi atau lembaga lain diluar yang menyusun kebijakan pertahanan siber negara;
6. *Equity/winners and losers* – berkaitan dengan adanya dampak lain dari kebijakan pertahanan siber terhadap komunitas atau kelompok populasi masyarakat lainnya di luar sektor pertahanan;
7. *Enabling/constraining factors* – berkaitan dengan faktor-faktor eksternal yang berpotensi mempengaruhi obyektif yang ingin dicapai dalam kebijakan pertahanan siber yang disusun dan diberlakukan;
8. *Cost/cost-effectiveness* – berkaitan dengan besaran biaya yang perlu dialokasikan dan dikeluarkan untuk menjalankan kebijakan pertahanan siber ini agar efektif mencapai targetnya;
9. *Time frame* – berkaitan dengan ketepatan dan momentum implementasi kebijakan pertahanan siber sesuai kebutuhan negara;
10. *Feasibility/implementability* – berkaitan dengan kelayakan implementasi kebijakan pertahanan siber dalam sektor pertahanan negara;
11. *Acceptability* – berkaitan dengan keberterimaan kebijakan pertahanan siber di kalangan para pemangku kepentingannya;
12. *Stakeholder involvement* – berkaitan dengan partisipasi para pemangku kepentingan dalam implementasi kebijakan pertahanan siber dimaksud; dan
13. *Any other factors* – berkaitan dengan faktor-faktor lain yang berkaitan dengan keberadaan kebijakan pertahanan siber, seperti:

potensi transformasi, relasi lintas generasi, keterkaitan global, dampak sosio-kultural, intervensi politik, penegak hukum, keselarasan standar, dan lain sebagainya.

Berikut ini adalah hasil penelitian berkaitan dengan ketigabelas butir pengukuran efektivitas pertahanan siber di atas. Perlu diperhatikan bahwa kebijakan pertahanan siber yang dimaksud adalah kumpulan dari seluruh peraturan yang secara langsung maupun tidak langsung berkaitan dengan siber dalam sektor pertahanan.

*Goal achievement* dapat dengan mudah dinilai dengan melihat kinerja pertahanan siber Indonesia saat ini. Rendahnya peringkat Indonesia dalam berbagai indikator penilaian hasil penelitian sejumlah lembaga independen terkemuka memperlihatkan masih belum efektifnya kebijakan pertahanan siber yang disusun dan diimplementasikan. Hasil survei terhadap para *stakeholder* pada sektor pertahanan memperlihatkan pula pandangan mayoritas responden yang menganggap bahwa kondisi pertahanan siber Indonesia yang sangat jauh dari sempurna. Mereka juga beranggapan bahwa tidak dimilikinya kedaulatan dan kemandirian pertahanan siber dalam wilayah NKRI. Masih banyaknya serangan efektif ke situs-situs siber pada sektor pertahanan juga merupakan bukti tambahan bagaimana kebijakan pertahanan siber masih belum dapat mencapai obyektif yang diinginkan. Kasus bocornya data karyawan di sektor pertahanan dan militer melalui pihak ketiga memperkuat penilaian mengenai tingkat ketercapaian tujuan dari disusun dan diberlakukannya berbagai kebijakan pertahanan siber. Bisyron Wahyudi mengatakan secara jelas dalam wawancara bahwa:

*“Regulasi yang dimiliki Indonesia saat ini tidak cukup untuk membentuk sebuah pertahanan siber yang kokoh, karena keberadannya masih fokus pada tindakan kriminal atau yang lebih dikenal sebagai cyber crime.”* (Wahyudi, komunikasi personal, 1 Juni 2020)

Pernyataan senada disampaikan oleh Rudi Luhmanto yang pernah menakhodai lembaga pengawas internet Indonesia ID-SIRTII terhadap kebutuhan akan regulasi untuk membangun pertahanan siber di Indonesia:

*“Negara membutuhkan undang-undang yang holistik dan komprehensif dalam menghadapi berbagai ancaman dan serangan siber yang semakin hari semakin kompleks serta membahayakan keberlangsungan negara serta keselamatan masyarakatnya.”*  
(Luhmanto, komunikasi personal, 4 Juni 2020)

*Unintended effect* atau adanya dampak yang tidak diinginkan karena adanya kebijakan pertahanan siber terlihat dari sejumlah fenomena. Contohnya adalah fenomena pemikiran sektoral yang menganggap bahwa kebijakan siber hanya mengatur sektor lembaga atau institusi yang mengeluarkannya (Sadiyah, 2016). Kebijakan yang dikeluarkan oleh Menteri Pertahanan hanya mengikat sektor pertahanan, kebijakan Kepala BSSN hanya untuk internal organisasinya, kebijakan dari Menteri Kominfo hanya untuk sektor informatika, dan lain sebagainya. Padahal ruang siber tidak mengenal batasan ruang dan waktu, sehingga berfikir secara sektoral atau silos-silos justru akan membuat kebijakan yang disusun serta diberlakukan tidak efektif (Denning, 2014). Fenomena lain yang tak diinginkan akibat berfikir sektoral ini adalah tidak adanya koordinasi, kolaborasi, dan kerjasama yang baik antar institusi – sesuatu yang mutlak dibutuhkan dalam membangun pertahanan siber yang kokoh. Sementara dampak tak dikehendaki lainnya adalah adanya berkurangnya inovasi dan kreasi akibat banyak kebijakan yang dibuat terlampau *rigid* pasal-pasalanya. Kemajuan teknologi yang sedemikian pesat jauh melampaui kesiapan regulasi yang mengaturnya, sehingga banyak pengadaan peralatan sistem teknologi yang sudah ketinggalan jaman (Conklin, 2009). Dominggu Pakel mengatakan dalam berbagai kesempatan:

*“Seharusnya setiap lembaga dan institusi di dalam lingkungan Kementerian Pertahanan saling bekerjasama sharing information. Kondisi saat ini dimana masing-masing institusi saling bekerja sendiri-sendiri menyulitkan usaha untuk membangun sistem informasi pertahanan negara yang terintegrasi dan terpadu.”* (Pakel, komunikasi personal, 4 Juni 2021)



*Baseline* atau dasar pengembangan kebijakan biasanya dimulai dengan disusunnya naskah akademik. Namun sudah menjadi rahasia umum bahwa tidak selalu naskah akademik yang dibuat dijadikan sebagai dasar dalam pengembangan kebijakan karena keberadaannya yang cenderung bersifat formalitas semata. Cukup banyak ditemukan kebijakan siber yang melenceng dari naskah akademik yang menjiwainya. Kenyataan tersebut pada dasarnya sangatlah logis mengingat lembaga legislatif adalah institusi politik yang beroperasi berdasarkan logika kepentingan. Keberadaan kerangka pengembangan kebijakan siber sangatlah penting mengingat ruang virtual ini kerap disebut sebagai “tanah tak bertuan”, sehingga perlu kecermatan dan kehati-hatian dalam mengembangkan peraturan di sekitarnya (Theohary, 2015) . Mizamil selaku praktisi dan pemerhati *cyberlaw* mengatakan:

*“Sudah menjadi rahasia umum bahwa naskah akademik yang dibuat sebelum menyusun regulasi lebih banyak untuk memenuhi syarat formal semata. Banyak prinsip-prinsip penting yang tidak diakomodasi dalam pasal-pasal kebijakan. Akibatnya adalah selain kurang efektifnya implementasi kebijakan dimaksud, juga kerap menyebabkan terjadinya tumpang tindih dengan kebijakan lainnya.”* (Mizamil, komunikasi personal, 1 Juni 2021)

*Coherence* antar kebijakan adalah merupakan tantangan tersendiri bagi pemerintahan Indonesia. Selama ini kerap kali terjadi tidak adanya konsistensi atau banyaknya tumpang tindih antar satu peraturan dengan peraturan lainnya (Young, 2010). Konflik antar peraturan ini adalah salah satu penyebab terjadinya ketidakefektifan penerapan sebuah kebijakan. Salah satu jalan paling baik untuk menghindari tumpang tindih dan tambal sulam peraturan adalah adanya cetak biru peraturan atau *blueprint* yang holistik dan komprehensif (Rizal, 2016). Hingga saat dokumen tersebut belum pernah disusun dan dikembangkan. Banyaknya pengaduan ke Mahkamah Konstitusi untuk menguji sejumlah undang-undang atau peraturan terkait siber, digital, dan elektronik merupakan salah satu fenomena yang memperlihatkan ketiadaan koherensi antar sejumlah peraturan. Sebagaimana disampaikan oleh Rabin Mudiardjo dalam wawancara:

*“Kebanyakan peraturan di bidang siber saling tumpang tindih karena tidak dimilikinya blueprint atau cetak biru kebijakan yang komprehensif terkait ekosistem siber di Indonesia.”* (Mudiardjo, komunikasi personal, 4 Mei 2021)

*Co-benefit* atau adanya manfaat diluar pembuat undang-undang sangat relatif sifatnya. Sebagai contoh Pedoman Pertahanan Siber Kementerian Pertahanan lebih bersifat internal, karena ditujukan untuk pengelolaan pengembangan teknologi siber dalam lingkungan kementerian terkait. Sejumlah peraturan dari Kepala BSSN misalnya, walaupun bersifat nasional, namun masih banyak pihak yang menganggap bahwa keberadaannya hanya mengikat secara internal institusi. Demikian pula dengan peraturan sektoral lainnya terkait dengan siber seperti dalam lingkungan Kementerian Komunikasi dan Informatika, Kepolisian Republik Indonesia, Bank Indonesia, dan lain sebagainya. Memang terdapat sejumlah pasal pada berbagai peraturan yang memberikan manfaat kepada beragam sektor, namun pada saat yang sama terdapat pula banyak pasal yang tidak saling mendukung satu dan lainnya. Dalam wawancara Kemal Stamboel menyatakan:

*“Sebagian besar peraturan di Indonesia disusun hanya untuk kepentingan satu sektor, tanpa melihat sektor-sektor lain yang terpengaruh karenanya. Pemerintah dan DPR perlu melihat isu siber secara holistik, utuh, sistemik, dan komprehensif agar setiap kebijakan yang dikeluarkan memberikan manfaat ke sebanyak mungkin stakeholder.”* (Stamboel, komunikasi personal, 2 Mei 2021)

*Equity* dalam konteks kebijakan menggambarkan apakah ada pihak yang diuntungkan serta dirugikan dalam bingkai penerapan peraturan dimaksud. Tentu saja pihak pertama yang diuntungkan dengan adanya kebijakan adalah para *stakeholders* dari institusi pembuat kebijakan. UU ITE misalnya sangat membantu Kemenkominfo dan Kepolisian Republik Indonesia dalam mengelola ekosistem teknologi informasi dan komunikasi di tanah air dan menangkal berbagai modus kejahatan atau kriminal di dunia siber. Namun ditemukan pula sejumlah peraturan yang dianggap merugikan sejumlah kalangan dan menjadi kontroversi hingga saat ini. Sebut saja peraturan Peraturan Menteri Kominfo tentang Data Center yang dianggap merugikan para pelaku usaha industri di Indonesia, seperti: perbankan, keuangan, perdagangan (*e-commerce*), dan lain

sebagainya. Contoh lainnya terkait dengan Undang-Undang Keterbukaan Informasi Publik yang dianggap banyak melanggar hak *privacy*. Rudi Luhmanto secara tegas mengatakan:

*“Setiap peraturan terkait dengan siber di Indonesia selalu penuh dengan kontroversi – ada yang mendukung sepenuhnya, namun banyak pula yang mengkritiknya. Memang sebuah kebijakan tidak dapat menyenangkan semua pihak. Namun paling tidak dalam tahap penyusunannya sebanyak mungkin stakeholder dilibatkan.”*  
(Luhmanto, komunikasi personal, 2 Mei 2021)

*Constraining factors* atau faktor penghambat dalam menerapkan berbagai kebijakan siber relatif cukup banyak. Pertahanan siber yang kuat, berdaulat, dan mandiri kerap bertentangan dengan agenda perdagangan global (Colarik, 2017). Sudah merupakan kenyataan bahwa hampir seluruh perangkat keras dan lunak dalam lingkungan siber di Indonesia adalah buatan dalam negeri. Ketergantungan tinggi terhadap produk luar negeri ini mempersulit dibangunnya sistem pertahanan siber yang berdaulat dan mandiri (Klemas, 2019). Beberapa kali dilakukan usaha untuk menjalin keberpihakan pada industri teknologi informasi dalam negeri, namun inisiatif tersebut mendapatkan cukup banyak tantangan dari para pemasok produk-produk digital dari luar negeri – terutama perusahaan-perusahaan besar. Gildas Deograt yang konsisten dalam melahirkan berbagai produk dalam negeri mengatakan:

*“Bagaimana Indonesia akan berdaulat di bidang siber jika semua aplikasi yang dipergunakan sehari-hari merupakan buatan luar negeri? Tidak saja aplikasinya, namun data serta informasi penting negara tersimpan di berbagai data center luar negeri. Jika kondisi ini dibiarkan terus menerus akan membahayakan pertahanan negara.”*  
(Deograt, komunikasi personal, 2 Mei 2021)

*Cost Effectiveness* dalam membangun pertahanan siber yang kuat merupakan tantangan tersendiri bagi negara maritim seperti Indonesia. Pertama adalah dibutuhkan infrastruktur raksasa untuk menghubungkan setiap titik komunitas yang ada di tanah air. Indonesia telah berhasil membangun jaringan infrastruktur *broadband backbone* yaitu Palapa Ring. Pekerjaan rumah berikutnya adalah membangun koneksi *last mile*-nya, agar semua masyarakat terhubung dengannya. Kedua adalah perlu dibangunnya sejumlah *internet exchange*

*backbone* dan *nodes* di seluruh nusantara. Minimal setiap provinsi memiliki *internet exchange*-nya masing-masing. Ketiga adalah perlu diadakan dan diinstalasinya sensor-sensor pada titik-titik strategis yang berhubungan dengan sumber daya komputasi berkaitan dengan pertahanan siber. Dan yang terakhir adalah dibangunnya *command center* atau *sistem pemantauan pertahanan siber* yang terpadu dan terintegrasi – untuk memastikan terjaganya kedaulatan Indonesia di ruang siber. Tentu saja semua ini membutuhkan biaya besar yang hanya efektif dan efisien apabila pemerintah bekerjasama dengan industri – misalnya dalam kerangka kerjasama *Public Private Partnerships (PPP)*. Zainal Hasibuan anggota Dewan TIK Nasional menyatakan:

*“Negara Indonesia yang sedemikian besar dan luas membutuhkan begitu banyak sumber daya untuk membangun pertahanan sibernya. Pemerintah tidak dapat bekerja sendiri karena keterbatasan anggaran yang dimiliki. Kerjasama dengan industri dan masyarakat adalah sebuah keniscayaan.”* (Hasibuan, komunikasi personal, 2 Januari 2021)

*Time frame* penyusunan dan pemberlakuan kebijakan siber di Indonesia dipandang cukup terlambat dibandingkan dengan negara-negara tetangga ASEAN lainnya. Contohnya adalah UU ITE yang membutuhkan lebih dari 5 tahun dalam penyusunan dan pemberlakuannya. Demikian pula regulasi turunan serta peraturan lainnya yang dikembangkan kerap bersifat reaktif, bukan antisipatif. Tantangan lainnya adalah kecepatan teknologi siber yang jauh melampaui ketangkasan serta kegesitan manusia dalam membuat peraturan berkaitan dengannya. Bahkan untuk kondisi saat ini, banyak sekali regulasi seputar siber yang dibutuhkan dalam tataran nasional yang belum disusun apalagi diberlakukan. Fenomena memperlihatkan banyaknya kebijakan siber yang dibuat hanya untuk keperluan sektoral atau internal tertentu, yang kurang memberikan dampak signifikan pada tataran negara – terutama dalam meningkatkan kinerja dan kekuatan pertahanan siber nasional. Mantan Wakil Ketua ID-SIRTII Muhammad Salahuddien dalam wawancara mengatakan:

*“Dibandingkan negara-negara ASEAN dan Asia Pasifik lainnya, Indonesia cukup tertinggal/terlambat dalam penyusunan berbagai kebijakan sibernya. Situasi tersebut terjadi pula saat ini ketika cepatnya perkembangan teknologi dan kejahatan siber tidak*

*diimbangi dengan pemutakhiran dan revisi kebijakan yang dibutuhkan.”* (Salahuddien, komunikasi personal, 2 Januari 2021)

*Feasibility* dalam konteks kebijakan pertahanan siber berkaitan dengan aspek implementasinya (Lehmann, 2015). Secara umum, dari segi konsep, berbagai aturan yang diberlakukan dapat diterapkan – dalam arti kata tidak ada pasal-pasal yang mustahil untuk diterapkan. Namun demikian terdapat sejumlah permasalahan yang mengemuka. Pertama berkaitan dengan masih belum lengkapnya perangkat peraturan turunan yang termaktub dalam sebuah regulasi, sehingga ada beberapa pasal yang tertunda implementasinya. Kedua berhubungan dengan belum efektifnya penegakan hukum dalam meng-*enforce* agar pasal-pasal yang ada dalam sebuah kebijakan benar-benar dilaksanakan oleh subyek atau obyek dimaksud. Ketiga berkaitan dengan adanya sejumlah konten yang sudah tidak relevan lagi untuk dijalankan akibat berkembangnya teknologi informasi dan digital secara cepat. Ketiga aspek ini membuat kurang efektifnya penerapan berbagai kebijakan yang disusun dan diberlakukan. Praktisi pertahanan dan keamanan siber Bisyrn Wahyudi dalam wawancara berkesempatan mengatakan bahwa:

*“Banyak pasal-pasal dalam sejumlah kebijakan siber tidak bisa dilaksanakan karena sudah ketinggalan jaman atau tidak relevan dengan situasi masa kini. Disamping itu juga banyak hal-hal penting yang seharusnya diatur namun belum ada peraturan atau undang-undang yang mengaturnya.”* (Wahyudi, komunikasi personal, 2 Januari 2021)

*Acceptability* atau keberterimaan masyarakat terhadap kebijakan seputar siber biasanya dapat dilihat melalui banyaknya *pros* dan *cons* yang disampaikan (DeSouza, 2013). Walaupun telah melalui uji publik, tetap saja terdapat pasal-pasal yang dikritisi setelah peraturan diberlakukan. *Pros* kerap disampaikan sebagai apresiasi adanya niat negara dalam meregulasi berbagai aspek terkait dengan siber demi kepentingan masyarakat. Sementara aspek *cons* berkisar pada sejumlah pasal yang dinilai tidak tepat, keliru, atau salah konsep. Apapun bentuk dukungan maupun kritikan yang ada, regulasi telah ditetapkan. Tingkat keberterimaan masyarakat terlihat dari semangat dan

konsistensi penerapannya di lapangan. Mantan Ketua APJII Heru Nugroho menyatakan:

*“Walaupun banyak kebijakan yang disusun dan dikembangkan terlambat, namun masyarakat cukup menyambutnya dengan positif. Kalangan yang berkeberatan kebanyakan justru dari para praktisi siber itu sendiri, karena mereka mengetahui seluk beluk karakteristik digital yang harus diatur keberadaan dan tata kelolanya.”* (Nugroho, komunikasi personal, 2 Januari 2021)

*Stakeholder involvement* atau keterlibatan pemangku kepentingan menandakan seberapa besar regulasi tersebut didukung dan bermanfaat bagi banyak orang (Gunduz, 2020). Permasalahan timbul ketika dalam penyusunan sejumlah peraturan terkait dengan siber, tidak semua *stakeholder* diajak berpartisipasi dan diminta pendapatnya. Entah disengaja atau tidak, peristiwa ini selain menurunkan kualitas regulasi yang disusun, juga mengurangi dukungan banyak pihak ketika kebijakan tersebut diberlakukan. Pada sejumlah kasus, terdapat usulan kebijakan yang gagal diberlakukan akibat tidak dilibatkannya sejumlah pemangku kepentingan dari awal – sehingga pada saat uji publik terjadi penolakan dari berbagai kalangan. Mantan Ketua Federasi Teknologi Informasi Indonesia Teddy Sukardi mengatakan bahwa:

*“Banyaknya penolakan terhadap sejumlah kebijakan siber adalah karena dibuat secara terburu-buru, dan tidak melibatkan para pakar maupun stakeholder yang berkepentingan dengannya.”* (Sukardi, komunikasi personal, 2 Januari 2021)

Faktor-faktor lain yang dijumpai dalam sejarah penyusunan sejumlah kebijakan siber di tanah air memperlihatkan betapa strategisnya sebenarnya kebijakan siber dimaksud. Literasi masyarakat yang masih rendah di satu pihak membuat lambatnya regulasi seputar siber disusun dan dikembangkan, sementara di pihak lain tidak banyak masyarakat yang mampu menerapkan berbagai kebijakan yang disusun secara tepat. Aspek penegakan hukum yang masih diwarnai dengan fenomena *false positive* dan *false negative* menandakan rendahnya kualitas kebijakan yang disusun dan diberlakukan (Limnell, 2016). Demikian pula situasi dan kondisi masyarakat Indonesia yang pluralis dan heterogen menghasilkan gap pemahaman yang berbeda-beda terhadap

pentingnya menyusun dan menerapkan kebijakan pertahanan siber dengan benar. Sementara intervensi politik maupun pihak asing juga kerap terlihat dalam setiap rencana penyusunan kebijakan seputar siber, digital, dan teknologi informasi .

#### Model Ekosistem Pertahanan Siber Ideal

Mengembangkan ekosistem pertahanan siber yang ideal dan cocok diterapkan dalam lingkungan NKRI membutuhkan pemikiran yang holistik dan komprehensif. Model sistem pertahanan siber dimaksud tidak berada dalam dunia hampa, namun harus berada dalam konteks negara Indonesia yang merdeka dan berdaulat.

