NASKAH AKADEMIK
RANCANGAN UNDANG-UNDANG
TENTANG
KEAMANAN DAN KETAHANAN SIBER

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

Dunia saat ini sedang berada pada era digital yang memungkinkan manusia untuk saling terhubung tanpa terhambat oleh batas-batas wilayah negara. Kemudahan akses, kecepatan dan konektifitas dari internet menjadi suatu hal yang banyak dimanfaatkan oleh masyarakat pada berbagai Negara dalam berbagai aspek kehidupan dengan persebaran informasi yang mudah. Seiring dengan pemakaian jaringan sistem komputer yang menggunakan infrastruktur sistem telekomunikasi membuat masyarakat sebagai penggunanya seolah-olah mendapati dunia baru, konsep ini sering dinamakan sebagai *cyberspace*.[1]

Awalan *cyber* (siber dalam bahasa Indonesia) menjadi awalan yang dipakai untuk hampir segala sesuatu yang melibatkan komunikasi lewat komputer. *Cyberspace* (ruang siber) adalah tempat maya yang dimana komunikasi tersebut terjadi.[2] Istilah *cyberspace* pertama kali diperkenalkan oleh William Gibson pada tahun 1980 dalam novelnya yang berjudul Neuromancer.[3] Karena hal tersebut berada pada novel, maka yang dikatakan oleh William Gibson dapat dikatakan hanya sebuah ilustrasi gambaran semata. Hingga kini banyak definisi dari istilah *cyberspace* yang dikemukakan oleh para ahli, sebagai gambaran lain pada faktanya, *cyberspace* merupakan jaringan internet sebagaimana dijelaskan oleh Abdul Wahid dan

---

[1] M. Arsyad Sanusi, Hukum Teknologi dan Informasi, Bandung: Tim Kemas Buku, 2005, hlm. 92-93

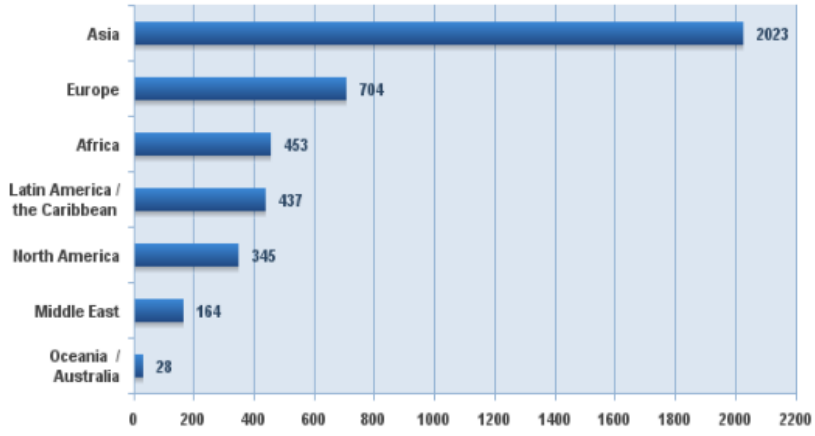
[2] John Vivian, Teori Komunikasi Massa, Jakarta: Kencana, 2008, hlm. 264

[3] Menurut William Gibson, *"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts ... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding."* Dalam Joanna Buick dan Joran Jevtic, Mengenal Cyberspace For Beginners, (Bandung: Mizan, 1997), hlm. 4

Mohammad Labib bahwa *cyberspace* adalah realitas atau alam baru yang terbentuk oleh medium internet yang menciptakan masyarakat baru sebagai warganya (netizen). [4] Kehadiran internet ini telah menghadirkan paradigma baru dalam kehidupan manusia. Adanya realitas baru yang sebelumnya hanya bersifat nyata (*real*) kini ditambah dengan yang bersifat maya (*virtual*). Realitas yang bersifat maya ini sering dikaitkan dengan internet dan *cyberspace*.[5]

Jumlah statistik penggunaan ruang siber atau internet oleh masyarakat di Dunia terus mengalami peningkatan dari tahun ke tahun. Hal ini dapat dilihat pada data rilis terakhir yang disajikan dari Miniwatts Marketing Group pada tanggal 31 Desember 2017, pengguna internet di Dunia mencapai 4,2 miliar. Meningkat dari tahun 2016 yang hanya mencapai 3,7 miliar pengguna internet di Dunia. Maka sesuai dengan data tersebut pengguna internet di Dunia telah mencapai 54,4 % dari keseluruhan populasi manusia Dunia yaitu sekitar 7,6 miliar. Lebih lanjut jumlah statistik pengguna internet di Dunia dapat dibagi menurut wilayah geografis, berikut bagan persebaran pengguna internet pada beberapa wilayah di Dunia:[6]

Gambar 1. Pengguna internet di Dunia menurut wilayah geografis



[4] Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara (cyber crime), (Jakarta: Refika Aitama, 2005), hlm. 32

[5] *Ibid.*, hlm. 103

[6] Miniwatts Marketing Group, Internet Usage Statistic, https://www.internetworldstats.com/stats.htm diakses pada 20 Agustus 2018

Sumber: Miniwatts Marketing Group, Internet Users in the World by Geographics Regions, December 31. 2017

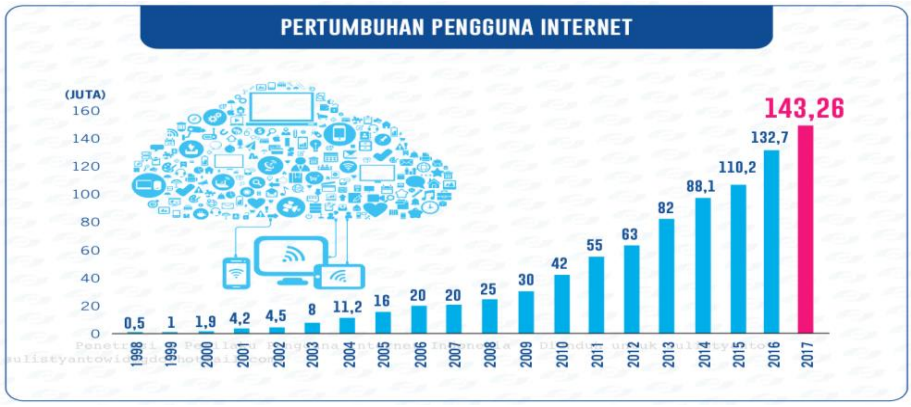
Pada data tahun 2017 tersebut pengguna internet paling banyak berada pada wilayah asia, dengan jumlah 2,023 miliar orang dengan total populasi 4,2 miliar orang, sehingga persentase pengguna internet di Asia yaitu 48,1%. Urutan kedua jumlah pengguna internet berada pada wilayah Eropa dengan jumlah pengguna 704 juta orang pada total populasi 827 juta orang, sehingga presentase pengguna internet di Eropa yaitu 85,2%. Urutan ketiga jumlah pengguna internet berada pada wilayah Afrika dengan jumlah 453 juta orang dengan total populasi 1,3 miliar orang, sehingga persentase pengguna internet di Afrika yaitu 35,2%. Pada wilayah Amerika Latin (the Caribbean) jumlah pengguna internet mencapai 437 juta orang dengan total populasi 652 juta orang, sehingga presentase pengguna internet di wilayah Amerika Latin sebesar 67%. Wilayah berikutnya yaitu Amerika Utara memiliki pengguna internet dengan jumlah 345 juta orang dengan jumlah populasi sebanyak 363 juta orang, sehingga presentase pengguna internet di wilayah Amerika Utara sebesar 95%. Pada wilayah Timur Tengah jumlah pengguna internet yaitu 164 juta orang dengan jumlah populasi sebesar 254 juta orang, sehingga presentase pengguna internet di wilayah Timur Tengah sebesar 64,5%. Terakhir jumlah pengguna internet di wilayah Australia (Oceania) sebesar 28 juta orang dengan jumlah populasi yaitu 41 juta orang, sehingga persentase pengguna internet di Australia yaitu 68,9 % dari keseluruhan jumlah populasinya.[7]

Di Indonesia, pengguna internet juga memiliki peningkatan dari tahun ke tahun. Menurut data yang dikeluarkan oleh APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) tahun 2017, berikut bagan data perkembangan pengguna internet dari tahun 1998 hingga 2017:[8]

[7] *Ibid.*

[8] APJII, Infografis Penetrasi & Perilaku Pengguna Internet Indonesia, Hasil Survey 2017, 2017

Gambar 2. Perkembangan pengguna internet di Indonesia



Sumber: APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), Penetrasi & Perilaku Pengguna Internet Indonesia, 2017

Jumlah pengguna internet di Indonesia pada tahun 2017 sebesar 143,26 juta atau sekitar 54,68% dari total jumlah penduduk Indonesia sebesar 262 juta jiwa. Jumlah tersebut meningkat dari tahun 2016 yang hanya berjumlah 132,7 juta pengguna internet atau sekitar 51,5 persen dari total jumlah penduduk Indonesia sebesar 256,2 juta. Dalam data survey ini menunjukan penyebaran penggunaan internet hampir menyeluruh di wilayah Indonesia dengan pengguna internet paling tinggi di wilayah Jawa yaitu 58,08 %, lalu disusul dengan Sumatera 19,0 %, Kalimantan 7,97 %, Sulawesi 6,73%, Bali-Nusa 5,63 %, dan terendah adalah Maluku-Papua sebesar 2,49 %.[9]

Komposisi usia pengguna internet juga beragam, mulai dari 13 tahun hingga lebih dari 54 tahun. Pengguna internet paling banyak berada pada kisaran usia 19-34 tahun dengan persentase sebesar 49,52%, lalu usia 35-54 tahun dengan persentase sebesar 29,55%, usia 13-18 tahun dengan presentasi sebesar 16,68%, dan terendah berada pada usia diatas 54 tahun dengan presentase sebesar 4,24% dari keseluruhan jumlah pengguna internet. Usia produktif dari

[9] *Ibid.*

kalangan muda dan remaja memiliki tingkat penetrasi pengguna internet yang paling tinggi yaitu pada usia 13-18 tahun dengan presentase 75,50% dan usia 19-34 tahun sebesar 74,23%, lalu disusul oleh usia 35-54 tahun sebesar 44,06% dan diatas 54 tahun sebesar 15,72%. Hal tersebut menunjukan bahwa usia produktif kalangan muda dan remaja dapat dikatakan memiliki ketergantungan yang tinggi terhadap internet, dan atas data tersebut menggambarkan hampir seluruh lapisan usia memanfaatkan adanya internet.[10]

Pada hasil survey yang dilakukan oleh APJII ini dapat dilihat persebaran internet pada masyarakat Indonesia hampir menyeluruh di wilayah Indonesia, selain itu semua lapisan usia pun ikut memanfaatkan adanya internet. Ditambah lagi tingkat level ekonomi tidak memengaruhi persebaran penggunaan internet, seluruh masyarakat pada berbagai tingkat level ekonomi menggunakan internet dari strata level ekonomi sosial atas, menengah bagian atas, menengah bagian bawah, dan strata level ekonomi sosial bawah. Dengan pengguna internet paling banyak malah justru pada pengguna internet level ekonomi sosial bawah sebesar 74,62%, namun penetrasi penggunaan internet paling tinggi berada pada level ekonomi sosial atas yaitu sebesar 93,10%. Durasi penggunaan internet di Indonesia juga dapat dikatakan memiliki intensitas yang cukup tinggi, dengan persentase pengguna internet setiap minggunya sebesar 65,98 % setiap hari, dan durasi penggunaan internet lebih dari 7 jam setiap harinya sebesar 26,48% pengguna internet, 29,63% pengguna internet menggunakan 4-7 jam sehari, dan yang paling banyak dengan presentase 43,89% pengguna menggunakan internet selama 1-3 jam. [11]

Data-data tersebut menunjukan bahwa seluruh lapisan masyarakat dalam seluruh wilayah Indonesia menikmati dan memanfaatkan Perkembangan siber dan berbagai teknologi yang mendukungnya mempunyai arti dan peranan yang penting dalam

[10] *Ibid.*
[11] *Ibid.*

segala aspek kehidupan. Hal tersebut berdampak pada masuknya era baru dalam berbagai bidang kehidupan manusia, mulai dari kehidupan ekonomi, sosial, budaya, politik dan hukum.[12] Misalnya saja penggunaan perkembangan lingkup siber dalam transaksi perbankan, analisis dan komputasi data di perusahaan maupun pemerintahan, teknologi militer, hingga masyarakat umum yang memanfaatkan ruang siber sebagai media komunikasi. Adanya ruang siber yang berdampak pada lancarnya arus informasi, juga dapat membantu perekonomian masyarakat terlebih meningkatnya perekonomian suatu Negara.[13]

Pemanfaatan siber dan berbagai teknologi yang mendukungnya kini telah mampu dalam melakukan pengumpulan, penyimpanan, pembagian, dan bahkan yang terbaru adalah penganalisaan data secara otomatis. Berbagai sektor kehidupan masyarakat telah menggunakan ruang siber dan sistem teknologi informasi yang ada, misalnya pemanfaatan siber bidang di bidang ekonomi atau perdagangan/bisnis (*e-commerce*) yang digunakan misalnya untuk mencari harga baik barang ataupun jasa, membantu pekerjaan, mendapatkan informasi membeli, melakukan pembelian secara *online*, mencari informasi pekerjaan, melakukan transaksi perbankan, dan sarana untuk perdagangan secara online. Pemanfaatan siber juga digunakan dalam bidang layanan publik atau pemerintahan *(e-government),* misalnya saja untuk mencari informasi tentang undang-undang/peraturan, memberikan informasi administrasi, pendaftaran KTP/SIM/PASPOR/BPJS, pelaporan pajak, laporan pengaduan, dan berbagai sistem lain yang diberikan negara untuk melakukan

[12] Edmon Makarim, Pengantar Hukum Telematika, Raja Grafindo Persada, Jakarta, 2005, hlm. 56.

[13] Tri Andika, Kedaulatan di Bidang Informasi dalam Era Digital: Tinjauan Teori dan Hukum Internasional, Jurnal Bina Mulia Hukum, Volume 1, Nomor 1, 2016, hlm. 44

pelayanan publik, serta dimanfaatkan masyarakat untuk akses keterbukaan publik.[14]

Pemanfaatan siber lainnya juga dapat dilihat dalam bidang pendidikan/edukasi *(e-education).* Hal ini misalnya internet digunakan untuk membaca artikel, melihat video pendidikan atau tutorial, menyebarkan informasi pendidikan seperti artikel dan video edukasi, melakukan pendidikan atau kursus secara *online,* hingga yang terbaru melakukan kegiatan pendaftaran pada instansi pendidikan dengan menggunakan internet.[15] Pemanfaatan siber kini juga dapat digunakan dalam bidang kesehatan *(e-health).* Hal ini misalnya penggunaan internet untuk mencari informasi tentang kesehatan dan melakukan konsultasi kesehatan dengan para ahli kesehatan. Dalam bidang sosial-politik, internet digunakan misalnya untuk mencari berita baik tentang hal-hal sosial, politik, maupun lingkungan, seperti membaca informasi keagamaan, membaca berita politik, dan untuk kegiatan amal.[16]

Pemanfaatan siber kiranya paling popular digunakan dalam bidang gaya hidup dan sebagai hiburan. Hal ini misalnya penggunaan internet dalam mengakses sosial media, melakukan pengunduhan musik atau lagu, melakukan pengunduhan atau menonton film, mencari informasi tentang *entertainment* atau hobi, membaca cerita, membaca berita olahraga, dan yang kini sedang berkembang bermain *game* pada berbagai perangkat elektronik. Siber juga digunakan sebagai *search engines, social networks,* dalam konektifitas *smartphone* dan *mobile internet* serta perkembangan industri komputasi awan atau *cloud computing* sebagai media penyimpanan data.[17]

Kemajuan teknologi informasi dan komunikasi yang semakin pesat menyebabkan perubahan perilaku masyarakat dan peradaban

---

[14] Berdasarkan data yang diungkapkan oleh APJII dalam perilaku pemanfaatan dan penggunaan internet di Indonesia, APJII, Infografis Penetrasi & Perilaku Pengguna Internet Indonesia, 2017

[15] *Ibid.*

[16] *Ibid.*

[17] *Ibid.*

manusia secara global, serta memberikan perubahan sosial yang secara signifikan berlangsung dengan cepat.[18] Pada data statistik tentang penetrasi internet di dunia memperlihatkan bahwa pada akhir tahun 2017 telah mencapai kurang lebih 54% dari total 7,634 miliar penduduk dunia. Hal ini berarti bahwa satu dari dua individu di dunia ini merupakan pengguna internet.[19] Penggunaan ruang siber dan teknologinya yang terus berkembang memiliki banyak manfaat positif yang dapat dirasakan, namun juga perlu diperhatikan lebih lanjut tentang dampak negatif yang dapat terjadi dalam penggunaan teknologi siber ini. Penggunaan ruang siber serta teknologi yang ada tanpa adanya kontrol yang baik dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan berbagai kegiatan yang dapat merugikan pihak lain.

Walaupun memberikan berbagai manfaat dan keuntungan yang ada dari penggunaan internet, ruang siber dalam kaitannya dengan hubungan internasional dapat menjadi sumber berbagai potensi ancaman, kerentanan, dan ketidakamanan pada tatanan internasional.[20] Pemanfaatan ruang siber yang tidak mengenal batas-batas wilayah Negara, membuat penggunaan siber oleh suatu pihak yang merugikan pihak lain dapat dilakukan oleh aktor Negara (s*tate actor)* maupun aktor bukan negara *(non-state actor).* Aktor Negara sebagai aktor hubungan internasional yang menjadi subyek interaksi antar Negara-negara yang berdaulat. Merujuk pada sejarah yang ada, Negara-negara di dunia memiliki potensial konflik yang berujung pada perang, misalnya saja Perang Dunia I dan Perang Dunia II.[21] Selain aktor Negara, terdapat juga aktor bukan Negara yang perilakunya mempunyai pengaruh terhadap kehidupan Negara maupun bangsa itu sendiri, seperti misalnya *intergovernmental*

[18] Ahmad M. Ramli, Cyber Law & HAKI dalam Sistem Hukum Indonesia, Bandung, Refika Aditama, 2004, hlm.1

[19] Miniwatts Marketing Group, Internet Usage Statistic

[20] Nazli Choucri dan David Clark, Cyberspace and International Relations; Toward an Integrated System (Massachusettes: MIT press. 2011) hlm. 2

[21] Soeprapto, R., Hubungan Internasional: Sistem, Interaksi dan Perilaku, Jakarta: RajaGrafindo Persada, 1997

organizations (IGOs), *international non-governmental organizations* (INGOs), *non-governmental organizations* (NGOs) dan *transnational companies* (TNCs) atau *multinational corporations* (MNCs).[22]

Era yang ada sekarang ini mendorong potensi perang antar Negara tidak lagi menggunakan cara perang tradisional dan konvensional. Akibatnya, kekuatan negara tidak lagi dilihat pada kekuatan persenjataan, tetapi juga pada segi budaya, perekonomian, politik, dan teknologi. Bentuk dari peperangan pun berubah yang menimbulkan ancaman baru pada ruang siber.[23] Ancaman serangan yang terjadi pada ruang siber pada suatu Negara pun juga dapat dilakukan oleh aktor-aktor non Negara yang mempunyai pengaruh terhadap kehidupan suatu Negara misalnya individu hacker, kelompok hacker, kegiatan para hacker, *non-government organization* (NGO), terorisme, kelompok kejahatan terorganisir (*organized criminal groups*) dan sektor swasta (seperti *internet companies and carries*, *security companies*) dapat mengancam pertahanan dan kedaulatan Negara.[24]

Sumber ancaman kejahatan yang dilakukan oleh aktor-aktor tersebut dalam ruang siber dapat dilakukan secara sengaja maupun tidak sengaja dengan berbagai motif yang ada misalnya untuk mendapatkan keuntungan finansial, militer, politik maupun tujuan lainnya. Siber menjadi ancaman bagi Negara disebabkan ruang lingkupnya yang dapat dimanfaatkan untuk mencuri informasi, penyebaran ide yang bersifat destruktif, maupun serangan terhadap sistem informasi di berbagai bidang, seperti data perbankan, jaringan militer, bahkan sistem pertahanan Negara. [25] Isu siber menjadi bahasan di level *high politic* setelah terdapat kejadian seperti

---

[22] Perwita, A.A.B. & Yani, Y.M., Pengantar Ilmu Hubungan Internasional, Bandung: Rosda, 2006. Hlm. 1

[23] Ineu Rahmawati, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense, Jurnal Pertahanan & Bela Negara, Vol. 7 No. 2, 2017, hlm. 52

[24] W. Pearlman & K.G. Cunningham, "Non-State Actors, Fragmentation, and Conflict Processes", Journal of Conflict Resolution, Vol.2 No. 56, 2012

[25] Michael Smith, "Research Handbook on International Law and Cyberspace", (Massachusetts: Edwar Elgar Publishing Limited, 2015), hlm. 1-3

serangan siber di Georgia dan Estonia, serta penggunaan serangan berbasis siber pada sistem nuklir Iran. Hal ini menunjukan bahwa ancaman kenegaraan yang berevolusi menjadi serangan siber bukan sekedar konsep saja.[26]

Peristiwa Estonia pada tahun 2007 dan Georgia pada tahun 2008 merupakan contoh serangan kejahatan siber (*cyber crime*) yang memanfaatkan *Distributed Denial of Service* (DdoS), hal ini mampu melumpuhkan aktivitas negara karena banyak sektor infrastruktur kritis yang diserang. Serangan siber di Estonia terjadi dari 27 April hingga 18 Mei tahun 2007, beberapa komponen infrastruktur siber diserang dengan DdoS, *website defacements, DNS server attacks, mass e-mail*, dan *comment spam.* Serangan terjadi pada beberapa infrastruktur siber yang ada pada Estonia, mulai dari situs pemerintahan, perbankan, hingga situs-situs surat kabar lokal. Bahkan jaringan perbankan, telekomunikasi dan jaringan vital lainnya lumpuh total, yang pada akhirnya berakibat pada lumpuhnya perekonomian dan beberapa aktivitas masyarakat terganggu.[27]

Serangan siber di Georgia terjadi pada tahun 2008, serangan siber menjadi awal permulaan serangan dari Rusia sebelum melakukan serangan fisik kepada Georgia. Serangan ini bertujuan mengganggu, merusak dan meruntuhkan infrastruktur siber milik pemerintah dan masyarakat sipil Georgia, bahkan untuk dimanfaatkan oleh musuhnya seperti pemblokiran, *re-routing of traffic* dan pengambil alihan kendali dari berbagai infrastruktur siber di Georgia. Serangan tersebut menjadi pola baru dalam sejarah peperangan, dimana serangan fisik kepada suatu Negara oleh Negara

[26] Nazli Choucri dan David Clark, Cyberspace and International Relations; Toward an Integrated System

[27] Andreas Schmidt, The Estonian Cyberattacks, dalam Jason Healey ed., The fierce domain – conflicts in cyberspace 1986-2012, Washington, D.C.: Atlantic Council, 2013 hlm. 1-3

lain dikoordinasikan dengan serangan siber yang terkoordinir dengan baik.[28]

Serangan siber berikutnya yang cukup mengkhawatirkan adalah serangan Stuxnet. Stuxnet ditemukan pada Juni 2010 setelah menyerang fasilitas nuklir Iran di Natanz. Serangan siber ini berupa *malware/worm/virus* yang sangat canggih yang mampu melumpuhkan seperlima sistem kendali pengayaan nuklir dari pembangkit listrik tenaga nuklir milik Iran.[29] Tidak hanya hal tersebut Stuxnet telah menginfeksi lebih dari 60.000 komputer yang merupakan lebih dari setengah jumlah komputer yang ada di Iran. Virus ini menyebar dan menginfeksi sistem komputer melalui internet, sehingga serangan siber Stuxnet ini dapat dikatakan sebagai senjata siber untuk melumpuhkan sistem siber target.[30] Contoh serangan siber diatas hanya beberapa dari sekian banyak serangan siber yang terjadi di dunia.