#### Tujuan Negara Kesatuan Republik Indonesia

Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa tujuan Pemerintah Negara Indonesia adalah melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. Dalam konteks pertahanan dan keamanan siber, dua tujuan sangat jelas berkaitan dengannya, yaitu melindungi segenap bangsa dan tumpah darah Indonesia serta ikut melaksanakan ketertiban dunia (Kemenhan, 2015). Serangan siber yang menyerang infrastruktur kritis dan vital nasional tentu saja akan sangat membahayakan kehidupan masyarakat. Bisa dibayangkan apa yang akan terjadi apabila penjahat siber berhasil mengambil kendali terhadap jaringan backbone listrik nasional, infrastruktur telekomunikasi, sistem moda transportasi, instalasi militer, dan lain sebagainya. Kasus besar seperti yang menimpa negara Estonia, Georgia, Palestina, Rusia, Iran, dan lain-lain dapat dijadikan sebagai referensi bagaimana terganggunya keamanan warga negara karena mereka selain tidak dapat beraktivitas, dibayang-bayangi dengan dampak dari serangan dimaksud (Janeliunas, 2020; Bryan, 2010). Bentuk ancaman lain yang tidak

kalah bahayanya adalah serangan terhadap pola pikir maupun ideologi masyarakat, yang biasa dikenal dengan mindset war (Lehmann, 2015). Fenomena seperti hoax dalam media sosial telah terbukti mampu mengadu domba dan menciptakan polarisasi dalam kehidupan masyarakat, yang pada akhirnya akan sangat membahayakan warganegara itu sendiri. Fenomena serangan siber tidak saja terjadi di Indonesia, tapi hampir pada seluruh negara. Walaupun tidak bisa dirasakan dalam kehidupan sehari-hari, perang siber terjadi setiap detiknya (Mishra, 2013). Perdamaian dunia yang diharapkan banyak pihak selalu mendapatkan tantangan dari mereka yang tidak mendambakannya. Perdamaian abadi hanya akan terjadi apabila setiap negara menghargai berbagai negara yang telah memiliki kedaulatan penuh, dan tidak berusaha melakukan perbuatan atau aneksasi yang akan menggangukannya.

#### Ancaman Non-Militer dalam Ranah Siber

Tren dan laporan statistik beragam institusi pengawas dunia siber memperlihatkan semakin tingginya volume dan frekuensi serangan siber antar negara dari hari ke hari (Limnell, 2016). Dibandingkan dengan ancaman konvensional berbasis militer, keberadaan serangan siber berkali-kali lipat banyaknya dan meningkat secara eksponensial. Dengan kata lain, pada era moderen ini pendulum berpindah menuju ancaman dan serangan melalui atau dalam dunia siber (Mikolic-Torreira, 2017; Chotimah, 2019). Bentuk peperangan yang memanfaatkan teknologi digital dan arena siber beranekaragam, seperti: perang proksi, perang asimetri, perang *hybrid*, perang mindset, perang siber, dan lain sebagainya.

#### Lingkungan Strategis Dalam dan Luar Negeri

Dinamika lingkungan lokal, regional, nasional, dan internasional memperlihatkan betapa chaos-nya kondisi global saat ini, yang sering diistilahkan sebagai istilah VUCA (Volatile, Uncertain, Complex, dan Ambiguous). *Volatile* karena dianggap sangat sulitnya memprediksi tren yang ada di kemudian hari. Kondisi ekonomi, politik, maupun sosial berfluktuasi dari hari ke hari.



*Uncertain* mengarah pada tidak adanya kepastian mengenai apa yang sedang dan akan terjadi. Kondisi mata uang sangat tidak menentu, perselisihan Amerika-China tidak jelas mengarah ke mana, dan pandemi tak pasti kapan berakhirnya adalah contoh ketidakmenentuan yang dimaksud. *Complex* adalah akibat dari semakin banyaknya pihak yang berkepentingan secara langsung dan tidak langsung, situasi dan kondisi semakin tambah rumit. Pihak dimaksud adalah para aktor lintas negara yang saling memiliki kepentingan dalam mengelola maupun mengeksekusi berbagai inisiatif melalui berbagai kesepakatan. Sementara dikatakan *ambiguous* karena banyaknya sinyal-sinyal keliru (atau sengaja dibuat keliru) yang banyak menyesatkan para pelaku usaha maupun pimpinan penyelenggara negara. Pengambilan keputusan yang didasarkan pada data yang salah atau keliru bukannya menyelesaikan isu, justru makin menambah masalah baru. Jika dilihat secara lebih mendalam, terlihat bahwa VUCA banyak disebabkan akibat kemajuan teknologi informasi, komunikasi, dan digital yang meruntuhkan batas-batas ruang dan waktu yang selama ini menghalangi manusia dalam beraktivitas secara cepat, murah, dan berkualitas. Suasana VUCA itu tidak hanya terjadi dalam lingkungan global atau luar negeri, tapi terjadi juga di dalam negeri.

#### Pola Pikir dan Perilaku

Menghadapi fenomena yang penuh dengan ketidakpastian, ketidakaturan, dan ketidakmenentuan, dibutuhkan perubahan cara berfikir dari para penyelenggara dan pimpinan negara. Disadari atau tidak, selama ini banyak orang melihat NKRI dari dua dimensi sebagaimana mereka melihat sebuah peta – hanya berisi “tanah” (darat) dan “air” (laut). Dalam konteks peperangan moderen, ada tiga arena yang dimanfaatkan secara intensif, dan merupakan bagian tak terpisahkan dari sebuah negara, yaitu ranah udara, antariksa, dan siber (Tuukkanen, 2013). Negara besar seperti Amerika Serikat, Rusia, India, China, dan Eropa Barat menganggap justru ketiga arena inilah menjadi tempat baru yang sangat strategis dalam konteks kedaulatan negara – dimana terjadi perebutan “wilayah” agar dapat menguasai dunia. Kepercayaan ini berdasarkan pemahaman bahwa pada dasarnya harta yang paling bernilai harganya adalah

informasi, dimana dalam era moderen keberadaannya telah direpresentasikan dalam bentuk digital (Ormrod, 2016; Andress, 2014). Sehingga bangsa yang menguasai informasi berpotensi untuk mengatur dunia. Oleh sebab itulah maka perlombaan meluncurkan serta mengoperasikan satelit, mendapatkan slot frekuensi, menerbangkan drone tanpa awak, dan memperebutkan wilayah udara adalah fenomena yang mendasari pola pikir dimaksud (Al-Shamisi, 2014; Geers, 2012).

#### Doktrin Pertahanan Siber

Dalam rangka menjaga, melindungi, dan memelihara keamanan nasional, Pasal 30 UUD 1945 mengamanatkan bahwa usaha pertahanan dan keamanan negara dilaksanakan melalui sistem pertahanan dan keamanan rakyat semesta (Sishankamrata) dengan Tentara Nasional Indonesia dan Kepolisian Negara Republik Indonesia sebagai kekuatan utama, dan rakyat sebagai kekuatan pendukung. Sishankamrata adalah doktrin dan sekaligus strategi pertahanan negara yang menggunakan segenap kekuatan dan kemampuan komponen militer dan non militer secara menyeluruh dan terpadu (Kemenhan, 2015). Sishankamrata adalah juga strategi penangkalan yang bersifat kerakyatan, kewilayahan, dan kesemestaan. Dalam rangka menjamin kepentingan keamanan nasional, Sishankamrata melibatkan secara komprehensif segenap departemen dan lembaga pemerintah non departemen serta keikutsertaan yang sah semua elemen bangsa. Salah satu wujud Sishankamrata adalah bela negara yang diimplementasikan ke dalam semangat cinta tanah air, persatuan dan kesatuan dalam rangka menjaga keutuhan Negara Kesatuan Republik Indonesia. Pada saat ini, doktrin Sishankamrata ini sedang mengalami pemutakhiran agar sesuai dengan situasi dan kondisi abad ke-21 yang sarat dengan perkembangan teknologi digital. Pemutakhiran doktrin pertahanan nasional dilakukan oleh berbagai negara sebagai bentuk adaptasi terhadap era digital (Main, 2018; Andress, 2014).

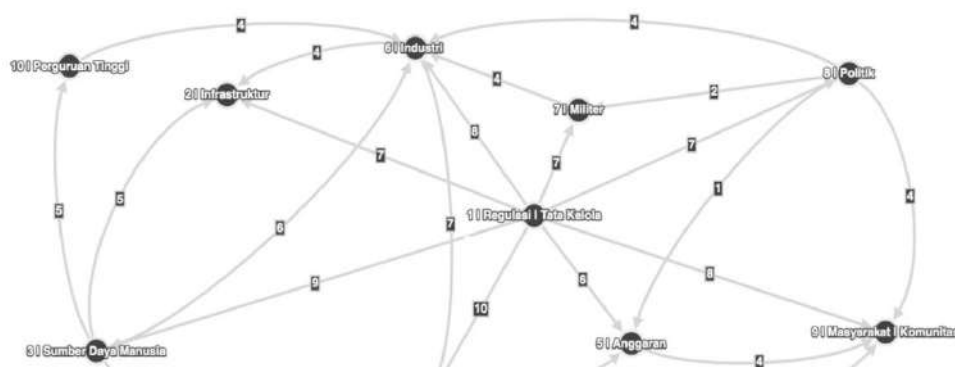
#### Kerangka Ekosistem Pertahanan Siber

Hasil penelitian dengan data yang diperoleh dari literatur, studi kasus, maupun wawancara dapat dijadikan dasar dalam memahami ekosistem ideal sebuah pertahanan siber. Melalui analisa mendalam yang melibatkan sejumlah pakar, dapat disimpulkan bahwa minimal terdapat 11 (sebelas) komponen yang saling berinteraksi satu dan lainnya.

Pertama adalah komponen regulasi, dimana menjadi sentra dari keseluruhan ekosistem, mengingat pertahanan dan kedaulatan siber tidak akan terwujud apabila tidak diinstitusionalisasikan keberadaannya (Byrne, 2014; Mikolic-Torreira, 2017a). Episentrum ini berfungsi sebagai basis pengelolaan terhadap komponen-komponen lain dalam ekosistem (Sadiyah, 2016).

Kedua adalah komponen infrastruktur, dimana hanya karena adanya keterhubungan koneksi antar sumber daya komputasi via jejaring telekomunikasi, maka arena siber terbentuk (Arganata, 2019; Soewardi, 2013). Sebagaimana diketahui, infrastruktur telekomunikasi dibangun oleh pihak pemerintah maupun swasta – baik perusahaan dalam maupun luar negeri.

Ketiga adalah komponen sumber daya manusia, mengingat seluruh sistem pertahanan siber pada dasarnya direncanakan, dirancang, diterapkan, dan dikendalikan oleh manusia (DeSouza, 2013; Janeliunas, 2020). Sumber daya manusia dalam ekosistem siber harus memiliki kompetensi dan keahlian yang diperlukan, terutama untuk memastikan kuatnya pertahanan siber negara yang berdaulat dan mandiri.



Gambar 4. 91 Regulasi sebagai Episentrum  
Ekosistem Pertahanan Siber

Sumber : Regulasi sebagai Episentrum Ekosistem Pertahanan Siber

(hasil pengolahan data oleh peneliti)

Keempat adalah teknologi, yaitu berbagai peralatan yang diperlukan untuk mengoperasikan internet agar dapat dinikmati oleh masyarakat secara luas. Di atas infrastruktur yang ada perlu dibangun *data center*, *internet exchange*, *cyber operation center*, dan lain sebagainya (Hemanidhi, 2017; Geers, 2012; Saltzman, 2013). Keseluruhan aset ini harus selalu dimutakhirkan sejalan dengan perkembangan teknologi yang sedemikian cepat.

Kelima adalah anggaran, karena untuk membantun seluruh suprastruktur dan infrastruktur pada sistem siber dibutuhkan biaya finansial yang tidak sedikit. Anggaran negara biasa tidak cukup untuk memenuhi semua kebutuhan sehingga harus dicari alternatif pembiayaannya, terutama dari industri swasta – misalnya melalui mekanisme *public private partnerships* (Sun2018; Kanniainen, 2019).

Keenam adalah industri, mengingat bahwa internet adalah infrastruktur yang dibutuhkan oleh para pelaku bisnis dan ekonomi dalam menjalankan aktivitas usahanya sehari-hari. Meningkatnya kebutuhan industri akan internet

yang meningkat secara signifikan, maka pada saat yang sama kinerja dunia siber pun harus disesuaikan dengan kebutuhan dimaksud (Dupont, 2019; Carayannis, 2014).

Ketujuh adalah militer, sebagaimana disampaikan dalam doktrin terdahulu yang perlunya melihat kedaulatan negara sebagai sesuatu yang utuh. Sehingga selain Angkatan Darat, Angkatan Laut, dan Angkatan Udara, perlu adanya pasukan siber yang bekerjasama dengan seluruh matra militer untuk menjaga kedaulatan siber nasional – apalagi infrastruktur internet dikategorikan sebagai salah satu aset kritikal negara (Chotimah, 2019; Vaseashta, 2014).

Kedelapan adalah politik, dimana keberadaan partai dan wakil rakyat sebagai representatif suara masyarakat yang bertanggung jawab dalam membuat legislasi atau peraturan untuk memastikan kedaulatan siber benar-benar menjadi prioritas utama (Durante, 2015; Lewis, 2015). Tanpa adanya dukungan politik atau *political will*, mustahil masalah kedaulatan siber akan menjadi perhatian parlemen.

Kesembilan adalah masyarakat dan komunitas, karena selain mereka adalah pengguna atau *user* internet, dalam konteks pertahanan siber peran komunitas bawah tanah atau *underground* sangatlah dibutuhkan (Yeli; 2017). Para *hackers* merah putih selama ini telah terbukti banyak membantu negara setiap kali terjadi serangan terhadap pertahanan dan keamanan di ranah siber.

Kesepuluh adalah perguruan tinggi, dalam konteks posisinya sebagai pusat penelitian dan pengembangan, serta tempat mempersiapkan lulusan yang kapabel di bidang pertahanan dan keamanan siber (Carayannis, 2014; Armstrong, 2020). Disamping itu perguruan tinggi juga menjadi pusat ilmu pengetahuan dan teknologi yang sanggup menciptakan berbagai penemuan penting di bidang teknologi informasi dan komunikasi yang dibutuhkan masyarakat industri.

Kesebelas adalah media, karena posisi strategisnya yang dapat mendiseminasikan informasi kepada masyarakat luas secara cepat. Media pula yang akan memegang pengaruh terhadap terciptanya masyarakat Indonesia dengan literasi dan kultur siber yang kuat dan kokoh – sehingga berpengaruh

langsung terhadap kekuatan pertahanan siber negara (Nastiti, 2018; Awan, 2017).

#### Ekosistem Pertahanan Siber Nasional

Istilah “ekosistem” jika disematkan ke dalam konteks “pertahanan siber nasional” dapat dimaknai sebagai suatu kesatuan sistem yang di dalamnya terdiri dari sejumlah komponen yang saling berinteraksi secara dinamis serta agile untuk membentuk sebuah kapabilitas pertahanan siber negara yang kuat, kokoh, dan berdaulat (Lin, 20). Secara prinsip, komponen yang dimaksud terbagi menjadi tiga komponen besar: *people*, *process*, dan *technology* (Hu, 2018). Komponen *people* mewakili seluruh pemangku kepentingan dalam ekosistem pertahanan siber, termasuk di dalamnya institusi, organisasi, komunitas, dan masyarakat – baik yang bersifat formal maupun informal. Sementara komponen *process* pada dasarnya merepresentasikan regulasi, aturan, struktur, kebijakan, aktivitas, manajemen, dan tata kelola yang dibutuhkan. Dan pada akhirnya *technology* yang pada hakekatnya adalah seluruh sumber daya atau *tools* yang berada dalam ekosistem, seperti: infrastruktur, jaringan, *software*, sistem operasi, *data center*, dan lain sebagainya. Ekosistem pertahanan siber nasional ini merupakan sub-sistem dari ekosistem siber nasional, dan bagian dari sub-sistem ekosistem siber global – sehingga sifatnya tidak berdiri sendiri tapi memiliki hubungan ketergantungan (Kovacs, 2019; Zrahia, 2018).

#### Modus Dua Lingkungan Pertahanan Siber

Hasil studi terhadap berbagai negara memperlihatkan bahwa pada dasarnya, sistem siber dunia terdiri dari dua domain besar, sebut saja “yang terlihat” dan “yang tak terlihat” (Omand, 2015). Domain “yang terlihat” dibangun oleh sebuah sistem formal berskala global yang teratur, formal, dan berbasis sistem. Sistem siber global diselenggarakan dengan menggunakan sejumlah kesepakatan strategis maupun teknis yang dinyatakan dalam bentuk standar, protokol, dan tata kelola. Semua ini dibutuhkan agar dunia siber benar-benar dapat memberikan manfaat semaksimal mungkin, melalui jaminan dapat

terkoneksinya berbagai perangkat komputasi yang jenisnya beraneka-ragam. Sementara domain “yang tak terlihat” dibicarakan karena kenyataan adanya semacam “gerakan bawah tanah” yang berperan aktif dalam dunia siber (Persson, 2014; Hatta, 2020). Lihatlah contohnya bagaimana dark net dan deep web dapat terbentuk dan bekerja hingga kini. Atau komunitas hackers lintas negara yang dengan mudahnya saling berkomunikasi secara rahasia via internet. Contoh lain adalah terciptanya *underground economy* dengan *crypto currency* sebagai mata uangnya yang sekarang telah merambah masuk ke dunia nyata. Sejumlah catatan dari kasus penyerangan berbagai negara dan kemampuan menghadapinya memperlihatkan bahwa kerjasama kedua dunia tersebut merupakan kunci keberhasilan yang harus dipertahankan keberadaannya (Arnold et.al, 2019). Beberapa pihak menyebutkan domain “yang tak terlihat” itu sebagai *the dark side* yang bekerja efektif dengan menggunakan *ghost protocols* (prosedur tak terlihat karena sifatnya yang tidak resmi dan jauh dari formalitas). Sementara suprastruktur dimaknai sebagai semua entitas yang bersifat non-materi yang berasal dari ide masyarakat antara lain, lembaga-lembaga politik, hukum atau undang-undang, peraturan/regulasi, penyelenggara/ pengelola, pemikiran, etika, dan lain sebagainya. Selayaknya mata uang bersisi ganda, infrastruktur dan suprastruktur adalah dua entitas yang saling melengkapi (Byrne, 2014).

#### Anatomi dan Struktur Kebijakan Siber

Pada posisi yang formal dan resmi (sisi yang terlihat) terdiri dari dua bagian penting, yaitu infrastruktur dan suprastruktur. Infrastruktur adalah segala sesuatu yg merupakan penunjang utama terselenggaranya suatu proses, dimana dalam konteks ini adalah aset dan sumber daya yang terkait dengan beroperasinya arena siber. Sementara istilah suprastruktur diberikan pada semua entitas yang bersifat non-materi yang berasal dari ide masyarakat antara lain: lembaga politik, hukum, undang-undang, regulasi, pemikiran, prosedur, standar, pengelola, penyelenggara dan lain sebagainya. Artinya suprastruktur adalah seluruh komponen yang bertanggung jawab sebagai subyek dan instrumen yang mengoperasikan seluruh infrastruktur siber yang ada. Infrastruktur dan suprastruktur adalah layaknya sebuah coin bersisi dua, dimana keduanya tidak dapat dipisahkan karena merupakan kesatuan (Byrne, 2014).

Pada infrastruktur siber, akan terlihat beragam komponen seperti jaringan, perangkat keras, piranti komputasi, server, perangkat lunak (*software*), sistem basis data, *data center*, dan lain sebagainya. Sementara pada suprastruktur siber, akan ditemukan komponen seperti penyelenggara jasa internet, pengelola nama domain, regulasi dunia maya, peraturan terkait internet dan telekomunikasi, pengawas pertahanan dan keamanan siber, dan lain sebagainya. Anatomi infrastruktur dan suprastruktur ini bertumbuh secara dinamis dari hari ke hari sejalan dengan kemajuan teknologi. Sebagaimana sebuah *borderless ecosystem*, seluruh komponen pada infrastruktur dan suprastruktur siber nasional ini tidak dapat dipisahkan dari sistem siber global secara keseluruhan, sehingga pengelolaannya dilakukan secara kolektif dan kolaboratif.

#### Politik dan Tata Kelola Siber Dunia

Seperti yang telah dijelaskan sebelumnya, ekosistem pertahanan siber nasional merupakan sub-sistem dari keseluruhan sistem siber dunia yang telah tumbuh berkembang dari pertama kali ditemukannya konsep internet (Urgessa, 2020). Di dalamnya juga terdapat infrastruktur dan suprastruktur dengan ruang lingkup global, dimana mayoritas dimiliki, diselenggarakan, dan dikelola oleh negara maju. Sebagai sebuah super-sistem siber dunia, di dalamnya mengandung banyak unsur politik bisnis dan perdagangan. Bukan lagi merupakan rahasia umum bahwa negara besar seperti Amerika Serikat memimpin ekosistem global internet bersama negara-negara maju Eropa Barat. Oleh karena itulah negara seperti China tidak merasa segan untuk membangun ekosistem sibernya secara tertutup, yang disinyalir kelak akan menjadi ekosistem alternatif internet global menyaingi yang selama ini dirancang-bangun dan ditumbuh-kembangkan dunia barat (Janeliunas, 2020). Dalam konteks sistem pertahanan siber nasional, para *invisible hands* yang dikatakan sebagai kekuatan “yang tak terlihat” tersebut bermain dan beroperasi dalam lingkungan siber ini. Mereka yang kerap dijuluki sebagai *underground hackers* atau *dark communities* dari berbagai negara (termasuk Indonesia) merupakan kekuatan tersendiri yang tidak dapat tersentuh oleh segalanya yang bersifat formal dan resmi. Bahkan



dalam berbagai permasalahan siber yang pernah terjadi di masa lalu, justru komunitas bawah tanah inilah yang berhasil menyelesaikannya.