Ruang siber yang tidak mengenal adanya batas Negara membuat beberapa serangan siber juga pernah terjadi di Indonesia. Sekitar tahun 1998 misalnya terkait dengan masalah politik dan sosial yang terjadi di Indonesia, serangan siber terjadi ketika kerusuhan tentang rasial, Indonesia berperang di dunia maya dengan para hacker dari China dan Taiwan. Lalu pada tahun 1999, juga muncul kerusuhan di dunia maya antara Indonesia dan Portugal terkait kasus pembebasan Timor Timur. Bahkan ketika saling serang dalam ruang siber terjadi hingga memasuki sistem dan mampu menghapus semua data yang ada. Dalam beberapa tahun terakhir ini sering terjadi saling serang dalam ruang siber antara hacker Indonesia dan Malaysia. Aksi ini biasanya bermula ketika muncul

---

[28] Georgia Government, Russian Invasion of Georgia: Russian Cyberwar on Georgia, http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf hlm. 1, diakses 22 Agustus 2018

[29] Michael B Kelley, The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought, https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11/?IR=T diakses 22 Agustus 2018

[30] John P. Farwell and Rafal Rohozinski, Stuxnet and the Future of Cyber War, Survival 53, no. 1 (2011): 23-40.

konflik politik ataupun persaingan kedua Negara. Meskipun tidak melibatkan pemerintah kedua Negara, namun aksi para hacker ini menyerang infrastruktur siber milik pemerintah Malaysia maupun Indonesia.[31]

Serangan siber oleh Stuxnet ternyata selain menyerang infrastruktur nuklir di Iran, efeknya pun menyebar ke Negara Indonesia.[32] Seperti yang dilansir oleh Symantec produsen Antivirus, Indonesia berada di urutan kedua setelah Iran di antara 10 negara yang mengalami serangan siber Stuxnet. Dengan adanya hal tersebut membuat komputer-komputer di Indonesia terindikasi terjangkit virus Stuxnet ini.[33] Lalu pada tahun 2013 berdasarkan bocoran dokumen dari Edward Snowden, mantan anggota National Security Agency (NSA) Amerika Serikat, Indonesia menjadi korban penyadapan oleh badan intelijen Australia. Pada dokumen yang dibocorkan Snowden tersebut berisi daftar target penyadapan yang menunjukan nama Presiden Indonesia Susilo Bambang Yudhoyono, istrinya, dan beberapa orang terdekat dalam lingkungan presiden.[34] Penyadapan terhadap Indonesia ini dilakukan NSA Amerika Serikat bekerja sama dengan Direktorat Sandi Pertahanan (DSD) Australia. Alasan Australia membantu Amerika Serikat melakukan penyadapan adalah untuk memajukan kepentingan nasionalnya sendiri serta sebagai kontribusi terhadap aliansi dengan Amerika Serikat.[35]

Beberapa serangan kejahatan siber yang ada tersebut hanya sebagian kecil yang ada di Indonesia, masih banyak lagi serangan siber yang terjadi di Indonesia dengan berbagai pola modus dan tujuannya. Misalnya saja yang serangan siber besar yang baru terjadi

---

[31] Reda Manthovani, Problematika dan Solusi Penanganan Kejahatan CYBER di Indonesia, Malibu, Jakarta, 2006, h. 67-68.

[32] John P. Farwell and Rafal Rohozinski, Stuxnet and the Future of Cyber War, hlm. 23

[33] Symantec, W32.Stuxnet, https://www.symantec.com/security-center/writeup/2010-071400-3123-99 diakses pada 23 Agustus 2018

[34] Richard Tanter, "Indonesia, Australia and Edward Snowden: ambiguous and shifting asymmetries of power," The Asia Pacific Journal, Vol. 12, Issue 10, No. 3, 2014.

[35] Lisbet, Sikap Indonesia Terhadap Isu Penyadapan Amerika Serikat dan Asutralia, Pusat Pengkajian, Pengolahan Data dan Informasi (P3DI) Sekretariat Jenderal DPR RI, Vol. V, No. 21, 2013, hlm. 6

kemarin oleh Ransomware Wannacry. Malware ini terdeteksi awal memasuki wilayah Indonesia sejak menyerang sistem siber milik Rumah Sakit Harapan Kita dan Dharmais, ratusan server dan komputer yang digunakan untuk operasional rumah sakit terkena dampaknya, sehingga kegiatan di rumah sakit pun terganggu.[36] Setelah menyerang rumah sakit, Ransomware Wannacry dengan cepat menyebar pada server dan komputer di Indonesia, hingga Kementerian Komunikasi dan Informatika menerbitkan *press release* untuk memberitahukan informasi dari malware ini dengan mengeluarkan siaran pers siaran pers no. 55/HM/KOMINFO/05/2017 tentang himbauan serta langkah tindakan pencegahan atas malware Ransomware Wannacry.[37]

Menurut data yang diungkapkan oleh ID-SIRTII, serangan siber di Indonesia pada tahun 2016 berjumlah 135.672.984, hal ini meningkat dari tahun 2015 yang hanya berjumlah 28.430.843. Pada tahun 2016 tersebut presentasi serangan siber paling banyak dilakukan dengan malware yaitu sebesar 47%, selanjutnya 44% merupakan kasus penipuan pada ruang siber, dan sisanya berbentuk kejahatan siber lainnya, seperti website *defacement*, dan aktivitas manipulasi data dan kebocoran data.[38] Pada tahun 2017, dilihat dari hasil pemantauan trafik anomali nasional dari Januari sampai November 2017, tercatat oleh Id-SIRTII/CC ada sebanyak 205.502.159 serangan. Total dari seluruh aktivitas malware yang terdeteksi, sebanyak 37,72% berkaitan dengan serangan DOS, 20,93% merupakan *exploit*, 18% adalah trojan atau berkaitan dengan aktivitas trojan, 15% tercatat sebagai *bad unknown* dan sisanya tercatat sebagai *adware, shell code, cnc, misc attack, network scan,*

---

[36] Oik Yusuf, Kronologi Serangan Ransomware Wannacry, https://tekno.kompas.com/read/2017/05/15/09095437/kronologi.serangan.ransomware.wannacry.yang.bikin.heboh.internet diakses pada 23 Agustus 2018

[37] Indonesia, Siaran Pers Kementerian Komunikasi Dan Informatika No. 55/Hm/Kominfo/05/2017 Tentang Himbauan Agar Segera Melakukan Tindakan Pencegahan Terhadap Ancaman Malware Khususnya Ransomware Jenis Wannacry

[38] ID-SIRTII., Tren Serangan Siber Nasional 2016 dan Prediksi 2017, ID-SIRTII., 2017

dan *web application attack*.[39] Sedangkan pada tahun 2018, penelitian yang dilakukan oleh Akamai menemukan di Indonesia serangan siber yang bersifat *web attack* berjumlah 364,551,895. Sekitar setengah dari lalu lintas penyalahgunaan siber ini ditujukan kepada jalur pelayaran, penerbangan, dan situs perjalanan.[40]

Dampak serangan siber yang terjadi, kepada sektor perekonomian Indonesia cukup memberikan kerugian yang besar pada Negara Indonesia. Pada penelitian yang dilakukan oleh Daka advisory, mereka menghitung nilai kerugian dalam pengeluaran atas adanya serangan siber atau kejahatan siber dengan menggunakan metode yang dilakukan oleh Anderson, et al. [41] Hasil dari penghitungan yang ada dibagi menjadi beberapa kategori seperti sebagai berikut:[42]

Gambar 3. Perkiraan Kerugian Ekonomi Akibat Kejahatan Siber

	Global	Indonesia
GDP:*	USD 71, 620bn	USD 895bn
Per cent of global GDP*:		1,20%
Cost of:**		
Genuine cybercrime:	USD 3,457m	USD 43m
Transitional cybercrime:	USD 46,600m	USD 582m
Cybercriminal infrastructure:	USD 24,840m	USD 310m
Traditional crimes becoming cyber:	USD 150,200m	USD 2,748m

Sumber: Daka advisory, Meeting The Cyber Security Challenge in Indonesia, An Analysis of The Threats and Responses

Dari tabel perkiraan tersebut, Indonesia menderita kerugian ekonomi dari kejahatan siber yang sebenarnya sebesar USD 43

[39] Agus Tri Haryanto, Indonesia dibombardir 205 Juta Serangan Cyber, https://inet.detik.com/security/d-3781096/indonesia-dibombardir-205-juta-serangan-cyber diakses pada 23 Agustus 2018

[40] Akamai Internasional, State of the Internet/security, Web Attacks, 2018, https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf diakses pada 23 Agustus 2018

[41] Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. and Levi, M. (2012) Measuring the cost of cybercrime. Retrieved September 2013, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf diakses pada 23 Agustus 2018

[42] Daka advisory, Meeting The Cyber Security Challenge in Indonesia, An Analysis of The Threats and Responses, Commissioned by British Embassy Jakarta, 2013, hlm. 22

miliar, lalu kejahatan siber transisional sebesar USD 582 miliar, kejahatan siber pada infrastruktur yang ada sebesar USD 310 miliar, dan kejahatan tradisional yang cenderung menjadi siber sebesar USD 2,478 miliar.[43] Selanjutnya berdasarkan data dari Norton Symantec selama tahun 2015 sampai dengan Februari 2016, kejahatan online di Indonesia menimbulkan total kerugian Rp 194.6 miliar.[44] Pada tahun 2017 menurut data yang dikeluarkan juga oleh Norton Symantec, kerugian yang diderita Indonesia sebesar USD 3,2 billion.[45] Terakhir potensi kerugian ekonomi akibat dari insiden keamanan siber tahun 2018 menurut hasil penelitian Frost dan Sullivan yang diprakarsai oleh Microsoft, akan mencapai nilai sebesar USD 34,2 miliar.[46]

Hal tersebut memunculkan gambaran tentang kerugian ekonomi yang diderita Indonesia dari adanya insiden keamanan siber, masih banyak lagi penelitian-penelitian lain yang mencoba mencari tahu seberapa banyak kerugian suatu Negara lebih utama Indonesia dari adanya insiden keamanan siber. Perbedaan perhitungan kerugian ekonomi yang di derita Indonesia, serta kenaikan dan penurunan dari angka kerugian setiap tahunnya tidak berarti perlu untuk diperdebatkan. Namun intinya seluruh hasil penelitian tentang angka kerugian ekonomi yang di derita Indonesia dari serangan siber, kejahatan siber, ataupun insiden keamanan siber tidak ada yang menunjukan angka kecil atau sedikit. Hingga kerugian yang di derita Indonesia dari insiden keamanan siber ini perlu usaha untuk dikurangi, ditanggulangi, bahkan dihilangkan.

---

[43] *Ibid.*

[44] Norton Symantec, 2016 Norton Cyber Security Insights Report Global Result, Symantec Corporation, 2017, lihat juga Maulia Jayantina Islami, Tantangan dalam Implementasi Startegi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index, Jurnal Masyarakat Telematika dan Informasi, Volume: 8 No. 2, 2017, hlm. 138

[45] Norton Symantec, 2017 Norton Cyber Security Insights Report Global Result, Symantec Corporation, 2018, hlm. 13

[46] Wilfridus Setu Embu, Insiden Keamanan Siber Bisa Picu Kerugian Indonesia hingga Rp 483 Triliun, https://www.merdeka.com/uang/insiden-keamanan-siber-bisa-picu-kerugian-indonesia-hingga-rp-483-miliar.html diakses pada 23 Agustus 2018

Kerusakan infrastruktur siber yang ada akibat dari adanya insiden keamanan siber juga mampu menambah derita Indonesia bila insiden keamanan siber tidak ditanggulangi dengan baik. Hal ini seperti misalnya yang terjadi pada kejadian serangan siber di Georgia. Dampak dari adanya serangan siber di Georgia membuat masyarakat Georgia mengalami kekurangan informasi, hal ini akan berujung pada banyak hal, misalnya psikologi masyarakat itu sendiri. Keadaan ini terjadi karena masyarakat Georgia tidak dapat berkomunikasi dan mengetahui apa yang terjadi pada dunia luar, bahkan informasi tentang apa yang terjadi di negaranya sendiri, serta instruksi yang perlu dilakukan dalam keadaan tersebut yang diberikan oleh pemerintah Georgia terhambat, sehingga dapat dikatakan masyarakat Georgia terisolasi dengan adanya serangan siber tersebut.[47]

Adanya insiden serangan siber ini juga membuat sistem perekonomian Negara pun terganggu, misalnya saja serangan siber pada sistem perbankan yang juga ikut diserang sehingga sistem siber perbankan yang ada di Georgia menjadi *offline*. Pada periode serangan yang bersamaan, beberapa bank di Georgia dibanjiri dengan transaksi penipuan, maka bank internasional untuk menghindari penipuan tersebut melakukan langkah mitigasi kerusakan dengan memutus atau menghentikan transaksi dan operasinya dengan perbankan di Georgia selama serangan siber berlangsung.[48] Adanya hal tersebut berujung pada terganggunya penilaian kelayakan kredit pemerintah Georgia yang terbukti dengan menurunnya peringkat default mata uang lokal dan asing jangka panjang di Georgia dari BB- menjadi B+.[49]

Dampak yang dialami oleh Georgia atas adanya serangan siber terhadap infrastruktur siber di negaranya membuat kesulitan pada

---

[47] David Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, 6 Januari 2011, hlm. 2

[48] Kenneth Corbin, "Lessons from the Russia-Georgia Cyberwar," internetnews. com: Real time IT News, 12 March 2009, (16 October 2010)

[49] Polya Lesova, "Fitch Lowers Georgia's Debt Ratings to B+," https://www.marketwatch.com/story/fitch- lowers-georgias-debt-ratings-to-b?dist=msr_2, diakses 22 Agustus 2018

berbagai sektor sehari-hari kehidupan masyarakat Georgia. Selain itu insiden serangan siber di Estonia yang tidak hanya berdampak pada infrastruktur siber saja namun juga secara tidak langsung mempengaruhi keadaan pada dunia nyata. Terganggu dan rusaknya infrastruktur internet mengakibatkan pelayanan Pemerintah Estonia dan beberapa perusahaan komersial kepada masyarakat terhambat. Sistem pelayanan di negara ini sangat tergantung kepada layanan *online*. Terganggunya pelayanan online dapat menimbulkan gejolak sosial di tengah masyarakat. Selain itu, kerugian secara materil juga dirasakan oleh Pemerintah dengan adanya infrastruktur internet yang harus diperbaiki.[50]

Serangan yang terjadi pada infrastruktur siber tidak jarang terhubung dengan objek lain yang berada di dunia nyata, sehingga akan menimbulkan kerugian dan korban yang nyata. Serangan siber dapat menimbulkan dampak ketakutan secara luas kepada masyarakat, yang berujung pada kepanikan akan adanya serangan siber susulan. Serangan siber dapat merugikan secara ekonomi karena menimbulkan ketidakpercayaan pelaku ekonomi kepada Negara tersebut. Para pelaku usaha menjadi tidak percaya atas sistem keamanan informasi yang dibangun oleh Negara tersebut, karena Negara dianggap tidak mampu menjaga sistem keamanan sibernya. Misalnya saja pada kasus penyebaran *spyware* dalam ruang siber yang disebarkan untuk mengumpulkan informasi dan kemudian mengumpulkan informasi di Negara tersebut kepada si penyerang. [51]

Sejatinya di ruang siber yang sangat luas ini sedang terjadi perang tak kasat mata antara *cyber defender* dengan *cyber attacker*. Dampak fisik dari perang tersebut dapat berupa *deface* situs-situs pemerintah atau pencurian data transaksi keuangan secara elektronik atau percobaan intrusi ke dalam sistem informasi

---

[50] Petrus Reinhard Golose, Invasi Terorisme ke Cyberspace, (Jakarta: Penerbit Yayasan Pengembangan Kajian Ilmu Kepolisian, 2015), hlm. 141

[51] *Ibid.*, hlm. 25-26

Indonesia.[52] Maka berdasarkan fakta tersebut infrastruktur siber perlu dilindungi keamanannya dari serangan-serangan yang mungkin terjadi. Keamanan siber menjadi suatu yang penting agar infrastruktur siber terus dapat berjalan bagaimanapun meski terdapat serangan siber. Keamanan siber perlu mendapatkan perhatian serius demi menjamin efektivitas keandalan, ketersediaan, dan integritas jaringan informasi, baik secara nasional maupun global.[53]

Pada pemeringkatan Global Cybersecurity Index (GCI) tahun 2017 yang dilakukan oleh International Telecommunication Union (ITU), mereka menilai kemampuan keamanan siber kepada 165 negara-negara dunia. Penilaian ini juga dilakukan kepada Indonesia berdasarkan konsep lima kategori penilaian atau dinamakan *The Five Pilars of GCI Framework* yaitu *legal, technical and procedure, organizational, capacity building,* dan *international cooperation*. Dalam penilaiannya Indonesia mendapatkan nilai 0.424 pada peringkat 70 dan masih berada pada *mature stage,* yang berarti belum termasuk dalam jajaran Negara-negara yang dianggap memiliki komitmen tinggi terhadap keamanan siber, atau dalam tahap persiapan pengembangan komitmen dan terlibat dalam program serta inisiatif keamanan siber. Hal ini sangat jauh tertinggal dengan Singapura yang memimpin di peringat pertama dengan nilai 0.925 dan Malaysia di peringkat ketiga dengan nilai 0.893. [54] Indonesia perlu meningkatkan usahanya dalam keamanan siber agar kerugian-kerugian yang ada dapat dihindarkan serta berbagai manfaat yang dapat dirasakan salah satunya untuk meningkatkan perekonomian Negara.

---

[52] Dewan Ketahanan Nasional R.I., "Melindungi Infrastruktur Kritis Nasional dari Serangan Cyber: Perspektif Kebijakan Ketahanan Nasional," https://dkn.go.id/berita/55/melindungi-infrastruktur-kritis-nasional-dari-serangan-cyber--perspektif-kebijakan-ketahanan-nasional.html diakses pada 24 Juli 2018

[53] Ahmad Budi Setiawan, "Kajian Strategi Pengamanan Infrastruktur Sumber Daya Informasi Kritis," Buletin Pos dan Telekomunikasi, vol. 13, No. 1 (2015), hlm. 57

[54] International Telecommunication Union (ITU), Global Cybersecurity Index (GCI) 2017, Geneva, 2017

Upaya untuk meningkatkan keamanan siber salah satunya dapat dicapai dengan adanya kolaborasi antara pemerintah dan pihak swasta. Atas banyaknya insiden keamanan siber di dunia, baik yang memiliki pengaruh besar maupun kecil, melahirkan konsep baru untuk menciptakan keamanan pada ruang siber yaitu kolaborasi antara pemerintah dan pihak swasta dengan beberapa sebutan seperti misalnya *public-pivate partnership* atau *public-private collaboration.* Para pembuat kebijakan terutama pemerintah suatu Negara dengan para pemilik bisnis yang bersifat private mulai menyadari perlunya kolaborasi yang lebih banyak dan lebih baik antara sektor publik dan swasta mengenai isu-isu yang berkaitan dengan keamanan siber seperti enkripsi data, *data sharing* dan *data localization*.[55]

Beberapa Negara yang telah menerapkan konsep ini yaitu misalnya Amerika Serikat yang hampir 85% infrastruktur sibernya dimiliki oleh pihak private. Strategi yang digunakan oleh Amerika Serikat adalah *sector-based approach.* Dengan pendekatan ini maka setiap sektor infrastruktur memiliki *lead agency* baik yang dipegang oleh pemerintah federal maupun Department of Homeland Security (DHS). Terkait hal ini pemerintah Amerika Serikat membentuk *Sector Co-ordinating Council* yang keanggotaanya terdiri dari perwakilan pemilik atau operator infrastruktur dari setiap sektor, serta berurusan dengan isu lintas sektor diantara industri privat, terdapat juga *Government Co-ordinating Councils* yang keanggotaanya merupakan perwakilan dari seluruh instansi pemerintah yang terlibat, serta berurusan dengan *government cross- sector review*. Pihak pemilik atau operator infrastruktur bertanggungjawab untuk melakukan perlindungan, restorasi, koordinasi, dan memberikan

[55] Walter Bohmayr, Stefan Deutscher, & David Mkrtchian, Towar A Model For Public-Private Collaboration in Cybersecurity, The Boston Consulting Group, Inc., 2018

masukan, rekomendasi, serta pendapat ahli kepada pemerintah federal.[56]

Pada Negara Jerman, diperkirakan 90% dari infrastruktur siber dimiliki oleh privat. Pola pemetaan perlindungan infrastruktur tidak tersentralisasi namun lebih menempatkan privat sebagai pemeran utama. Meskipun begitu tetap ada lembaga yang bertanggung jawab atas koordinasi kebijakan perlindungan infrastruktur pada tingkat pemerintahan, yaitu Centre for the Protection of Critical Infrastructure within the Federal Office for Civil Protection and Disaster Response (Federal Ministry of Interior). Badan tersebut bertugas untuk menyebarkan informasi dan kesadaran akan perlindungan infrastruktur kritis, *public-private partnership*, analisis dan konsep perlindungan, dan tindakan-tindakan perlindungan, dengan kerangka kebijakan yaitu *baseline protection concept*.[57] Pada gambaran konsep di Negara Amerika Serikat dan Jerman tersebut maka dapat disimpulkan bahwa strategi perlindungan infrastruktur siber merupakan *shared responsibility* dan membutuhkan kerjasama yang erat antara pemerintah dengan pemilik atau operator infrastruktur. Secara umum, pemilik atau operator infrastruktur bertanggung jawab atas tindakan-tindakan perlindungan, yang mana kebanyakan didasarkan oleh parameter atau standar yang telah ditetapkan oleh Pemerintah.

Pada Negara Indonesia belum terdapat pengaturan yang memadai mengenai keamanan siber. Peraturan yang ada masih banyak memiliki keterbatasan dan kelemahan dalam melindungi infrastruktur siber dan keamanan siber. Beberapa kebijakan dan peraturan di Indonesia yang terkait dengan keamanan siber, misalnya pada institusi Kementerian Pertahanan atau Tentara Nasional Indonesia (TNI) dengan peraturan seperti Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan, Undang-Undang Nomor 34 Tahun 2004 tentang TNI, Undang-Undang Nomor 43 Tahun 2008 tentang

[56] Jupling, "The Protection of Critical Infrastructures," special report, Oct 2007, hlm. 11-13

[57] *Ibid.*, hlm. 14-15

Wilayah Negara, dan Peraturan Pemerintah Nomor 68 Tahun 2014 tentang Penataan Wilayah negara, yang memiliki keterbatasan tentang ruang siber yang belum menjadi wilayah pertahanan dan dalam tugas nirmiliter TNI hanya ditugaskan sebagai pendukung. Terpisahnya fungsi keamanan yang dimiliki Kepolisian Republik Indonesia dalam Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian dan fungsi pertahanan yang dimiliki TNI, hal ini dirasakan dapat menghambat tindakan pencegahan insiden siber.[58]

Pada institusi intelijen Indonesia, Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen memiliki keterbatasan untuk melakukan *cyber espionage* maupun untuk melakukan respon serangan siber terbatas. Dapat dilihat juga pada institusi Kementerian Komunikasi dan Informatika dalam Undang-Undang Nomor 36 Tahun 1999 tentang telekomunikasi, Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, masih memiliki keterbatasan dalam konteks infrastruktur telekomunikasi, penyiaran dan informatika untuk pelayanan publik. Undang-Undang tentang Informasi dan Transaksi Elektronik juga dianggap belum mampu mencakup seluruh aspek kemanan siber yang begitu luas.[59] Selain itu terdapat pula Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber, namun pedoman ini disusun sebagai acuan bagi tahapan persiapan, pembangunan, pelaksanaan dan pemantapan pertahanan siber hanya pada lingkungan Kementerian Pertahanan dan TNI.