#### Interaksi dan Kolaborasi Stakeholder Siber

Terlepas dari keberadaan dua dunia yang membentuk ekosistem pertahanan siber nasional, seluruh komponen pembentuknya saling membutuhkan satu dan lainnya. Para pemangku kepentingan membutuhkan proses komunikasi, kolaborasi, kooperasi, transaksi, interaksi, dan koordinasi antara mereka. Kebutuhan akan keseluruhan proses itu adalah merupakan konsekuensi logis dari membentuk jejaring raksasa yang dinamakan internet. Tanpa adanya kerjasama saling menguntungkan antar seluruh *stakeholders* dalam ekosistem siber nasional, maka tidak mungkin akan terbentuk sebuah arena siber yang dikenal seperti sekarang (Arianto, 2019). Aliansi antar berbagai negara telah terbentuk saat ini, seperti yang dicontohkan pada komunitas CSIRT (Computer Security Incident Response Team), seperti: APCERT (Asia Pacific CERT), ASEAN-CERT, OIC-CERT (Islamic Countries), dan lain sebagainya (Rizal, 2016).

#### Ragam Komponen Pendukung Ekosistem

Untuk memastikan kompatibilitas dalam menyelenggarakan dan mengelola sistem siber, dikembangkan secara bersama berbagai komponen pendukung, seperti: protokol, standar, teknologi, kompetensi, aliansi, instrumen, konvensi, dan lain-lain (Gunduz, 2020). Gambar terkait memperlihatkan hubungan keterkaitan antar seluruh komponen dalam kerangka holistik lingkungan strategis pertahanan siber nasional. Pada gambar tersebut terlihat, bahwa pada sisi sebelah kiri (ditandai dengan warna background abu-abu) merupakan sistem kebijakan yang berada dalam kendali negara. Domain inilah yang memerlukan pendalaman lebih lanjut untuk dikembangkan sebagai kebijakan yang harus disusun oleh bangsa Indonesia agar memiliki pertahanan siber yang kuat dan kokoh. Perhatikan pada diagram tersebut adanya umpan

balik hasil layer interaksi dan kolaborasi siber terhadap lingkungan strategis dalam maupun luar negeri, yang membentuk sebuah siklus tak berkesudahan.

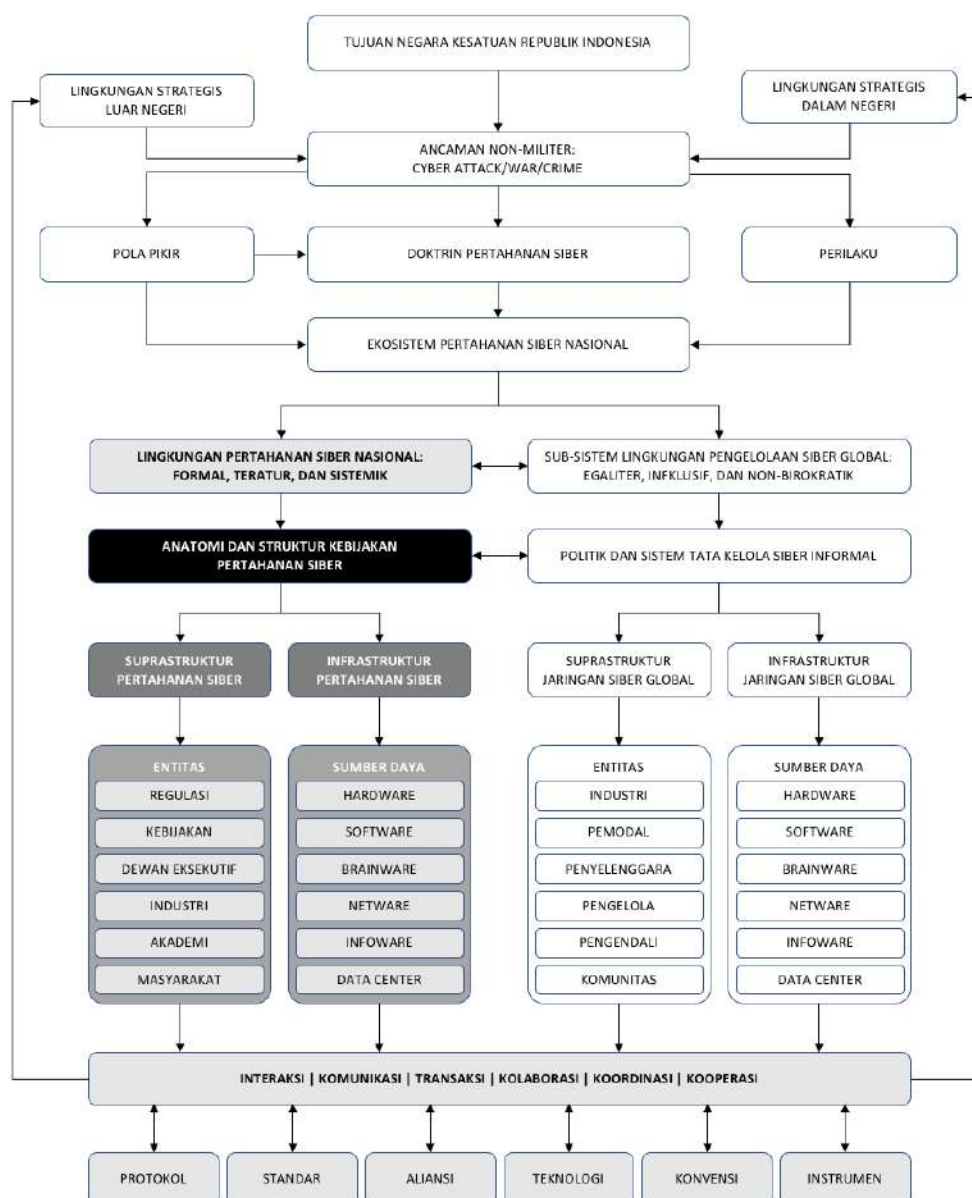
Melalui diagram yang dikembangkan di atas dapat dilihat sejumlah prinsip terkait dengan pengembangan strategi kebijakan dalam lingkungan pertahanan siber sebagaimana disampaikan berikut ini.

Pertama, terciptanya jenis dan ancaman baru di bidang pertahanan berupa ancaman siber disebabkan karena bergolaknya lingkungan strategis dari dalam maupun luar negeri (Soewardi, 2013). Dari luar negeri disebabkan karena perseteruan antara Barat dan Timur (sebut saja Amerika Serikat dan China) dalam berbagai hal telah menciptakan berbagai ketidakseimbangan ekonomi dan sosial yang memicu berbagai negara lain bersikap (Urgessa, 2020). Serangan siber adalah salah satu manifestasi atas ketidakpuasan tersebut karena sifatnya yang relatif mudah dilakukan, tidak membutuhkan biaya besar, berdampak masif, dan sulit dicari jejaknya. Sementara kondisi dari dalam negeri terlihat bahwa mulai terjadi gejolak pada saat pasca reformasi, dimana berbagai serangan siber seperti *hoax* yang menjamur di media sosial bertujuan untuk mengadu domba masyarakat dengan cara membentuk sejumlah polarisasi, terutama yang berbau SARA. Keadaan semakin menjadi dinamis dan tak menentu dengan adanya fenomena VUCA dalam berbagai sektor kehidupan seperti ekonomi, sosial, budaya, ideologi, dan pertahanan keamanan (Kemhan-RI, 2018). Tentu saja kondisi ini berdampak langsung pada keselamatan masyarakat, bangsa dan negara. Jumlah serangan siber ke situs-situs Indonesia yang terus meningkat, dengan sumber serangan dari dalam maupun luar negeri, adalah sinyal bahwa modus peperangan baru antar negara maupun di dalam negara sedang dan akan terus terjadi (Arianto, 2019). Sebagai sebuah negara berdaulat, Indonesia harus mampu memiliki pertahanan canggih dalam menghadapinya.

Kedua, ancaman siber sebagaimana disampaikan sebelumnya tentu saja akan mengganggu Indonesia dalam mencapai tujuannya, terutama dalam hal melindungi segenap bangsa dan tumpah darah Indonesia serta turut melaksanakan ketertiban dunia. Serangan siber yang sudah lama terjadi masih dianggap sebagai sesuatu yang baru bagi pimpinan dan penyelenggara negara (Sadiyah, 2016). Kebanyakan dari mereka masih merasa bahwa memiliki

pertahanan siber yang kuat adalah sesuatu yang penting namun tidak genting (*important but not urgent*). Salah satu penyebabnya selain ketidaktahuan atau kekurangan informasi, adalah posisi serangan siber yang dalam konteks doktrin pertahanan negara berada dalam sub-bagian kecil dari contoh ancaman non-militer. Oleh karena itulah maka perlu dirumuskan kembali, peran dan posisi siber dalam konteks sishankamrata. Kata “semesta” yang dimaksud meliputi ranah kedaulatan NKRI dalam berbagai dimensi, dimana dalam era moderen didefinisikan sebagai teritori darat, laut, udara, antariksa, dan siber.

#### KERANGKA HOLISTIK LINGKUNGAN STRATEGIS PERTAHANAN SIBER NASIONAL



Gambar 4. 92 Kerangka Holistik Lingstra Pertahanan Siber Nasional

Sumber : Kerangka Holistik Lingstra Pertahanan Siber Nasional

(hasil pengolahan data oleh peneliti)

Hanya jika dimensi siber disetarakan dengan keempat dimensi lainnya maka ancaman terhadap serangan siber akan mendapatkan prioritas tinggi untuk diperhatikan. Perlu diperhatikan bahwa dalam konteks pertahanan, serangan siber yang berhasil dapat membahayakan kedaulatan bangsa dan keselamatan masyarakat.

Ketiga, sistem pertahanan siber Indonesia akan terbentuk dan kokoh apabila seluruh pihak yang berada di dalamnya dapat bekerjasama dan berkoordinasi dengan baik. Walaupun sistem pertahanan siber nasional merupakan bagian dari ekosistem siber Indonesia yang juga merupakan bagian dari ekosistem siber dunia, namun ada satu bagian yang berada dalam kendali negara – yaitu hal apapun yang berada dalam ruang lingkup

pemerintahan (Srinivas, 2019). Negara dapat merancang sebuah ekosistem pertahanan siber yang berdaulat penuh dan berada dalam kendali pemerintah. Pengendalian dimaksud adalah melalui strategi yang tepat, dengan didukung dan ditopang oleh kebijakan dan regulasi yang efektif. Kebijakan yang dibuat tidak boleh kaku, namun harus memiliki agilitas yang tinggi karena dinamika jaman (VanHorenbeeck, 2018). Mengingat bahwa teknologi berkembang secara cepat, melebihi kecepatan pembuatan regulasi, maka harus dibuat model strategi pengembangan kebijakan yang tepat. Strategi pengembangan kebijakan yang tepat hanya dapat disusun apabila memenuhi sejumlah persyaratan sebagai berikut:

1. Butir-butir aturan yang dituliskan dalam pasal-pasal maupun ayat-ayat kebijakan adalah yang bersifat prinsip dan esensial, tidak terlampau teknis;
2. Ragam kebijakan yang dikembangkan harus bersifat modular, dalam arti kata jika terjadi perubahan pada salah satu aspek, tidak perlu mengganti seluruh kebijakan yang ada;
3. Kebijakan yang disusun dan dikembangkan selaras dengan cara kerja ekosistem pertahanan siber yang holistik serta komprehensif; dan
4. Keterlibatan mayoritas *stakeholders* dalam ekosistem pertahanan siber merupakan kunci keberhasilan dalam menyusun dan menerapkan kebijakan secara efektif.

Keempat, tantangan terbesar dalam konteks ini adalah mengelola dua wilayah yang berada di luar kendali negara, yaitu: sistem siber global, dan gerakan siber tak terlihat (Wilson, 2005). Sebagai super sistem, sistem siber global bukanlah sesuatu yang harus dijaui, namun justru harus diadopsi – agar Indonesia tidak kehilangan manfaat dari perkembangan internet. Oleh karena itulah maka Indonesia harus mentaati seluruh standar dan protokol yang berlaku secara global, agar sistem siber dapat beroperasi secara normal. Isu terbesarnya adalah bagaimana menyusun strategi agar berbagai entitas penting negara (data, konten, informasi, aplikasi, dan lain-lain) yang ada dalam sistem siber

nasional aman dari jangkauan atau serangan mereka yang berada di luar sistem (tentu saja tanpa melanggar aturan main sistem siber global). Sementara untuk menghadapi gerakan siber dalam negeri yang tidak terlihat, strategi yang tepat dan ampuh harus disusun bersama. Pengalaman berbagai negara memperlihatkan bahwa mereka sangat membutuhkan keberadaan komunitas ini, karena jika dikelola dengan baik, mereka akan sangat bermanfaat dan ampuh dalam membantu menguatkan pertahanan siber nasional (Robinson, 2018).

Kelima, jika kedua wilayah siber tersebut dapat dikelola dengan pengembangan strategi kebijakan yang tepat, maka aktivitas kolaborasi, kooperasi, komunikasi, aliansi, dan interaksi antar berbagai institusi formal maupun informal dapat terwujud secara natural – karena adanya bahasa dan kepentingan yang sama (*shared dream*). Untuk dapat menjalin kerjasama tersebut, harus jelas konteksnya, seperti: penyusunan standar, konvensi istilah, pengembangan protokol, penetapan kompetensi, sosialisasi dan edukasi literasi, pembentukan CERT/CSIRT, latihan gabungan siber (*cyber drill*), inovasi teknologi, pelatihan dan penelitian (R&D), penerbitan panduan, penyelenggaraan *summit*, dan lain sebagainya (Sabillon, 2016; Permana, 2021; Lubua, 2019).

#### The Indonesia Cyber Terrain

Diskursus mengenai dapat tidaknya perimeter siber dikendalikan menyisakan begitu banyak perdebatan tak berkesudahan. Satu pihak mengatakan bahwa sifat dan karakteristik *borderless* siber adalah alasan mustahilnya domain tersebut dikendalikan oleh siapapun (Crowther, 2018). Sementara pendapat lain mengatakan bahwa siber dapat dikendalikan melalui posesi terhadap infrastruktur dan sumber daya komputasi terkait dengannya. Belajar dari US Department of Defence, Indonesia dapat melakukan pengendalian terbatas pada teritori siber yang dimilikinya melalui pemetaan berbagai *layer* pembentuknya. The Indonesia Cyber Terrain dapat dipergunakan untuk memetakan sistem pertahanan siber nasional sebagai berikut:

|                        |           |                         |                   |                       |          |
|------------------------|-----------|-------------------------|-------------------|-----------------------|----------|
| NEGARA                 |           |                         |                   |                       | Layer-17 |
| PEMERINTAH PUSAT       |           |                         | PEMERINTAH DAERAH |                       | Layer-16 |
| KELOMPOK PERMANEN      |           | KELOMPOK SEMI PERMANEN  |                   | KELOMPOK TEMPORER     | Layer-15 |
| PERSONA                |           |                         |                   |                       | Layer-14 |
| DIGITAL DEVICE         |           | MOBILE DEVICE           |                   | SMART DEVICE          | Layer-13 |
| APLIKASI UMUM          |           |                         | APLIKASI KHUSUS   |                       | Layer-12 |
| SISTEM OPERASI TERBUKA |           | SISTEM OPERASI TERTUTUP |                   | SISTEM OPERASI KHUSUS | Layer-11 |
| BAHASA MESIN           |           |                         |                   |                       | Layer-10 |
| BROADCAST              | INTERAKSI | KOMUNIKASI              | NAVIGASI          | KOLABORASI            | Layer-9  |
| TEKS                   | GAMBAR    |                         | AUDIO             | VIDEO                 | Layer-8  |
| SESI TERPOLA           |           | SESI TERPROGRAM         |                   | SESI CERDAS           | Layer-7  |
| SEGMENT STATIS         |           |                         | SEGMENT DINAMIS   |                       | Layer-6  |
| JARINGAN TERBUKA       |           | JARINGAN TERTUTUP       |                   | JARINGAN TERBATAS     | Layer-5  |
| DATA PROTOKOL SISTEM   |           |                         | DATA KONTEN       |                       | Layer-4  |
| SERVER                 | KOMPUTER  | NETWORK DEVICES         |                   | DATA CENTER           | Layer-3  |
| TRANSMISI KABEL        |           | TRANSMISI FIBER OPTIC   |                   | TRANSMISI WIRELESS    | Layer-2  |
| DARAT                  | LAUT      |                         | UDARA             | ANTARIKSA             | Layer-1  |

Gambar 4. 93 The Indonesia Cyber Terrain

Sumber : The Indonesia Cyber Terrain

(hasil pengolahan data oleh peneliti)

1. Layer-1 merupakan komponen geografis yang merepresentasikan wilayah fisik dari sebuah negara, baik secara *de facto* maupun *de jure*. Lapisan ini diperlukan karena di area inilah akan diletakkan berbagai aset dan sumber daya teknologi. Wilayah yang dapat dimanfaatkan adalah darat, laut, dan udara/antariiksa. Lokasi beragam institusi dan unit pada sektor pertahanan maupun militer adalah titik-titik yang harus dipetakan untuk menggambarkan perimeter ruang siber pertahanan.
2. Layer-2 adalah gelaran entitas untuk mentransmisikan sinyal elektronik dan digital dari satu tempat ke tempat yang lain. Di sinilah instalasi kabel laut, *fiber optic*, dan satelit diletakkan. Gelaran infrastruktur ini pada dasarnya yang menghubungkan seluruh institusi dan unit pada sektor pertahanan maupun militer di Indonesia.

3. Layer-3 adalah kumpulan dari perangkat teknologi yang diletakkan pada sejumlah institusi untuk menghubungkan antara satu “ujung” entitas transmisi dengan lainnya. Pada lapisan ini terdapat komputer, *server*, *network devices*, dan *data center* (sumber daya komputasi). Lapisan ini sungguh penting karena merupakan pemicu terbentuknya ruang siber yang ingin dikendalikan. Sektor pertahanan maupun militer perlu memiliki arsitektur *data center* yang kuat dan efektif, karena fasilitas ini adalah komponen utama dalam pembentukan ruang siber pada sektor pertahanan.
4. Layer-4 merupakan lapisan pertama dalam ruang siber, yang berhubungan erat dengan keberadaan data digital yang mengalir dari satu entitas komputasi ke entitas komputasi lainnya. Pada lapisan maya ini, data mengalir dari satu titik ke titik lainnya sesuai dengan protokol teknis yang telah ditentukan. Data pada sektor pertahanan dan militer bersifat rahasia, sehingga seyogyanya memiliki protokol khusus untuk mengenkripsi atau menyandikannya.
5. Layer-5 berkaitan dengan pengelompokkan *server* atau komputer dalam sejumlah jaringan terbuka, tertutup, maupun terbatas sesuai dengan keinginan. Katakanlah setiap angkatan di militer membentuk jaringan terbatasnya, dimana antar jaringan tersebut membentuk sebuah jejaring tertutup yang lebih besar untuk kebutuhan koordinasi, kolaborasi, maupun kooperasi.
6. Layer-6 berhubungan dengan segmentasi jaringan, karena dalam dunia pertahanan dan militer, dapat dibentuk segmen-segmen yang sifatnya statis maupun dinamis. Segmen jaringan statis diperuntukkan bagi aktivitas rutin dalam lingkungan sektor pertahanan. Sementara segmen dinamis untuk berbagai kebutuhan aktivitas yang bersifat *ad hoc* atau temporer, seperti untuk melayani operasi atau penugasan khusus.
7. Layer-7 merupakan lapisan yang berbicara mengenai sesi, yaitu aktivitas atau proses yang dijadwalkan untuk dilakukan. Sesi terpola



adalah aktivitas yang memiliki jadwal yang jelas dan rutin dilakukan. Sementara sesi terprogram mengatur aktivitas yang telah diprogramkan sebelumnya. Program cerdas yang dapat “berfikir” merupakan salah satu variasi yang dapat memicu adanya sesi tertentu. Seluruh aktivitas dalam sektor pertahanan dan militer seyogyanya dipetakan dan dijadwalkan dalam konteks ini.

8. Layer-8 berbicara mengenai lapisan presentasi, dimana data yang ditransfer dari satu tempat ke tempat lainnya telah dimodifikasi menjadi berbagai bentuk format. Format yang paling banyak dimanifestasikan adalah dalam bentuk teks, gambar, audio, video, maupun multimedia (gabungan di antaranya). Data dari lapangan dalam sektor pertahanan dan militer terdiri dari berbagai format sesuai karakteristik dan posturnya.
9. Lapisan-9 memiliki fungsi memilih dan mengatur berbagai jenis komunikasi yang terjadi dalam dunia siber. Komunikasi dapat terjadi secara satu arah, dua arah, maupun multi-arah. Masing-masing jenis komunikasi memiliki protokol dan aturannya masing-masing agar terjadi sinkronisasi. Yang dimaksud komunikasi adalah berbagai bentuk interaksi dengan menggunakan perangkat digital yang terhubung dalam ruang siber.
10. Lapisan-10 memperlihatkan bagaimana komputer dan perangkat teknologi informasi bekerja berdasarkan instruksi yang diberikan dalam bahasa mesin. *Low level language* ini merupakan *software* untuk menggerakkan berbagai perangkat komputasi berbasis algoritma yang disusun. Alat-alat teknologi yang ada di lingkungan pertahanan dan militer, terutama yang moderen, telah beroperasi dengan menggunakan bahasa komputer.
11. Lapisan-11 adalah *operating system* yang merupakan perangkat lunak untuk mengoperasikan berbagai komputer, *server*, dan perangkat komputasi lainnya. Sistem operasi yang dipergunakan dalam lingkungan pertahanan dan militer cukup banyak, mulai dari

yang bersifat *open source* hingga yang spesifik atau *proprietary*. Keseluruhan sistem operasi tersebut harus bekerja secara sinkron dan teroskestrasi dengan baik.