Belum adanya ketentuan-ketentuan yang secara khusus mengatur mengenai keamanan siber, menimbulkan kerentanan dan gangguan pula terhadap Hak Asasi Manusia. Pada penjabaran

---

[58] David Putra S., & Datumaya W. Sumari, Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives, Jurnal Penelitian Politik, Vol. 13 No. 1, 2016, hlm. 9

[59] *Ibid.*, hlm. 10

tentang beberapa kasus dan berbagai kebutuhan masyarakat dalam ruang siber, mengambarkan hubungan yang saling ketergantungan antara Hak Asasi Manusia dengan Keamanan Siber. Untuk itu perlunya pengaturan terhadap Keamanan Siber untuk mewujudkan dua hal penting dalam usaha melindungi Hak Asasi Manusia pada ruang siber yaitu menciptakan ruang siber yang aman bagi semua penggunanya, dan juga membuat lingkungan yang aman untuk Hak Asasi Manusia pada ranah siber. Kedua hal yang relative baru ini antara Keamanan Siber dan Hak Asasi Manusia, sangat terkait dan saling terikat yang tidak bisa diabaikan salah satunya.[60]

Pada beberapa Negara bahkan akses internet dilihat menjadi Hak Asasi Manusia yang perlu dilindungi seperti misalnya di Estonia, Finlandia, Perancis, Yunani dan Spanyol.[61] Hal ini menjadi terkait dengan teori atau konsep tentang *Human Security* yang dibangun oleh Perserikatan Bangsa-Bangsa.[62] Konsep ini menggunakan pendekatan "*state-centric*" untuk memberikan keamanan dan menempatkan kebutuhan rakyat pada tingkat pertama. Munculnya konsep *Human Security* membantu meluncurkan gagasan kebutuhan individu atau masyarakat dan bagaimana keamanan nasional dapat dikonseptualisasikan sebagai orientasi utama untuk membantu memenuhi kebutuhan melalui berbagai layanan beragam yang perlu dilakukan pemerintah Negara.[63] Salah satu hak asasi manusia yang perlu mendapatkan pelayanan misalnya hak untuk menerima dan menyampaikan informasi, akan terganggu bila terjadi insiden keamanan siber, seperti yang telah dijelaskan sebelumnya misalnya pada kasus yang terjadi di Georgia. Maka Negara berkewajiban tidak hanya untuk memastikan warga Negara mereka dapat menggunakan

[60] Nezir Akyesilmen, Cybersecurity And Human Rights: Need For A Paradigm Shift?, Cyberpolitik Journal Vol. 1, No. 1, 2016, hlm. 40

[61] Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, 2012, hlm. 164

[62] UNDP, Human Development Report, New Dimensions of Human Security, Oxford and New York: Oxford University Press, 1994

[63] *Ibid.*, hlm. 45

hak-hak hukum mereka, tetapi juga memastikan perlindungan dan keamanan mereka.[64]

Perlunya melakukan pengelolaan urusan pemerintahan pada bidang keamanan siber dengan perumusan tata kelola yang dapat dirasakan efektif dalam penerapannya di Indonesia. Banyaknya infrastruktur siber yang dimiliki swasta membuat adanya kolaborasi antara pemerintah dan pihak swasta (*public-pivate partnership*) kiranya dapat menjadi suatu konsep yang akan mewujudkan keamanan siber yang efektif. Konsep baru tersebut kini telah banyak diterapkan pada Negara-negara yang telah terlebih dahulu memberikan perhatian lebih kepada keamanan siber. Atas berbagai penjelasan yang ada baik tentang kerugian yang diakibatkan dari adanya serangan siber, maupun peraturan yang belum memadai dalam memberikan perlindungan pada keamanan siber untuk melindungi keamanan masyarakat, maka perlu adanya pengaturan secara khusus yang mampu mencakup keseluruhan aspek tentang keamanan siber.

B. Identifikasi Masalah

Berdasarkan uraian latar belakang di atas, permasalahan utama dalam Keamanan Siber adalah tidak adanya undang-undang yang mengaturnya secara khusus. Maka dalam rangka merumuskan permasalahan yang dibahas dalam penyusunan Naskah Akademik Rancangan Undang-Undang tentang Keamanan Siber adalah sebagai berikut:

1. Bagaimana perkembangan kajian teori dan praktik empiris Keamanan Siber selama ini?
2. Bagaimana pengaturan mengenai Keamanan Siber dalam ketentuan peraturan perundang-undangan yang ada?
3. Apa yang menjadi landasan filosofis, sosiologis, dan yuridis dalam pelaksanaan Keamanan Siber?

[64] *Ibid.*, hlm. 166

4. Apa yang menjadi jangkauan, arah pengaturan, dan ruang lingkup pengaturan mengenai Keamanan Siber?

C. Tujuan dan Kegunaan Kegiatan Naskah Akademik

Sesuai dengan ruang lingkup identifikasi masalah yang dikemukakan di atas, tujuan kegiatan ini adalah untuk menyusun Naskah Akademik Rancangan Undang-Undang tentang Keamanan Siber, yaitu berupa naskah ilmiah yang memuat gagasan tentang perlunya materi-materi hukum yang bersangkutan diatur dengan segala aspek terkait, dilengkapi dengan referensi yang memuat konsepsi, landasan dan prinsip yang digunakan serta pemikiran tentang norma-normanya. Hal tersebut dilakukan untuk:

1. Menjelaskan mengapa Rancangan Undang-undang Keamanan Siber perlu dibentuk menjadi Undang-undang, dengan merumuskan permasalahan yang dihadapi dalam kehidupan berbangsa, bernegara, dan bermasyarakat terkait Keamanan Siber.
2. Merumuskan landasan, dasar pemikiran, dan hal lain tentang perlunya Rancangan Undang-Undang tentang Keamanan Siber.
3. Mengetahui dan merumuskan pertimbangan atau landasan filosofis, sosiologi, dan yuridis perlunya pembentukan Rancangan Undang-Undang tentang Keamanan Siber.
4. Mengetahui jangkauan, sasaran, ruang lingkup, serta arah pengaturan Rancangan Undang-Undang tentang Keamanan Siber.

Kegunaan penyusunan Naskah Akademik Rancangan Undang-Undang ini merupakan masukan dan landasan pemikiran dalam penyusunan Rancangan Undang-Undang Keamanan Siber, dalam kata lain merupakan acuan atau referensi penyusunan dan pembahasan Rancangan Undang-Undang sebagai solusi terhadap permasalahan dan kebutuhan hukum masyarakat.

D. Metode Penelitian

Penyusunan Naskah Akademik Rancangan Undang-Undang pada dasarnya merupakan suatu kegiatan penelitian, dengan

menggunakan metode penelitian hukum. Berbasis pada metode penelitian hukum, maka penyusunan Naskah Akademik Rancangan Undang-Undang tentang Keamanan Siber ini digunakan metode penelitian yuridis normatif yang kemudian diupayakan untuk menarik asas-asas hukum dalam rumusan norma yang akan menjadi acuan dalam penyusunan Rancangan Undang-Undang tentang Keamanan Siber. Data analisis dilakukan secara kualitatif berdasarkan aspek dan fakta-fakta filosofis, yuridis dan sosiologis. Dalam menggunakan metode ini, penyusun melakukan kajian literatur atau studi kepustakaan dengan menelaah (terutama) data sekunder berupa: bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.

Bahan hukum primer yaitu berupa aneka peraturan perundang-undangan yang menyangkut Keamanan Siber, baik dalam lingkup nasional maupun internasional. Bahan hukum sekunder, yaitu buku-buku, hasil-hasil penelitian dan artikel tulisan para ahli di bidang Keamanan Siber, baik dalam lingkup nasional maupun internasional, serta jurnal pemaparan hasil survei internasional dan berbagai referensi lainnya yang didapatkan dari hasil studi kepustakaan. Sedangkan bahan hukum tersier yang digunakan di antaranya adalah Kamus Besar Bahasa Indonesia, kamus hukum, kamus teknologi informasi, dan juga ensiklopedia yang memaparkan bidang terkait Kemanana Siber. Selain itu juga digunakan metode pendekatan komparatif untuk membandingkan dengan bentuk-bentuk regulasi di negara lain, serta penelusuran kajian literatur lebih jauh terhadap instrumen hukum internasional yang terkait dengan Keamanan Siber.

Dalam melengkapi data sekunder dilakukan pengumpulan data primer melalui penelitian lapangan, yaitu melaksanakan kegiatan *Focus Group Discussion* (FGD) dengan *stakeholder* terkait dari instansi pemerintahan, akademisi, praktisi, sektor swasta/bisnis, untuk mempertajam kajian dan analisis. Selain itu, dilakukan juga wawancara yang mendalam dengan para pemangku kepentingan ahli

yang dilakukan dengan studi banding ke beberapa Negara. Hal ini ditempuh untuk mendapatkan masukan guna memenuhi persyaratan formal dan ideal penyusunan undang-undang sebagaimana disyaratkan Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan, dan menampung kebutuhan riil masyarakat sebagaimana diharapkan.

BAB II
KAJIAN TEORETIS DAN PRAKTIK EMPIRIS

A. Kajian teoretis

Teknologi internet telah banyak digunakan dan banyak membantu dalam berbagai kegiatan manusia sehari-hari. Aktivitas melalui intenet dapat dilakukan secara virtual dan seolah ada di tempat tersebut melakukan hal yang nyata. Banyak hal yang dapat dilakukan melalui internet, misalnya *e-banking, e-education, e-commerce, e-government,* dan lainnya. Perkembangan internet yang semakin luas dan pesat baik teknologi maupun penggunanya telah membawa banyak dampak positif namun juga dampak negatif. Dampak positif yang diperoleh sudah selayaknya dimanfaatkan dengan sebaik-baiknya. Namun perlu diwaspadai kemungkinan terjadinya dampak negatif seperti tindakan kriminal dengan memanfaatkan teknologi internet atau yang lebih dikenal dengan *cyber crime*. Perkembangan kejahatan dengan menggunakan teknologi internet juga semakin beragam seiring dengan perkembangan teknologi itu sendiri, mulai dari *internet abuse, hacking, carding,* dan sebagainya.

Secara umum manusia menginginkan privasi, keamanan, dan perasaan aman dalam hidup, termasuk juga dalam hal penggunaan internet. Tentunya sangat diharapkan bahwa apa yang dikerjakan dengan menggunakan teknologi internet bisa aman dan jauh dari

kemungkinan untuk dirusak, dicuri, atau disalahgunakan oleh pihak yang tidak mempunyai hak.

Penggunaan dan pemberdayaan teknologi informasi dan komunikasi (TIK) dalam berbagai aspek kehidupan berbangsa dan bernegara sudah semakin masif dan menjadi kebutuhan hidup masyarakat modern. Pemanfaatan TIK pada saat ini sudah memasuki semua aspek kehidupan masyarakat di dunia. Seiring dengan meningkatnya pemanfaatan TIK, khususnya melalui jaringan internet, diiringi pula dengan meningkatnya aktivitas ancaman antara lain upaya membobol kerahasiaan informasi, merusak sistem elektronik, dan berbagai perbuatan melawan hukum lainnya.

Pembangunan nasional adalah proses berkelanjutan yang harus tanggap dan antisipatif terhadap berbagai dinamika yang terjadi di masyarakat. Globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia yang mengharuskan dilakukannya pengaturan dan pengelolaan aktivitas di ruang siber agar dapat berjalan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna kesejahteran kehidupan bangsa dengan aman. Dampak perkembangan dan kemajuan teknologi informasi yang demikian pesat telah pula menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk perbuatan hukum baru.

Dalam konteks pembangunan nasional, penggunaan dan pemberdayaan TIK harus terus dikembangkan untuk menjaga, memelihara, dan memperkokoh persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan demi kepentingan nasional. Pemanfaatan TIK telah nyata berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat. Pemerintah perlu mendukung pengembangan dan pemberdayaan TIK melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatannya dapat dilakukan secara aman untuk mencegah penyalahgunaannya

dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia.

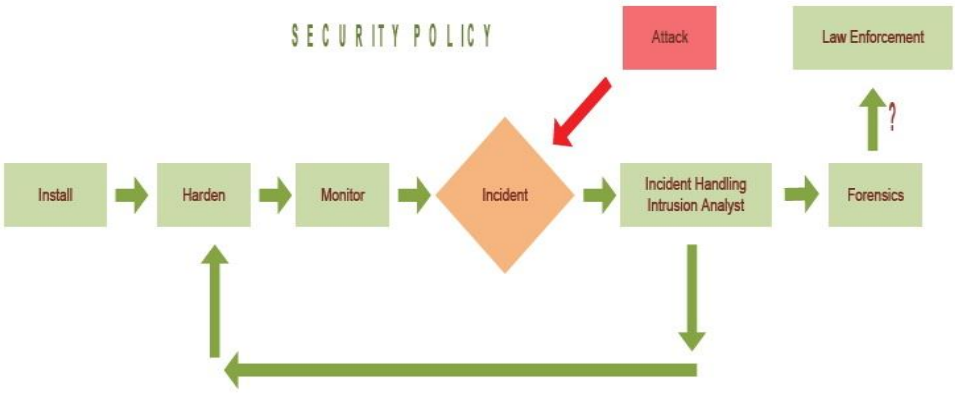
Secara umum keamanan siber didefinisikan sebagai kemampuan untuk mengendalikan akses terhadap sistem jaringan dalam ranah siber termasuk juga pengendalian terhadap informasi yang berada di dalamnya. Jikalau keamanan ranah siber terpelihara dengan efektif, maka ranah siber tersebut akan dikategorikan sebagai sebuah infrastruktur digital yang dapat diandalkan, dinamis dan, terutama, terpercaya. Sebaliknya ketika keamanan siber tidak terpelihara dengan baik, maka ranah siber akan dikategorikan sebagai bagian dunia digital yang berisiko tinggi bagi perekonomian dan hajat perikehidupan bangsa dan negara.

Persoalan keamanan siber telah menjadi pusat perhatian komunitas global. Lebih dari lima puluh negara tidak hanya telah memiliki institusi keamanan siber dalam negerinya tapi secara resmi telah mempublikasikan dokumen strategisnya yang mengelaborasi posisi resminya dalam melihat ruang siber, kejahatan siber dan/atau keamanan siber itu sendiri (Solms & Nierkerk, 2013, hal. 97). Walaupun posisi sebuah negara terkait keamanan siber sering secara sempit diklasifikasikan sebagai bagian keamanan informasi (*information security*), tentu saja hal ini kurang tepat adanya karena keamanan informasi bisa pula menyasar segala hal yang berhubungan dengan proses-proses mengamankan berbagai data milik pemerintah, warga negara, perusahaan, organisasi masyarakat dan sebagainya dalam bentuk apapun termasuk yang dituangkan dalam media cetak (printed media).

Hal ini membuat perlu definisi yang ajeg dan pasti mengenai ruang lingkup keamanan siber. Sebagai contoh adalah definisi kamus Merriam Webster yang mendefinisikan keamanan siber sebagai segala bentuk upaya dalam melindungi komputer atau sistem komputer (sebagaimana tersedia di dalam internet) dari akses yang tidak sah maupun dari segala macam bentuk serangan.

The International Telecommunications Union (ITU) (2008) mendefinisikan keamanan siber sebagai seperangkat perkakas, kebijakan, konsep keamanan, bentuk-bentuk perlindungan, haluan, pendekatan berbasis manajemen resiko, tindakan, pelatihan, praktik yang lumrah (best practices), jaminan dan teknologi yang dapat digunakan dalam rangka menlindungi ranah siber atau ruang siber (cyber environment) mapun aset-aset dari pengakses ruang siber tersebut. Aset-aset dimaksud terdiri dari perangkat komputer yang terkoneksi ke internet, personil, infrastruktur, aplikasi, jasa, sistem telekomunikasi dan kesatuan infromasi yang ditransmisikan dan/atau disimpan di dalam ruang siber. Keamanan siber berupaya untuk menjamin pencapaian dan pemeliharaan aset dari risiko-risko di ranah siber.

Dari penjabaran ITU soal keamanan siber di atas, maka dapat kita tarik simpulan bahwa keamanan siber merupakan segala aspek berkaitan dengan keamanan informasi yang khusus berada di ruang siber atau bisa pula disebut segala bentuk upaya mengamankan hal-hal yang ada di internet (internet of things/IoT). Adapun jaminan keamanan tersebut terutama diberikan terhadap potensi-potensi serangan siber (cyber attacks) seperti segala bentuk tindakan kejahatan di ranah siber, penyebaran malware, pencurian data pribadi, peretasan (hacking), tindakan spionase siber dan lain sebagainya.



Bagan Ruang Lingkup Keamanan Siber

Sumber: Technology Perspective: National Cyber-Security, Universitas Pertahanan Indonesia (2014)

Keamanan siber merupakan segala usaha yang diperlukan untuk melindungi informasi dari adanya serangan siber (cyber attack) dengan elemen-elemen utama sebagai berikut (Ardiyanti, 2016, hal. 99).:

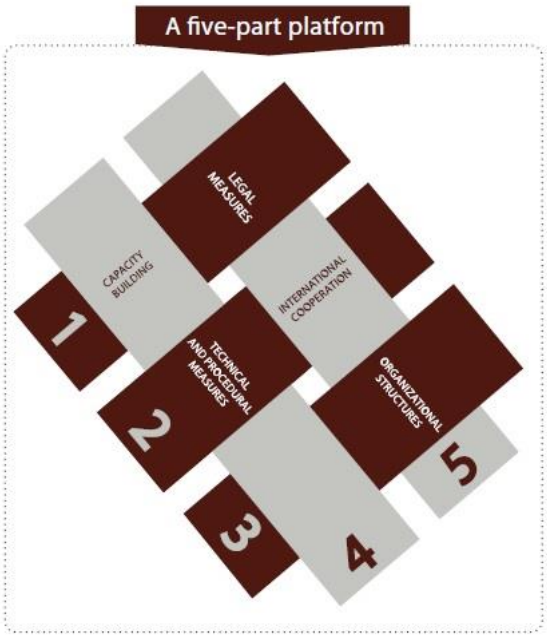
1. Dokumen kebijakan dan strategi keamanan siber yang bisa dibuat di level nasional, sektoral maupun regional yang menjadi acuan dalam menjalankan semua proses terkait keamanan informasi di dunia siber dari segala bentuk serangan siber.
2. Infrastruktur siber yang berupa media dengan peran dalam kelangsungan operasi informasi meliputi perangkat keras (hardware), perangkat lunak (software) seperti router, switch, server, operating system, database, website dan lain-lain.
3. Perimeter defense yaitu media yang berperan sebagai komponen pertahanan pada infrastruktur informasi seperi IDS, IPS dan firewall.
4. Network Monitoring System yaitu media yang fungsinya memonitor kelayakan, utilisasi dan kinerja infrastruktur siber.
5. System Information and Event Management yaitu media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
6. Network Security Assessment yaitu elemen keamanan siber yang berperan dalam mekanisme kontrol dan memberikan penilaian level keamanan siber (measurement level).
7. Sumber daya manusia dan kesadaran terhadap urgensitas keamanan siber.

Adapun lebih lanjut International Telecommunication Union (ITU) menglasifikasikan lima hal dasar (pilar) dari agenda keamanan siber nasional yang secara minimal harus dimiliki institusi keamanan siber secara global. Kelima hal tersebut adalah kepastian hukum (legal measures), aspek-aspek teknis dan prosedural, struktur

organisasi, pembangunan kapasitas (capacity building) dan kerjasama internasional (Wamala, 2011, hal. 20).

Apabila kelima pilar yang disebut pula sebagai Global Cybersecurity Agenda (GCA) tersebut dielaborasi lebih lanjut dalam konteks kepentingan nasional setiap yurisdiksi maka dapat dijabarkan sebagai berikut:

1. Kepastian hukum berarti perlunya sebuah negara memiliki legislasi nasional mulai dari dokumen kebijakan dan strategi keamanan siber nasional yang berisikan rincian perencanaan implementasi keamanan siber hingga berbagai peraturan perundang-undangan yang menopangnya.
2. Aspek-aspek teknis dan prosedur yang fokus pada penjabaran terkait standarisasi, akreditasi protokol maupun fokus menemukan kerentanan dari perangkat lunak untuk keamanan siber.
3. Struktur organisasi yang diciptakan dalam rangka menciptakan strategi dan implementasi untuk mencegah, mendeteksi dan merespon segala bentuk serangan terhadap infrastruktur-infrastruktur informasi yang penting.
4. Pembangunan kapasitas yaitu fokus dalam meningkatkan pemahaman dan keahlian dari para personil keamanan siber untuk lebih mendorong keberhasilan tujuan-tujuan dari agenda kebijakan keamanan siber nasional.
5. Kerjasama internasional yaitu urgensitas setiap negara untuk melibatkan diri dalam kerjasama, dialog dan koordinasi dalam menjawab isu-isu terkini dari keamanan siber yang begitu dinamis.



Lima Pilar Keamanan Siber Global (Global Cybersecurity Agenda)
Sumber: ITU National Cybersecurity Strategy Guide (2011)

Dalam keadaan perang, seluruh sumber daya digunakan untuk mempertahankan sistem elektronik khususnya yang strategis dan meredam serangan siber dan menyerang untuk melumpuhkan serangan dan tentara nasional memiliki peran strategis. Merupakan tantangan besar dalam mempertahankan dan menjaga kerahasiaan, integritas, dan ketersediaan informasi serta sistem elektronik yang strategis karena selalu ada kemungkinan terjadinya perang siber (*cyber war*) yaitu perang yang tidak kasatmata, melainkan perang laten berupa serangan siber (*cyber attack*) yang tidak dilangsungkan atas nama negara tertentu.

Kebijakan penegakan hukum bidang teknologi informasi meliputi proses yang disebut sebagai kebijakan kriminal atau *criminal policy*. Konsep kebijakan penegakan hukum diaplikasikan secara institusional melalui suatu sistem yang dinamakan *criminal justice system* (sistem peradilan pidana). Keterkaitan antara kebijakan penegakan hukum dengan sistem peradilan pidana, yaitu sub sistem dari sistem peradilan pidana yang akan melaksanakan kebijakan penegakan hukum berupa pencegahan dan penanggulangan

terjadinya suatu kejahatan yang menjadi lebih *acceptable* bersama-sama dengan peran masyarakat.

Oleh karena itu, pembudayaan kesadaran akan keamanan siber sangat penting. Masyarakat tidak hanya bertanggung jawab untuk mengurangi angka kejahatan siber, melainkan juga harus ikut serta dalam proses menganalisa, mengenal dan memahami ancaman kejahatan tersebut dengan cara melakukan pengamanan terhadap jaringan komputer, *hardware*, dan masing-masing pribadi masyarakat.

B. Kajian asas-asas terkait penyusunan rancangan undang-undang

Dalam Lampiran 1 Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan, menyatakan bahwa kajian asas ini berisi mengenai analisis terhadap aspek bidang kehidupan terkait dengan Peraturan Perundang-Undangan yang akan dibuat yang berasal dari hasil penelitian. Selanjutnya dalam Pasal 5 Undang-Undang Nomor 12 Tahun 2011 menyatakan bahwa dalam membentuk peraturan perundangan-undangan harus dilakukan berdasarkan pada asas Pembentukan Peraturan Perundang-Undangan yang baik, seperti kejelasan tujuan, kelembagaan atau pejabat pembentuk yang tepat, kesesuaian antara jenis, hierarki, dan materi muatan, dapat dilaksanakan, kedayagunaan dan kehasilgunaan, kejelasan rumusan, dan keterbukaan.

Asas yang ada dalam RUU Keamanan dan Ketahanan Siber melandasi penyelenggaraan Keamanan Siber dalam upaya-upaya baik pencegahan, penanggulangan, hingga pemulihan dari insiden siber atau serangan siber. Upaya pencegahan, penanggulangan, hingga pemulihan hanya merupakan bagian luas dari beberapa upaya penyelenggaraan Keamanan Siber. Masih banyak lagi upaya lain yang lebih bersifat praktis bahkan teknis yang perlu diatur dalam RUU Keamanan dan Ketahanan Siber. Dalam kajian asas ini akan mencerminkan aspek bidang kehidupan terkait dengan RUU Keamanan dan Ketahanan Siber, sehingga dalam asas yang ada

nantinya dapat menggambarkan kejelasan tujuan, kelembagaan, kesesuaian dari undang-undang, dan keterbukaan.