12. Lapisan-12 merupakan lapisan tertinggi dari ruang siber, yaitu tempat berbagai aplikasi atau *software* diinstalasi. Seluruh perangkat lunak yang ada dalam lingkungan pertahanan maupun militer berada pada lapisan ini. Kumpulan aplikasi ini sangatlah penting mengingat seluruh proses dan aktivitas yang ada dalam sektor pertahanan dan militer berjalan di atas *software* dimaksud.
13. Lapisan-13 merupakan lapisan fisik pertama di atas ruang siber karena merepresentasikan perangkat digital seperti tablet, *handphone*, dan piranti keras lainnya untuk mengakses beragam aplikasi yang ada pada ruang siber. Seluruh perangkat teknologi informasi dan komunikasi dalam sektor pertahanan dan militer masuk ke dalam lapisan ini.
14. Lapisan-14 adalah manusia atau *users* yang mengoperasikan berbagai perangkat keras atau *gadget* untuk berhubungan ke dunia siber melalui beragam aplikasi. Para pengguna langsung atau tidak langsung seperti pimpinan dan karyawan Kementerian Pertahanan serta anggota TNI berada dalam lapisan yang sangat penting ini.
15. Lapisan-15 terbentuk ketika sejumlah manusia membentuk kelompok sesuai dengan kepentingannya. Kelompok dapat berupa komunitas, kelompok kerja, organisasi, institusi, perusahaan, dan badan hukum lainnya. Seluruh entitas formal maupun non-formal yang berada dalam sektor pertahanan dan militer berada dalam lapisan dimaksud.
16. Lapisan-16 merepresentasikan pemerintah pusat dan pemerintah daerah dalam teritori NKRI yang bertugas mengatur seluruh kehidupan bermasyarakat – yang terdiri dari begitu banyak kelompok-kelompok kehidupan.

17. Lapisan-17 merupakan lapisan tertinggi yang merepresentasikan NKRI sebagai sebuah negara yang mandiri dan berdaulat tempat seluruh sumber daya komputasi fisik dan ruang siber yang terbentuk berada.

### Strategi Pengembangan Kebijakan Pertahanan Siber Nasional

Pada dasarnya model pertahanan siber ideal dalam perspektif sistem yang holistik dan komprehensif terdiri dari delapan komponen utama:

1. Undang-Undang Dasar Republik Indonesia – sebagai konstitusi negara yang paling tinggi posisinya dan telah mengalami adendum beberapa kali sesuai dengan semangat reformasi dan situasi kondisi jaman yang dinamis;
2. Doktrin Pertahanan Kedaulatan Siber Nasional – yang merupakan tambahan konsep doktrin hannege yang sedang mengalami pemutakhiran;
3. Kerangka Ekosistem Pertahanan Siber Nasional – penggambaran berbagai komponen yang saling terhubung beserta peran dan fungsinya;
4. Domain Kebijakan Perlindungan Siber (*Cyber Safeguarding*) – menyangkut standar keamanan yang harus dipenuhi serta dipatuhi oleh seluruh aset strategis dalam lingkungan pertahanan dan militer;
5. Domain Kebijakan Pertahanan Siber (*Cyber Defense*) – berhubungan dengan langkah-langkah yang diambil untuk menahan ancaman atau serangan yang terjadi sewaktu-waktu;
6. Domain Kebijakan Penyerangan Siber (*Cyber Offense*) – berkaitan dengan tahapan untuk melakukan langkah-langkah pelumpuhan (penyerangan aktif) karena adanya situasi yang memaksa;
7. Domain Kebijakan Peperangan Siber (*Cyber Warfare*) – walaupun jarang dipergunakan, harus ada landasan kokoh dalam menghadapi peperangan siber yang sebenarnya sudah terjadi namun jarang atau tidak lumrah untuk dideklarasikan; dan
8. Ragam Kebijakan Pendukung Tata Kelola Pertahanan Siber - menyangkut semua aturan, standar, konvensi, dan panduan

strategis maupun teknis yang dibutuhkan untuk memastikan ekosistem pertahanan siber berjalan dengan baik.

Kedelapan komponen tersebut merupakan pijakan dalam mengembangkan kebijakan terkait dengan pertahanan siber di Indonesia. Perlu diperhatikan bahwa sebagaimana disampaikan sebelumnya, kebijakan yang ada haruslah bersifat *agile*, sehingga dapat secara fleksibel mengikuti perubahan perkembangan jaman. Berikut adalah penjelasan secara lebih mendalam mengenai masing-masing komponen dimaksud.

#### UUD-RI dan Tujuan Negara

Keberadaan NKRI tidak bisa dilepaskan dengan sejarah lahirnya UUD-1945 yang sudah mengalami adendum beberapa kali. Undang-Undang Dasar RI sangatlah penting karena di sanalah tertulis tujuan negara Indonesia. Sehingga apapun kebijakan yang dikembangkan harus berakar pada konstitusi utama ini. Walaupun tujuan negara tidak berubah, namun interpretasinya harus dilihat dari kondisi termutakhir – terutama yang berkaitan dengan lingkungan strategis dari dalam dan luar negeri. Kebutuhan akan pertahanan siber yang kuat harus dapat menemukan konteksnya pada keempat tujuan negara Indonesia.

#### Tujuan Perlindungan

Melindungi segenap warganegara dan seluruh tumpah darah Indonesia mengandung arti menjauhkan mereka dari berbagai ancaman yang berpotensi mengganggu aktivitas sehari-hari, serta kedaulatan dan keutuhan negara. Sekecil apapun ancamannya, negara tidak boleh tinggal diam. Ancaman dan serangan yang senantiasa tumbuh berkembang sesuai jamannya harus dapat dijauhkan sedemikian rupa dari wilayah NKRI – baik yang berasal dari dalam maupun luar negara (Soewardi, 2013; Putra, 2018). Seandainya serangan berlangsung pun, antisipasi dampak yang ditimbulkan harus ditekan sedemikian rupa sehingga tidak membahayakan seluruh masyarakat. Oleh karena itulah

beraneka ragam ancaman dan serangan siber yang setiap harinya terjadi harus benar-benar dicegah serta diantisipasi sungguh-sungguh.

#### Tujuan Kesejahteraan

Ekonomi digital telah mengubah tatatan masyarakat Indonesia selama dua puluh tahun terakhir. Kehadiran berbagai perusahaan berbasis digital telah membuat pertumbuhan ekonomi meningkat tajam, terlihat dari besarnya frekuensi dan volume perdagangan terkait dengannya (Cheung, 2019). Bahkan Indonesia berhasil melahirkan sejumlah perusahaan berskala unicorn yang disegani dunia karena keberhasilan bisnisnya. Geliat ekonomi online telah memberikan kontribusi nyata bagi kesejahteraan masyarakat tanah air, terutama mereka yang berada di bottom of the pyramid (kaum ekonomi kecil-menengah). Serangan siber memiliki potensi mengganggu berbagai infrastruktur perekonomian nasional yang dapat mengganggu kegiatan ekonomi digital. Jika tidak dicegah dan diatasi, dampaknya fatal terhadap situasi dan kondisi masyarakat – yang tentu saja berpengaruh terhadap kestabilan keamanan nasional.

#### Tujuan Pencerdasan

Pendidikan dan pengalaman adalah sumber kecerdasan manusia Indonesia. Internet telah menyebabkan terjadinya disrupsi pada sektor pendidikan, karena sekat-sekat ruang dan waktu telah diruntuhkan olehnya (Ertl, 2008; Yang, 2009). Setiap manusia Indonesia dapat dengan mudah mengakses sumber belajar dari negara manapun melalui beragam software dan aplikasi. Konten dan pengetahuan termutakhir dapat diperoleh secara terbuka dan cuma-cuma oleh para pembelajar di manapun mereka berada (Sobiesk, 2015). Disamping itu kondisi pandemi Covid-19 yang dialami telah menyadarkan manusia betapa krusialnya peranan teknologi dalam kondisi sulit. Oleh karena itulah maka infrastruktur internet harus dijaga benar-benar agar tetap beroperasi

secara normal. Serangan terhadapnya berarti ancaman terhadap dunia pendidikan di Indonesia.

### Tujuan Perdamaian

Politik luar negeri Indonesia adalah bebas dan aktif. Bebas berarti kita bebas menentukan sikap dan pandangan kita terhadap masalah - masalah internasional dan terlepas dari ikatan-ikatan kekuatan raksasa dunia. Dan Bangsa Indonesia punya hak penuh untuk menentukan sikap dan keinginannya sendiri sebagai negara yang merdeka dan berdaulat. Aktif berarti senantiasa aktif memperjuangkan terbinanya perdamaian dunia. Dan Bangsa Indonesia tetap memberikan sumbangan baik dalam bentuk pemikiran maupun keikutsertaan secara aktif dalam menyelesaikan berbagai konflik. Perang siber yang terjadi setiap detiknya secara langsung dan tidak langsung telah melibatkan Indonesia, terutama karena dilancarkannya perang proksi, perang mindset, perang hibrida, perang asimetri, dan lain-lain. Keseluruhan jenis perang itu memanfaatkan internet sebagai infrastruktur dan media melakukan agitasi (Austin, 2020; Reinhold, 2019). Oleh karena itulah maka Indonesia harus “bebas dan aktif” berperan dalam konstalasi perang siber masa kini.

### Doktrin Pertahanan Kedaulatan Siber Nasional

Pemutakhiran doktrin pertahanan siber perlu dilandasi dengan argumentasi yang kuat. Argumentasi kuat akan diperoleh apabila cara pandang terhadap dunia dipebaharui melalui pola pikir terbuka (Tuukkanen, 2013). Sebagaimana disampaikan sebelumnya, Negara Kesatuan Republik Indonesia tidak hanya terdiri dari “tanah” dan “air” semata – namun memiliki dimensi tak terlihat lainnya, yaitu udara, antariksa, dan siber. Kemajuan teknologi mau tidak mau telah memaksa negara-negara di dunia untuk menginterpretasikan kembali wilayah kedaulatannya (dalam makna yang lebih luas). Batasan darat dan lautan sudah dianggap final (walaupun masih ada beberapa sengketa perbatasan) bagi

NKRI, namun jika dilihat dari tiga domain lainnya yaitu udara, antariksa, dan siber – nampak sekali masih jauh dari berdaulatnya negara Indonesia.

#### Domain Kebijakan Perlindungan Siber (Cyber Safeguarding)

Sebagaimana sebuah rumah yang dikelilingi pagar dan berbagai pintu masuknya dikunci rapat, demikian pula seluruh aset penting yang berkaitan dengan pertahanan negara harus dijaga keamanannya (Sabillon, 2016). Dibutuhkan sejumlah kebijakan agar beragam aset negara kritikal dan penting benar-benar mendapatkan perlindungan prima. Dalam domain ini, ada tujuh aspek kebijakan yang harus dipersiapkan oleh negara.

#### Penetapan Wilayah Pertahanan Siber

Kebijakan ini berkaitan dengan penentuan perimeter atau ruang lingkup negara yang asetnya dianggap sebagai bagian dari pertahanan siber. Penetapan dilakukan berdasarkan definisi dari pertahanan siber yang disepakati oleh para pemangku kepentingan. Definisi ini akan melahirkan sejumlah indikator yang dijadikan sebagai acuan dalam menentukan parameter dimaksud (Raffaele Bolla et al., 2018). Minimal seluruh aset yang berada di dalam wilayah Kementerian Pertahanan dan Militer akan menjadi bagian dari perimeter dimaksud.

#### Identifikasi Aset Vital dan Strategis Sektor Pertahanan

Kebijakan ini berkaitan dengan penentuan aset mana saja di dalam wilayah pertahanan siber yang dianggap vital dan sangat penting. Biasanya aset tersebut akan dikalsifikasikan berdasarkan tingkat kepentingannya. Aset yang dimaksud dapat berupa perangkat keras, perangkat lunak, sistem informasi, basis data, konten, jaringan, sentra komputasi, pusat komando, dan fasilitas maupun sarana prasarana lainnya (Raffaele Bolla et al., 2018; Carvalho, 2015).



Klasifikasi terhadap aset ini akan sangat menentukan tingkat perlindungan yang diberikan terhadapnya.

#### Asesmen Kekuatan dan Kelemahan Institusi Pertahanan

Kebijakan ini berkaitan dengan proses analisis mendalam terhadap kekuatan dan kelemahan dari aset vital dan strategis yang ada dalam teritori pertahanan siber. Untuk mengetahuinya perlu dilakukan proses seperti audit keamanan, *penetration test*, *vulnerabilities analysis*, dan lain sebagainya (Al-Khurafi & Al-Ahmad, 2016; Borah, 2015). Temuan dari proses ini menjadi bagian penting untuk mengetahui dalam aspek apa saja aset terkait harus dilindungi.

#### Analisa Risiko Dampak Serangan pada Hanneg dan Kamnas

Kebijakan ini berkaitan dengan analisa risiko terhadap aset vital dan strategis yang telah ditetapkan. Sebagaimana sebuah asesmen risiko, fokus analisis adalah pada probabilitas aset terkait akan diserang via siber, dan eksposur dampak yang dihasilkannya. Semakin tinggi probabilitas dan eksposur terhadap sebuah aset, akan semakin tinggi tingkat perlindungan dan biaya yang dialokasikan untuk mengamankannya (Romanosky et al., 2019).

#### Adopsi Standar dan Pengembangan Strategi Hanneg

Kebijakan ini berkaitan dengan persyaratan bagi aset yang telah ditetapkan untuk dikelola dengan menggunakan standar *best practices* terkait dengannya. Standar yang dimaksud tidak saja berkaitan dengan kualitas aset yang dimiliki, namun berhubungan pula dengan cara mengelolanya. Sifat adopsi standar ini adalah *mandatory*, dimana jika tidak dilakukan oleh pemilik aset maka akan ada konsekuensi hukum yang harus dihadapi (Lubua & Pretorius, 2019).

### Implementasi Tata Kelola Sistem Pertahanan Siber Institusi

Kebijakan ini berkaitan dengan tata cara dan keharusan mengelola seluruh sistem pertahanan siber dalam wilayah dan perimeter yang telah ditetapkan secara holistik dan komprehensif. Mengelola seluruh aset penting dan strategis yang ditetapkan tidak boleh dilakukan secara sporadis karena sifatnya yang saling terhubung satu dan lainnya (Eldem, 2020; Geers, 2012).

### Audit Sistem Keamanan Siber pada Sektor Pertahanan dan Militer

Kebijakan ini berkaitan dengan proses untuk memastikan bahwa seluruh aset vital dan strategis dalam wilayah atau perimeter pertahanan siber dikelola dengan baik, sesuai dengan standar yang telah ditetapkan (Anderson, 1994; Szczepaniuk et al., 2020). Hasil audit harus segera ditindaklanjuti agar seluruh kendali atau kontrol yang dibutuhkan untuk membuat sistem bekerja secara efektif benar-benar bekerja dengan baik.

### Domain Kebijakan Pertahanan Siber (Cyber Defense)

Walaupun aset-aset vital dan strategis dalam wilayah perimeter pertahanan siber telah dilindungi dengan sebaik-baiknya, tetap saja serangan dapat diluncurkan oleh berbagai pihak dari dalam maupun luar negeri. Jika serangan tersebut terjadi, negara harus mampu mempertahankannya agar tidak merusak situasi dan kondisi negara yang dapat berakibat fatal terhadap pertahanan dan keamanan nasional. Oleh karena itulah maka dibutuhkan sejumlah kebijakan untuk menjamin terciptanya kekuatan pertahanan yang kuat dan kokoh.

### Pemantauan Situasi dan Kondisi Perimeter Pertahanan Siber Nasional

Kebijakan ini berkaitan dengan kebutuhan melakukan pemantauan penuh selama 24/7 terhadap aset siber penting dan strategis dalam perimeter

pertahanan negara. Melalui proses *monitoring* trafik internet misalnya, atau lalu lintas data maupun informasi di dalam perimeter, dapat diketahui apakah semuanya berjalan secara normal atau ada hal-hal mencurigakan yang perlu diperhatikan (Bhardwaj et al., 2016; Sun et al., 2018).

#### Deteksi Aktif Keberadaan Serangan Siber dalam Teritori Hanneq

Kebijakan ini berkaitan dengan proses mendeteksi adanya serangan siber dalam wilayah perimeter pertahanan negara. Serangan siber dapat terlihat dari adanya anomali terhadap suatu aktivitas yang terjadi dalam sebuah sistem komputasi (Eric Talbot Jensen, 2012; Zou et al., 2021). Melalui kajian mendalam via forensik digital misalnya, dapat disimpulkan telah terjadi atau tidaknya serangan yang membahayakan negara sehingga harus disiapkan “perisai digital” untuk menahan kehadirannya.

#### Penetapan Formal Kejadian Serangan Siber pada Institusi Pertahanan

Kebijakan ini berkaitan dengan penetapan formal secara cepat berdasarkan hasil identifikasi dan investigasi terhadap adanya serangan yang membahayakan bagi pertahanan negara. Penetapan formal diperlukan karena serangan yang terjadi bukan sekedar insiden biasa, tapi dinilai berbahaya bagi pertahanan negara (Dinstein, 2012; Rosenfield, 2009). Alasan lainnya perlunya ada penetapan formal ini adalah agar dapat dijalankan protokol atau prosedur khusus untuk menanganinya (*incident response procedure*).

#### Pemilihan dan Penerapan Strategi Respon Serangan Siber pada Pertahanan Negara

Kebijakan ini berkaitan dengan keputusan untuk memilih dan menerapkan model strategi untuk merespon terhadap serangan yang terjadi. Memang dalam kenyataannya proses ini terjadi sangat cepat (*split of second*), namun tetap dibutuhkan keberadaannya untuk mendukung mobilisasi sumber

daya penting yang dibutuhkan untuk bertahan – agar serangan tidak berhasil merusak atau membahayakan negara dan keamanan nasional (Van der Kleij et al., 2017; West-Brown et al., 2003).

#### Pengumpulan Fakta dan Bukti Forensik Peristiwa Serangan Siber

Kebijakan ini berkaitan dengan pengumpulan fakta yang diperlukan terkait dengan serangan yang dilakukan. Tujuan utamanya adalah untuk mencari tahu siapakah pihak yang bertanggung jawab terhadap kejadian dan apakah motivasinya (Chiluwa & Samoilenko, 2019; Mandia et al., 2003). Kajian terhadap fakta ini juga bertujuan untuk mengetahui tingkat kerentanan yang ada pada sistem, sehingga dapat dilakukan sejumlah usaha untuk memperbaikinya.

#### Pemulihan Situasi dan Kondisi pada Keadaan Semula

Kebijakan ini berkaitan dengan proses pemulihan situasi dan kondisi pasca serangan berhenti dan diselesaikan. Tidak selalu semua usaha pertahanan berhasil menghadang serangan yang ada. Kecil atau besar, biasanya terjadi kerusakan pada sistem yang menjadi target serangan. Setelah serangan berlalu, situasi dan kondisi aset dimaksud harus dipulihkan (*resilience*). Tujuan akhirnya adalah agar aset dapat berfungsi dan dipergunakan kembali sebagaimana seharusnya (Carías et al., 2020).

#### Pemutakhiran Kualitas Pertahanan Siber Pasca Serangan dan Pemulihan

Kebijakan ini berkaitan dengan perbaikan sistem setelah atau pasca serangan dilakukan. Berhasil atau tidaknya serangan tersebut, pasti akan banyak hal yang menjadi pembelajaran. Jika serangan berhasil ditangkal, kewaspadaan harus ditingkatkan – karena biasanya pihak lawan akan mencari jalan lain sebagai target dan modus. Sementara jika serangan berhasil, maka selain pemulihan, perlu dilakukan perbaikan terhadap aset yang ada agar di kemudian hari hal serupa tidak menimpa sistem terkait (Gisladdottir et al., 2017).

### Domain Kebijakan Penyerangan Siber (Cyber Offense)

Konteks penyerangan dalam dunia siber sering menjadi perdebatan, apalagi jika dihubungkan dengan filosofi pertahanan negara berbasis *active defense* atau *total defense*. Dalam konteks ancaman atau serangan siber, ada dua alasan besar aktivitas ini harus dikelola dan diterapkan. Alasan pertama adalah ketika serangan bertubi-tubi dilakukan tanpa henti oleh mesin/komputer maupun manusia terhadap aset teknologi dalam perimeter pertahanan negara. Cara satu-satunya adalah melumpuhkan mesin komputer, sumber daya, maupun pihak yang aktif melakukan serangan tanpa henti. Tanpa dilakukan serangan balik, mustahil agitasi tersebut akan berakhir. Alasan kedua adalah karena adanya informasi intelijen yang mensinyalir adanya rencana melakukan serangan siber pada saat tertentu, sehingga harus dilakukan tindakan pencegahan terhadapnya. Tentu saja tindakan pencegahan ini akan bermuara pada penyerangan atau pelumpuhan pihak-pihak yang menjadi ancaman tersebut.

### Pengerahan Intelijen Pertahanan Siber

Kebijakan ini berkaitan dengan aktivitas pencarian informasi secara diam-diam, terutama dengan mendengarkan kegiatan *underground*, untuk memastikan tidak ada rencana dari pihak manapun untuk menyerang Indonesia melalui siber. Biasanya kegiatan intelijen ini dilakukan dengan cara masuk ke *dark-net* atau *deep-web* untuk berinteraksi dengan berbagai pihak bawah tanah. Kegiatan *threat intelligence* merupakan salah satu cara untuk mencegah atau mengantisipasi terjadinya serangan siber ke suatu negara (Griffioen et al., 2020; Keim & Mohapatra, 2019).

### Penetapan Situs Entitas Target Serangan Siber

Kebijakan ini berkaitan dengan penentuan sekaligus penetapan aset, entitas, atau sumber daya mana yang akan dijadikan target untuk diserang dan/atau dilumpuhkan. Mekanisme penetapan terkait harus dilakukan secara hati-hati dan rahasia agar tidak tercium oleh intelijen lawan. Target yang dijadikan sebagai obyekatif serangan pun harus dideskripsikan secara detil agar tidak terjadi kesalahan dalam mengeksekusinya (Perloff-Giles, 2018).

#### Analisis Kerawanan dan Kerentanan Target Serangan Siber

Kebijakan ini berkaitan dengan aktivitas analisis terhadap kelemahan situs yang dijadikan sebagai target penyerangan. Untuk melakukan kajian tersebut, perlu dilakukan sejumlah aktivitas seperti *profiling*, *fingerprinting*, *screening*, dan lain sebagainya – yang secara hukum formal bersifat “melanggar aturan” jika diketahui pihak yang diserang (Al-Khurafi & Al-Ahmad, 2016). Oleh karena itulah maka perlu dilakukan sejumlah langkah teknis yang *prudent* dan terukur untuk memastikan ditemukannya kerawanan dan kerentanan target tanpa yang bersangkutan mengetahuinya.

#### Penyusunan Skenario Strategi Penyerangan

Kebijakan ini berkaitan dengan pemilihan dan penyusunan skenario yang tepat untuk menyerang. Banyak hal yang perlu dipertimbangkan dalam konteks ini, terutama terkait dengan kebutuhan sumber daya dan besaran risiko yang dihadapi (Ahn et al., 2015). Perlu diperhatikan bahwa tidak semua serangan akan membuahkan hasil yang diinginkan, sehingga perlu disiapkan berbagai alternatif skenario apabila strategi utama gagal mencapai hasil.

### Eksekusi Serangan Siber

Kebijakan ini berkaitan dengan keputusan dan perintah untuk mengeksekusi serangan siber ke target yang telah ditetapkan. Seluruh skenario yang telah disusun dan disetujui, dengan didukung oleh sumber daya komputasi yang diperlukan, dijalankan dengan target sasaran dan level kerusakan yang telah ditetapkan. Tim *red* yang dibentuk untuk menyerang juga ditetapkan dan diberikan tugasnya masing-masing (Perloff-Giles, 2018; Saltzman, 2013).

### Penghapusan Jejak dan Penyangkalan

Kebijakan ini berkaitan dengan kenyataan bahwa aksi menyerang secara terencana dalam dunia siber dapat dianggap sebagai “*the act of war*” – atau tindakan memicu peperangan. Oleh karena itulah maka diperlukan usaha untuk melakukan penghapusan jejak digital dan penyangkalan apabila ada pihak yang menuduh terjadinya aktivitas penyerangan. Kedua usaha yaitu penghapusan atau penyangkalan dapat dikombinasikan menjadi sebuah aktivitas pengalihan, sehingga pihak yang diserang salah menuduh entitas yang melakukan serangan karena adanya jejak yang difabrikasi (McGhee, 2016; Saltzman, 2013).

### Kajian Efektivitas Serangan dan Langkah Lanjut Aktivitas Siber

Kebijakan ini berkaitan dengan analisis terhadap efektivitas serangan yang diluncurkan. Efektif atau tidaknya penyerangan ditentukan oleh tercapainya obyektif yang diinginkan termasuk besarnya dampak yang terjadi pada lawan. Seandainya serangan gagal pun perlu dilakukan perhitungan terhadap kerugian yang diderita, dan dipelajari pula kesalahan yang dilakukan sebagai bahan pembelajaran di kemudian hari agar jika usaha serupa dilakukan tidak mengalami kegagalan kembali (Truong et al., 2020).

Walaupun makna perang siber atau *cyber warfare* masih diperdebatkan, namun keberadaannya tidak dapat disangkal karena adanya bukti penyerangan yang dilakukan *state actor* maupun *non-state actor* setiap detiknya. Oleh karena itulah maka disadari atau tidak, dideklarasikan atau tidak, perang siber telah, akan, dan terus terjadi di masa mendatang. Mengingat bahwa bentuk perang apapun pasti membutuhkan dukungan sumber daya, maka perlu adanya sejumlah kebijakan terkait dengannya.

#### Pengembangan Efek Gentar Pertahanan Siber Nasional

Kebijakan ini berkaitan dengan Kebijakan ini berkaitan dengan pembentukan *cyber deterrence*. Pada model peperangan maya dan virtual, *cyber deterrence* memegang peranan sangat penting. Contohnya adalah peretas China dan Eropa Timur sangat ditakuti dalam hal penyerangan, sementara negara Israel dan Estonia sangat dihormati dalam hal pertahanan (Beidleman, 2009; Wilner, 2020). Indonesia harus memiliki strategi agar menjadi negara yang memiliki efek gentar di bidang siber sebagai bagian terintegrasi dari pertahanannya.

#### Pelaksanaan Diplomasi Pertahanan Siber Nasional

Kebijakan ini berkaitan dengan diplomasi siber, mengingat tidak semua peperangan dapat dimenangkan. Dalam sejumlah situasi perang siber, perlu pula dilakukan usaha diplomasi. Perang bukanlah suatu tujuan, namun jalan mencapai tujuan apabila seluruh pilihan telah tertutup. Oleh karena itulah, keberadaan *cyber diplomacy* sangatlah dibutuhkan jika berdasarkan asesmen terlihat bahwa perang akan sulit dimenangkan karena kuatnya pihak lawan (Barrinha & Renard, 2017; Hamonangan & Assegaff, 2020).



### Pernyataan Perang Siber Resmi dan Terbuka

Kebijakan ini berkaitan dengan pendeklarasian terjadinya perang karena hampir tidak ada perang fisik moderen yang tidak diikuti oleh perang siber. Tidak jarang pemerintah sebuah negara mendeklarasikan perang siber terhadap pihak lain sebagaimana dilakukan pemerintah Korea Utara, Rusia, maupun China. Pernyataan ini berfungsi untuk meningkatkan *awareness* negara sekaligus untuk menjalankan protokol perang khusus yang memperbolehkan dilakukannya sejumlah aktivitas spesifik (Borah, 2015; Lundbohm, 2017).

### Penetapan Strategi Perang Siber dan Mobilisasi Sumber Daya

Kebijakan ini berkaitan dengan pemilihan dan penetapan strategi perang siber yang dipilih, termasuk penentuan sumber daya yang dibutuhkan. Dalam pelaksanaannya kerap dilakukan mobilisasi terhadap sejumlah aset penting negara karena sifatnya yang penting dan genting. Sumber daya dimaksud termasuk manusia sebagai *“the man behind the gun”* atau yang kerap disebut sebagai pasukan siber, yang akan menjadi tulang punggung negara dalam perang (Geers, 2010; Milevski, 2016).

### Pengerahan dan Koordinasi Aliansi Tentara Siber Nasional

Kebijakan ini berkaitan dengan rekrutmen dan pelibatan berbagai institusi maupun komunitas untuk bergabung sebagai “tentara siber nasional” yang memiliki tugas utama memenangkan peperangan. Aliansi dibutuhkan mengingat negara memiliki sumber daya yang terbatas, sementara pihak lawan melakukan hal yang sama untuk memperkuat armadanya (Setiawan, 2018).

### Pelaksanaan Peperangan Semesta Siber

Kebijakan ini berkaitan dengan tata kelola proses peperangan itu sendiri, dari mulai perencanaan, pengorganisasian, persiapan, pengerahan,

pelaksanaan, pengawasan, dan penilaian. Sebagaimana sebuah perang fisik, akan banyak “korban” dalam perang siber, yang dapat secara langsung maupun tidak langsung mengganggu kestabilan negara dan keamanan nasional (Kanniainen, 2019; Rosenfield, 2009)cyb. Tidak ada *invisible hand* dalam perang siber, karena semuanya harus benar-benar dirancang dan dieksekusi dengan baik. Kemenangan hanya dapat diperoleh apabila strategi dan taktik yang dipergunakan benar-benar tepat dan efektif.

### Pernyataan Akhir Peperangan Siber

Kebijakan ini berkaitan dengan penetapan telah berakhirnya perang, sehingga seluruh aktivitas mobilisasi sumber daya utama dan pendukungnya dapat dihentikan. Sebagaimana disampaikan terdahulu, tidak semua peperangan diakhiri dengan kemenangan. Dalam konteks perang siber, kalah atau menang bersifat relatif, karena sifatnya yang *intangible* dan multi-dimensi. Inti yang paling penting adalah mendapatkan *lessons learnt* melalui peristiwa yang dialami bersama sebagai bahan pembelajaran di kemudian hari dalam usahanya mempertahankan pertahanan negara di arena siber (Dinstein, 2012; Lehto, 2015).

### Ragam Kebijakan Pendukung Tata Kelola Pertahanan Siber

Domain terakhir berisi kumpulan kebijakan pendukung untuk mengelola pertahanan siber sebagaimana telah dipaparkan sebelumnya. Domain terakhir ini pada dasarnya terdiri dari tiga kelompok utama, yaitu: *people*, *process*, dan *technology* (Calder, 2013; H. Hu et al., 2018)

Manusia adalah komponen terpenting dalam ekosistem kebijakan pertahanan siber. Mereka adalah pihak yang merencanakan, mengelola, dan mengawasi pelaksanaannya. Sejumlah kebijakan terkait dengan superstruktur, pasukan siber, tim insiden, *triple helix*, dan lain sebagainya perlu disusun agar jelas pihak-pihak yang memiliki akuntabilitas, wewenang, dan tanggung jawab sesuai dengan peran dan fungsinya masing-masing. Berdasarkan sejumlah

studi, manusia dianggap sebagai komponen utama dan terpenting dalam ekosistem pertahanan siber (Majid, 2019). Pada saat yang sama, manusia juga dianggap sebagai *“the weakest link”* dalam rantai jejaring siber.

Proses berkaitan dengan seluruh aktivitas dan prosedur terkait dengan pengelolaan dan manajemen berbagai komponen yang perlu digerakkan dan diatur dalam ekosistem pertahanan siber. Aktivitas seperti kolaborasi, kooperasi, komunikasi, interaksi, diplomasi, dan protokol – termasuk pemutakhiran peraturan – adalah kegiatan rutin maupun *ad-hoc* yang akan mewarnai proses mengembangkan dan menjalankan pertahanan siber (Geers, 2010).

Pada level negara, berbagai standar *good practices* maupun *best practice* harus diterapkan untuk memastikan berjalannya proses tata kelola yang efektif, efisien, dan terkendali dengan baik.

Teknologi merupakan perangkat atau piranti yang dibutuhkan untuk membangun serta mengembangkan pertahanan siber itu sendiri. Serangkaian teknologi dimaksud termasuk infrastruktur, jaringan, perangkat keras, perangkat lunak, *data center*, *internet exchange*, dan lain sebagainya. Agar seluruh perangkat tersebut dapat saling berkomunikasi, perlu pula ditetapkan spesifikasi, konvensi, standar, dan model interoperabilitas yang dibutuhkan (Cebula, 2010, Sun, 2018). Selain itu perlu pula dirancang hal-hal terkait dengan arsitektur maupun topologi teknologi yang dibangun.

Domain kedelapan ini berpotensi menjadi entitas dimana akan banyak disusun, diundangkan, dan dimutakhirkan berbagai kebijakan terkait dengan pertahanan siber. Sifat dari masing-masing kebijakan adalah modular, sehingga dapat menjamin adanya agilitas dalam pengembangan kebijakan. Hal ini sesuai dengan kenyataan bahwa dalam dunia nyata, perkembangan teknologi jauh melampaui kecepatan pembuatan regulasi atau kebijakan. Oleh karena itulah maka seluruh kebijakan pada domain ini harus dilakukan secara modular – independen tapi memiliki interkoneksi (Mueller, 2019).

#### KERANGKA KEBIJAKAN PERTAHANAN SIBER NASIONAL

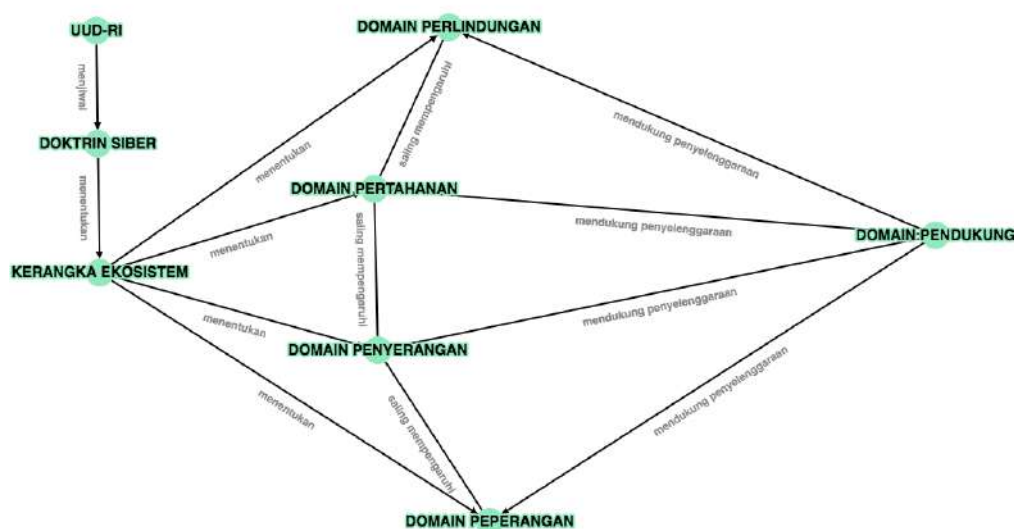




Gambar 4. 94 Kerangka Kebijakan Pertahanan Siber Nasional

Sumber : Kerangka Kebijakan Pertahanan Siber Nasional  
(hasil pengolahan data oleh peneliti)

Strategi pengembangan kebijakan adalah pendekatan yang dipergunakan dalam mendefinisikan, menyusun, menetapkan, dan mengembangkan kebijakan agar dapat secara dinamis menyesuaikan diri dengan perubahan (*agile*). Oleh karena itulah maka perlu dikembangkan struktur anatominya agar mudah mengembangkannya.



Gambar 4. 95 Profil dan Kapabilitas Pertahanan Siber Negara

Sumber : Profil dan Kapabilitas Pertahanan Siber Negara

(hasil pengolahan data oleh peneliti)

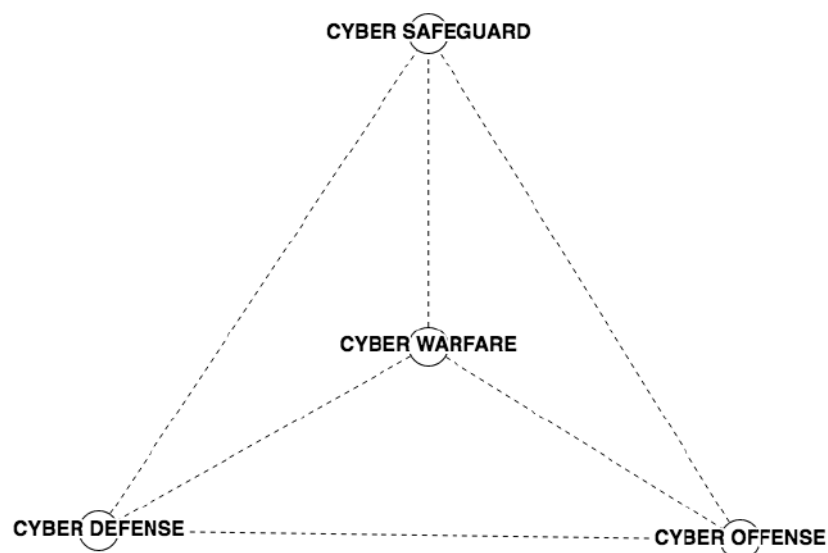
Sebagaimana dipahami bersama, UUD-RI adalah konstitusi paling tinggi di Indonesia, sehingga keberadaannya dikategorikan sebagai kebijakan nasional, karena mewarnai seluruh peraturan yang ada di Indonesia. Dengan semangat pencapaian tujuan negara yang ditetapkan secara eksplisit dalam

UUD 1945, maka perlu dikembangkan Doktrin Siber termutakhir yang sesuai dengan era digital. Doktrin Siber Pertahanan Nasional ini berada pada tataran kebijakan umum, karena posisinya sebagai penggarisan ketentuan-ketentuan yang bersifat garis besar dalam rangka pelaksanaan tugas umum pemerintahan serta pembangunan sebagai pelaksanaan UUD 1945, ketetapan MPR ataupun undang undang untuk mencapai tujuan nasional. Berdasarkan kedua hal tersebut, maka dikembangkan strategi kebijakan, yaitu salah satu kebijakan pelaksanaan secara hirarki dibentuk setingkat menteri, gubernur, walikota/bupati berbentuk surat keputusan yang mengatur tata laksana kerja dan juga segala sesuatu yang berhubungan dengan sumber daya manusia. Strategi diartikan sebagai serangkaian sasaran organisasi yang kemudian mempengaruhi penentuan tindakan komprehensif dalam mencapai sasaran yang telah ditentukan ataupun alat dengan tujuan yang akan dicapai. Pada tingkatan teratas dalam strategi adalah penggambaran terhadap ekosistem pertahanan siber nasional yang dijadikan sebagai bahasa atau panduan bersama dalam bernegara.

#### Rangkaian Proses pada Empat Domain Siber

Belajar dari sejumlah peristiwa serangan siber di masa lalu, dapat disimpulkan terdapat empat domain kapabilitas yang harus dikuasai oleh para pasukan siber. Keempat domain kapabilitas ini berasal dari empat proses utama yang dibutuhkan dalam berbagai kondisi. Adapun keempat domain tersebut adalah: (i) Domain Perlindungan; (ii) Domain Pertahanan; (iii) Domain Penyerangan; dan (iv) Domain Peperangan. Domain Perlindungan berkaitan dengan serangkaian proses untuk meningkatkan posisi keamanan dan ketahanan aset siber strategis yang berkaitan erat dengan pertahanan negara. Dengan ditingkatkannya status tersebut, maka akan mempersulit pihak lawan dalam melakukan penetrasi, akses, atau kerusakan pada aset digital yang ada (Kraus, 2014). Domain Pertahanan terkait dengan kemampuan dalam menghadapi berbagai serangan yang terjadi agar sedapat mungkin tidak merusak, mengganggu, atau melumpuhkan aset strategis yang dimiliki. Sistem pertahanan ini tentu saja akan membutuhkan sejumlah strategi dan kemampuan optimal

(Burton, 2015). Domain Penyerangan berhubungan dengan kapabilitas dalam melakukan agitasi, penetrasi, dan pelumpuhan sistem lawan. Kemampuan ini diperlukan mengingat begitu banyaknya serangan yang dilakukan oleh mesin, bukan manusia – sehingga hanya dengan penyerangan balik maka sistem dapat dihentikan (Arts, 2018). Dan domain peperangan memiliki relasi dengan kemampuan dalam melakukan perang siber dengan segala karakteristiknya. Melalui kemampuan ini diharapkan dapat membantu negara dalam memenangkan pertempuran maupun peperangan di ruang siber (Kassab, 2019).



Gambar 4. 96 Empat Dimensi Ruang Siber

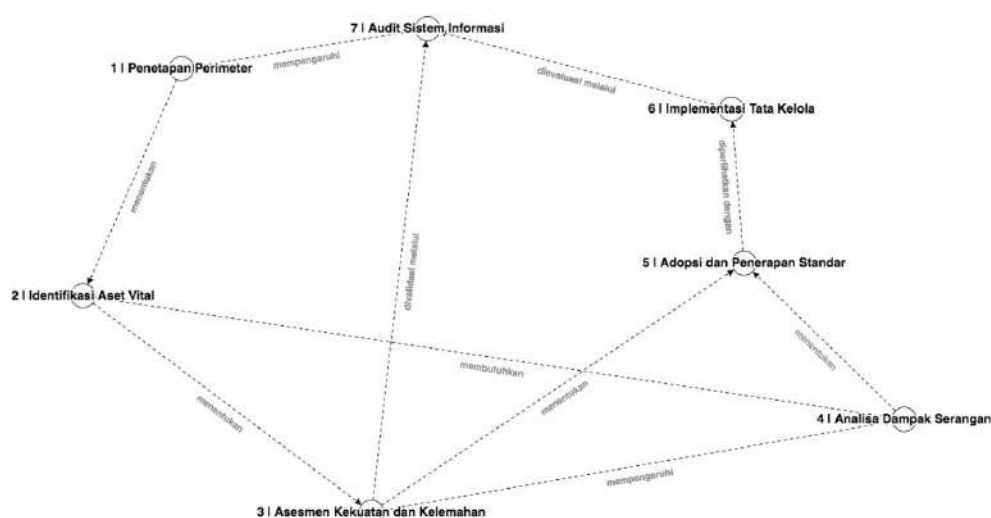
Sumber : Empat Dimensi Ruang Siber (hasil pengolahan data oleh peneliti)

#### Rangkaian Proses Perlindungan Siber (*Cyber Safeguarding*)

Pada domain ini terlihat hubungan keterkaitan antara satu kebijakan dengan lainnya dalam konteks perlindungan siber. Walaupun secara konseptual



ketujuh kebijakan dasar yang perlu dimiliki bersifat sekuensial, namun ada beberapa kebijakan yang saling memiliki relasi yang sangat dekat, seperti:



Gambar 4. 97 Relasi pada Domain Kebijakan Perlindungan Siber

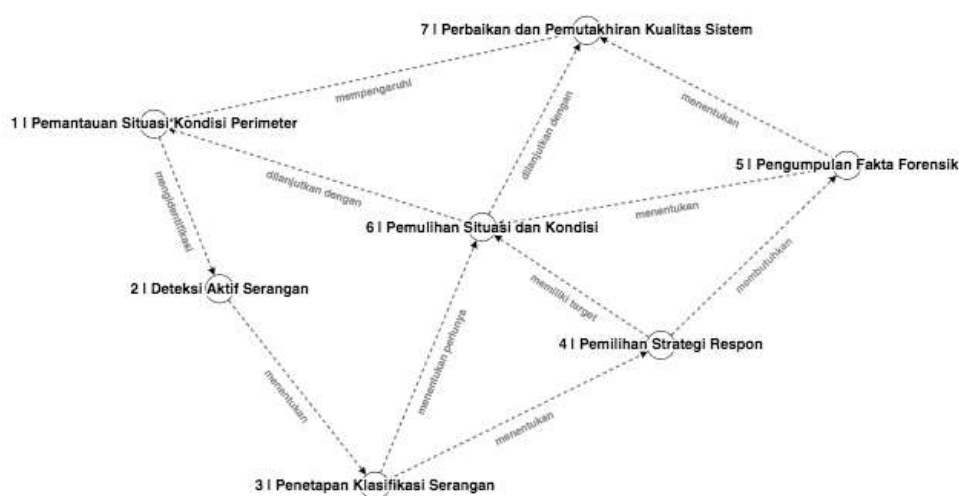
Sumber : Hasil pengolahan data oleh peneliti

1. Kebijakan terkait dengan identifikasi aset vital akan membutuhkan proses lebih lanjut yaitu analisis dampak serangan, karena keduanya berkaitan dengan eksposur *impact* yang terjadi apabila terjadi sesuatu dengan aset dimaksud;

2. Kebijakan terkait dengan asesmen kekuatan dan kelemahan akan menentukan adopsi dan pemilihan standar seperti apa yang akan ditetapkan untuk diterapkan, karena jenisnya ditentukan oleh hasil kajian kelemahan aset; dan
3. Kebijakan terkait dengan asesmen kekuatan dan kelemahan akan divalidasi dengan cara melakukan audit secara lengkap dan menyeluruh.