Cerminan asas dalam berbagai perwujudan aspek bidang kehidupan dalam RUU Keamanan dan Ketahanan Siber tersebut pada akhirnya akan menjadi prinsip dasar Pembentukan Peraturan Perundang-undangan yang baik. Asas tersebut sebagai acuan dasar bila terjadi perdebatan, pertentangan, atau ketidaksesuaian baik dari peraturan perundang-undangan maupun implementasi ketentuan yang ada nantinya pada masyarakat, maka akan kembali untuk melihat asas-asas yang ada. Hal ini berarti suatu peraturan perundang-undangan yang kongkrit didasari pada konsep asas yang lebih luas, sehingga dalam penerapan peraturan jika memang muncul potensi perdebatan, maka akan ditarik kembali untuk melihat asas-asas dari peraturan yang ada tersebut. Melihat kembali konsep asas diharapkan mampu untuk menyelesaikan perdebatan yang nantinya muncul.

Sebelum masuk pada asas Keamanan Siber, akan dijelaskan terlebih dahulu konsepsi lebih luas dari Keamanan Siber, yaitu Keamanan Nasional. Secara filosofis, melekat dua fungsi pada negara sebagai suatu unit politik, yaitu fungsi keamanan dan fungsi kesejahteraan. Fungsi keamanan yang melekat pada negara tersebut kemudian melahirkan istilah keamanan nasional. Jika dilihat dari tujuannya, keamanan nasional dimaksudkan untuk melindungi negara dari berbagai ancaman yang dapat meruntuhkan negara. Dalam kerangka statis, keamanan nasional biasanya selalu menyangkut tentang aktor, tanggung jawab untuk menyelenggarakan keamanan nasional selalu dilekatkan pada negara.[65]

Glenn Snyder memandang bahwa keamanan nasional menyangkut dua konsep yaitu penangkalan (*deterrence*) dan pertahanan (*defence*). Pada hakikatnya keamanan nasional merupakan kepentingan nasional yang paling hakiki bagi suatu

[65] Andi Widjajanto, *Penataan Kebijakan Keamanan Nasional. Dian Cipta Publisher, 2013*, hlm. 15

negara, sehingga dengan kata lain keamanan nasional merupakan suatu kemampuan untuk melindungi nilai hakiki negara terhadap berbagai ancaman dari dalam maupun luar negeri. Dengan demikian keamanan nasional harus dilihat secara luas dan komprehensif dengan mempertimbangkan kemampuan pertahanan, keselamatan negara, dan kepastian hukum dalam rangka menjamin kelangsungan hidup bangsa dan negara dari setiap ancaman yang ada.[66]

Definisi dari keamanan nasional sendiri memiliki banyak perdebatan yang belum menemukan titik tengah. Dalam kerangka hukum internasional, konsep keamanan nasional diserahkan kepada masing-masing negara asal tidak menyelahi konsepsi negara demokratis. [67] Berkowitz dan Bock membuat suatu definisi dari keamanan nasional yang luas yaitu kemampuan dari suatu bangsa untuk melindungi nilai-nilai internalnya dari ancaman pihak luar. Definisi yang luas menurut Berkowitz dan Bock ini diharapkan dapat sangat bermanfaat untuk memperluas lingkup keamanan nasional.[68]

Konsep keamanan nasional berkembang lebih banyak di Amerika Serikat setelah Perang Dunia II, sehingga pada peraturan perundang-undangan di Amerika Serikat terkait tentang Keamanan Nasional dan perubahan-perubahannya hingga kini tidak memiliki batasan atau definisi spesifik tentang apa yang dimaksud dengan keamanan nasional. Bahkan bagi Amerika Serikat *national security* atau keamanan nasional menjadi keamanan kawasan dunia yang memiliki ancaman bagi negara Amerika Serikat, sedangkan untuk keamanan dalam negeri mereka mengembangkan *homeland security*.[69] Selain Amerika Serikat, Inggris dan negara-negara Eropa dalam peraturan perundang-undangannya juga tidak secara spesifik mendefinisikan terminologi keamanan nasional. Fleksibilitas menjadi

---

[66] Douglas J. Murray dan Paul R. Viotti (Ed), The Defense Policies of Nations: A Comparative Study, Baltimore: The John Hopkins University, 1985, hal. 4.

[67] Indah Amaritasari, Keamanan Nasional dalam Konsep dan Standar Internasional, Jurnal Keamanan Nasional, Vol. 1 No. 2, 2015

[68] Berkowitz, Morton, and Bock, P.G, eds. American National Security. New York: Free Press, 1965.

[69] Sidratahta Mukhtar, Keamanan Nasional: Antara Teori dan Prakteknya di Indonesia, Sociae Polities, Edisi Khusus, 2011, hlm. 130

suatu alasan mengapa keamanan nasional tidak didefinisikan secara jelas dan rinci, sehingga memudahkan adaptasi dalam berbagai situasi yang berubah.[70]

Namun dalam bahasan ini, perlu melihat suatu definisi guna menemukan konsep keamanan nasional. Cohen, Ira dan Tuttle menganggap keamanan nasional sebagai suatu kondisi protektif yang para negarawan berusaha capai atau jaga, dalam rangka mengamankan berbagai macam komponen politik dari ancaman baik dalam maupun luar.[71] G. Kennan memberikan pengertian keamanan nasional sebagai "*the continued ability of the country to pursue the development of its internal life without serious interference, or threat of interference, from foreign powers*" yaitu kemampuan yang dimiliki negara secara berkelanjutan untuk mencapai perkembangan kehidupan internalnya tanpa gangguan, atau ancaman gangguan dari kekuatan-kekuatan asing.[72]

Prabhakaran Paleri, mengatakan keamanan nasional sebagai *"the whole range of measures affecting the welfare of a population, as well as provision against aggression from abroad or subversion within"* atau dalam terjemahannya yaitu seluruh ukuran dari tindakan yang berdampak pada kesejahteraan populasi, dan perlindungan terhadap agresi dari luar maupun pemberontakan dari dalam. Pengertian ini dapat dikatakan juga meluas, Paleri tidak secara langsung menyebut sebagai *state* atau negara atau bahkan nasional, namun populasi yang perlu dilindungi dari berbagai ancaman terutama dikatakan disini sebagai pemberontakan. Selain itu Paleri membagi keamanan nasional ke dalam 15 bagian yaitu *military security, economic security, resource security, border security, demographic security, disaster security, energy security, geostrategic security, informational security,*

---

[70] Indah Amaritasari, Keamanan Nasional dalam Konsep dan Standar Internasional

[71] Cohen, Ira S., and Tuttle, Andrew C. National Security Affairs: A Syllabus. 1972

[72] Bergen, P., Garrett, L., Report of the Working Group on State Security and Transnational Threats, New Jersey, Princeton University.

food security, health security, ethnic security, environmental security, cyber security, genomic security. [73]

Keamanan nasional termasuk juga dalam meminimalisir bahaya dan ancaman. Ancaman dapat dilihat sebagai antisipasi terhadap penghalang dari beberapa nilai-nilai. Ketika berbicara mengenai perlindungan maka biasanya terkait dengan bebas dari penghalang dan rintangan dari apa yang dinikmati sebagai hasil yang bernilai. Keamanan nasional akhirnya berujung menjadi kepentingan nasional dengan mengacu pada hasil bernilai yang diinginkan oleh mereka yang berada dalam basis efektif politik suatu bangsa, sehingga nilai yang ada tersebut biasanya diasosiasikan dengan konsep kepentingan nasional. Konsep keamanan nasional akan terus berkembang dan berubah, terutama pada hasil nilai yang diinginkan, lingkungan internasional, kondisi domestik, sifat ancaman, dan strategi menghadapi ancaman.[74]

Keamanan nasional yang dapat dikatakan sudah sangat tua umurnya dan terus menerus mengalami perkembangan kini memasuki fase baru. Penulis akan menjelaskan sedikit tentang hal ini, untuk menggambarkan tentang kebutuhan keamanan siber pada keamanan nasional. Perkembangan isu-isu strategis yang ada saat ini seperti globalisasi, demokrasi, penegakan hak asasi manusia dan fenomena terorisme telah memperluas cara pandang dalam melihat kompleksitas ancaman yang ada dan mempengaruhi perkembangan konsepsi keamanan.[75] Ancaman tidak lagi hanya berupa ancaman militer tetapi juga meliputi ancaman politik, ancaman sosial, ancaman ekonomi, maupun ancaman ekologis.[76] Konsepsi ini menilai

---

[73] Paleri, P., National Security: Imperatives and Challenges, New Delhi: Tata McGraw-Hill Education. 2008

[74] Lasswell, Horold D., and Kaplan, Abraham. Power and Security. New Haven: Yale University Press. 1950.

[75] Heather Exner-Pirot, Human Security in the Arctic: The Foundation of Regional Cooperation, Munk School of Global Affairs, 2012, DOI: 10.13140/RG.2.2.18371.40480

[76] Adger,W.N., J.M. Pulhin, J. Barnett, G.D. Dabelko, G.K. Hovelsrud, M. Levy, Ú. Oswald Spring, and C.H. Vogel, 2014: Human security. In: Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the

bahwa keamanan tidak bisa hanya diletakan dalam perspektif kedaulatan nasional dan kekuatan militer. Konsepsi keamanan juga ditujukan kepada upaya menjamin keamanan warga negara atau keamanan manusianya.[77] Gagasan ini disebut sebagai *human security* atau keamanan manusia, yang dapat dilihat dalam Laporan UNDP mengenai Human Development Report of the United Nations Development Program pada tahun 1994.[78]

Secara rinci, konsep keamanan manusia dapat dilihat dalam tujuh komponen yang harus mendapatkan perhatian yaitu, 1) *economic security* (bebas dari kemiskinan dan jaminan pemenuhan kebutuhan hidup, 2) *food security* (kemudahan akses terhadap kebutuhan pangan), 3) *health security* (kemudahan mendapatkan layanan kesehatan dan proteksi dari penyakit), 4) *environmental security* (proteksi dari polusi udara dan pencemaran lingkungan, serta akses terhadap air dan udara bersih), 5) *personal security* (keselamatan dari ancaman fisik yang diakibatkan oleh perang, kekerasan domestik, kriminalitas, penggunaan obat-obatan terlarang, dan bahkan kecelakaan lalu lintas), 6) *community security* (kelestarian identitas kultural dan tradisi budaya), dan 7) *political security* (perlindungan terhadap hak asasi manusia dan kebebasan dari tekanan politik). Tujuh komponen diatas bisa disimplifikasi menjadi dua komponen utama, yaitu *freedom from fear* (bebas dari rasa takut) dan *freedom from want* (bebas dari ketidakmampuan untuk memiliki).[79]

Intergovernmental Panel on Climate Change [Field, C.B., V.R. Barros, D.J. Dokken, K.J. Mach, M.D. Mastrandrea, T.E. Bilir, M. Chatterjee, K.L. Ebi, Y.O. Estrada, R.C. Genova, B. Girma, E.S. Kissel, A.N. Levy, S. MacCracken, P.R. Mastrandrea, and L.L.White (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, pp. 755-791. DOI: 10.1017/CBO9781107415379.017

[77] Lihat juga Heru Susetyo, Menuju Paradigma Keamanan Komprehensif Berperspektif Keamanan Manusia dalam Kebijakan Keamanan Nasional Indonesia, Lex Jurnalica, Vol. 6 No. 1, 2008, hlm. 3

[78] Oscar A. Gómez & Des Gasper, Human Security: A Thematic Guidance Note for Regional and National Human Development Report Teams, United Nations Development Programme (UNDP) Human Development Report Office

[79] lihat juga dalam Elpeni Fitrah, Gagasan Human Security dan Kebijakan Keamanan Nasional Indonesia, Jurnal Insignia, Vol. 2, No. 1, 2015

Berdasarkan penjabaran tersebut, maka dapat dikatakan bahwa keamanan siber menjadi subsistem dari keamanan nasional. Seperti yang disebutkan oleh Paleri misalnya *cyber security* muncul menjadi salah satu bagian dari keamanan nasional. Ditambah lagi bila digabungkan dengan konsep baru keamanan manusia, perhatian atas konsep keamanan manusia, *personal security* memiliki keterkaitan erat dengan Keamanan Siber. Ringkasnya menurut penulis komponen dari keamanan nasional yang perlu mendapatkan perhatian sebagai upaya perlindungan kepada negara dan bangsa yaitu 1) sumber daya manusia, termasuk pada militer dan aparat terkait serta masing-masing warga negara, 2) teknologi, yaitu baik infrastruktur yang mendukung kehidupan masyarakat maupun perangkat-perangkat teknologi dalam upaya memberikan perlindungan pada keamanan nasional, dan juga 3) hukum atau norma yang mengatur tentang perlindungan terkait keamanan. Komponen teknologi menjadi dasar untuk melihat kepentingan Keamanan Siber dalam upaya perlindungan keamanan nasional.[80] Ancaman dari insiden siber atau serangan siber yang tidak bisa dianggap ringan seperti yang telah dijabarkan sebelumnya, membuat kebutuhan akan perlindungan keamanan siber menjadi sangat penting.

Pasal 6 ayat (2) Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan menyatakan bahwa selain mencerminkan asas materi muatan, peraturan perundang-undangan tertentu dapat berisi asas lain yang sesuai dengan bidang hukum perundang-undangan yang bersangkutan. Sehingga bila terjadi suatu insiden yang mengancam keamanan siber maka upaya-upaya perlindungan yang perlu diambil harus mencerminkan keseluruhan asas seperti :

1. Asas keterpercayaan

   Keterpercayaan, merupakan kondisi ketika seseorang atau sesuatu dapat diandalkan kejujurannya, kebenarannya, dan/atau

[80] Barry Buzan and Lenen Hansen, The Evolution of International Security Studies, United Kingdom: Cambridge University Press, 2009, hlm. 42-60.

kemampuannya. Hal ini dapat digambarkan misalnya pada penyelenggaraan Keamanan Siber, akan terdapat izin akses keamanan siber, bila terjadi ancaman siber yang berupa insiden atau serangan siber dalam perimeter keamanan. Perimeter keamanan tersebut merupakan area yang hanya dapat diakses oleh orang yang memiliki izin akses keamanan siber. Sehingga diharapkan orang-orang yang memiliki izin akses keamanan siber, bila terjadi insiden atau serangan dalam perimeter keamanan wajib mengetahui apa yang harus dikerjakan, dan bagaimana tanggung jawab keseluruhan dari upaya-upaya untuk melindungi Keamanan Siber. Keterpercayaan perlu diberikan kepada orang-orang atau pihak yang memiliki izin akses keamanan siber untuk masing-masing bekerja secara maksimal efektif dan efisien dalam melakukan pencegahan, penanggulangan dan pemulihan dalam urusan perlindungan Keamanan Siber. Dengan salah satu contoh tersebut, keterpercayaan merupakan hal dasar dan menjadi prinsip dalam pelaksanaan upaya-upaya penyelenggaraan dan perlindungan Keamanan Siber.

2. Asas kesiagaan

   Kesiagaan merupakan kondisi ketika seseorang atau sesuatu sepenuhnya siap untuk melakukan tindakan dan/atau menghadapi suatu serangan atau ancaman. Seperti yang telah disebutkan sebelumnya, ancaman siber dan serangan siber dapat terjadi kapan pun, bahkan tanpa dapatnya diprediksi terlebih dahulu. Kerugian yang muncul sebagai dampak dari ancaman dan serangan siber perlu mendapatkan perhatian lebih. Kerugian tidak hanya bersifat materiil kepada negara, bahkan mampu mempengaruhi psikologi dari warga negara. Hal ini menunjukan tidak boleh lengahnya para pihak yang terkait dengan penyelenggaraan Keamanan Siber dalam menghadapi ancaman dan serangan siber. Sehingga seluruh orang atau pihak-pihak pemangku kepentingan di bidang Keamanan Siber perlu selalu siap siaga dalam keadaan bagaimana pun menghadapi ancaman

dan serangan siber serta melakukan upaya-upaya perlindungan Keamanan Siber, dan melaksanakan fungsi Keamanan Siber.

3. Asas kolaboratif

   Kolaboratif adalah kondisi ketika dua pihak atau lebih saling bekerjasama untuk mewujudkan tujuan yang disepakati bersama. Penyelenggaran Keamanan Siber nasional yang dilaksanakan oleh berbagai pemangku kepentingan baik pada kementerian dan lembaga serta badan terkait, perlu bekerja sama secara efektif dan efisien dalam satu tujuan utama yaitu penyelenggaraan Keamanan Siber nasional. Selain itu Penyelenggaraan Keamanan Siber, tidak dapat berjalan maksimal jika hanya dilakukan oleh pemerintah selaku otoritas negara dalam melaksanakan penyelenggaraan Keamanan Siber. Infrastuktur-infrastruktur kritis yang kini banyak dipegang oleh pihak swasta baik orang maupun badan, juga perlu ikut berkontribusi dalam menyelenggarakan Keamanan Siber, terutama dalam melindungi infrastruktur yang dioperasikannya. Kolaborasi atau kerjasama yang dilakukan oleh berbagai pemangku kepentingan baik otoritas kenegaraan maupun pihak swasta harus dibina dan dikonsolidasikan secara efektif dan efisien agar terwujud satu kesatuan komponen keamanan nasional yang padu dalam melaksanakan fungsi Keamanan Siber. Sehingga bila terjadi suatu insiden atau serangan siber, pihak-pihak yang terkait wajib untuk saling bekerja sama dalam melakukan upaya-upaya perlindungan Keamanan Siber termasuk pada upaya penanggulangan dan pemulihan agar tidak menimbulkan banyak kerugian.

C. Kajian terhadap praktik penyelenggaraan, kondisi yang ada, serta permasalahan yang dihadapi masyarakat

1. Hasil Pengumpulan Data

   Pengumpulan data dalam rangka penyusunan Naskah Akademik dan RUU tentang Keamanan Siber menghasilkan beberapa temuan terkait penyelenggaraan siber di Indonesia.

Berdasarkan hal tersebut didapatkan gambaran mengenai kondisi yang ada dan permasalahan yang dihadapi dalam praktik penyelenggaraan siber di Indonesia. Pengumpulan data juga mendapatkan masukan konsep mengenai pengaturan siber sehingga dapat dijadikan bahan rujukan dalam proses penyusunan Naskah Akademik dan RUU tentang Keamanan Siber.

a. Batasan dan ruang lingkup pengertian siber

Akademisi Fakultas Hukum Universitas Airlangga [81] berpendapat bahwa hingga saat ini belum ada kesepakatan terkait dengan definisi pasti tentang hukum siber. Sebagai contoh, *cyberlaw* atau hukum siber dalam beberapa literatur disebut sebagai hukum telematika, hukum teknologi informasi, hukum internet.

Pengertian *cyberlaw* tersebut selalu didefinisikan sebagai area hukum yang berhubungan dengan Internet, elemen teknologi dan elektronik termasuk komputer, perangkat lunak, perangkat keras, dan sistem informasi (SI). Hal ini mungkin tidak terlepas dari pengertian siber dalam Kamus Besar Bahasa Indonesia (KBBI). Siber dalam KBBI memiliki beberapa arti, yakni: 1) sistem komputer dan informasi; 2) dunia maya; 3) berhubungan dengan internet.

Di Indonesia kebijakan di bidang siber mulai dikenal sejak diundangkannya Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Akan tetapi dalam pelaksanaannya, banyak permasalahan yang muncul. Salah satunya adalah bahwa UU ITE mencampuradukan ranah privat dan ranah publik di dalam satu regulasi. Belum lagi adanya tumpang tindih dengan berbagai rezim regulasi yang lain.

[81] Diskusi Pakar dengan Akademisi Masitoh Indriani di Fakultas Hukum Universitas Airlangga Surabaya pada tanggal 27 Maret 2018.

Kontestasi kebijakan 'persiberan' di Indonesia tidak terlepas dari tata kelola Internet (*Internet Governance*). Tata kelola Internet merupakan kajian baru yang memiliki tingkat kompleksitas tinggi dan membutuhkan konsep baru serta pendekatan yang bersifat multidisipliner yang mencakup kajian hukum, teknologi, sosial, ekonomi dan pembangunan, serta kajian politik. Hal ini diperkuat dengan pendapat Ziewitz dan Pentzold yang menyatakan bahwa kontestasi tata kelola internet merujuk pada kajian lintas baik dipandang secara politis maupun dari segi ideologis.[82] Sementara itu Benkler berpendapat bahwa tata kelola internet harus meliputi tiga bidang garap: (i) infrastuktur fisik, (ii) kode atau pemrograman, (iii) konten yang meliputi segala informasi yang melewati jaringan Internet.[83]

Sementara itu Akademisi Fakultas Hukum Universitas Pattimura,[84] mengutip pendapat Pavan Dugal dalam bukunya *Cyberlaw the Indian Perspective*, yang mengatakan bahwa hukum siber adalah istilah umum yang menyangkut semua aspek legal dan peraturan internet dan juga *World Wide Web*, serta hal apapun yang berkaitan atau timbul dari aspek legal atau hal yang berhubungan dengan aktivitas para pengguna internet aktif dan juga yang lainnya di dunia siber.

Berkaitan dengan ruang lingkup siber, ketua umum *Indonesia Cyber Law Community* (ICLC) Teguh Arifiyadi mengatakan bahwa ruang lingkup *cyberlaw* sangatlah luas, antara lain mencakup *object identifier*, *virtual currency*, *Over the Top*, *E-Procurement*, *Internet censorship*, sengketa nama domain, intersepsi, digital forensik, sertifikasi perangkat keras,

---

[82] Malte Ziewitz & Christian Pentzold, "In Search of Internet Governance: Performing Order in Digitally Networked Environments", New Media & Society 16 (2014), hal. 306-322.

[83] Yochai Benkler, "From Consumers to Users: Shifting the Deeper Structures of Regulation Towards Sustainable Commons and User Access" Archived 9 March 2012 at the Wayback Machine.,52 Fed. Comm. L.J. 561, (2000).

[84] Diskusi Pakar dengan Akademisi Nancy Silvana Haliwela di Fakultas Hukum Universitas Airlangga Surabaya pada tanggal 27 Maret 2018.

hacking dan *cracking*, data pribadi, agen elektronik, data center, pornografi internet, dan media sosial.[85]

Beberapa pakar mengartikan siber sebagai internet namun beberapa pakar yang lain mengatakan bahwa siber lebih luas dari internet. Ketua program studi rekayasa keamanan siber Sekolah Tinggi Sandi Negara (STSN) Obrina Candra Briliyant berpendapat bahwa semua sinyal elektronik yang dikomunikasikan melalui jaringan elektronik pada dasarnya masuk ke dalam ruang lingkup siber, sehingga ruang lingkup siber dapat dikatakan lebih luas daripada internet.[86]

b.Keterkaitan antara siber dan persandian

Akademisi Fakultas Hukum Universitas Airlangga berpendapat bahwa keterkaitan antara persandian dengan siber adalah teknologi yang diterapkan. Teknologi persandian menggunakan *encryption* dimana teknologi ini juga digunakan dalam aktivitas siber. *Encryption* dibuat menggunakan sistem algoritma untuk menciptakan kompleks code menjadi data yang sederhana. Enkripsi digunakan secara luas untuk keamanan data karena *ciphertext* dan *coding* membuat data menjadi sulit untuk di susupi.[87]

Sejalan dengan pendapat tersebut, Obrina Candra Briliyant mengatakan bahwa persandian adalah *core technology* dari keamanan siber. Kegiatan persandian meliputi kriptografi (menyandi data), kriptoanalisis (mengupas sandi), dan steganografi (menyembunyikan pesan dalam data). Kriptografi dapat menjamin bahwa data yang dikirimkan melalui jaringan tidak berubah/dimodifikasi pihak lain.

---

[85] Diskusi Pakar dengan Ketua ICLC Teguh Arifiyadi di Pusat PUU pada tanggal 20 Februari 2018.

[86] Diskusi Pakar dengan Ketua Program Studi Rekayasa Keamanan Siber STSN Obrina Candra Briliyant di Pusat PUU pada tanggal 23 Februari 2018.

[87] Diskusi Pakar dengan Akademisi Dr. Intan Soeparna di Fakultas Hukum Universitas Airlangga Surabaya pada tanggal 27 Maret 2018.

Kriptografi juga dapat memastikan identitas seseorang di ruang siber.

Akademisi Universitas Pattimura berpendapat setidaknya persandian dan siber memiliki satu keterkaitan erat, yaitu bahwa keduanya diterapkan untuk menjaga dan mempertahankan keamanan dan kerahasiaan (*confidentialy*), integritas (*integrity*), dan ketersediaan (*availability*) informasi atau sistem elektronik. Persandian dan Siber merupakan bidang tanggung jawab pemerintah yang perlu didorong dan diperkuat sebagai upaya meningkatkan bidang keamanan untuk mewujudkan kemanan nasional. [88]

c. Materi muatan

Beberapa hal yang dapat diatur dalam RUU siber dalam konteks pertahanan dan keamanan negara:[89]

1) *Data protection*

untuk memperkenalkan konsep "informasi pribadi yang sensitif", dan memberikan tanggung jawab pada setiap entitas terhadap data pribadi. Di sisi lain, ada baiknya mengambil tindakan hukum seorang individu untuk pelanggaran kerahasiaan dan privasi, di bawah kontrak yang sah.

2) *Cyber security*

Ketentuan yang memberikan otoritas pada pemerintah dalam mendefinisikan kebijakan persandian (*encryption policy*) untuk memperkuat keamanan pada komunikasi elektronik, tujuannya untuk melindungi kegiatan *e-government* atau bahkan *e-commerce*. Konsep kemanan siber melingkupi empat aspek yaitu:

[88] Diskusi Pakar Akademisi Univ. Pattimura, *Op.Cit.*
[89] Diskusi Pakar Akademisi Univ. Airlangga, *Op.Cit.*

a) *Privacy/Confidentiality*: Aspek terkait jaminan kerahasiaan isi dari informasi.
b) *Authentication*: Aspek yang menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses/memberikan informasi adalah betul-betul orang yang dimaksud.
c) *Integrity*: Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi.
d) *Accesibility*: Aspek ini berhubungan denganketersediaan informasi ketika dibutuhkan.
e) *Access control*: Aspek ini berhubungan dengan cara pengaturan akses kepadainformasi
f) *Non repudiation*: Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

Keamanan siber adalah kumpulan alat, kebijakan, konsep keamanan, keamanan perlindungan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan siber dan organisasi dan aset pengguna.

3) *Critical Information Infrastructure*

Ketentuan mengenai hal yang berkaitan dengan informasi yang terkoneksi dalam suatu sistem atau networks, dimana apabila terjadi gangguan atau penghancuran akan mengakibatkan dampak yang serius pada infrastruktur umum yang berkaitan dengan kesehatan, keamanan, perekonomian atau efektifitas pemerintahan dan lain sebagainya.

4) Penyadapan
5) Cyber terorisme
6) *E-government*
7) Ketentuan pidana dan penegakan hukum

Selain konteks pertahanan dan keamanan negara, materi muatan yang diperlukan dalam RUU Siber antara lain:[90]

1) Aspek Ekonomi

   Peran Pemerintah untuk menata ranah siber harus memberikan perlindungan dan kenyamanan bagi masyarakat dalam menjalankan roda perekonomian seperti: *E-Commerce, E-Business* sebagai jembatan penyelenggaraan perekonomian nasional, ranah siber harus mampu meningkatkan devisa negara, juga taraf hidup masyarakat dan memberikan edukasi dan wawasan menghadapi persaingan regional masyarakat ekonomi ASEAN.

2) Aspek Ideologi

   Ranah siber perlu dikelola sebagai sarana demokrasi rakyat yang sehat dan kondusif.

3) Aspek Sosial Budaya

   Ranah siber merupakan saluran interaksi dan komunikasi yang cepat dan mampu menyentuh individu secara personal dan harus menjadi ruang publik yang edukatif, beretika dan berlapis nilai-nilai luhur peningkatan moral bangsa.

Menurut Obrina Candra Briliyant, pengaturan penyelenggaraan keamanan siber secara garis besar idealnya terdiri dari proteksi, identifikasi, deteksi, penanggulangan, dan pemulihan. [91] RUU Siber ini sebisa mungkin harus menjabarkan suatu visi keadaan siber yang diinginkan negara, yakni suatu kondisi yang akan menjadi target pencapaian BSSN sebagai lembaga koordinator di bidang siber, setidaknya meliputi dan tidak terbatas pada:

---

[90] Diskusi Pakar Akademisi Univ. Pattimura, *Op.Cit.*

[91] Diskusi Pakar Obrina Candra Briliyant, *Op.Cit.*

1) Pendekatan keamanan siber yang digunakan negara yakni kolaborasi keterlibatan pemerintah, swasta, asosiasi/ komunitas, dan masyarakat (*collaborative network*);
2) Strategi keamanan siber nasional, hendaknya meliputi: *privacy, critical cyber infrastructure*, dan lain sebagainya;
3) Tata kelola/arsitektur yang cukup jelas memetakan komponen-komponen negara dan keterkaitannya*;*
4) Adaptibilitas dan fleksibilitas strategi keamanan siber nasional, mengingat teknologi informasi dan teknologi siber merupakan bidang yang bergerak cepat.

Disamping itu, menurut Ferdinandus Setu terdapat beberapa hal yang perlu diatur dalam RUU Keamanan dan Ketahanan Siber, yaitu:[92]

1) Tanggung jawab korporasi

   Badan hukum bertanggung jawab atas tindak pidana terkait teknologi informasi yang dilakukan untuk kepentingannya oleh setiap orang yang memiliki posisi kepemimpinan dalam badan hukum tersebut, baik bertindak sendiri maupun bertindak sebagai bagian dari organ di dalam badan hukum dimaksud.
2) Tanggung jawab penyelenggara sistem elektronik

   Wajib menyediakan sarana penyimpanan data komputer dan/atau informasi elektronik termasuk data trafik yang berkaitan dengan sistem komputer atau sistem elektronik yang dikelolanya dan menjaga keutuhan data dimaksud sehingga tidak mudah hilang dan/atau tidak mudah diubah.
3) Kerjasama internasional

   Dalam rangka penyelidikan, penyidikan, pengumpulan bukti dan/atau proses hukum lain menyangkut tindak

[92] Diskusi Pakar dengan pihak Kementerian Komunikasi dan Informatika, Ferdinandus Setu di Pusat PUU pada tanggal 21 Februari 2018

pidana teknologi informasi yang terkait dengan sistem komputer atau sistem elektronik dan data komputer atau informasi elektronik dan/atau dokumen elektronik, penegak hukum dapat melakukan kerja sama internasional dengan negara-negara peserta konvensi sesuai ketentuan peraturan perundang-undangan.

4) Ekstradisi

   Ekstradisi dapat dilakukan terkait dengan tindak pidana teknologi informasi sepanjang dilakukan oleh dan untuk negara peserta konvensi sesuai dengan ketentuan peraturan perundang-undangan.

5) Bantuan timbal balik

   Dalam rangka penyelidikan, penyidikan, pengumpulan bukti dan/atau proses hukum lain menyangkut tindak pidana teknologi informasi penegak hukum dapat melakukan kerjasama bantuan timbal balik dengan negara peserta konvensi sesuai dengan ketentuan peraturan perundang-undangan.

6) Titik kontak

   Dalam rangka pemberian bantuan langsung untuk penyelidikan, penyidikan atau proses hukum sehubungan dengan tindak pidana teknologi informasi dan komunikasi. Penegak hukum menunjuk titik kontak untuk mendukung pembentukan jaringan kerjasama internasional.

Keenam hal tersebut perlu diatur karena belum ada pengaturannya dalam undang-undang bidang teknologi informasi dan komunikasi yang telah ada saat ini. Selain itu, RUU Siber juga diharapkan dapat menjadi landasan hukum yang lebih kuat bagi BSSN. RUU Siber juga diharapkan berisi pengaturan koordinasi antar-instansi pengatur dan pengawas siber (Kemenkominfo, BSSN, Kemenhan, Polri, dsb).

d. Konteks keamanan siber terkait pertahanan dan keamanan negara

Internet pada dasarnya membawa perubahan yang fundamental dalam interaksi masyarakat, pemerintah dalam memberikan jasa, ekspansi bisnis dan transaksi individual. Saat internet membawa manfaat yang sangat besar, menghemat biaya, dan membawa efisiensi terdapat ancaman yang besar. Ancaman-ancaman siber dapat merusak kepentingan nasional, membahayakan fungsi industri dan membahayakan pengguna individu atau pengguna akhir. Hal ini akan menciptakan posisi keamanan siber sebagai hal yang penting dalam elemen keamanan nasional. Hal ini dapat dituangkan pada kebijakan negara melalui inisiatif pengaturan yang ditujukan untuk melindungi publik, pribadi dan hak milik individu.[93]

Tata kelola ranah siber dengan mengacu pada aspek keamanan nasional harus mampu mengakomodir kebutuhan dan kepercayaan masyarakat. Penanganan permasalahan di ranah siber di Indonesia saat ini masih belum terintegrasi dan terpadu, sehingga tata kelolanya masih bersifat parsial. Melihat kondisi yang demikian, celah kerawanan di ranah siber masih jelas terlihat. Hal ini akan menjadi ancaman ketahanan dan keamanan siber bagi masyarakat, korporasi dan penyelenggara pelayanan publik yang tentunya dapat berdampak strategis atau sistemik, sehingga dengan sendirinya akan mempengaruhi stabilitas bangsa yang konsekuensinya juga sebagai ancaman terhadap aspek ideologi, politik, ekonomi, sosial budaya, pertahanan dan keamanan.

Di era informasi dan sosial media berbasis internet, keamanan siber sangat terkait erat dengan stabilitas ideologi,

[93]Diskusi Pakar dengan Akademisi Dr. Intan Soeparna di Fakultas Hukum Universitas Airlangga Surabaya pada tanggal 27 Maret 2018.

politik, ekonomi, sosial, budaya, pertahanan, dan keamanan, dan bahkan kedaulatan negara. Sebagai contoh, serangan siber pada reaktor nuklir Iran (kasus stuxnet) dan serangan *crypto ransom* di sektor transportasi dan kesehatan (kasus wannacry). Akan tetapi salah satu tipe serangan siber yang paling berbahaya dan dapat mengganggu stabilitas nasional seringkali bukan serangan siber secara langsung terhadap instalasi sistem atau perangkat komputer, melainkan melalui propaganda *social engineering* melalui media internet.[94]

Oleh karena itu kehadiran negara untuk mengintegrasikan secara terpadu pengelolaan ranah siber mutlak diperlukan untuk mencegah ancaman pada aspek-aspek kehidupan berbangsa dan bernegara. Hadirnya negara dalam rangka melindungi warganya dan menjaga kedaulatan negara khususnya di ranah siber adalah dengan pembentukan RUU di bidang siber sebagai payung hukum di bidang siber dan berfungsi menentukan kebijakan siber nasional dengan peran dan kerjasama pemerintah, sektor swasta serta masyarakat.

Keamanan siber di Indonesia dipengaruhi oleh dua faktor utama, yakni infrastruktur dan teknologi yang memiliki kesadaran bahwa keamanan dunia siber adalah permasalahan penting terkait dengan pertanahan negara. Indonesia masih perlu meningkatkan infrastruktur dan teknologi yang dimiliki. Keamanan siber sangat perlu dalam keamanan negara, terutama pertahanan negara. Hal tersebut dikarenakan kepentingan negara termasuk kepentingan daerah. Walaupun telah berlaku otonomi daerah, akan tetapi pertahanan dan keamanan negara yang baik pasti akan berimplikasi positif bagi daerah, terutama provinsi-provinsi di Indonesia timur yang memiliki karakteristik wilayah kepulauan.[95]

---

[94] Diskusi Pakar Obrina Candra Briliyant, *Op.Cit.*
[95] Diskusi Pakar Akademisi Univ. Pattimura, *Op.Cit.*

e. Kelembagaan di bidang siber

Lembaga-lembaga yang terlibat dalam penanganan Siber di Indonesia, antara lain adalah: [96]

1) Kementerian Komunikasi dan Informatika (Kemenkominfo)
2) Badan Intelijen Negara (BIN)
3) Kepolisian Republik Indonesia (Polri)
4) Tentara Nasional Indonesia (TNI)
5) Badan Siber dan Sandi Nasional (BSSN)

Lembaga-lembaga tersebut merupakan satuan siber (*cyber force*) yang saat ini telah mengelola keamanan siber secara mandiri. Akan tetapi masing-masing lembaga tersebut memiliki perbedaaan tugas dan fungsi dalam menangani masalah siber di Indonesia.

Menurut Edmon Makarim, wilayah kewenangan keamanan siber nasional (*national cybersecurity*) yang ada di Indonesia, meliputi 6 (enam) wilayah, yakni: pertahanan siber (*cyber defence*), kejahatan siber (*cyber crime*), intelijen siber (*cyber intelligence*), keamanan siber (*cyber security*), ketahanan siber (*cyber resilience*), dan diplomasi siber (*cyber diplomacy*). Keenam wilayah kewenangan tersebut ditangani oleh lembaga yang berbeda yang dapat dilihat dalam tabel berikut:[97]

Saat ini penanganan masalah siber belum terkordinasi secara terstruktur. Sinergi kelembagaan siber di Indonesia masih terkotak-kotak dan terkendala dengan adanya kelemahan koordinasi karena ego sektoral. Salah satu cara untuk mengatasi permasalahan tersebut adalah dibutuhkannya tata kelola dan arsitektur keamanan siber

[96] *Ibid*

[97] Diskusi Pakar dengan Dr. Edmon Makarim di Pusat PUU pada tanggal 26 Februari 2018.

nasional yang jelas dan detail. Ada baiknya kelembagaan yang ada saat ini ditambah dengan lembaga berikut:[98]

1) *Computer Emergency Response Team* (CERT)

   Tugas dan fungsinya adalah agen sentral dalam mengkordinasikan kejadian yang berkaitan dengan keamanan siber. CERT berfungsi untuk memonitor ancaman yang berimbas pada sistem komputer, berkolaborasi secara internasional dalam merespon ancaman keamanan siber, menelusuri insiden keamanan siber yang berdampak baik pada sektor publik dan privat.

2) *Unique Identification Authority*

   Lembaga yang bertanggung jawab pada program untuk mengeliminir duplikasi dan identitas palsu melalui verifikasi dan autentifikasi yang efektif.

3) Lembaga *Cyber Forensic*

   Lembaga ini bertanggung jawab pada kegiatan investigasi dan teknis analisis dalam mengumpulkan dan menyimpan data dari alat digital (termasuk komputer). Tujuan dari *cyber forensic* adalah untuk melakukan penyelidikan terstruktur sambil mempertahankan rantai bukti yang terdokumentasi untuk mencari tahu persis apa yang terjadi pada perangkat komputasi dan siapa yang bertanggung jawab. Lembaga ini dapat berkolaborasi dengan Kepolisian RI.

Terkait kelembagaan di bidang siber, diharapkan BSSN akan menjadi lembaga yang mengoordinasikan kewenangan di bidang siber yang ada di kementerian/lembaga lain. BSSN hendaknya memiliki prioritas sebagai berikut:[99]

1) Memaksimalkan sertifikat digital dan pembuatan *certificate authentication*;
2) Penanganan cepat terhadap insiden siber (CERT)

[98] Diskusi Pakar Akademisi Univ. Airlangga, *Op.Cit.*
[99] Diskusi Pakar Obrina Candra Briliyant, *Op.Cit.*

3) Diseminasi informasi terkait insiden keamanan;
4) Koordinasi antarlembaga terkait serangan siber.

Oleh karena itu diperlukan pengaturan lebih lanjut mengenai tata kelola postur siber nasional yang membagi habis pekerjaan keamanan siber dan meminimalisir tumpang tindih fungsi dan kewenangan.

f. Partisipasi masyarakat

Terkait partisipasi masyarakat, di Provinsi Maluku peran serta masyarakat masih minim dalam penyelenggaraan siber di daerahnya. Pemerintah daerah dianggap perlu melakukan sosialisasi, literasi, dan pendidikan di sekolah-sekolah dan masyarakat mengenai penggunaan internet yang benar dan sehat. Saat ini peran serta masyarakat sangat dibutuhkan dan dirasakan manfaatnya diberbagai sendi kehidupan berbangsa dan bernegara. Ini karena untuk pencegahan kejahatan siber memang memerlukan pelibatan partisipasi masyarakat, melalui: (a) sosialisasi tentang peraturan, penggunaan teknologi informasi secara baik dan benar, termasuk sanksi hukum bagi pelanggar; (b) melibatkan akademisi atau penggiat/pelaku dibidang teknologi informasi sebagai narasumber maupun tenaga ahli pada berbagai kasus kejahatan siber.

Hal tersebut berbeda dengan yang terjadi di masyarakat Jawa Timur yang secara umum telah ikut berpartisipasi secara aktif dalam memanfaatkan media sosial yang terfasilitasi oleh pemerintah daerahnya, sebagai contoh media sosial yang dikelola oleh KPU Provinsi Jawa Timur sehingga masyarakat dapat mengetahui perkembangan terkait isu-isu pemilu dan pilkada Jawa Timur.

Menurut Obrina Candra Briliyant peran serta masyarakat dalam melakukan pencegahan kejahatan siber dapat dilakukan melalui pola perilaku internet yang sehat.

Pola perilaku internet sehat dapat dicapai melalui edukasi kepada masyarakat untuk menumbuhkan kesadaran diri (*self awareness*).[100]

g. Larangan dan sanksi

Kasus kejahatan siber di Indonesia makin marak dan diperlukan tanggung jawab pemerintah untuk mengatasinya. Hal ini disebabkan karena Indonesia merupakan pasar potensial bagi pelaku kejahatan siber seiring makin tingginya ketergantungan masyarakat Indonesia terhadap internet. Untuk mengimbangi laju perkembangan teknologi dan akibat kejahatan yang terjadi, maka diperlukan regulasi untuk memberikan kepastian hukum dalam menangani kejahatan siber.

Pemerintah telah menerbitkan UU ITE sebagai dasar penegakan hukum kejahatan siber, namun jika dikaji UU ITE masih lemah dan banyak mengatur hal-hal yang umum, sehingga tidak menjelaskan secara spesifik mengenai apa saja yang diatur dan bagaimana pengaturan dalam undang-undang tersebut. Demikian pula pada aspek pembuktian belum diatur secara komprehensif dalam UU ITE, sehingga tidak maksimal dalam menekan terjadinya kejahatan siber.

Untuk itu perlu adanya perbaikan dari sisi regulasi untuk memaksimalkan penegakan hukum kejahatan siber. Meskipun telah berlaku UU ITE, KUHP serta UU Telekomunikasi, namun mengingat cepatnya kemajuan teknologi perlu diimbangi dengan kesiapan regulasi yang lebih kuat. Sampai saat ini Indonesia belum memiliki regulasi khusus yang mengatur mengenai siber. Dalam UU ITE hanya beberapa pasal yang digunakan untuk memberikan sanksi terhadap pelanggaran siber. Beberapa aspek yang harus

[100] *Ibid*

menjadi muatan pelanggaran dan sanksi dalam regulasi siber, antara lain:

1) Perbuatan yang dilarang
2) Perbuatan melawan hukum
3) Perlindungan terhadap korban
4) Perlindungan terhadap data pribadi

Sanksi yang harus diatur dalam regulasi siber adalah sanksi pemidanaan yang didasarkan pada aspek pembuktian, sesuai dengan akibat dari perbuatan yang dilakukan dengan menggunakan pendekatan *multi-stakeholder core regulation*, tidak merugikan pasar, sektor swasta, pemerintah dan tetap punya otoritas untuk mengatur pemanfaatan teknologi internet. Hingga saat ini regulasi yang mengatur penggunaan teknologi informasi di Indonesia masih belum maksimal dalam menekan terjadinya kejahatan siber.

Kejahatan siber terbagi menjadi dua karakter yaitu, komputer sebagai sarana kejahatan dan komputer sebagai target kejahatan. Dalam ketentuan mengenai pelarangan dan sanksi harus merujuk pada dua karakter kejahatan siber tersebut. Pelarangan dapat diberlakukan dan disertai sanksi pidana dengan pertimbangan:

1) Efek dari kejahatan tersebut menggunakan skala berbasis kepentingan individu dan nasional;
2) Efek jera pada pelaku; dan
3) Kepastian hukum.

Hal-hal yang dapat menjadi batasan pelarangan dan sanksi dalam regulasi masalah kejahatan siber di Indonesia:

1) Ilegal akses;
2) Pencurian kartu kredit;
3) Penyebaran informasi palsu (hoax);
4) Pemerasan atau kejahatan yang memanfaatkan teknologi informasi (internet, komputer, dan lain sebagainya); dan

5) Batasan sanksi kurungan maksimal 12 tahun penjara dirasa sudah cukup membuat pelaku jera.

Ketentuan pidana yang belum diatur dalam undang-undang bidang teknologi informasi dan komunikasi antara lain:[101]

1) Penipuan *online*;
2) Pelanggaran hak cipta *online*;
3) Kejahatan data pribadi;
4) Penggunaan perangkat elektronik untuk mengirimkan pesan yang sama secara bertubi-tubi tanpa dikehendaki oleh penerimanya (*spam*); dan
5) Penyebaran informasi yang sesungguhnya tidak benar tetapi dibuat seolah-olah benar adanya (pemberitaan palsu/*hoax*).

Penjatuhan sanksi bagi pelanggar RUU Siber sebaiknya berorientasi pada pemberdayaan masyarakat karena pelanggaran hukum siber tidak serta merta sama dengan pelaku kriminal. Oleh karena itu baik korban ataupun pelaku bisa menerima sanksi dan sanksi tersebut diharapkan dapat memberikan kemanfaatan bagi orang banyak.

h. Penyelenggaraan siber di Indonesia

Kedaulatan siber (*cyber sovereignty*) adalah istilah yang digunakan dalam bidang tata kelola internet untuk menggambarkan keinginan pemerintah untuk melakukan kontrol atas internet di dalam wilayah mereka sendiri, termasuk kegiatan politik, ekonomi, budaya dan teknologi. Bagi sebagian orang, kontrol atas internet dianggap bertentangan dengan prinsip internet itu sendiri, dimana dikatakan bahwa internet tidak memiliki tata kelola terpusat baik dalam implementasi teknologi maupun kebijakan untuk akses dan penggunaannya.