### Rangkaian Proses Pertahanan Siber (*Cyber Defense*)

Pada domain ini terlihat hubungan keterkaitan antara satu kebijakan dengan lainnya dalam konteks pertahanan siber. Walaupun secara konseptual ketujuh kebijakan dasar yang perlu dimiliki bersifat sekuensial, namun ada beberapa kebijakan yang saling memiliki relasi yang sangat dekat, seperti:



Gambar 4. 98 Relasi pada Domain Kebijakan Pertahanan Siber

Sumber : Hasil pengolahan data oleh peneliti

1. Kebijakan terkait penetapan klasifikasi serangan menentukan perlunya langkah-langkah spesifik dalam pemulihan situasi dan kondisi pasca serangan;
2. Kebijakan terkait pemilihan strategi respon juga akan sangat menentukan model pemulihan situasi dan kondisi yang dibutuhkan;
3. Kebijakan terkait pengumpulan fakta forensik pasca serangan juga berpengaruh langsung terhadap pendekatan langkah-langkah pemulihan yang diambil; dan
4. Kebijakan terkait pemulihan pasca serangan akan menjadi masukan untuk memutakhirkan proses pemantauan untuk memastikan tidak akan terjadi lagi peristiwa yang sama di kemudian hari.

### Rangkaian Proses Penyerangan Siber (Cyber Offense)

Pada domain ini terlihat hubungan keterkaitan antara satu kebijakan dengan lainnya dalam konteks penyerangan siber. Walaupun secara konseptual ketujuh kebijakan dasar yang perlu dimiliki bersifat sekuensial, namun ada beberapa kebijakan yang saling memiliki relasi yang sangat dekat, seperti:



Gambar 4. 99 Relasi pada Domain Kebijakan Penyerangan Siber

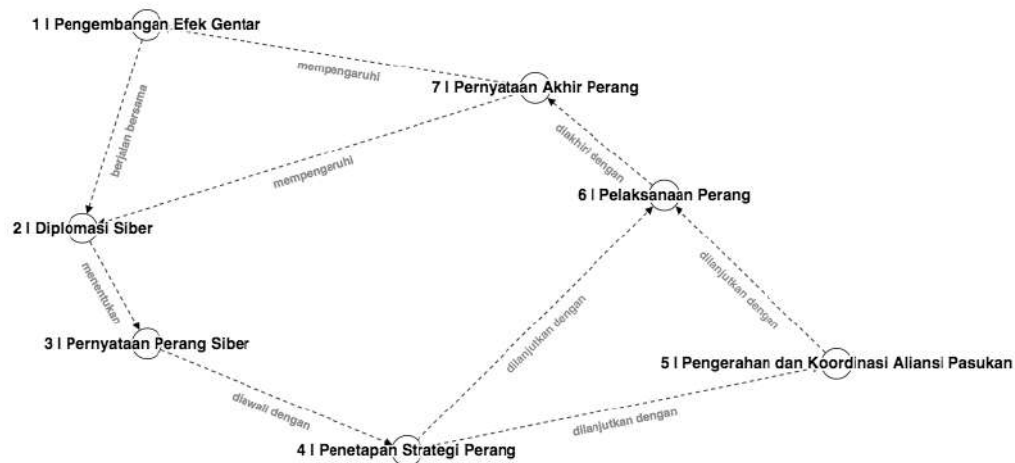
Sumber : Hasil olahan data oleh peneliti

1. Kebijakan terkait penyusunan strategi penyerangan harus memikirkan cara penghapusan jejak dan penyangkalan di kemudian hari, agar tidak terjadi serangan balasan; dan
2. Kebijakan terkait eksekusi serangan siber akan selalu dibarengi sekaligus diawasi oleh intelijen siber.

### Rangkaian Proses Peperangan Siber (Cyber Warfare)

Pada domain ini terlihat hubungan keterkaitan antara satu kebijakan dengan lainnya dalam konteks peperangan siber. Walaupun secara konseptual

ketujuh kebijakan dasar yang perlu dimiliki bersifat sekuensial, namun ada beberapa kebijakan yang saling memiliki relasi yang sangat dekat, seperti:



Gambar 4. 100 Relasi pada Domain Kebijakan Peperangan Siber

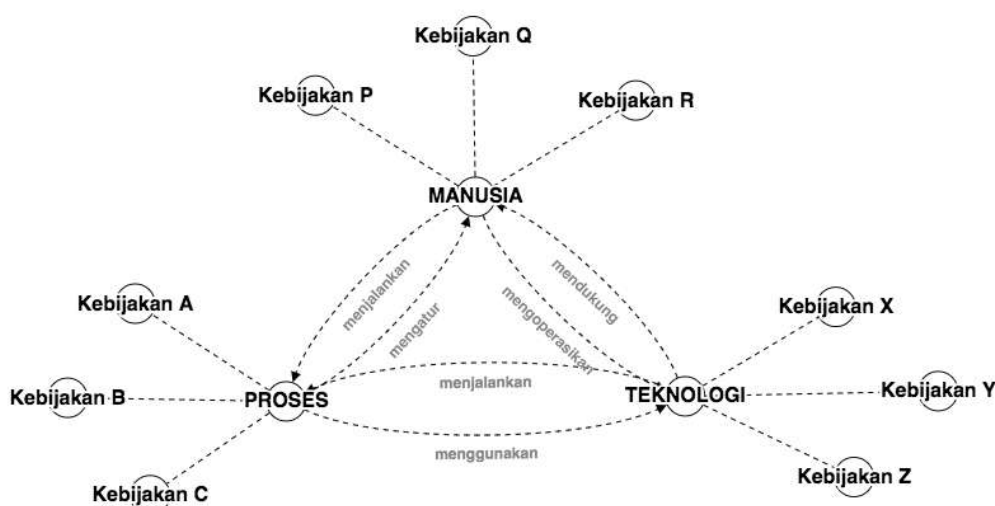
Sumber : Hasil pengolahan data oleh peneliti

1. Kebijakan terkait penetapan strategi perang akan dilanjutkan dengan pelaksanaan perang itu sendiri; dan
2. Kebijakan terkait pernyataan akhir perang berpengaruh terhadap konten diplomasi siber yang harus disampaikan.

#### Rangkaian Proses Pendukung Tata Kelola Pertahanan Siber

Domain ini adalah yang paling banyak menghasilkan kebijakan, karena di dalamnya menyangkut berbagai hal terkait dengan *people*, *process*, dan

*technology* – atau meliputi berbagai aspek terkait dengan infrastruktur dan suprastruktur. Masing-masing sub-domain manusia, proses, atau teknologi akan melahirkan berbagai kebijakan terkait dengannya. Untuk memastikan tidak adanya tumpang tindih atau tambal sulam, maka proses keselarasan (alignment) dilakukan pada tingkatan ketiga sub-domain. Dengan demikian paka kebijakan-kebijakan yang ada di bawahnya tidak akan bertabrakan satu dan lainnya, sekaligus mengurangi kompleksitas yang ada.



Gambar 4. 101 Relasi antar Komponen pada Domain Kebijakan Pendukung Tata kelola Pertahanan Siber

Sumber : Hasil pengolahan data oleh peneliti

Perlu dicatat bahwa keempat domain utama yaitu Perlindungan Siber, Pertahanan Siber, Penyerangan Siber, dan Peperangan Siber merupakan empat domain yang lebih lengkap serta holistik terutama jika dibandingkan dengan

model US Cyber Command yang hanya bertumpu pada tiga kapabilitas yaitu: CND, CAN, dan CNE (Efthymiopoulos, 2019).

#### Pasukan Siber dan Kompetensinya

Trafik pengawasan terhadap dunia siber memperlihatkan terjadinya jutaan serangan antar negara per-harinya. Fenomena ini memperlihatkan bagaimana ancaman siber membayangi setiap negara tanpa kecuali. Tidak sedikit dari serangan tersebut yang berdimensi serius, karena sifatnya yang cenderung merusak dan membahayakan pertahanan negara. Serangan yang ditujukan untuk melumpuhkan bahkan menghancurkan sistem komputasi yang berkaitan dengan infrastruktur vital nasional dapat dikategorikan sebagai bentuk deklarasi perang. Menghadapi kemungkinan terburuk ini, negara perlu memiliki pasukan siber yang tangguh untuk mengatasinya (Setiawan, 2018). Penelitian ini fokus pada identifikasi kemampuan sumber daya manusia yang diperlukan untuk menghadapi perang siber. Metodologi yang dipergunakan adalah perbandingan studi terkait proses dan kapabilitas pasukan siber di berbagai negara dunia. Hasilnya adalah teridentifikasinya empat domain utama kapabilitas proses perang siber yang harus dimiliki oleh pasukan siber di dunia, yaitu: perlindungan siber, pertahanan siber, penyerangan siber, dan peperangan siber. Terlepas dari berbagai definisi perang siber yang mengemuka, kenyataannya adalah terjadinya percobaan serangan per detiknya yang melibatkan berbagai pihak antar negara (Watts, 2012). Selain mencoba menyerang berbagai infrastruktur vital, cukup banyak pula yang mencoba melakukan serangan ke sektor pertahanan maupun militer. Fenomena ini terjadi tidak dengan sendirinya, karena berkaitan erat dengan tingginya dinamika global dalam berbagai sektor kehidupan manusia. Oleh karena itulah maka sejumlah negara telah membentuk pasukan atau tentara siber, yang tujuannya adalah melindungi negara dari kehancuran karena dipicu oleh serangan siber (Danet, 2019). Setiap negara membentuk pasukan sibernya dengan cara berbeda. Ada pasukan siber yang bersifat formal, sehingga menjadi angkatan keempat setelah angkatan darat, angkatan laut, dan angkatan udara. Namun banyak pula yang bersifat informal, karena berupa task force yang terdiri dari berbagai komponen komunitas dengan tugas khusus. Pasukan siber ini terdiri dari sejumlah individu dengan kemampuan khusus dan

unik, yang secara kolektif membentuk kapabilitas ketahanan terhadap serangan siber yang mengemuka.

#### Kapabilitas pada Domain Perlindungan

Organisasi yang berada dalam sektor pertahanan dan militer perlu memiliki pasukan siber dengan kapabilitas yang berkaitan dengan delapan proses utama (Rosenfield, 2009). Pertama dan utama adalah mendeklarasikan lingkungan atau perimeter yang harus dijaga (Geers, 2009). Dalam konteks peperangan siber, paling tidak sektor pertahanan negara dan militer harus menjadi fokus pertahanan dimaksud. Kedua terkait dengan proses mengidentifikasi aset mana saja yang memiliki peran penting dan strategis. Untuk menentukan tingkat atau nilai strategis, harus ditetapkan sejumlah indikator yang harus terpenuhi. Ketika berhubungan erat dengan kemampuan dalam mengkaji kekuatan dan kelemahan sistem atau aset digital strategis yang telah ditetapkan (Farwell, 2012). Pasukan siber harus memiliki kemampuan dalam melakukan aktivitas seperti penetration test maupun *vulnerability analysis*. Keempat berhubungan erat dengan kemampuan menganalisa dampak seandainya aset yang menjadi target perlindungan berhasil diretas atau diserang pihak lain. Pada tahapan ini harus dilakukan kajian kerugian berbasis ekonomi, politik, pertahanan, keamanan, dan sosial budaya. Tahap kelima adalah pengetahuan dan kemampuan dalam mengadopsi berbagai standar good practices dalam berbagai aspek, seperti misalnya: ISO27001 untuk keamanan informasi, ISO31000 untuk manajemen risiko, ISO38500 untuk IT governance, TOGAF untuk enterprise architecture, ITIL untuk IT service management, CMMI untuk system development, dan lain sebagainya (Gunduz, 2020; Srinivas, 2019). Keenam adalah kemampuan dalam meyakinkan terpenuhinya unsur tata kelola yang baik dalam menjalankan dan mengendalikan sistem pertahanan berbasis siber. Organisasi atau institusi terkait harus memiliki kemampuan strategis dan manajerial dalam menerapkan *good corporate IT governance* dalam konteks ini. Dan ketujuh yang merupakan proses terakhir adalah kemampuan mengaudit sistem teknologi informasi yang dimiliki, untuk memastikan kekokohan dan kehandalan sistem. Pasukan siber harus memiliki individu yang mampu



melakukan audit secara profesional, yang ditandai misalnya dengan kepemilikan sertifikat CISA (Certified Information System Auditor).

#### Kapabilitas pada Domain Pertahanan

Pada domain ini, cukup banyak kapabilitas dan kemampuan teknis yang dibutuhkan oleh organisasi atau institusi terkait, dimana harus dimiliki oleh pasukan siber secara kolektif. Pertama adalah kemampuan dalam melakukan pemindaian dan pengawasan secara 24/7 terhadap aset strategis. Sejumlah *tools*, perangkat keras, dan *software* aplikasi dibutuhkan untuk melakukan pemantauan ini. Keahlian yang dibutuhkan adalah membuat rules atau algoritma untuk mengkaji ada tidaknya anomali pada trafik jaringan dan internet dalam perimeter pertahanan negara (Crowther, 2018). Kedua adalah kapabilitas dalam mendeteksi terjadinya serangan, baik yang bersifat aktif maupun pasif. Tidak semua jenis serangan dapat terdeteksi oleh aplikasi atau software (Lilienthal, 2015). Dalam sejumlah kasus, pasukan siber harus memiliki pengetahuan mengetahui adanya pola serangan atau keanehan yang terjadi pada sistem. Ketiga adalah aktivitas untuk mengklasifikasikan jenis serangan. Tidak semua serangan berbahaya, namun cukup banyak yang berpotensi merusak dan destruktif (Mishra, 2013). Kategori serangan akan mempengaruhi tingkat kepentingan, kepentingan, dan pendekatan response yang dipilih. Keempat adalah kegiatan menjawab serangan yang terjadi dengan cara melakukan serangkaian aktivitas. Tujuan utamanya adalah memastikan serangan dapat diatasi dan aset strategis dapat diproteksi semaksimal mungkin. Kelima adalah kemampuan dalam melakukan forensik digital untuk mengetahui pihak yang melakukan serangan dan motivasinya. Keahlian melakukan forensik juga dibutuhkan untuk mendapatkan pemahaman penuh mengapa serangan berhasil dilakukan beserta modus skenarionya (Serketzis, 2019). Keenam berkaitan dengan aktivitas memulihkan sistem yang berhasil diserang, seandainya tindakan musuh tersebut berhasil membuat kerusakan. Pemulihan sistem hanya dapat dilakukan apabila berkumpul para ahli atau pakar yang memahami secara sungguh-sungguh karakteristik sistem yang diserang. Ketujuh adalah melakukan perbaikan serta penyempurnaan terhadap sistem agar tidak dapat lagi diserang

dengan cara yang sama di kemudian hari. Sejumlah kemampuan teknis dibutuhkan untuk memutakhirkan sistem dimaksud.

### Kapabilitas pada Domain Penyerangan

Sebagaimana disampaikan sebelumnya, pasukan siber harus mampu melakukan tindakan ofensif untuk menghentikan berbagai serangan berbasis mesin, seperti botnet atau model DDOS lainnya. Penyerangan dini juga dibutuhkan apabila ditemukan adanya rencana atau skenario musuh untuk melakukan serangan pada waktu tertentu (Eom, 2012). Tindakan antisipatif maupun reaktif ini membutuhkan sejumlah pengetahuan, keahlian, dan pengalaman. Pertama berkaitan dengan kemampuan dalam menjalankan aktivitas intelijen di dunia siber. Dalam konteks ini, diperlukan keahlian CTI atau Cyber Threat Intelligence untuk masuk ke dalam darknet mendengarkan berbagai diskursus oleh komunitas bawah tanah (Barde, 2020). Kedua adalah proses menetapkan target yang ingin menjadi sasaran serangan. Target yang ditetapkan haruslah jelas dan detil, dan obyektif kerusakan yang diinginkan haruslah didefinisikan sebelum serangan diluncurkan. Ketiga berkaitan dengan aktivitas analisis terhadap kelemahan dan kerentanan sistem yang ditargetkan. Melalui *penetration test* dan *vulnerability analysis*, pasukan siber dapat mengetahui titik lemahnya sistem lawan untuk dapat dieksploitasi dalam sebuah skenario perekaman (Keim, 2019). Keempat adalah mengembangkan strategi serangan yang efektif. Pada tahapan ini, seluruh individu dengan kemampuan beragam berdiskusi dan mengembangkan skenario ampuh bersama. Ahli yang dibutuhkan adalah yang memiliki kemampuan dalam melakukan *social engineering*, *digital identity theft*, *malware plantation*, *ransomware*, *cryptojacking*, dan lain sebagainya (Mouton, 2016; Huber, 2009). Kelima adalah proses melakukan serangan itu sendiri dengan mengeksploitasi kelemahan melalui eksekusi skenario yang telah disusun. Perlu dipahami bahwa dalam sejumlah kasus, penyerangan membutuhkan durasi waktu yang relatif panjang (Kuusisto, 2015). Pada tahapan ini seluruh potensi pasukan siber yang dimiliki harus dikerahkan sesuai perannya masing-masing. Keenam adalah tahap yang paling sulit, yaitu menghapus jejak. Serangan menjadi tidak berarti apabila tertinggal jejak digital yang dapat mengundang pembalasan. Oleh karena itulah pasukan siber harus dilengkapi dengan keterampilan melakukan penghapusan terhadap jejak digital. Dengan demikian maka risiko adanya serangan balik akan menjadi kecil karena minimnya informasi yang diperoleh pihak lawan. Ketujuh adalah

melakukan evaluasi terhadap hasil dari serangan yang dilakukan. Tidak semua serangan berhasil, dan belum tentu skenario ofensif yang dilakukan gagal. Inti dari evaluasi adalah belajar dari kesuksesan dan kegagalan untuk memperbaiki kinerja di kemudian hari (Ghafir, 2018).

#### Kapabilitas pada Domain Peperangan

Walaupun ada banyak definisi mengenai yang dimaksud dengan perang siber, namun keberadaanya tidak dapat dipungkiri. Paling tidak dalam setiap perseteruan atau konflik dua negara di era moderen ini selalu disertai dan diikuti dengan serangan siber (Rosenfield, 2009). Oleh karena itulah maka negara harus mempersiapkan pasukan sibernya untuk menghadapi perang siber yang singkat maupun berkepanjangan. Pertama berkaitan dengan kemampuan membangun dan mengembangkan fasilitas siber yang menimbulkan efek gentar bagi lawan. Efek gentar terkadang efektif dalam menghindari perang siber yang berkepanjangan dan melelahkan (Wilner, 2020; Lukasik, 2010). Banyak cara dapat dipergunakan untuk menimbulkan efek ini, seperti ditakutinya hackers setempat, canggihnya teknologi yang dipergunakan, militansinya komunitas bawah tanah, dan lain sebagainya. Kedua berhubungan dengan kemampuan pasukan siber dalam melaksanakan apa yang dimaksud dengan diplomasi siber. Tujuan diplomasi siber adalah untuk bernegosiasi dengan pihak lawan sebagai jalan terakhir untuk menghindari perang (Danca, 2015). Apabila gagal, maka terpaksa tahapan selanjutnya dilakukan. Ketiga terkait dengan dideklarasikannya perang siber oleh sebuah negara. Deklarasi ini diperlukan sebagai sinyal keseriusan pemerintah dan negara dalam menghadapi pilihan terakhir tersebut karena ada hak-haknya yang dilanggar. Pendeklarasian perang juga akan mengundang pihak-pihak yang bersimpati untuk membantu, terutama apabila negara terkait berada dalam situasi lemah (Powers, 2015). Keempat adalah penyusunan strategi pertempuran dan peperangan yang akan dipilih. Tentu saja strategi ini sangat berkaitan dengan ketiga domain terdahulu, yaitu perlindungan, pertahanan, dan penyerangan. Pasukan siber di sini harus terlibat secara kolektif dalam mengembangkan strategi yang tepat agar dapat memenangkan peperangan. Kelima adalah kemampuan dalam memobilisasi dan mengelola

pasukan serta tentara siber (Lancelot, 2020). Pasukan siber dapat terdiri dari komponen formal maupun informal. Keseluruhannya harus bersatu untuk membela negara. Keenam adalah peristiwa pertempuran dan peperangan itu sendiri, dimana di dalamnya terjadi berbagai aktivitas dinamis yang kerap tak terduga kejadiannya. Perang siber dapat terjadi dalam hitungan menit hingga bertahun-tahun, tergantung dari konteks yang dihadapi. Tujuan dari peperangan ini adalah memenangkan serangkaian pertempuran agar pada akhirnya nanti pihak lawan menyerah tanpa syarat (Valeriano, 2019). Ketujuh adalah situasi berakhirnya perang, yang ditandai dengan deklarasi usainya perang. Hasilnya dapat merupakan perjanjian perdamaian, atau gencatan senjata siber secara sementara.