[101] Diskusi Pakar Ferdinandus Setu, *Op.Cit.*

Kekhawatiran terbesar adalah jika pemerintah kemudian melakukan pemantauan terhadap seluruh aktivitas seseorang di internet, termasuk akun email, media sosial, grup diskusi dan lain-lain yang berpotensi melanggar hak asasi manusia pemilik akun. Namun dari sisi kepentingan pemerintah dalam bidang keamanan siber nasional terutama tentang keamanan data serta informasi milik pemerintah yang sifatnya konfidensial, tidak bisa kita pungkiri bahwa saat ini infrastruktur siber Indonesia belum terlalu bagus, masih banyak hal-hal yang perlu diperbaiki terkait dengan berbagai aspek nya. Mulai dari kondisi sumberdaya manusia yang kurang mumpuni, akses internet yang lambat, aplikasi-aplikasi yang belum teruji, sampai dengan aspek keamanan yang seringkali kurang diperhatikan. Misalnya dari sisi aplikasi, adalah kurang stabil nya layanan email yang diberikan oleh suatu instansi/lembaga pemerintah kepada para penyelenggara negara bukanlah hal yang sukar ditemui, dimana seringkali layanan yang diberikan sulit diakses ataupun mati pada saat-saat tertentu. [102]

Pengaturan mengenai keamanan siber harus dibedakan antara karakteristik geografis di tiap provinsi, sebagai contoh rentang kendali di provinsi Maluku menjadi hambatan dalam keamanan siber. Di Kabupaten Maluku Barat Daya yang berbatasan dengan Timor Timur, sinyal yang paling kencang adalah sinyal dari Timor Timur. Demikian pula dengan transportasinya lebih dekat dibandingkan dengan ibukota Provinsi Maluku. Saat ini belum ada BTS yang dibangun di Maluku Barat Daya dikarenakan pembangunan BTS oleh provider cenderung berorientasi profit. Jika kecenderungan untuk mendapatkan profit di daerah tersebut masih rendah, maka sulit bagi provider untuk membangun BTS di daerah tersebut. Hal ini menyebabkan masih banyak *blank spot* di

[102] Diskusi Pakar Akademisi Univ. Airlangga, *Op.Cit.*

Kabupaten Pulau Aru, Maluku Barat Daya, dan Maluku Tenggara.[103]

Dinas Kominfo Pemprov Maluku mengacu pada Instruksi Presiden RI No. 03 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *e-Government*. Penjabaran lebih lanjut tentang Instruksi Presiden tersebut melalui Peraturan Daerah atau Peraturan Gubernur sampai saat ini belum dilakukan, namun dalam konteks pelayanan publik telah diimplementasikan melalui berbagai aplikasi yang telah dimiliki oleh berbagai Organisasi Perangkat Daerah (OPD) sesuai tugas pokok dan fungsinya dalam rangka peningkatan efisiensi, efektivitas, transparansi dan akuntabilitas penyelenggaraan pemerintahan daerah.

D. Kajian terhadap implikasi penerapan Rancangan Undang-Undang Keamanan Siber terhadap aspek kehidupan masyarakat dan beban keuangan negara

Dengan adanya UU Keamanan Siber diharapkan:

a. hubungan tugas dalam pelaksanaan fungsi keamanan siber pada masing-masing instansi K/L/D dapat terorganisir efektif sesuai dengan porsinya masing-masing,
b. penyelenggaraan keamanan siber nasional akan didorong untuk mengedepankan tindakan kolaboratif dari unsur pemerintah maupun swasta,
c. akan membentuk dan meningkatkan kesiap-siagaan dari seluruh komponen dalam penyelenggaraan keamanan siber nasional, dan
d. terwujudnya keterpercayaan dari segenap pihak di dalam dan di luar negeri untuk beraktifitas secara aman di ruang siber yang menjadi tanggung jawab Indonesia

[103] Diskusi Pakar dengan Diskominfo di Provinsi Maluku pada tanggal 27 Maret 2018.

Dari aspek keuangan negara, pengalokasian anggaran untuk penyelenggaraan keamanan siber adalah suatu hal yang mutlak diperlukan. Ketersediaan ruang siber yang aman tidak dapat digantungkan pada sumber daya dan kemampuan finansial orang perorangan, melainkan merupakan tanggung jawab negara. Terlebih lagi dalam era revolusi industri 4.0, keamanan siber akan menjadi hal yang sangat penting karena pada era tersebut dapat dikatakan hampir segenap perikehidupan masyarakat akan terkait erat dengan pemanfaatan teknologi informasi. Oleh karena itu tersedianya ruang siber yang aman dapat disejajarkan dengan bidang pendidikan atau kesehatan yang mengharuskan negara untuk hadir dan menunjukkan komitmennya dengan segenap sumber dayanya.

E. Praktik Pengaturan Keamanan Siber di Beberapa Negara Lain

Secara umum pengaturan tentang Keamanan Siber di negara lain dimuat dalam suatu Undang-Undang tersendiri, tidak digabungkan dengan pengaturan terkait telekomunikasi (yang fokus pada pengaturan tata niaga dan perizinan di sektor telekomunikasi), pengaturan terkait legalitas transaksi elektronik (yang fokus pada pengaturan tentang legalitas bukti elektronik dan upaya untuk mendorong pembudayaan penggunaan sistem elektronik), dan/atau pengaturan terkait tindak pidana siber (yang fokus pada pengaturan tentang kejahatan siber).

Di tingkat regional yaitu ASEAN tercatat ada 2 (dua) negara yang telah memiliki Undang-Undang tentang Keamanan Siber, yaitu Singapura dan Vietnam. Kemudian ada 2 (dua) negara lain yang sudah membahas Rancangan Undang-Undang tentang Keamanan Siber yaitu Thailand dan Malaysia. Beberapa negara yang dari segi kapasitas perekonomian dan teknologi telah maju juga telah memiliki Undang-Undang tentang Keamanan Siber secara tersendiri. Diantaranya Russia, Swiss, China, Uni Eropa, Amerika Serikat, dan Jepang.

BAB III
EVALUASI DAN ANALISIS PERUNDANG-UNDANGAN TERKAIT

Pada penyusunan Naskah Akademik RUU Keamanan dan Ketahanan Siber, perlu dilakukan analisa terhadap peraturan perundang-undangan yang telah ada sebelumnya. Hal ini dilakukan untuk menemukan keterkaitan antara RUU Keamanan dan Ketahanan Siber dengan Undang-Undang yang telah ada sebelumnya sehingga menemukan harmonisasi baik secara vertikal maupun horizontal. Bab ini akan memuat hasil analisis terhadap Peraturan Perundang-undangan terkait dengan Keamanan Siber yang telah kami temukan, antara lain:

1. Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara

Tujuan dalam pembuatan peraturan perundang-undangan dari kedua peraturan baik Undang-Undang Pertahanan Negara dengan RUU Keamanan dan Ketahanan Siber memiliki tujuan dasar yang sama yaitu melindungi kedaulatan segenap bangsa dan Negara Indonesia. Memberikan perlindungan menjadi ciri khas utama dalam peraturan perundang-undangan yang bernuansa pertahanan maupun keamanan Negara, seperti dalam Pasal 4 Undang-Undang Pertahanan Negara menyatakan "Pertahanan negara bertujuan untuk menjaga dan melindungi kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari segala bentuk ancaman".

Tujuan dari Undang-Undang Pertahanan Negara dengan RUU Keamanan dan Ketahanan Siber sama-sama memberikan perlindungan terhadap Negara Kesatuan Republik Indonesia dari berbagai bentuk ancaman, terutama ancaman siber pada RUU Keamanan dan Ketahanan Siber. Potensi ancaman yang datang baik secara domestik maupun internasional menjadi salah satu

dasar pijakan kenapa peraturan perundang-undangan ini perlu dibuat, hingga pada akhirnya Indonesia memiliki kemampuan dalam upaya melindungi Negara pada umumnya dan warga Negara pada khususnya dari potensi ancaman yang perlu dicegah maupun ditanggulangi.

Selain itu undang-undang ini juga secara tidak langsung menjadi dasar amanat lebih lanjut dalam melindungi Negara Kesatuan Indonesia dengan RUU Keamanan dan Ketahanan Siber dari potensi ancaman siber yang begitu dekatnya dihadapan kita. Segala bentuk ancaman yang dimaksud pada tujuan Undang-Undang Pertahanan membuat luas potensi ancaman yang dapat terjadi di Indonesia. Kemajuan teknologi informasi yang ada mendesak kita juga untuk sadar bahwa ancaman siber menjadi salah satu ancaman yang mampu mengganggu keamanan, stabilitas dan ketahanan Negara. Sehingga tidak dapat dipungkiri bahwasannya Keamanan Siber menjadi mendesak untuk diatur dalam suatu peraturan perundang-undangan.

Penjelasan Pasal 4 Undang-Undang Pertahanan Negara memberikan penjelasan tentang ancaman adalah setiap usaha dan kegiatan, baik dari dalam negeri maupun luar negeri yang dinilai membahayakan kedaulatan negara, keutuhan wilayah negara, dan keselamatan segenap bangsa. Dalam RUU Keamanan dan Ketahanan Siber juga mencantumkan Ancaman Siber baik yang datang dari domestik maupun internasional yang perlu dilakukan upaya-upaya baik secara umum dengan pencegahan maupun penanggulangannya.

2. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara

Undang-undang Intelijen menjadi suatu gambaran besar yang dapat ditarik dalam komponen RUU Keamanan dan Ketahanan Siber untuk melindungi dan menjaga Keamanan Siber di Indonesia. Pada Undang-Undang Intelijen dalam Pasal 6 ayat

(1) menyatakan Intelijen Negara menyelenggarakan fungsi penyelidikan, pengamanan, dan penggalangan. Selain itu Pasal 6 ayat (5) Undang-Undang Intelijen menyatakan bahwa dalam menyelenggarakan fungsinya harus menghormati hukum, nilai-nilai demokrasi, dan hak asasi manusia. Fungsi Keamanan Siber sendiri memiliki komponen yang pada intinya mencakup fungsi pendeteksian dan pengidentifikasian, pemroteksian, penanggulangan dan pemulihan, pemantauan dan pengendalian ekosistem Keamanan Siber. Dalam menyelenggarakan fungsi tersebut memiliki keserupaan dengan Undang-Undang Intelijen seperti harus mengindahkan perlindungan hak asasi manusia, kepentingan inovasi IPTEK, dan kepentingan pemajuan perekonomian nasional.

Penyelenggara fungsi Intelijen Negara dalam Pasal 9 Undang-Undang Intelijen menyatakan terdiri atas Badan Intelijen Negara, Intelijen Tentara Nasional Indonesia, Intelijen Kepolisian Negara Republik Indonesia, Intelijen Kementerian/Lembaga pemerintahan nonkementerian. Terkait dalam memberikan perlindungan siber Indonesia maka pada RUU Keamanan dan Ketahanan Siber, para pemangku kepentingan juga ikut menyelenggarakan fungsi Keamanan Siber seperti Badan Siber dan Sandi Negara, Siber Tentara Nasional Indonesia, Siber Kepolisian Negara Republik Indonesia, Siber Intelijen Negara, Siber Kementerian/Lembaga, serta ditambah dengan Siber Pemerintah Daerah. Masing-masing pemangku kepentingan melaksanakan fungsi siber pada masing-masing bidang otoritas kewenangannya seperti fungsi Keamanan Siber dalam dan luar negeri oleh BSSN, fungsi Keamanan Siber pertahanan dan/atau militer pada TNI, fungsi Keamanan Siber kepolisian pada POLRI, fungsi Keamanan Siber penegakan hukum pada Kejaksaan, fungsi Keamanan Siber Intelijen Negara pada BIN, fungsi Keamanan Siber Kementerian/Lembaga non Kementerian/Lembaga non Struktural/Kesekretarian Lembaga Negara pada Kementerian/Lembaga terkait, fungsi Keamanan

Siber Pemerintah Daerah Provinsi/Pemerintah Daerah Kabupaten/Pemerintah Daerah Kota pada Pemerintah Daerah masing-masing.

Pasal 1 angka 4 Undang-Undang Intelijen menyatakan bahwa ancaman adalah setiap upaya, pekerjaan, kegiatan, dan tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat membahayakan keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan kepentingan nasional di berbagai aspek, baik ideologi, politik, ekonomi, sosial budaya, maupun pertahanan dan keamanan. Selain ancaman yang dapat dikatakan bersifat konvensional, ancaman siber yang berpotensi merugikan Negara juga perlu tercantum dalam RUU Keamanan dan Ketahanan Siber demi mendapatkan kepastian hukum dalam upaya perlindungan dari ancaman keamanan siber.

Kerugian yang muncul kepada orang akibat dari pelaksanaan fungsi intelijen dapat mengajukan permohonan rehabilitasi, kompensasi, dan restitusi, seperti yang tercantum dalam Pasal 15 ayat (1) Undang-Undang Intelijen. Layaknya pelaksanaan fungsi Intelijen, Keamanan Siber pun berpotensi merugikan orang dalam pelaksanaan fungsi-fungsinya, maka komponen klausul dalam Pasal 15 ayat (1) Undang-Undang Intelijen perlu ada dalam RUU Keamanan dan Ketahanan Siber. Hal ini untuk memberikan perlindungan kepada hak asasi manusia masing-masing individu jika dalam kegiatan Keamanan Siber, terdapat kesalahan yang akan merugikan seseorang. Sehingga perlunya upaya-upaya untuk mengganti atau mengurangi kerugian pihak-pihak yang menderita baik dengan rehabilitiasi, kompensasi dan/atau restitusi.

Pada pasal 27 Undang-Undang Intelijen menjelaskan bahwa Badan Intelijen Negara berada di bawah dan bertanggung jawab kepada Presiden. Serupa dengan hal tersebut, dalam RUU Keamanan dan Ketahanan Siber juga perlu pasal penegasan

bahwa BSSN sebagai *focal point* dalam urusan Keamanan Siber berkedudukan di bawah dan bertanggung jawab kepada Presiden. Dalam hal fungsi dari Intelijen Negara seperti yang telah disebutkan di atas, pada RUU Keamanan dan Ketahanan Siber juga perlu menegaskan hal yang serupa tentang fungsi BSSN yaitu seperti fungsi Keamanan Siber, Diplomasi Siber, Pelayanan Keamanan Siber, dan Penyidikan dan Penindakan baik dalam lingkup domestik maupun internasional.

Pasal 30 Undang-Undang Intelijen menyebutkan tentang wewenang dari Badan Intelijen Negara seperti a. menyusun rencana dan kebijakan nasional di bidang Intelijen secara menyeluruh; b. meminta bahan keterangan kepada kementerian, lembaga pemerintah nonkementerian, dan/atau lembaga lain sesuai dengan kepentingan dan prioritasnya; c. melakukan kerja sama dengan Intelijen negara lain; dan d. membentuk satuan tugas. Sehingga dalam RUU Keamanan dan Ketahanan Siber juga dirasakan perlu untuk menegaskan wewenang BSSN dalam Keamanan Siber di Indonesia misalnya saja membentuk kebijakan tentang Keamanan Siber, merumuskan kerangka kerja Keamanan Siber Indonesia, melaksanakan upaya Keamanan Siber baik nasional maupun internasional, dan lainnya.

Dalam Pasal 31 Undang-Undang Intelijen, Badan Intelijen Negara memiliki wewenang lain seperti melakukan penyadapan, pemeriksaan aliran dana, dan penggalian informasi terhadap sasaran sebagai wujud perlindungan keamanan dan pertahanan Negara. Maka dari itu pada RUU Keamanan dan Ketahanan Siber, BSSN dalam upaya melindungi Keamanan Siber Indonesia memiliki wewenang melaksanakan identifikasi dan deteksi, proteksi, penanggulangan dan pemulihan, dan pemantauan dan pengendalian pada obyek pengamanan baik di dalam negeri dan di luar negeri.

Terkait dengan struktur organisasi dari Badan Intelijen Negara, dalam Pasal 35 Undang-Undang Intelijen menyatakan

bahwa Badan Intelijen Negara dipimpin oleh seorang kepala dan dibantu oleh seorang wakil kepala. Dalam RUU Keamanan dan Ketahanan Siber juga perlu ditegaskan tentang struktur organisasi BSSN terutama terkait dengan BSSN yang dipimpin oleh seorang kepala dengan dibantu oleh seorang wakil kepala, serta pengangkatan dan pemberhentiannya ditetapkan dengan Keputusan Presiden. Selanjutnya pada Pasal 37 Undang-Undang Intelijen, mengenai organisasi dan tata kerja Badan Intelijen Negara diatur dengan Peraturan Presiden, sehingga pada RUU Keamanan dan Ketahanan Siber pengaturan lebih lanjut dari struktur, organisasi dan tata kerja BSSN akan juga diatur dalam Peraturan Presiden.

Pada ketentuan pidana yang diatur dalam Pasal 44 Undang-Undang Intelijen menyatakan bahwa setiap Orang yang dengan sengaja mencuri, membuka, dan/atau membocorkan Rahasia Intelijen sebagaimana dimaksud dalam Pasal 26 dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah). Ketentuan pidana tersebut dapat dikatakan secara umum mengatur mengenai kejahatan terhadap Rahasia Negara yang dapat dikenakan sanksi pidana, Rahasia dalam lingkup Keamanan Siber juga termasuk pada Rahasia Negara yang dapat dikatakan vital dan merugikan jika terjadi pencurian, pembukaan, dan/atau pembocoran. Sehingga pada RUU Keamanan dan Ketahanan Siber juga perlu diatur mengenai sanksi pidana terhadap kejahatan kepada Rahasia Negara terutama pada lingkup Keamanan Siber.

3. Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia

Pasal 1 angka 22 Undang-Undang TNI menyatakan ancaman adalah setiap upaya dan kegiatan, baik dari dalam negeri maupun luar negeri yang dinilai mengancam atau membahayakan

kedaulatan negara, keutuhan wilayah negara, dan keselamatan segenap bangsa. Pola-pola konsep dan komponen yang ada mengenai ancaman yang bersifat konvensional, perlu dan dapat menjadi dasar dalam rumusan tentang ancaman siber yang dirasakan urgensinya untuk hadir dalam RUU Keamanan dan Ketahanan Siber.

Dalam diplomasi siber, selain adanya keterkaitan dengan Undang-Undang Nomor 37 Tahun 1999 tentang Hubungan Luar Negeri, ketentuan mengenai kewenangan diplomasi siber sebagai bagian dari Keamanan Siber oleh otoritas Negara yang berwenang seperti Pasal 9 huruf c Undang-Undang TNI menyatakan bahwa angkatan laut bertugas melaksanakan tugas diplomasi angkatan laut dalam rangka mendukung kebijakan politik luar Negari yang ditetapkan oleh pemerintah. Sedangkan pada Keamanan Siber, kewenangan Diplomasi siber dilaksanakan oleh BSSN yang dapat berkolaborasi dengan Kementerian yang bertanggung jawab dalam urusan luar negeri.

Pasal 7 Undang-Undang TNI menyatakan bahwa tugas pokok TNI dilakukan dengan operasi militer untuk perang. Keamanan Siber yang sangat erat kaitannya dengan insiden serangan siber baik oleh *state actor* maupun *non state actor*, yang memiliki potensi berujung pada keadaan perang. Sehingga dalam RUU Keamanan dan Ketahanan Siber sebagai salah satu bagian kegiatan operasi militer dalam keadaan perang, kewenangan pengendalian Keamanan Siber diberikan pelaksanaannya oleh Tentara Nasional Indonesia.

4. Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia

Pada Pasal 15 ayat (1) huruf j Undang-Undang POLRI menyatakan “dalam rangka menyelenggarakan tugas secara umum berwenang menyelenggarakan Pusat Informasi Kriminal Nasional….”. Terkait dengan RUU Keamanan dan Ketahanan

Siber demi memberikan wadah sebagai tempat untuk melakukan penanggulangan dan pemulihan dari insiden siber, maka perlu membuat Pusat Operasi Keamanan Siber Nasional yang diselenggarakan oleh BSSN. Disamping itu masing-masing dari Penyelenggara Keamanan Siber juga perlu diwajibkan membentuk Pusat Operasi Keamanan Siber yang berkoordinasi dengan Pusat Operasi Keamanan Siber Nasional.

Pasal 8 ayat (1) Undang-Undang Kepolisian juga menjelaskan bahwa Kepolisian Negara Republik Indonesia berada dibawah Presiden, dan dalam ayat (2) Kepolisian Negara Republik Indonesia dipimpin oleh Kapolri yang dalam pelakasanaan tugasnya bertanggung jawab kepada Presiden sesuai dengan peraturan perundang-undangan. Serupa dengan hal tersebut, dalam RUU Keamanan dan Ketahanan Siber juga perlu pasal penegasan bahwa BSSN sebagai otoritas Negara yang memiliki kewenangan dalam urusan Keamanan Siber berkedudukan di bawah dan bertanggung jawab kepada Presiden, serta dipimpin oleh seorang kepala yang dibantu oleh seorang wakil kepala. Selanjutnya mengenai susunan stuktur organisasi dan tata kerja dari POLRI dalam Pasal 7 Undang-Undang Kepolisian akan diatur lebih lanjut dengan keputusan presiden. Begitupun dalam RUU Keamanan dan Ketahanan Siber untuk lebih menegaskan tentang struktur, organisasi dan tata kerja dari BSSN, akan diatur lebih lanjut dalam Peraturan Presiden.

Pasal 16 huruf g Undang-Undang POLRI menyatakan bahwa dalam rangka menyelenggarakan tugas di bidang proses pidana, POLRI berwenang untuk mendatangkan ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara. Terkait dengan hal tersebut, maka dalam RUU Keamanan dan Ketahanan Siber BSSN dapat memberikan dukungan penegakan hukum pidana seperti melakukan penganalisaan bukti digital, memberikan keterangan ahli bidang forensik digital, serta dukungan teknis dalam tahap penyelidikan dan penyidikan.

Pasal 41 ayat (2) Undang-Undang POLRI, menyatakan bahwa dalam keadaan darurat militer dan keadaan perang, Kepolisian Negara Republik Indonesia memberikan bantuan kepada Tentara Nasional Indonesia sesuai dengan peraturan perundangan-undangan. Pada bidang Keamanan Siber pun sangat erat kaitannya dengan insiden serangan siber baik oleh *state actor* maupun *non-state actor*, yang pada ujungnya berpotensi ke keadaan perang. Sehingga dalam RUU Keamanan dan Ketahanan Siber perlu penegasan tentang kewenangan pengendalian Keamanan Siber yang dapat dilaksanakan oleh Tentara Nasional Indonesia bila terjadi keadaan perang.

5. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Pasal 39 ayat (1) Undang-Undang Telekomunikasi menyatakan bahwa Penyelenggara telekomunikasi wajib melakukan pengamanan dan perlindungan terhadap instalasi dalam jaringan telekomunikasi yang digunakan untuk penyelenggaraan telekomunikasi. Dalam Undang-Undang Telekomunikasi tersebut, Negara memberikan kewajiban kepada penyelenggara telekomunikasi untuk mengamankan dan melindungi instalasi dalam jaringan telekomunikasi, sehingga terdapat pemberian wewenang kewajiban kepada para pihak penyelenggara telekomunikasi dari Negara untuk tertib dan taat melindungi infrastrukturnya. Sedangkan terkait dengan RUU Keamanan dan Ketahanan Siber, memahami dasar bahwa perlunya ada kolaborasi antara Negara dengan pihak-pihak yang memiliki kepentingan dalam Keamanan Siber termasuk pihak swasta.

Faktanya banyak infrastruktur kritis siber di Indonesia dimiliki oleh pihak swasta, sehingga perlu adanya pula tanggung jawab yang diberikan Negara kepada pihak-pihak swasta dalam mengelola Keamanan Siber pada infrastruktur yang dimilikinya.

Kolaborasi sebagaimana yang dimaksud tersebut harus dibina dan dikonsolidasi dengan efektif dan efisien demi terwujudnya satu kesatuan komponen keamanan nasional yang terpadu dan senantiasa siap siaga dalam melaksanakan fungsi Keamanan Siber terutama dari ancaman kejahatan siber.

Dalam konsep *public-private partnership,* upaya Penyelenggara Keamanan Siber memiliki kewajiban-kewajiban melindungi obyek pengamanan dengan identifikasi dan deteksi ancaman siber, proteksi, penanggulangan dan pemulihan, serta pemantauan dan pengendalian. Karena pihak swasta ikut berperan dalam melakukan upaya-upaya tersebut sebagai wujud *public-private partnership* maka perlu adanya peran pemerintah sebagai otoritas Negara dalam melakukan pembinaan. Hal ini serupa dengan bunyi ketentuan Pasal 4 ayat (1) Undang-Undang Telekomunikasi yang berbunyi "Telekomunikasi dikuasai oleh Negara dan pembinaannya dilakukan oleh Pemerintah".

6. Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Pasal 32 ayat (1) dan ayat (3) Undang-Undang ITE menyatakan bahwa setiap orang dengan sengaja tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik. Terhadap perbuatan tersebut yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. Tindakan tersebut memiliki konsekuensi hukuman pidana seperti yang tercantum dalam Pasal 48 ayat (3) dengan pidana penjara paling

lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Keterkaitan hal tersebut dengan RUU Keamanan dan Ketahanan Siber ada pada tindak pelanggaran dan ketentuan pidana. Pada pasal-pasal yang ada dalam Undang-Undang ITE tersebut, tindak pelanggaran yang dilakukan merupakan membuat terbukanya suatu informasi atau dokumen yang bersifat rahasia secara tanpa hak, dengan berbagai cara dan upaya terkait. Dalam lingkup Keamanan Siber, juga terdapat baik informasi maupun dokumen yang bersifat rahasia. Informasi dan Dokumen yang bersifat rahasia tersebut juga berpotensi secara tanpa hak terbuka untuk umum atau terjadinya kebocoran. Kebocoran kerahasiaan tersebut akan menimbulkan dampak kerugian negara, dapat digambarkan misalnya terjadi kebocoran rahasia Negara kepada Negara lain yang bersifat keamanan nasional atau pertahanan, hal tersebut tidak menutup kemungkinan akan berpotensi menganggu keamanan dan pertahanan Negara. Belum lagi rahasia-rahasia lain yang bersifat private, kerugian nyata akan dirasakan oleh warga Negara.

Maka dari itu ketentuan mengenai rahasia dalam lingkup Keamanan Siber yang dengan sengaja dicuri, dibuka dan/atau dibocorkan oleh pihak yang tidak berhak, perlu adanya sanksi pidana. Dalam menentukan ketentuan pidana dalam RUU Keamanan dan Ketahanan Siber tersebut, atas kesamaan potensi tindak pelanggaran terutama pada pencurian, pembukaan, dan pembocoran rahasia. Maka jumlah ancaman pidana dan pengenaan besaran sanksi akan dirumuskan mengacu pada Undang-Undang ITE. Tindak pelanggaran mencuri, membuka, dan/atau membocorkan rahasia dalam lingkup Keamanan Siber akan dikenakan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000,00 (lima milyar rupiah).

Pasal 40 ayat (2a), (2b), (3), (4), dan (5) Undang-Undang ITE menyatakan bahwa:

(2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundangundangan.

(2a) Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.

(2b) Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum.

(3) Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi.

(4) Instansi atau institusi sebagaimana dimaksud pada ayat (3) harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data.

(5) Instansi atau institusi lain selain diatur pada ayat (3) membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya.

Dalam kaitannya dengan ketentuan tersebut muncul ketidaksesuaian dengan konsep RUU Keamanan dan Ketahanan Siber yang menggunakan *public-private partnership,* sehingga dirasakan perlu perubahan Pasal 40 UU ITE ini yang akan

mengikuti RUU Keamanan dan Ketahanan Siber. RUU Keamanan dan Ketahanan Siber dalam hal upaya melakukan identifikasi dan deteksi ancaman siber, proteksi, penanggulangan dan pemulihan, serta pemantauan dan pengendalian menjadi kewajiban Penyelenggara Keamanan Siber untuk melindungi obyek pengamanan. Penyelenggara Keamanan Siber merupakan perwujudan dari konsep *public-private partnership,* hal ini karena Penyelenggara Keamanan Siber tidak hanya terdiri dari otoritas kenegaraan, tetapi juga pihak swasta yang memiliki infrastruktur kritis di Indonesia.

Jadi kewajiban memberikan perlindungan kepada Negara pada Keamanan Siber menjadi tanggung jawab bersama antara pemerintah dan pihak swasta, bukan hanya oleh pemerintah. Pemerintah tetap memiliki peran sentral dalam upaya perlindungan Keamanan Siber di Indonesia yang dipegang oleh BSSN. BSSN dapat dikatakan sebagai *focal point* dan memiliki peran sebagai pembina dalam bidang Keamanan Siber yang mampu melaksanakan identifikasi dan deteksi ancaman siber, proteksi, penanggulangan dan pemulihan, serta pemantauan dan pengendalian obyek pengamanan dengan kegiatan-kegiatan yang perlu ditegaskan dalam RUU Keamanan dan Ketahanan Siber.

7. Undnag-Undang Nomor 20 Tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian

Pada Pasal 19 ayat (1) Undang-Undang Standardisasi dan Penilaian Kesesuaian menyatakan setiap orang dilarang memalsukan SNI atau membuat SNI palsu. Dalam Pasal 26 ayat (2) menyatakan bahwa setiap orang dilarang memalsukan Tanda SNI dan/atau Tanda Kesesuaian atau membuat Tanda SNI dan/atau Tanda Kesesuaian palsu. Selanjutnya dalam Pasal 37 ayat (4) menyatakan bahwa setiap orang dilarang memalsukan sertifikat Akreditasi atau membuat sertifikat Akreditasi palsu.

Ketentuan Pidana yang terkait dengan hal tersebut berada pada Pasal 62 yang menyatakan bahwa Setiap orang yang memalsukan SNI atau membuat SNI palsu sebagaimana dimaksud dalam Pasal 19 ayat (1) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah). Pada Pasal 69 menyatakan bahwa setiap orang yang memalsukan tanda SNI dan/atau Tanda Kesesuaian atau membuat Tanda SNI dan/atau Tanda Kesesuaian palsu sebagaimana dimaksud dalam Pasal 26 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah). Selanjutnya dalam Pasal 71 menyatakan bahwa setiap orang yang memalsukan sertifikat Akreditasi atau membuat sertifikat Akreditasi palsu sebagaimana dimaksud dalam Pasal 37 ayat (4) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah).

Keterkaitan bunyi Pasal mengenai tindak pelanggaran dan ketentuan pidana dalam Undang-Undang Standardisasi dan Penilaian Kesesuaian tersebut dengan RUU Keamanan dan Ketahanan Siber adalah mengenai tindak pelanggaran serta ketentuan pidana yang terdapat dalam RUU Keamanan dan Ketahanan Siber. Pada pasal-pasal yang telah disebutkan diatas, tindak pelanggaran yang dapat dilakukan merupakan pemalsuan. Tindakan pemalsuan tersebut dilakukan baik kepada SNI, Tanda SNI atau Tanda Kesesuaian, dan sertifikasi Akreditasi.

Sedangkan pada RUU Keamanan dan Ketahanan Siber sebagai bentuk Pelayanan Keamanan Siber dalam upaya menjamin Keamanan Siber, adanya kewajiban sertifikasi elektronik bagi setiap Penyelenggara Keamanan Siber yang diterapkan dalam sistem informasi dan sistem elektroniknya. Selain itu dalam RUU Keamanan dan Ketahanan Siber juga

muncul hal-hal mengenai Izin Akses Keamanan Siber, Izin Penyedia Jasa Keamanan Siber, Akreditasi Lembaga Pendidikan dan Pelatihan Keamanan Siber, Akreditasi Lembaga Sertifikasi Profesi Keamanan Siber, Sertifikat Produk Keamanan Siber, dan/atau Sertifikat Digital. Keseluruhan mengenai produk layanan yang ada dalam upaya menjamin Keamanan Siber tersebut berpotensi dilanggar oleh pihak-pihak yang tidak bertanggungjawab. Pelanggaran yang mungkin terjadi baik berupa memalsukan maupun menggunakan hasil pemalsuan.

Dalam menentukan ketentuan pidana RUU Keamanan dan Ketahanan Siber, atas kesamaan potensi tindak pelanggaran terutama pemalsuan. Maka jumlah ancaman pidana dan pengenaan besaran sanksi akan dirumuskan mengacu pada Undang-Undang Standardisasi dan Penilaian Kesesuaian. Pelanggaran memalsukan dan/atau menggunakan hasil pemalsuan dari Izin Akses Keamanan Siber, Izin Penyedia Jasa Keamanan Siber, Akreditasi Lembaga Pendidikan dan Pelatihan Keamanan Siber, Akreditasi Lembaga Sertifikasi Profesi Keamanan Siber, Sertifikat Produk Keamanan Siber, dan/atau Sertifikat Digital akan dikenakan pidana penjara paling lama 7 (tujuh) tahun, dengan besaran sanksi paling banyak 10.000.000.000,00 (sepuluh milyar rupiah).

8. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional

Pada bagian pengalokasian dana pendidikan dalam Pasal 49 ayat (1) menyatakan bahwa dana pendidikan selain gaji pendidik dan biaya pendidikan kedinasan dialokasikan minimal 20% dari Anggaran Pendapatan dan Belanja Negara (APBN) pada sektor pendidikan dan minimal 20% dari Anggaran Pendapatan dan Belanda Daerah (APBD).

Keterkaitan RUU Keamanan dan Ketahanan Siber dengan hal tersebut, yaitu pada pendanaan penyelenggaraan Keamanan Siber

pemerintah. Pendanaan dalam penyelenggaraan Keamanan Siber pemerintah menjadi suatu yang penting untuk mendukung pelaksanaan penyelenggaraan Keamanan Siber. Berbagai kebutuhan yang harus dipenuhi baik dari infrastruktur maupun sumber daya manusia perlu mendapatkan dukungan dana. Sehingga dalam RUU Keamanan dan Ketahanan Siber perlu diatur mengenai pendanaan dari penyelenggaran Keamanan Siber pemerintah dengan berbagai sumber dana. Salah satu sumber dana dalam penyelenggaraan Keamanan Siber pemerintah, diperoleh dari Anggaran Pendapatan dan Belanja Negara, serta Anggaran Pendapatan dan Belanja Daerah. Alokasi dana minimal 20% dari APBN pada sektor pendidikan menjadi dasar dalam merumuskan ketentuan sumber dana penyelenggaraan Keamanan Siber pemerintah.

Dalam mewujudkan penyelenggaraan Keamanan Siber pemerintah yang baik, diperlukan alokasi dana sebesar 20% dari Anggaran Pendapatan dan Belanja Negara. Besaran tersebut akan dikelola dalam pelaksanaan upaya-upaya terkait Keamanan Siber pemerintah yang perlu memiliki infrastruktur keamanan siber yang layak dan andal. Pembangunan dan penguatan perangkat serta pengembangan sumber daya manusia terkait Keamanan Siber menjadi salah satu upaya dalam memperkuat Keamanan Siber pemerintah. Kelemahan dan kekurangan pada infrastuktur keamanan siber pemerintah akan berakibat pada kerugian dalam berbagai segi kehidupan masyarakat Indonesia. Pada bagian sebelumnya telah dijelaskan betapa pentingnya Keamanan Siber dalam melindungi berbagai kepentingan nasional Indonesia, termasuk kesejahteraan dan keamanan masyarakat.

Dana yang dialokasikan dari APBN tersebut akan diperuntukan pada pembangunan dan penguatan perangkat dan infrastruktur keamanan siber serta pengembangan sumber daya manusia. Pembangunan dan penguatan pada perangkat serta infrastruktur Keamanan Siber akan dilakukan dengan pengadaan

melalui penunjukan langsung maupun pengadaan langsung. Pembangunan dan penguatan pada perangkat dan infrastruktur Keamanan Siber tidak akan berjalan secara maksimal tanpa ada sumber daya manusia yang mumpuni dalam pelaksanaannya. Untuk mewujudkan sumber daya manusia yang mumpuni dalam melaksanakan penyelenggaraan keamanan siber, diperlukan pula pengembangan sumber daya manusia dengan berbagai kegiatan terkait kompetensi dalam bidang Keamanan Siber. Sehingga sinergi antara penguatan perangkat dan infrastuktur dengan pengembangan kompetensi dari sumber daya manusia, diharapkan akan memberikan perlindungan Keamanan Siber yang maksimal secara efektif dan efisien di Indonesia.

9. Undang-Undang Nomor 2 Tahun 2017 tentang Jasa Konstruksi

Pada Pasal 42 ayat (1) Undang-Undang Jasa Konstruksi menyatakan bahwa pemilihan penyedia jasa yang menggunakan sumber pembiayaan dari keuangan Negara dilakukan dengan cara tender atau seleksi, pengadaan secara elektronik, penunjukan langsung, dan pengadaan langsung sesuai dengan ketentuan peraturan perundang-undangan. Pada ayat (4) menyatakan bahwa penunjukan langsung dapat dilakukan dalam hal:

a) Penanganan darurat untuk keamanan dan keselamatan masyarakat;
b) Pekerjaan yang kompleks yang hanya dapat dilaksanakan oleh penyedia jasa yang sangat terbatas atau hanya dapat dilakukan oleh pemegang hak;
c) Pekerjaan yang perlu dirahasiakan yang menyangkut keamanan dan keselamatan Negara;
d) Pekerjaan yang berskala kecil; dan/atau
e) Kondisi tertentu.

Pada Pasal 42 ayat (5) Undang-Undang Jasa Konstruksi menyatakan bahwa pengadaan langsung dilakukan untuk paket dengan nilai tertentu. Terkait dengan hal tersebut, pada RUU

Keamanan dan Ketahanan Siber pendanaan menjadi hal yang penting dalam penyelenggaraan Keamanan Siber. Dana yang diperoleh untuk penyelenggaraan Keamanan Siber pemerintah dikelola dan diperuntukan salah satunya untuk menerapkan pengadaan perangkat keras atau perangkat lunak. Pengadaan tersebut akan dilakukan dengan cara yang serupa dengan Undang-Undang Jasa Konstruksi terutama dengan pemilihan penyedia jasa yang dilakukan dengan cara penunjukan langsung atau pengadaan langsung.

Sehingga pengadaan dari perangkat keras dan perangkat lunak dalam pengelolaan dana penyelenggaraan Keamanan Siber pemerintah dapat dilakukan dengan cara penunjukan langsung atau pengadaan langsung. Kriteria perihal keadaan yang memerlukan penunjukan langsung, beberapa akan mirip dengan yang ada dalam Undang-Undang Jasa Konstruksi. Begitu juga dengan pengadaan langsung yang hanya dapat dilakukan untuk paket dengan nilai tertentu.

10. Undang-Undang Nomor 3 Tahun 2014 tentang Perindustrian

Pada Pasal 5 Undang-Undang Perindustrian menyebutkan bahwa Presiden berwenang menyelenggarakan urusan pemerintahan di bidang Perindustrian. Dimana kewenangan tersebut dilaksanakan oleh Menteri dengan melakukan pengaturan, pembinaan dan pengembangan perindustrian. Pasal ini menggambarkan bahwa Presiden sebagai pemimpin dari otoritas Negara yang diberikan kewenangan dalam bidang perindustrian, dengan menyerahkan kewenangan seperti pengaturan, pembinaan dan pengembangan di bidang Perindustrian kepada Menteri terkait. Pada Keamanan Siber pun memiliki kesamaan, dimana Presiden dalam upaya melindungi Negara dari ancaman siber misalnya memiliki kewenangan dalam lingkup Keamanan Siber. Dengan penyerahan wewenang seperti pengaturan, pengadministrasian, pengoperasionalisasian,

penerapan keputusan atau kebijakan, dan pelaksanaan kegiatan lain kepada otoritas Negara di bawah Presiden yang berwenang dalam lingkup keamanan siber. Pihak yang ditunjuk memiliki kompetensi sebagai otoritas Negara dalam melaksanakan lingkup Keamanan Siber disini adalah Badan Siber dan Sandi Negara (BSSN).

Pasal 7 ayat (1) Undang-Undang Perindustrian, mengamanatkan Pemerintah, Pemerintah Daerah Provinsi, dan Pemerintah Daerah Kabupaten/Kota secara bersama-sama atau sesuai dengan kewenangan masing-masing menyelenggarakan urusan pemerintahan di bidang Perindustrian. Selain pada bidang perindustrian, keserupaan pengaturan seperti ini pun perlu muncul pada pengaturan tentang Keamanan Siber segala pihak terkait seperti BSSN, Pemerintah Daerah Provinsi, dan Pemerintah Daerah kebupaten/kota secara bersama-sama atau sesuai dengan kewenangan masing-masing menyelenggarakan Keamanan Siber.

11. Istilah Keamanan Nasional

Keamanan siber sebagai bentuk dari keamanan nasional dapat dikatakan sebagai hal yang mengancam kepentingan pemerintah maupun warga Negara yang perlu dilindungi dalam lingkup ruang siber. Hal ini membuat keamanan siber dengan keamanan nasional memiliki persamaan maksud, namun dengan arti yang berbeda. Keamanan nasional sendiri telah digunakan dalam beberapa peraturan perundang-undangan untuk menjelaskan maksud dari keamanan Negara terkait pada Negara Indonesia. Hal ini seperti yang ada dalam undang-undang:

a) Undang-Undang Nomor 7 Tahun 2011 tentang Perdagangan

Pasal 50 ayat (2) huruf a Undang-Undang Perdagangan menyatakan bahwa “pemerintah melarang Impor atau Ekspor barang untuk kepentingan nasional dengan alasan untuk melindungi keamanan nasional atau kepentingan umum, termasuk sosial, budaya, dan moral masyarakat”. Sedangkan

pada pasal 54 ayat (1) huruf a menyatakan bahwa "pemerintah dapat membatasi ekspor dan impor barang untuk kepentingan nasional dengan alasan untuk melindungi keamanan nasional atau kepentingan umum".

b) Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara

Dalam Undang-Undang Intelijen, istilah keamanan nasional paling banyak diungkapkan, yaitu terdapat dalam klausula menimbang yang menyatakan "bahwa untuk memberikan kepastian hukum dan sesuai dengan kebutuhan hukum dalam masyarakat, penyelenggaraan Intelijen Negara sebagai lini pertama dari sistem keamanan nasional perlu diatur secara lebih komprehensif". Selain itu terdapat juga dalam Pasal 3 Undang-Undang Intelijen menyatakan bahwa "hakikat intelijen Negara merupakan lini pertama dalam sistem keamanan nasional". Dalam pasal 31 huruf a, menyatakan bahwa "intelijen negara memiliki wewenang melakukan penyadapan, pemeriksaan aliran dana, dan penggalian informasi terhadap sasaran yang terkait dengan: kegiatan yang mengancam kepentingan dan keamanan nasional…"

Pasal 4 Undang-Undang Intelijen menyatakan bahwa "Intelijen Negara berperan melakukan upaya, pekerjaan, kegiatan, dan tindakan untuk deteksi dini dan peringatan dini dalam rangka pencegahan, penangkalan, dan penanggulangan terhadap setiap hakikat ancaman yang mungkin timbul dan mengancam kepentingan dan keamanan nasional". Keamanan nasional juga muncul pada tujuan dari Intelijen Negara dalam Pasal 5 Undang-Undang Intelijen Negara yang menyatakan "Tujuan Intelijen Negara adalah mendeteksi, mengidentifikasi, menilai, menganalisis, menafsirkan, dan menyajikan Intelijen dalam rangka memberikan peringatan dini untuk mengantisipasi berbagai kemungkinan bentuk dan sifat ancaman yang potensial dan nyata terhadap keselamatan dan

eksistensi bangsa dan negara serta peluang yang ada bagi kepentingan dan keamanan nasional".

c) Undang-Undang Nomor 21 Tahun 2013 tentang Keantariksaan

Dalam Undang-Undang Keantariksaan, Keamanan Nasional muncul dalam Pasal 35 huruf d yang menyatakan "Dalam melaksanakan kegiatan peluncuran Wahana Antariksa, Penyelenggara Keantariksaan wajib : menjamin bahwa peluncuran tidak akan menimbulkan kemungkinan gangguan terhadap keamanan nasional serta tidak akan menimbulkan pelanggaran terhadap kebijakan luar negeri dan kewajiban internasional". Keamanan nasional juga masuk dalam ketentuan pidana pada Undang-Undang Keantariksaan yaitu dalam pasal 95 ayat (2) yang berbunyi "Dalam hal perbuatan sebagaimana dimaksud pada ayat (1) mengakibatkan terganggunya kepentingan keamanan nasional atau kepentingan pemerintah, pelaku dipidana dengan pidana penjara paling lama 2 (dua) tahun atau denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah)".

Selain yang telah penulis sebutkan dari tiga ketentuan pada peraturan perundang-undangan diatas, masih banyak lagi ketentuan pada peraturan perundang-undangan lainnya yang menyebutkan tentang keamanan nasional. Maksud penulis menjabarkan tentang hal ini adalah bahwasannya istilah keamanan siber atau keamanan nasional bukanlah sesuatu yang unik, karena beberapa undang-undang lain juga menyebutkan istilah yang serupa. Sehingga penggunaan istilah Keamanan Siber pada Rancangan Undang-Undang ini adalah sesuai.

BAB IV
LANDASAN FILOSOFIS, SOSIOLOGIS, DAN YURIDIS

A. Landasan Filosofis

Sebuah undang-undang yang baik harus mengandung norma hukum yang diidealkan oleh masyarakat yang menuntun kepada cita-cita luhur kehidupan bermasyarakat dan bernegara. Cita-cita luhur dapat menjadi landasan filosofis yang muncul dalam suatu peraturan perundang-undangan. Landasan filosofis dapat dikatakan merupakan pandangan hidup bangsa Indonesia dalam berbangsa dan bernegara, alasan yang menggambarkan bahwa peraturan yang dibentuk mempertimbangkan pandangan hidup, kesadaran, dan cita hukum yang meliputi suasana kebatinan serta falsafah bangsa Indonesia. Hal ini memunculkan bahwa landasan filosofis yang ada dalam suatu peraturan perundang-undangan bersumber dari *rechtsidee* (cita hukum) bangsa Indonesia yaitu, Pancasila dan Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Pancasila sebagai cita hukum bangsa Indonesia merupakan konstruksi pikiran atau ide yang mengarahkan hukum kepada apa yang dicita-citakan bangsa. Gustav Radbruch menyatakan bahwa "*rechtsidee*" berfungsi sebagai dasar yang bersifat konstitutif bagi hukum positif, memberi makna bagi hukum. Gustav Radbruch juga mengajarkan bahwa hukum harus memuat tiga nilai dasar yaitu nilai keadilan yang terkait dengan aspek filosofis, nilai kepastian yang terkait dengan aspek yuridis, dan nilai kemanfaatan yang terkait dengan aspek sosiologis. Sehingga *Rechtsidee* menjadi tolak ukur yang bersifat regulatif, yaitu menguji apakah hukum positif adil atau tidak. Cita hukum akan mempengaruhi dan berfungsi sebagai asas umum yang memberikan pedoman (*guiding principle*), norma kritik (kaidah evaluasi), dan faktor yang memotivasi dalam

penyelenggaraan hukum (pembentukan, penemuan, penerapan hukum dan perilaku hukum).[104]

Kesesuaian konsep pengaturan keamanan siber dengan Pancasila dalam satu materi muatan pada Undang-Undang Keamanan Siber yang relevan dengan Sila Pertama, Sila Ketuhanan Yang Maha Esa adalah terkait dengan fungsi keamanan siber untuk mengantisipasi *cyber terror*, *cyber conflict*, dan/atau konten destruktif. Materi muatan tersebut selaras dengan nilai-nilai pada Sila Pertama Pancasila, karena tujuan dari materi muatan dari antisipasi adanya insiden siber adalah untuk melindungi bangsa dan negara Indonesia dari tindakan para *cyber terrorist*, *cyber anarchist*, dan *cyber vandalist* yang tidak mengedepankan moral agama dalam perbuatannya, yang tidak mengindahkan kerukunan hidup bermasyarakat, dan yang menempuh cara-cara kekerasan dan pemaksaan keyakinan keagamaannya kepada orang lain.

Pada Sila Kedua Pancasila, salah satu materi muatan dalam Undang-Undang Keamanan Siber yang relevan dengan Sila Kemanusiaan yang Adil dan Beradab adalah terkait dengan diplomasi siber. Pentingnya aturan tersebut dikarenakan salah satu ancaman paling serius dalam ranah siber adalah adanya prospek perang siber antar negara atau berkembangnya suatu insiden siber menjadi perang konvensional. Oleh karena itu, materi muatan tersebut selaras dengan nilai-nilai pada Sila Kedua Pancasila, karena aturan diplomasi siber mencerminkan kesadaran bahwa bangsa Indonesia senantiasa hormat-menghormati dan bekerjasama dengan bangsa lain dalam rangka memelihara keamanan siber Internasional.