#### Kapabilitas dan Kemampuan

Berdasarkan keseluruhan proses tersebut, maka perlu dikembangkan kompetensi dan keahlian khusus bagi para individu dalam pasukan siber. Keahlian tersebut bersifat kolektif, dalam arti kata tidak dimonopoli oleh satu atau dua orang (Danet, 2019). Berikut adalah contoh kemampuan kolektif yang dibutuhkan oleh sebuah pasukan siber.

Tabel 4. 68 Pemetaan Kapabilitas dan Kemampuan Pasukan Siber

| No | Kapabilitas dan Kemampuan             | Cyber<br>Safeguard | Cyber<br>Defense | Cyber<br>Offense | Cyber<br>Warfare |
|----|---------------------------------------|--------------------|------------------|------------------|------------------|
| 1  | Vulnerability Analysis                | x                  | x                | x                | x                |
| 2  | Penetration Test                      | x                  |                  | x                | x                |
| 3  | Digital/Computer/Network<br>Forensics | -                  | x                | x                | x                |
| 4  | Social Engineering                    | x                  | x                | x                | x                |
| 5  | Technology System Audit               | x                  | x                | x                | -                |
| 6  | Network Defender                      | x                  | x                | -                | -                |

|    |                                             |   |   |   |   |
|----|---------------------------------------------|---|---|---|---|
| 7  | Cyber Threat Intelligence                   | - | - | X | X |
| 8  | Information System Security                 | X | X | - | - |
| 9  | SOC Analyst                                 | X | X | X | X |
| 10 | Cryptographer (Encryption Specialist)       | X | - | X | X |
| 11 | Cyber Forensics Investigator                | X | X | X | X |
| 12 | Incident Handler                            | - | X | X | X |
| 13 | Network Defense Architect                   | X | X |   | X |
| 14 | Application Security Engineer               | X | X | X | X |
| 15 | Secured Programmer (PHP, Python, C++, Java) | X | X | X | X |
| 16 | Security Specialist                         | X | X | X | X |
| 17 | Mobile and System Hacking                   | - | - | X | X |
| 18 | GDPR Data Protector                         | X | X | - | - |
| 19 | Phishing Specialist                         | - |   | X | X |
| 20 | Reverse Engineering Malware Developer       | - | X | - | - |
| 21 | Cryptojacker                                | - | X | X | X |
| 22 | Ransomware Expert                           | - | X | X | X |
| 23 | Cloud Security                              | X | X | - | - |
| 24 | Cyberlaw Specialist                         | X | X | - | - |
| 25 | Ethical Hackers                             |   |   | X | X |
| 26 | Security Strategic Planners and Leaders     | X | X | X | X |
| 27 | Internet Traffic Monitoring Engineer        | X | X | - | - |
| 28 | AI-based Security Specialist                | X | X | X | X |

|    |                                    |   |   |   |   |
|----|------------------------------------|---|---|---|---|
| 29 | Cyber War Scenario Developer       | - | - | x | x |
| 30 | Big Data Expert and Data Scientist | x | x | x | x |

Sumber : Pemetaan Kapabilitas dan Kemampuan Pasukan Siber (hasil pengolahan data oleh peneliti)

#### Prioritas Pengembangan Kebijakan Pertahanan Siber

Pada tahapan implementasinya, tidak seluruh empat domain kebijakan dapat dikembangkan sekaligus. Secara politik biasanya akan terjadi pentahapan dalam pengembangannya. Untuk menentukan urutan penyusunannya, dipergunakan metoda AHP dalam penelitian ini. Gambar berikut ini memperlihatkan struktur pengambilan keputusan berbasis AHP dimaksud.



Gambar 4. 102 Struktur AHP

Sumber : Struktur AHP (hasil pengolahan data oleh peneliti)

Tujuan atau obyektif utamanya adalah untuk menetapkan strategi prioritas kebijakan menjaga kedaulatan siber Indonesia. Terdapat empat pilihan domain kebijakan yang akan ditentukan tingkat kepentingannya, yaitu: Kebijakan Perlindungan Siber, Kebijakan Pertahanan Siber, Kebijakan Penyerangan Siber, dan Kebijakan Peperangan Siber. Untuk menentukan prioritas tersebut, ditetapkanlah lima kriteria utama, yaitu:

1. Urgensitas: tingkat kegentingan memiliki kebijakan terkait pada masa sekarang, dimana serangan dan perang siber terjadi di mana-mana;
2. Implementasi: kemudahan menyusun strategi menerapkan butir-butir aspek yang dijabarkan dalam kebijakan dimaksud;
3. Tantangan: besarnya permasalahan atau problema yang dihadapi dalam menyusun serta mengembangkan sejumlah aspek dalam kebijakan;
4. Efektivitas: probabilitas keberhasilan dalam penerapan kebijakan sesuai dengan target obyektif yang diinginkan; dan
5. Manfaat: berkaitan dengan nilai positif atau value yang dirasakan oleh negara, masyarakat, dan para pemangku kepentingan dari domain kebijakan yang disusun.

Sebanyak 5 (lima) orang pakar dengan latar belakang pengetahuan, wawasan, dan pengalaman dalam menyusun berbagai kebijakan terkait dengan siber dilibatkan dalam AHP. Kelima pakar tersebut secara simultan melakukan perbandingan terhadap 6 (enam) hal utama, yaitu:

1. Komparasi antar kelima kriteria utama dalam AHP;
2. Komparasi antar empat alternatif untuk kriteria urgensitas;
3. Komparasi antar empat alternatif untuk kriteria implementasi;
4. Komparasi antar empat alternatif untuk kriteria tantangan;
5. Komparasi antar empat alternatif untuk kriteria efektivitas; dan
6. Komparasi antar empat alternatif untuk kriteria manfaat.

#### Perbandingan antar Kriteria



Hasil penilaian oleh kelima pakar memperlihatkan adanya konsensus yang tinggi, yaitu 83,9%. Bobot kepentingan yang terdistribusi di antara kriteria adalah: Urgensitas (48,5%), Efektivitas (16,7%), Implementasi (16,3%), Manfaat (13,0%), dan Tantangan (5,5%).

Tabel 4. 69 Hasil Pengolahan Data AHP: Kriteria Utama

AHP group consensus: 83.9% high

| Participant                      | Urgensi | Implementasi | Tantangan | Efektivitas | Manfaat | CR <sub>max</sub> |
|----------------------------------|---------|--------------|-----------|-------------|---------|-------------------|
| Group result                     | 48.5%   | 16.3%        | 5.5%      | 16.7%       | 13.0%   | 1.2%              |
| Muhammad Salahuddien Manggalanny | 54.2%   | 27.1%        | 5.2%      | 7.3%        | 6.2%    | 2.4%              |
| Bisyron Wahyudi                  | 33.9%   | 26.0%        | 3.8%      | 27.3%       | 8.9%    | 3.3%              |
| Victor                           | 59.0%   | 5.2%         | 5.7%      | 12.1%       | 18.0%   | 7.9%              |
| ekoji                            | 37.8%   | 13.6%        | 5.8%      | 22.4%       | 20.3%   | 5.1%              |

Sumber : Hasil Pengolahan Data AHP: Kriteria Utama (hasil pengolahan data oleh peneliti)

#### Perbandingan antar Alternatif untuk Kriteria Urgensi

Pada penilaian ini, terlihat sangat tingginya tingkat konsensus dari kelima pakar. Dengan mempertimbangkan kriteria urgensi, terlihat peringkat urutan pengembangan domain kebijakan sebagai berikut:

1. Domain Perlindungan Siber (54,8%)
2. Domain Pertahanan Siber (30,9%)
3. Domain Penyerangan Siber (8,4%)
4. Domain Peperangan Siber (5,9%)

Tabel 4. 70 Hasil Pengolahan Data AHP: Ugensitas

AHP group consensus: 94.4% very high

| Participant     | Perlindungan | Pertahanan | Penyerangan | Peperangan | CR <sub>max</sub> |
|-----------------|--------------|------------|-------------|------------|-------------------|
| Group result    | 54.8%        | 30.9%      | 8.4%        | 5.9%       | 0.3%              |
| Bisyron Wahyudi | 61.1%        | 24.5%      | 9.1%        | 5.3%       | 1.3%              |
| Victor          | 63.5%        | 22.0%      | 9.8%        | 4.7%       | 4.6%              |

Sumber : Hasil Pengolahan Data AHP: Ugensitas (hasil pengolahan data oleh peneliti)

### Perbandingan antar Alternatif untuk Kriteria Implementasi

Sebagaimana penilaian terdahulu, pada kriteria implementasi terlihat pula nilai konsensus antar pakar yang sangat tinggi, yaitu berada pada kisaran 93,3%. Peringkat berdasarkan tingkat kepentingan dalam pengembangan kebijakan adalah:

1. Domain Perlindungan Siber (51,4%)
2. Domain Pertahanan Siber (34,5%)
3. Domain Penyerangan Siber (8,8%)
4. Domain Peperangan Siber (5,2%)

Tabel 4. 71 Hasil Pengolahan Data AHP: Implementasi

AHP group consensus: 93.3% **very high**

| Participant                      | Perlindungan | Pertahanan | Penyerangan | Peperangan | CR <sub>max</sub> |
|----------------------------------|--------------|------------|-------------|------------|-------------------|
| Group result                     | 51.4%        | 34.5%      | 8.8%        | 5.2%       | 1.1%              |
| ekoji                            | 40.4%        | 44.2%      | 7.7%        | 7.7%       | 0.2%              |
| Muhammad Salahuddien Manggalanny | 45.0%        | 45.0%      | 5.0%        | 5.0%       | 0.0%              |
| Bisyrn Wahyudi                   | 59.9%        | 25.9%      | 9.8%        | 4.4%       | 3.6%              |
| Victor                           | 57.6%        | 24.3%      | 14.1%       | 4.1%       | 4.5%              |

Sumber : Hasil Pengolahan Data AHP: Implementasi (hasil pengolahan data oleh peneliti)

### Perbandingan antar Alternatif untuk Kriteria Tantangan

Perhitungan pada kriteria tantangan ini memperlihatkan konsensus kelima pakar yang relatif tidak tinggi (moderate), yang diperlihatkan dengan nilai 66,1%. Kondisi ini dimungkinkan karena masing-masing pihak memiliki pengalaman dan pandangan yang berbeda mengenai aspek tantangan dalam mengimplementasikan kebijakan dimaksud. Hasilnya memperlihatkan peringkat sebagai berikut:

1. Domain Pertahanan Siber (32,9%)
2. Domain Perlindungan Siber (28,4%)
3. Domain Penyerangan Siber (25,8%)
4. Domain Peperangan Siber (12,9%)

Tabel 4. 72 Hasil Pengolahan Data AHP: Tantangan

AHP group consensus: 66.1% moderate

| Participant                      | Perlindungan | Pertahanan | Penyerangan | Peperangan | CR <sub>max</sub> |
|----------------------------------|--------------|------------|-------------|------------|-------------------|
| Group result                     | 28.4%        | 32.9%      | 25.8%       | 12.9%      | 0.7%              |
| Muhammad Salahuddien Manggalanny | 31.2%        | 31.2%      | 31.2%       | 6.2%       | 0.0%              |
| Bisyron Wahyudi                  | 24.6%        | 58.6%      | 12.4%       | 4.4%       | 7.2%              |
| Victor                           | 44.9%        | 25.1%      | 17.0%       | 12.9%      | 4.3%              |
| ekoji                            | 9.4%         | 13.4%      | 35.8%       | 41.4%      | 2.6%              |

Sumber : Hasil Pengolahan Data AHP: Tantangan (hasil pengolahan data oleh peneliti)

### Perbandingan antar Alternatif untuk Kriteria Efektivitas

Konsensus sangat tinggi kembali diperlihatkan ketika melakukan perbandingan terhadap alternatif untuk kriteria efektivitas, yaitu sebesar 93,0%. Adapun hasil pemeringkatan berdasarkan urutan tertinggi menuju terendah adalah sebagai berikut:

1. Domain Perlindungan Siber (46,4%)
2. Domain Pertahanan Siber (31,0%)
3. Domain Penyerangan Siber (16,5%)
4. Domain Peperangan Siber (6,2%)

Tabel 4. 73 Hasil Pengolahan Data AHP: Efektivitas

AHP group consensus: 93.0% very high

| Participant                      | Perlindungan | Pertahanan | Penyerangan | Peperangan | CR <sub>max</sub> |
|----------------------------------|--------------|------------|-------------|------------|-------------------|
| Group result                     | 46.4%        | 31.0%      | 16.5%       | 6.2%       | 2.4%              |
| Muhammad Salahuddien Manggalanny | 46.0%        | 31.8%      | 13.6%       | 8.6%       | 3.9%              |
| Bisyron Wahyudi                  | 30.1%        | 33.9%      | 29.3%       | 6.7%       | 7.7%              |
| Victor                           | 58.5%        | 25.6%      | 10.3%       | 5.5%       | 1.5%              |
| ekoji                            | 50.0%        | 30.2%      | 15.8%       | 4.0%       | 7.3%              |

Sumber : Hasil Pengolahan Data AHP: Efektivitas (hasil pengolahan data oleh peneliti)

### Perbandingan antar Alternatif untuk Kriteria Manfaat

Sementara untuk kriteria manfaat, kembali konsensus sangat tinggi sebesar 95,2% diperlihatkan oleh kelima pakar. Hasil memperlihatkan tingkat kepentingan domain kebijakan sebagai berikut:

1. Domain Perlindungan Siber (45,5%)
2. Domain Pertahanan Siber (38,5%)
3. Domain Penyerangan Siber (10,4%)
4. Domain Peperangan Siber (5,6%)

Tabel 4. 74 Hasil Pengolahan Data AHP: Manfaat

AHP group consensus: 95.2% very high

| Participant                      | Perlindungan | Pertahanan | Penyerangan | Peperangan | CR <sub>max</sub> |
|----------------------------------|--------------|------------|-------------|------------|-------------------|
| Group result                     | 45.5%        | 38.5%      | 10.4%       | 5.6%       | 1.9%              |
| Victor                           | 34.4%        | 51.7%      | 8.9%        | 5.0%       | 1.9%              |
| Bisyrn Wahyudi                   | 54.4%        | 29.3%      | 10.8%       | 5.5%       | 7.7%              |
| Muhammad Salahuddien Manggalanny | 42.4%        | 42.4%      | 11.4%       | 3.7%       | 4.9%              |
| ekoji                            | 50.8%        | 30.9%      | 9.8%        | 8.5%       | 8.8%              |

Sumber : Hasil Pengolahan Data AHP: Manfaat (hasil pengolahan data oleh peneliti)

Melalui perhitungan AHP tersebut, maka dapat disimpulkan bahwa domain pertama yang harus disusun dan dikembangkan adalah kebijakan terkait dengan perlindungan siber. Setelah itu barulah secara berturut-turut disusun serta dikembangkan kebijakan mengenai pertahanan siber, penyerangan siber,

dan peperangan siber. Urutan ini selaras dengan pengalaman berbagai negara berkembang maupun negara maju pada awal pembentukan kebijakan sibernya. Secara metodologis, urutan peringkat tersebut sejalan dengan metodologi pengembangan kapabilitas teknis dari pasukan siber karena berkaitan erat dengan spektrum body of knowledge di bidang pertahanan dan keamanan siber.

#### Kebutuhan Pengembangan Kebijakan Pertahanan Siber

Keseluruhan kebutuhan kebijakan sebagaimana diapaparkan sebelumnya harus ditempatkan pada konteks sistem peraturan dan perundang-undangan yang berlaku di Indonesia. Sebagaimana diketahui bersama, struktur atau tata urutan dimaksud adalah sebagai berikut:

1. UUD RI;
2. Ketetapan MPR;
3. Undang-Undang;
4. Peraturan Pemerintah;
5. Keputusan Presiden; dan
6. Peraturan Pelaksana: Peraturan Menteri dan Instruksi Menteri.

#### UUD Republik Indonesia

Sebagai kebijakan pada tataran tertinggi yang telah mengalami beberapa kali amandemen pasca reformasi tahun 1998, ada satu hal yang perlu dipikirkan untuk dimutakhirkan seandainya terjadi peluang amandemen kembali. Hal tersebut adalah dilakukan redefinisi dan/atau revisi terhadap wilayah negara yang tidak saja dibatasi pada ruang darat, laut, dan udara – namun juga menyangkut dimensi antariksa dan siber.



Tabel 4. 75 Daftar Usulan Amandemen UUD-RI

| No                                                    | Kebijakan                                                                                                                   | Ruang Lingkup                                                                                                                                       |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain Perlindungan Siber (Cyber Safeguarding)</b> |                                                                                                                             |                                                                                                                                                     |
| 1                                                     | Amandemen UUD Republik Indonesia terkait dengan Wilayah Negara dalam Dimensi Ruang Darat, Laut, Udara, Antariksa, dan Siber | Menjelaskan secara rinci dan detail batas-batas wilayah NKRI yang tidak terbatas pada batasan darat dan laut, tapi juga udara, antariksa, dan siber |

Sumber : Hasil olahan data dan usulan penalti

### Ketetapan MPR

Penetapan wilayah NKRI dalam dimensi baru yaitu udara, antariksa, dan siber ini perlu mendapatkan persetujuan oleh seluruh DPR dan DPD yang merupakan bagian dari MPR, mengingat akan terjadi pergeseran dan dampak yang signifikan dalam kehidupan berbangsa dan bernegara di kemudian hari.

Tabel 4. 76 Daftar Usulan Ketetapan MPR

| No                                                    | Kebijakan                                                                                                          | Ruang Lingkup                                                                                               |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Domain Perlindungan Siber (Cyber Safeguarding)</b> |                                                                                                                    |                                                                                                             |
| 1                                                     | Ketetapan MPR mengenai Sistem Kedaulatan Wilayah NKRI dalam Dimensi Ruang Darat, Laut, Udara, Antariksa, dan Siber | Mendefinisikan wilayah NKRI dalam lima dimensi terintegrasi, yaitu darat, laut, udara, antariksa, dan siber |

Sumber : Hasil olahan data dan usulan penalti

### Undang-Undang

Pada tataran praktis, undang-undang adalah kebijakan yang dianggap cukup tinggi untuk mengeksekusi dan mengatur berbagai regulasi turunannya. Oleh karena itulah maka perlu dimiliki sejumlah undang-undang yang secara eksplisit formal berbicara mengenai ruang siber dan pertahanan siber nasional.

Tabel 4. 77 Daftar Usulan Undang-Undang

| No                                                    | Kebijakan                                                                                         | Ruang Lingkup                                                                                                             |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Domain Perlindungan Siber (Cyber Safeguarding)</b> |                                                                                                   |                                                                                                                           |
| 1                                                     | Undang-Undang Republik Indonesia tentang Sistem Siber Nasional dan Model Tata Kelola Terintegrasi | Mendefinisikan dan memetakan wilayah serta perimeter sistem siber nasional beserta menetapkan model pengelolaannya secara |

|   |                                                                                     |                                                                                                       |
|---|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|   |                                                                                     | terintegrasi dan terpadu                                                                              |
| 2 | Undang-Undang Republik Indonesia tentang Pertahanan Siber Nasional                  | Menjelaskan dan mengatur mengenai postur serta mekanisme pengelolaan sistem pertahanan siber nasional |
| 3 | Undang-Undang Republik Indonesia tentang Infrastruktur Teknologi Strategis Nasional | Menetapkan infrastruktur negara mana saja yang dikategorikan vital dan strategis                      |

Sumber : Hasil olahan data dan usulan penalti

### Peraturan Pemerintah

Koordinasi dan kerjasama antar sektor adalah sebuah keniscayaan dalam mengembangkan pertahanan siber yang kokoh, terintegrasi, dan terpadu. Keberadaan peraturan pemerintah yang bersifat lintas sektoral sangatlah dibutuhkan untuk menjamin terjadinya kolaborasi dan kooperasi di antara berbagai lembaga, institusi, maupun kementerian yang ada dalam struktur pemerintahan negara.

Tabel 4. 78 Daftar Usulan Peraturan Pemerintah

| No                                                    | Kebijakan                                                                                                  | Ruang Lingkup                                                                                      |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <b>Domain Perlindungan Siber (Cyber Safeguarding)</b> |                                                                                                            |                                                                                                    |
| 1                                                     | Peraturan Pemerintah tentang Ekosistem Pertahanan Siber Nasional                                           | Menggambarkan ekosistem pertahanan siber nasional secara utuh, holistik, dan komprehensif          |
| 2                                                     | Peraturan Pemerintah tentang Peran dan Tanggung Jawab Stakeholder pada Ekosistem Pertahanan Siber Nasional | Menetapkan tugas dan tanggung jawab setiap pihak dalam konstelasi sistem pertahanan siber nasional |

Sumber : Hasil olahan data dan usulan penalti

### Keputusan Presiden

Sebagai kepala negara sekaligus kepala pemerintahan, Presiden RI perlu membuat sejumlah keputusan penting untuk memastikan terciptanya pertahanan siber yang kuat, kokoh, mandiri, dan berdaulat.

Tabel 4. 79 Daftar Usulan Keputusan Presiden

| No                                                    | Kebijakan                                                                | Ruang Lingkup                                                                                         |
|-------------------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Domain Perlindungan Siber (Cyber Safeguarding)</b> |                                                                          |                                                                                                       |
| 1                                                     | Keputusan Presiden tentang Doktrin Pertahanan Siber Negara               | Mendefinisikan secara tegas doktrin pertahanan siber dalam konteks bernegara                          |
| 2                                                     | Keputusan Presiden tentang Pembentukan Council Pertahanan Siber Nasional | Membentuk satuan kerja khusus yang bertanggung jawab dalam mengelola sistem pertahanan siber nasional |

Sumber : Hasil olahan data dan usulan penalti

### Peraturan (Bersama) Menteri

Secara khusus untuk konteks pertahanan siber, dibutuhkan tiga jenis peraturan penting, yaitu: (i) Peraturan Menteri Pertahanan; (ii) Keputusan Panglima TNI; dan (iii) Peraturan Bersama antara Menteri Pertahanan dan Panglima TNI.

Tabel 4. 80 Daftar Usulan Peraturan (Bersama) Menteri

| No                                                    | Kebijakan                                                     | Ruang Lingkup                                              |
|-------------------------------------------------------|---------------------------------------------------------------|------------------------------------------------------------|
| <b>Domain Perlindungan Siber (Cyber Safeguarding)</b> |                                                               |                                                            |
| 1                                                     | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang | Menetapkan wilayah siber mana saja yang berpengaruh secara |

|   |                                                                                                                                                             |                                                                                                                      |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
|   | Perimeter dan Demarkasi Wilayah Pertahanan Siber Nasional                                                                                                   | langsung terhadap pertahanan negara dan aset komputasi yang membentuknya                                             |
| 2 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Jenis, Klasifikasi, dan Daftar Aset Digital Strategis dalam Lingkungan Pertahanan dan Militer | Mendefinisikan dan membuat kategori serta daftar aset strategis dalam perimeter pertahanan negara                    |
| 3 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Asesmen Kekuatan dan Kelemahan Aset Digital Strategis dalam Lingkungan Pertahanan Negara      | Menjalankan proses asesmen terhadap kehandalan aset digital strategis dalam menghadapi berbagai serangan siber       |
| 4 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Analisa Dampak Serangan terhadap Sistem dan Sumber Daya Digital Strategis                     | Mengkaji dampak beragam serangan terhadap sistem dan sumber daya strategis terhadap kedaulatan dan pertahanan negara |
| 5 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Adopsi Penerapan Standar Keamanan pada Sistem dan Sumber Daya Digital Strategis               | Menentukan dan mengadopsi standar keamanan terhadap sistem dan sumber daya strategis pertahanan negara               |
| 6 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Tata Kelola Sistem dan Sumber Daya Pertahanan Siber                                           | Mengatur sistem tata kelola dan manajemen beragam sistem informasi dan komputasi dalam wilayah pertahanan negara     |
| 7 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Audit Sistem Informasi Pertahanan Negara yang Terpadu dan Terintegrasi                        | Melakukan audit independen secara menyeluruh terhadap sistem informasi dalam wilayah pertahanan negara               |

#### **Domain Pertahanan Siber (Cyber Defense)**

|   |                                                                                                                                                                       |                                                                                   |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 1 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pemantauan Situasi dan Kondisi Siber berbagai trafik dan anomali dari dalam Perimeter Pertahanan Negara | Melakukan monitoring atau pengawasan 24/7 terhadap dan ke beragam aset dan sumber |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|

|   |                                                                                                                    |                                                                                                                                                                                      |
|---|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |                                                                                                                    | daya sistem siber pertahanan                                                                                                                                                         |
| 2 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pendeteksian terjadinya Serangan Siber               | Mendeteksi adanya serangan siber ke dalam wilayah pertahanan negara                                                                                                                  |
| 3 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Penetapan Jenis dan Klasifikasi Serangan Siber       | Menganalisa dan mengkategorikan jenis serangan siber ke dalam wilayah pertahanan negara                                                                                              |
| 4 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Strategi dan Eksekusi Respon terhadap Serangan Siber | Menentukan strategi dan skenario respon yang sesuai dengan jenis serangan siber dan potensi dampak yang ditimbulkannya serta mengeksekusi berdasarkan skenario bertahan yang efektif |
| 5 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pengumpulan Fakta dan Aktivitas Forensik Digital     | Mengumpulkan bukti-bukti forensik digital terkait dengan serangan yang terjadi untuk dianalisa dan dimitigasi                                                                        |
| 6 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pemulihan Situasi dan Kondisi Pasca Serangan Siber   | Memulihkan kondisi situasi dan kondisi sistem pertahanan siber pasca terjadinya serangan                                                                                             |
| 7 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Perbaikan dan Pemutakhiran Sistem Pertahanan Siber   | Memperbaiki serta memutakhirkan sistem siber yang mengalami serangan agar lebih kokoh pertahanannya                                                                                  |

#### **Domain Penyerangan Siber (Cyber Offense)**

|   |                                                                                                 |                                                                                                                   |
|---|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 1 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pengerahan Intelijen Siber Global | Mengumpulkan informasi terutama dari underground atau dark web untuk mendeteksi adanya skenario penyerangan siber |
| 2 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Penetapan Target Serangan Siber   | Menetapkan target untuk diserang demi melumpuhkan sistem yang berbahaya atau mengantisipasi terjadinya serangan   |

- |   |                                                                                                                  |                                                                                                      |
|---|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| 3 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Analisa Kerentanan Sistem Siber Eksternal          | Mengkaji kekuatan dan kerentanan sistem target yang akan diserang                                    |
| 4 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Penyusunan Strategi dan Skenario Penyerangan Siber | Menyusun strategi dan skenario penyerangan yang efektif, efisien, dan terkendali                     |
| 5 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pelaksanaan Eksekusi Serangan Siber                | Mengeksekusi serangan terhadap target berdasarkan strategi dan skenario yang telah ditetapkan        |
| 6 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Penghapusan Jejak dan Penyangkalan Serangan Siber  | Menghapus jejak serangan siber agar guna menghindari tuntutan hukum atau pembalasan di kemudian hari |
| 7 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Asesmen Efektivitas Serangan Siber                 | Mengkaji efektivitas serangan yang dilakukan sebagai bahan evaluasi dan pembelajaran                 |

#### **Domain Peperangan Siber (Cyber Warfare)**

- |   |                                                                                                                |                                                                                                         |
|---|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 1 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pengembangan Efek Gentar Siber Pertahanan Negara | Mengembangkan sistem pertahanan siber yang kokoh guna mengurangi potensi serangan dari berbagai pihak   |
| 2 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Diplomasi Siber Internasional                    | Melakukan diplomasi siber untuk mengurangi perselisihan dan konflik yang bermuara pada serangan         |
| 3 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pernyataan Resmi Perang Siber                    | Mendeklarasikan mulainya perang siber secara resmi dengan berbagai pihak demi menjaga pertahanan negara |
| 4 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Penetapan Strategi Perang Siber                  | Menetapkan strategi peperangan siber yang ampuh guna meraih kemenangan                                  |
| 5 | Peraturan Bersama Menteri                                                                                      | Mengerahkan dan memobilisasi                                                                            |

- |   |                                                                                                                          |                                                                                                                              |
|---|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|   | Pertahanan dan Panglima TNI tentang segenap pasukan siber serta Pengerahan dan Koordinasi Aliansi Pasukan Siber Nasional | sumber daya komputasi yang dibutuhkan dalam peperangan                                                                       |
| 6 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pelaksanaan Perang Siber                                   | Mengeksekusi strategi peperangan secara berkesinambungan sampai diraih kemenangan                                            |
| 7 | Peraturan Bersama Menteri Pertahanan dan Panglima TNI tentang Pernyataan Akhir Perang Siber                              | Mendeklarasikan berakhirnya peperangan siber sekaligus melakukan evaluasi terhadap pelaksanaannya sebagai bahan pembelajaran |

#### **Domain Pendukung (People)**

- |   |                                                                                                     |                                                                                                                   |
|---|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 1 | Peraturan Menteri Pertahanan tentang Pembentukan Pasukan Siber di Lingkungan Kementerian Pertahanan | Membentuk pasukan siber di lingkungan Kementerian Pertahanan                                                      |
| 2 | Keputusan Panglima TNI tentang Pembentukan Pasukan Siber di Lingkungan Militer                      | Membentuk pasukan siber di lingkungan Tentara Nasional Indonesia                                                  |
| 3 | Peraturan Menteri Pertahanan tentang Pembentukan CERT di Lingkungan Kementerian Pertahanan          | Membentuk tim tanggap darurat siber di lingkungan Kementerian Pertahanan                                          |
| 4 | Keputusan Panglima TNI tentang Pembentukan CERT di Lingkungan Militer                               | Membentuk tim tanggap darurat siber di lingkungan Tentara Nasional Indonesia                                      |
| 5 | Peraturan Menteri Pertahanan tentang Kerangka Kualifikasi Kompetensi SDM di Bidang Pertahanan Siber | Mengembangkan kerangka kompetensi dan keahlian individu/profesional yang dibutuhkan dalam bidang pertahanan siber |
| 6 | Peraturan Menteri Pertahanan tentang Lembaga Pelatihan dan Sertifikasi SDM Pertahanan Siber         | Membentuk lembaga pelatihan dan sertifikasi individu/profesional di bidang pertahanan siber                       |

#### **Domain Pendukung (Process)**

- |   |                                                                          |                                                               |
|---|--------------------------------------------------------------------------|---------------------------------------------------------------|
| 1 | Peraturan Menteri Pertahanan tentang Ekosistem Pertahanan Siber Nasional | Mendesain ekosistem pertahanan siber dengan berbagai komponen |
|---|--------------------------------------------------------------------------|---------------------------------------------------------------|



pembentuknya

- 2 Peraturan Menteri Pertahanan tentang Mengembangkan model tata kelola  
Tata Kelola dan Manajemen Sistem dan manajemen sistem pertahanan  
Pertahanan Siber Nasional siber nasional
- 3 Peraturan Menteri Pertahanan tentang Menyusun sistem dan model  
Sistem Anggaran Pertahanan Siber anggaran yang sesuai dengan  
Nasional kebutuhan sistem pertahanan siber
- 4 Peraturan Menteri Pertahanan tentang Menyusun dan memberlakukan  
Standar Pertahanan dan Keamanan standar pertahanan dan keamanan  
Siber Nasional dalam lingkungan pertahanan iber
- 5 Peraturan Menteri Pertahanan tentang Membangun kerjasama antara  
Kerjasama Pertahanan Siber dengan Kementerian Pertahanan dengan  
Institusi dan Lembaga Eksternal berbagai lembaga maupun institusi  
Dalam Negeri dalam negeri
- 6 Peraturan Menteri Pertahanan tentang Membangun kerjasama antara  
Kerjasama Pertahanan Siber dengan Kementerian Pertahanan dengan  
Insitusi atau Lembaga Luar Negeri berbagai lembaga maupun institusi  
(Internasional) luar negeri

### Domain Pendukung (Technology)

- |   |                                                                                                                               |                                                                                                                                                  |
|---|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Peraturan Menteri Pertahanan tentang Seleksi dan Akreditasi Teknologi Digital dalam Lingkungan Pertahanan Siber               | Menyusun cara menseleksi dan akreditasi berbagai teknologi digital yang dipergunakan dalam lingkungan pertahanan siber                           |
| 2 | Peraturan Menteri Pertahanan tentang Sistem Pengadaan Peralatan Digital dalam Lingkungan Pertahanan Siber                     | Menetapkan mekanisme dan prosedur pengadaan peralatan teknologi digital dalam lingkungan pertahanan siber                                        |
| 3 | Peraturan Menteri Pertahanan tentang Lembaga Penelitian dan Pengembangan (R&D) Teknologi Siber                                | Membentuk dan mengembangkan lembaga penelitian untuk menghasilkan teknologi siber buatan dalam negeri                                            |
| 4 | Peraturan Menteri Pertahanan tentang Standar Interoperabilitas Sistem dan Teknologi Digital dalam Lingkungan Pertahanan Siber | Menyusun dan menetapkan standar interoperabilitas yang harus dipatuhi oleh seluruh pengembang sistem                                             |
| 5 | Peraturan Menteri Pertahanan tentang Arsitektur Sistem Pertahanan Siber yang Terintegrasi dan Terpadu                         | Merancang arsitektur sistem pertahanan siber yang terintegrasi dan terpadu                                                                       |
| 6 | Peraturan Menteri Pertahanan tentang Protokol Komunikasi dan Kriptografi dalam Lingkungan Pertahanan Siber                    | Menetapkan protokol komunikasi aman dan sistem kriptografi yang harus dipergunakan dalam berbagai model komunikasi dalam sistem pertahanan siber |

Sumber : Hasil olahan data dan usulan penalti

### Pembagian Tugas dan Wewenang Tata Kelola Siber

Tata kelola siber saat ini secara *de facto* dan *de jure* sedang diatur oleh pemerintah dan negara. Walaupun belum ideal, namun langkah awal ini cukup baik sebagai batu pijakan bagi pemerintah dan masyarakat Indonesia dalam memahami karakteristik dunia siber yang sebenarnya. Tabel berikut

memperlihatkan bagaimana kesepakatan tak tertulis mulai diadopsi oleh Indonesia paling tidak untuk beberapa tahun ke depan.

Tabel 4. 81 Pembagian Peran secara Kolektif

| No | Tema dan Ruang Lingkup Siber               | Leading Sector                                            |
|----|--------------------------------------------|-----------------------------------------------------------|
| 1  | <i>Cyber Defense &amp; Cyber War</i>       | Kementerian Pertahanan                                    |
| 2  | <i>Cyber Security</i>                      | Badan Siber dan Sandi Negara                              |
| 3  | <i>Cyber Crime</i>                         | Kepolisian Republik Indonesia                             |
| 4  | <i>Cyber Infrastructure &amp; Standard</i> | Kementerian Komunikasi dan Informatika                    |
| 5  | <i>Cyber Commerce</i>                      | Kementerian Perdagangan                                   |
| 6  | <i>Cyber Law</i>                           | Kementerian Hukum dan Hak Asasi Manusia                   |
| 7  | <i>Cyber Resilience</i>                    | Lembaga Ketahanan Nasional                                |
| 8  | <i>Cyber Economy</i>                       | Kementerian Keuangan                                      |
| 9  | <i>Cyber Terrorism</i>                     | Badan Nasional Penanggulangan Terorisme                   |
| 10 | <i>Cyber Literacy &amp; Society</i>        | Kementerian Pendidikan, Kebudayaan, dan Pendidikan Tinggi |

Sumber : Hasil olahan data dan usulan penalti

Tabel di atas memperlihatkan betapa pengaturan tata kelola siber masih bersifat kompartemental atau sektoral. Namun kenyataan ini dapat dipahami bagi negara yang masih berada dalam tataran peningkatan *cyber maturity governance*-nya. Alasan utamanya adalah karena teknologi informasi, digital, internet, dan ruang siber telah menjadi infrastruktur kehidupan manusia. Artinya adalah bahwa seluruh sektor dan sendi kehidupan tidak terlepas dari pemanfaatan ruang siber dan internet. Masing-masing tema dan ruang siber tersebut dalam tabel memiliki fokusnya masing-masing yang secara esensial memiliki karakteristik berbeda.

*Cyber defense* dan *cyber war* memiliki fokus pada kekuatan negara dalam menghadapi berbagai ancaman dari dalam maupun luar negeri di bidang siber. Kedaulatan dan keutuhan negara adalah sesuatu yang harus dipertahankan keberadaannya, sehingga fokus dalam menjaga negara adalah ruang lingkup utama dalam ranah ini (Kozowski, 2019). Sifatnya sungguh mirip dengan aktivitas militer, yang selalu harus siap siaga dalam kondisi peperangan maupun keadaan damai. Kata kunci yang menjadi komponen dalam sub-sistem ini antara lain adalah *cyber attack*, *cyber weapon*, *cyber espionage*, *cyber territory*, *cyber army*, dan lain sebagainya.

*Cyber security* fokus pada usaha memastikan bahwa seluruh institusi, lembaga, dan masyarakat benar-benar mengamankan dirinya dari berbagai kemungkinan buruk yang terjadi akibat adanya serangan siber yang akan mengganggu aktivitas sehari-hari. Setiap entitas atau organisasi harus memiliki standar minimum untuk melindungi dirinya dari berbagai eksploitasi para peretas yang hendak merusak atau mengganggu jalannya kegiatan (Oyelami, 2020). Masyarakat pun harus peduli akan fungsi mereka sebagai subyek aktif yang akan membangun sistem keamanan yang kuat. Dengan bertumpu pada konsep CIA (*Confidentiality, Integrity, Availability*), *cyber security* yang baik sangat tergantung pada kehandalan tiga unsur pokok, yaitu *people*, *process*, dan *technology*.

*Cyber crime* berhubungan erat dengan terjadinya tindakan kriminal melawan hukum, baik secara perdata dan/atau pidana, yang berpotensi mengganggu ketertiban masyarakat. Sebagai sebuah kejahatan, aspek siber ini erat kaitannya dengan dunia fisik atau nyata. Modusnya pun kurang lebih sama, seperti: pencurian identitas digital, penyalahgunaan wewenang, perampokan uang, pembunuhan karakter individu, penyebaran berita bohong, perbuatan tidak menyenangkan, perusakan sumber daya komputasi, dan lain sebagainya (Rahmawati, 2017; Gupta, 2020). Penegakan hukum terhadap para pelaku perbuatan kriminal menjadi aspek utama dalam ranah *cyber crime*.

*Cyber infrastructure and standard* fokus pada pembangunan dan pengelolaan jaringan internet sebagai infrastruktur yang membentuk ruang siber. Jaringan transmisi elektronik dan digital yang menghubungkan beragam sumber

daya komputasi perlu diatur rancangan serta protokol interoperabilitasnya (Gawthorpe, 2016; Bhardwaj, 2016). Demikian pula perlunya dipersiapkan berbagai mekanisme dan prosedur teknis yang berkaitan dengan model transmisi, kehandalan perangkat, perijinan frekuensi, ruang lingkup layanan, dan aspek-aspek terkait lainnya.

*Cyber commerce* adalah fenomena perdagangan dalam dunia virtual yang telah menjadi tulang punggung perekonomian berbagai negara di dunia. Sistem transaksi, mata uang, perdagangan, produk, dan model layanan adalah contoh aspek yang perlu diatur untuk melindungi berbagai pemangku kepentingan yang saling berinteraksi secara komersial (Sima, 2020). Keberadaannya tidak dapat dilepaskan dengan ekosistem perdagangan konvensional yang selama ini dikenal luas.

*Cyber law* merupakan sistem hukum yang disusun dan diberlakukan untuk mengatur berbagai aktivitas yang berkaitan dengan dunia siber. Dikatakan sebagai sistem hukum karena di dalamnya terdiri dari berbagai regulasi dan peraturan yang saling terkait satu dan lainnya (Mali, 2018). Repositori regulasi dalam *cyber law* terus berkembang sesuai dengan fenomena dan dinamika jaman.

*Cyber resilience* berkaitan erat dengan ketahanan siber negara dalam menghadapi berbagai serangan, tantangan, dan gangguan yang terjadi. Seberapa cepat kondisi siber negara dapat kembali ke kondisi terbaiknya setelah mendapatkan gangguan atau serangan dari berbagai pihak menentukan ketangguhan atau ketahanan siber yang dimiliki (Hopkins, 2020; Davidson, 2020).

*Cyber economy* bertanggung jawab terhadap pembentukan ekosistem makro ekonomi moderen yang bertumpu pada begitu banyak fenomena baru yang sangat disruptif. Konsep kontemporer seperti *sharing economy*, *crypto currency*, *technopreneurship*, *e-commerce*, *digital money*, dan lain-lain perlu diatur dan diintegrasikan dengan sistem konvensional untuk membentuk pondasi ekonomi makro yang kuat.

*Cyber terrorism* merupakan fenomena yang paling ditakuti dan menjadi perhatian dunia global dewasa ini. Tindakan untuk menakut-nakuti atau menyebarkan teror di masyarakat via dunia siber terbukti ampuh dan telah mampu membuat kekacauan yang sangat mengganggu ketertiban (Sima, 2020). Selain itu, sudah menjadi rahasia umum terkait dengan bagaimana para *terrorist* global memanfaatkan dunia siber untuk menggalang dana dan mencuci uang demi menjalankan aksinya.

*Cyber literacy* dan *society* adalah tugas bersama untuk meningkatkan kualitas pengetahuan, wawasan, dan keterampilan individu maupun masyarakat dalam mengoperasikan serta memanfaatkan dunia siber guna meningkatkan kualitas kehidupannya. Melalui berbagai program edukasi, sosialisasi, dan pelatihan, diharapkan manusia Indonesia meningkat literasinya, sehingga mampu memberikan kontribusi positif bagi pembangunan bangsa dan negara (Sobiesk, 2015).

Keseluruhan aspek dan ruang lingkup siber ini perlu dikembangkan regulasinya. Walaupun setiap aspek atau domain memiliki fokusnya masing-masing, namun di antaranya terdapat berbagai kesamaan dalam visi dan misi – yaitu bagaimana membangun dunia siber yang mampu memberikan kontribusi positif dan signifikan bagi bangsa dan negara. Karena setiap *leading sector* berpotensi menyusun regulasinya masing-masing, maka jelas dibutuhkan aturan pemersatu yang berada lebih tinggi tatarannya.