Materi muatan dalam Undang-Undang Keamanan Siber yang relevan dengan Sila Ketiga Pancasila, yaitu Persatuan Indonesia adalah terkait dengan pelaksanaan fungsi keamanan siber yang bersifat kolaboratif antara penyelenggara keamanan siber di sektor pemerintahan dan di sektor swasta. Materi muatan tersebut selaras

[104] FX. Adji Samekto, Hukum dalam Lintasan Sejarah, Indepth Publishing: Bandar Lampung, 2013, hlm. 48

dengan nilai-nilai pada Sila Ketiga Pancasila, karena mendorong segenap bangsa Indonesia untuk saling bergotong-royong, rela berkorban, dan bangga dengan potensi dan hasil karyanya, dalam melindungi keamanan siber Indonesia, dengan mengutamakan persatuan, kesatuan, kepentingan, dan keselamatan bangsa negara di atas kepentingan pribadi atau golongan.

Sesuai dengan Sila Keempat Pancasila materi muatan dalam Undang-Undang Keamanan Siber yang relevan dengan Sila Kerakyatan yang Dipimpin oleh Hikmat Kebijaksanaan dalam Permusyawaratan/Perwakilan adalah terkait dengan kolaborasi penyelenggara keamanan siber yang dilakukan antara Pemerintah dengan swasta. Muatan yang ada tentang kolaborasi pihak pemerintah maupun swasta dapat mendorong dan memberikan penghormatan terhadap aspirasi dan kepentingan orang perorangan maupun korporasi dalam pembentukan kebijakan di bidang keamanan siber, serta menciptakan peran publik secara bertanggung jawab. Hal ini menjadi selaras dengan nilai-nilai pada Sila Keempat Pancasila itu sendiri.

Terakhir kesesuaian Sila Kelima Pancasila dalam materi muatan Undang-Undang Keamanan Siber yang relevan dengan Sila Keadilan Sosial bagi Seluruh Rakyat Indonesia adalah terkait dengan *Cyber Security Operation Center* serta penyidikan dan penindakan. Materi muatan ini menjadi selaras dengan nilai-nilai pada Sila Kelima Pancasila, karena dengan adanya tatanan yang jelas dalam pelayanan keamanan siber misalnya pada *Cyber Security Operation Center*, diharapkan akan mendorong pengembangan usaha bersama dengan semangat tolong menolong dalam menanggulangi insiden/serangan siber dan/atau memasyarakatkan *digital signature*, yang untuk selanjutnya akan menciptakan kemandirian perekonomian dan kemajuan kesejahteraan yang berkeadilan. Sedangkan penyidikan dan penindakan menjadi penting agar kegiatan dalam lingkup siber yang memboroskan sumber daya dan

merugikan kesejahteraan umum dapat dicegah, diminimalkan, atau dijatuhi sanksi.

Kedaulatan Negara membuat Negara memiliki kewenangan untuk mengatur kehidupan berbangsa dan bernegara. Kewenangan Negara dalam mengatur kehidupan berbangsa dan bernegara tersebut dilakukan untuk mencapai tujuan-tujuan Negara. Tujuan Negara Indonesia sesuai dengan yang tercantum dalam Pembukaan UUD 1945, tujuan nasional Negara Indonesia yaitu seperti melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial.

Berdasarkan kesesuaian konsep dari pengaturan keamanan siber dengan Pancasila sebagai dasar konstitusi Negara. Konsep pengaturan dari keamanan siber perlu juga sesuai dengan tujuan nasional Negara Indonesia yang ada dalam Pembukaan UUD 1945. Maka dalam pengaturan keamanan siber ini, kesesuaian Undang-Undang Keamanan Siber dengan landasan filosofis cita hukum bangsa Indonesia adalah sebagai berikut:

1. bahwa untuk mewujudkan tujuan nasional sebagaimana diamanatkan dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, aneka upaya multi sektoral untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia, perlu diberikan pengamanan dari berbagai bahaya akibat penyalahgunaan sarana dan prasarana atau sumber daya siber;
2. bahwa segenap potensi sumber daya siber nasional untuk melakukan pengamanan terhadap kepentingan siber Indonesia, baik yang berada di sektor pemerintahan maupun yang berada di sektor swasta, perlu disinergikan dan diberikan peran yang

proporsional agar menjadi satu kesatuan komponen keamanan nasional yang padu dan senantiasa siap siaga;

3. bahwa penyeleggaraan pengamanan di bidang siber perlu disusun dalam suatu undang-undang agar pelaksanaan kekuasaan pemerintahan selaras dengan kepentingan perlindungan hak asasi manusia, kepentingan inovasi ilmu pengetahuan dan teknologi, serta kepentingan pemajuan perekonomian nasional;

B. Landasan Sosiologis

Pada dasarnya sistem hukum nasional merupakan refleksi dari dinamika masyarakat Indonesia. Perumusan ketentuan hukum tidak akan lepas dari nilai-nilai luhur bangsa, sehingga keberlakuan hukum akan diukur dari validitas dan efektifitasnya secara sosiologis. Hukum yang efektif dan valid harus dirancang sesuai norma yang hidup dalam masyarakat. Landasan sosiologis dalam suatu peraturan perundang-undangan dapat dikatakan merupakan pertimbangan atau alasan yang menggambarkan bahwa peraturan yang dibentuk, bertujuan untuk memenuhi kebutuhan masyarakat dalam berbagai aspek. Landasan sosiologis sesungguhnya menyangkut fakta empiris mengenai perkembangan masalah yang ada dan kebutuhan masyarakat serta Negara dalam mengatasi masalah tersebut.

Pada bagian sebelumnya kita ketahui bahwa pesatnya perkembangan teknologi informasi dan telekomunikasi yang memunculkan melahirkan ruang siber yang bersifat global dan dapat dikatakan tanpa batas (borderless). Kondisi tersebut berpotensi menimbulkan masalah-masalah yang dapat mengancam kedaulatan, keamanan dan menganggu stabilitas nasional dalam hal adanya ancaman serangan siber. Dampak-dampak yang dapat dirasakan tidak hanya merugikan perorangan, namun dalam lingkup yang lebih luas masyarakat secara keseluruhan bahkan kehidupan sosial, ekonomi, politik, dan hubungan internasional bagi Negara. Sehingga

keamanan siber merupakan hal genting dan penting yang dirasakan urgensinya dalam kehidupan sehari-hari masyarakat Indonesia.

Pemanfaatan ruang siber atau internet oleh masyarakat Indonesia yang telah menyebar dalam berbagai aspek kehidupan. Jumlah pengguna internet di Indonesia pada tahun 2017 yang telah sampai pada 54,68% dari total jumlah penduduk Indonesia, menunjukan bahwa seluruh lapisan masyarakat dalam seluruh wilayah Indonesia telah menikmati dan memanfaatkan perkembangan teknologi informasi dalam ruang siber (internet) yang dipergunakan untuk kehidupan sehari-hari tanpa terkecuali. [105] Penggunaan internet akan menjadi pedang bermata dua bila tidak diregulasi dengan baik. Ruang siber dapat menjadi sumber berbagai potensi kejahatan dari ancaman, kerentanan, dan ketidakamanan.[106]

Berbagai kejahatan siber yang mampu menjadi ancaman terutama dari kerentanan ruang siber dapat terjadi. Potensi kejahatan siber yang ada misalnya saja seperti penipuan komputer, pencurian uang atau harta benda dengan menggunakan sarana komputer/siber dengan melawan hukum, memasukan instruksi yang tidak sah pada sistem, perubahan data input, perusakan data, menggunakan ruang siber sebagai sarana pendukung pelanggaran keamanan siber, *hacking*, penggelapan, pemalsuan pemberian informasi melalui sistem komputer, *eavesdropping* (menguping), *masquerabe* (menyamar), *misrouting* (kesalahan penyampaian), serangan *denial of service* (dos). Selain itu yang kini banyak terjadi adalah serangan kejahatan siber dengan menggunakan malware (*malicious software*) yaitu sebuah program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer.

Berdasarkan *Indonesia Cyber Security Report* 2018 oleh ID-SIRTII, total serangan siber tahun 2017 mencapai 205,5 juta serangan, meningkat 66%. Dimana tahun 2017 lalu juga terjadi

---

[105] APJII, Infografis Penetrasi & Perilaku Pengguna Internet Indonesia, Hasil Survey 2017, 2017

[106] Nazli Choucri dan David Clark, Cyberspace and International Relations; Toward an Integrated System (Massachusettes: MIT press. 2011) hlm. 2

situasi kritis serangan *Wannacry Ransomware.*[107] Di tahun 2016 terjadi peningkatan jumlah serangan di bidang usaha yang cukup signifikan dibanding tahun sebelumnya. Selama enam bulan pertama tahun 2017, perusahaan menyumbang 42% dari total infeksi serangan *ransomware,* naik 30% dari tahun 2016 dan 29% dari tahun 2015. Peningkatan jumlah serangan siber yang utama diakibatkan oleh *WannaCry* dan *Petya*. Serangan siber oleh Stuxnet pada infrastruktur nuklir Iran yang dapat dikatakan sebagai senjata siber untuk melumpuhkan sistem siber target, efeknya telah menyebar ke Indonesia.[108] Seperti yang dilansir oleh Symantec produsen Antivirus, Indonesia berada di urutan kedua setelah Iran di antara 10 negara yang mengalami serangan siber Stuxnet. Dengan adanya hal tersebut membuat komputer-komputer di Indonesia terindikasi terjangkit virus Stuxnet ini.[109]

Fakta secara lebih rinci yang diungkapkan oleh ID-SIRTII, serangan siber di Indonesia pada tahun 2016 berjumlah 135.672.984, hal ini meningkat dari tahun 2015 yang hanya berjumlah 28.430.843. Pada tahun 2016 tersebut presentasi serangan siber paling banyak dilakukan dengan malware yaitu sebesar 47%, selanjutnya 44% merupakan kasus penipuan pada ruang siber, dan sisanya berbentuk kejahatan siber lainnya, seperti website *defacement*, dan aktivitas manipulasi data dan kebocoran data.[110] Pada tahun 2017, dilihat dari hasil pemantauan trafik anomali nasional dari Januari sampai November 2017, tercatat oleh Id-SIRTII/CC ada sebanyak 205.502.159 serangan. Total dari seluruh aktivitas malware yang terdeteksi, sebanyak 37,72% berkaitan dengan serangan DOS, 20,93% merupakan *exploit*, 18%

---

[107] Viska, Sesditjen Aptika Tegaskan Keamanan Siber jadi Isu Penting, https://kominfo.go.id/content/detail/12503/sesditjen-aptika-tegaskan-keamanan-siber-jadi-isu-penting/0/berita_satker diakses pada 23 Agustus 2018

[108] John P. Farwell and Rafal Rohozinski, Stuxnet and the Future of Cyber War, hlm. 23

[109] Symantec, W32.Stuxnet, https://www.symantec.com/security-center/writeup/2010-071400-3123-99 diakses pada 23 Agustus 2018

[110] ID-SIRTII., Tren Serangan Siber Nasional 2016 dan Prediksi 2017, ID-SIRTII., 2017

adalah trojan atau berkaitan dengan aktivitas trojan, 15% tercatat sebagai *bad unknown* dan sisanya tercatat sebagai *adware, shell code, cnc, misc attack, network scan,* dan *web application attack.*[111]

Berdasarkan penelitian yang dilakukan oleh Daka advisory, Indonesia menderita kerugian ekonomi dari kejahatan siber yang sebenarnya sebesar USD 43 miliar, lalu kejahatan siber transisional sebesar USD 582 miliar, kejahatan siber pada infrastruktur yang ada sebesar USD 310 miliar, dan kejahatan tradisional yang cenderung menjadi siber sebesar USD 2,478 miliar.[112] Selanjutnya berdasarkan data dari Norton Symantec selama tahun 2015 sampai dengan Februari 2016, kejahatan online di Indonesia menimbulkan total kerugian Rp 194.6 miliar.[113] Pada tahun 2017 menurut data yang dikeluarkan juga oleh Norton Symantec, kerugian yang diderita Indonesia sebesar USD 3,2 billion.[114] Terakhir potensi kerugian ekonomi akibat dari insiden keamanan siber tahun 2018 menurut hasil penelitian Frost dan Sullivan yang diprakarsai oleh Microsoft, akan mencapai nilai sebesar USD 34,2 miliar.[115]

Ancaman tambahan pada era yang ada sekarang ini mendorong potensi perang antar Negara tidak lagi menggunakan cara perang tradisional dan konvensional. Bentuk dari peperangan pun berubah yang menimbulkan ancaman baru pada ruang siber yang dapat mengancam pertahanan, keamanan dan kedaualatan negara.[116]

---

[111] Agus Tri Haryanto, Indonesia dibombardir 205 Juta Serangan Cyber, https://inet.detik.com/security/d-3781096/indonesia-dibombardir-205-juta-serangan-cyber diakses pada 23 Agustus 2018

[112] *Ibid.*

[113] Norton Symantec, 2016 Norton Cyber Security Insights Report Global Result, Symantec Corporation, 2017, lihat juga Maulia Jayantina Islami, Tantangan dalam Implementasi Startegi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index, Jurnal Masyarakat Telematika dan Informasi, Volume: 8 No. 2, 2017, hlm. 138

[114] Norton Symantec, 2017 Norton Cyber Security Insights Report Global Result, Symantec Corporation, 2018, hlm. 13

[115] Wilfridus Setu Embu, Insiden Keamanan Siber Bisa Picu Kerugian Indonesia hingga Rp 483 Triliun, https://www.merdeka.com/uang/insiden-keamanan-siber-bisa-picu-kerugian-indonesia-hingga-rp-483-miliar.html diakses pada 23 Agustus 2018

[116] Ineu Rahmawati, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense, Jurnal Pertahanan & Bela Negara, Vol. 7 No. 2, 2017, hlm. 52

Siber menjadi ancaman bagi Negara disebabkan ruang lingkupnya yang dapat dimanfaatkan untuk mencuri informasi, penyebaran ide yang bersifat destruktif, maupun serangan terhadap sistem informasi di berbagai bidang, seperti data perbankan, jaringan militer, bahkan sistem pertahanan Negara.[117] Isu siber menjadi bahasan di level *high politic* setelah terdapat kejadian seperti serangan siber di Georgia dan Estonia, serta penggunaan serangan berbasis siber pada sistem nuklir Iran. Hal ini menunjukan bahwa ancaman kenegaraan yang berevolusi menjadi serangan siber bukan sekedar konsep saja.[118]

Hal yang mengkhawatirkan adalah serangan siber di Indonesia belum ditangani secara menyeluruh salah satunya karena belum ditangani secara terintegrasi di antara kelembagaan yang ada. Kerawanan demikian tercermin dalam dokumen *Global Cyber Security Index 2017* yang diterbitkan oleh ITU D, Indonesia Indonesia mendapatkan nilai 0.424 pada peringkat 70 dan masih berada pada mature stage, yang berarti belum termasuk dalam jajaran Negara-negara yang dianggap memiliki komitmen tinggi terhadap keamanan siber, atau dalam tahap persiapan pengembangan komitmen dan terlibat dalam program serta inisiatif keamanan siber. Hal ini sangat jauh tertinggal dengan Singapura yang memimpin di peringat pertama dengan nilai 0.925 dan Malaysia di peringkat ketiga dengan nilai 0.893. [119]

Peretasan menjadi ancaman terhadap keamanan siber di Indonesia. Peretas mampu membobol secara otodidak berbagai sistem dan situs. Kemampuan meretas dipelajari dari berbagai komunitas peretas yang mempunyai kelompok diskusi di dunia maya. Misalnya, kasus anggota *Surabaya Black Hat (SBH*) yang ditangkap polisi Maret 2018 karena meretas 3000 sistem elektronik dan situs di 44 negara, dimaksudkan untuk sekedar menunjukkan kelemahan pada sistem.

---

[117] Michael Smith, "Research Handbook on International Law and Cyberspace", (Massachusetts: Edwar Elgar Publishing Limited, 2015), hlm. 1-3

[118] Nazli Choucri dan David Clark, Cyberspace and International Relations; Toward an Integrated System

[119] International Telecommunication Union (ITU), Global Cybersecurity Index (GCI) 2017, Geneva, 2017

Pihak dimaksud mengaku tidak pernah meminta uang dalam jumlah tertentu, tetapi ada pemilik sistem yang membayarnya.[120] Kemajuan teknologi seringkali tidak diimbangi dengan regulasi yang memadai dan sistem yang kuat. Hal yang demikian membuat peretasan bisa menimbulkan efek sangat besar bagi negara, tidak saja kerugian sosial dan kerugian ekonomi yang dialami, akan tetapi juga ancaman bagi kedaulatan negara, baik infiltrasi dari dalam negeri maupun kekuatan yang berasal dari luar negeri.

Penggunaan ruang siber yang telah dimanfaatkan dalam berbagai bidang dapat berpotensi buruk pada penyalahgunaan yang dilakukan oleh pihak yang tidak bertanggungjawab. Hal ini dapat menyebabkan kerugian baik secara perorangan, pada sektor swasta (bisnis), dan terlebih kepada pertahanan dan keamanan Negara atau keamanan nasional. Sehingga dengan adanya fakta-fakta baik yang terjadi secara nasional maupun internasional, jelaslah bahwa keamanan siber menimbulkan masalah yang perlu diselesaikan dan kebutuhan masyarakat untuk mendapatkan pengaturan yang jelas dalam bentuk undang-undang.

C. Landasan Yuridis

Landasan yuridis pada peraturan perundang-undangan dapat dikatakan merupakan pertimbangan atau alasan yang menggambarkan bahwa peraturan yang dibentuk dapat mengatasi permasalahan hukum atau mengisi kekosongan hukum dengan mempertimbangkan peraturan-peraturan yang telah ada, yang akan diubah atau yang akan dicabut guna menjamin kepastian hukum dan rasa keadilan masyarakat. Landasan yuridis menyangkut persoalan hukum yang berkaitan dengan substansi atau materi yang diatur sehingga dibentuk peraturan perundang-undangan yang baru. Persoalan hukum yang ada misalnya seperti peraturan yang ada sudah ketinggalan, peraturan yang tidak harmonis atau tumpang

[120] Wisnu Aji Dewabrata, Peretas di 44 Negara Belajar Otodidak, https://kompas.id/baca/utama/2018/03/16/peretas-di-44-negara-belajar-otodidak/ diakses pada 24 Agustus 2018

tindih, jenis peraturan yang lebih rendah dari Undang-Undang sehingga daya berlakunya lemah, peraturan sudah ada tapi tidak memadai, atau peraturan memang belum ada. Sehingga landasan yuridis akan digunakan sebagai dasar hukum dalam peraturan perundang-undangan yang akan disusun.

Amanat konstitusi Negara Kesatuan Republik Indonesia pada pembukaan Undang-Undang Dasar Tahun 1945 menyatakan bahwa 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. Secara singkat dapat disimpulkan bahwa tujuan nasional Indonesia pada dasarnya menekan untuk mengelola kesejahteraan masyarakat dan menjaga pertahanan serta keamanan Negara merupakan cita yang saling ketergantungan.

Perlu adanya tindakan tegas terhadap segala bentuk ancaman yang mengganggu keamanan warga Negara terlebih kedaulatan Negara termasuk pada ancaman siber dan serangan siber, sehingga berujung pada perlunya perhatian lebih pada keamanan siber. Sinergi antara pertahanan dan keamanan Negara serta kesejahteraan nasional diharapkan akan mewujudkan ketahanan nasional yang kuat. Apabila hal tersebut dapat diwujudkan dan dilindungi maka cita-cita Negara dan pemerintah untuk menjaga pertahanan dan keamanan Negara serta memajukan kesejahteraan umum untuk mencapai keadilan sosial dapat tercapai.

Amandemen keempat Undang-Undang Dasar Negara Kesatuan Republik Indonesia tahun 1945 yang ditetapkan oleh MPR pada tanggal 10 Agustus 2002 merupakan landasan yuridis bagi pembentukan peraturan perundang-undangan yang ada di Indonesia. Pasal 30 UUD NKRI tahun 1945 menyatakan bahwa tiap-tiap warga Negara berhak dan wajib ikut serta dalam usaha pertahanan dan keamanan Negara. Maka dari itu keamanan siber sebagai bagian dari pertahanan dan keamanan Negara tidak hanya

menjadi hak dan kewajiban aparat Negara saja namun seluruh warga Negara. Sehingga sudah menjadi suatu kewajiban bahwa seluruh rakyat dalam hal ini aktor-aktor pada berbagai sektor kehidupan di Indonesia untuk ikut serta berperan dalam mendukung mengenai keamanan siber dengan disesuaikan pada status dan kondisi masing-masing pihak. Pada Pasal 30 ayat (5) UUD NKRI tahun 1945 juga menyatakan bahwa segala hal terkait dengan pertahanan dan keamanan Negara diatur dengan undang-undang. Pada landasan yuridis ini, sesuai dengan dasar hukum tersebut maka keamanan siber yang merupakan aspek bagian dari pertahanan dan keamanan Negara wajib diatur dalam bentuk undang-undang.

Selain itu dalam Pasal 20 UUD NKRI tahun 1945 menyatakan Dewan Perwakilan Rakyat memiliki fungsi legislasi memegang kekuasaan membentuk undang-undang. Setiap rancangan undang-undang dibahas Dewan Perwakilan Rakyat dan Presiden untuk mendapat persetujuan bersama. Presiden mengesahkan rancangan undang-undang yang telah disetujui bersama untuk menjadi undang-undang. Selain itu Pasal 21 UUD 1945 juga memberikan kepada anggota Dewan Perwakilan Rakyat berhak mengajukan usul rancangan undang-undang.

Terkait dengan landasan yuridis dalam undang-undangan keamanan siber, sesuai dengan ketentuan yang ada dalam Pasal 10 Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan, materi muatan yang harus diatur dalam undang-undang berisi mengenai, pengaturan lebih lanjut mengenai ketentuan UUD 1945, perintah suatu undang-undang untuk diatur dengan undang-undang, pengesahan perjanjian internasional tertentu, tindak lanjut atas putusan Mahkamah Konstitusi, serta pemenuhan kebutuhan hukum dalam masyarakat. Peratuan perundang-undangan ini digunakan sebagai acuan dalam pembuatan suatu peraturan perundang-undangan lainnya.

Ketentuan yang ada tersebut menjadi suatu kesesuaian bahwa dalam undang-undang keamanan siber materi muatan yang

terkandung berisi mengenai ketentuan lebih lanjut dari UUD 1945 yaitu dalam Pasal 30 UUD 1945 yang menyatakan bahwa segala hal yang terkait dengan pertahanan dan keamanan Negara diatur dengan undang-undang. Amanat lain mengenai materi muatan isi dari sebuah undang-undang adalah bahwa undang-undang keamanan siber dirasakan urgensinya dalam pemenuhan kebutuhan hukum untuk masyarakat. Atas segala pemanfaatan ruang siber atau internet yang telah menyetuh berbagai aspek kehidupan masyarakat termasuk pada infrastruktur kritis dan berbagai potensi ancaman kejahatan siber yang mampu memberikan dampak yang begitu luas pada masyarakat dan Negara Indonesia, maka kebutuhan dalam membuat undang-undang keamanan siber menjadi penting untuk dilaksanakan.

Saat ini pengaturan yang berkaitan dengan keamanan siber belum secara khusus diatur dan masih tersebar pada beberapa peraturan perundangan-undangan yang masih bersifat sektoral dan parsial. Hal ini seperti yang telah dijabarkan pada bab sebelumnya, materi muatan pengaturan keamanan siber tersebar dalam beberapa peraturan perundangan-undangan seperti:

1) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
2) Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia
3) Undang-Undang Nomor 3 Tahun 2002 tentang Pertahan Negara
4) Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia
5) Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara
6) Undang-Undang Nomor 3 Tahun 2014 tentang Perindustrian
7) Undang-Undang Nomor Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik

Dapat dikatakan bahwa pengaturan yang ada tentang keamanan siber di Indonesia masih belum komprehensif atau bahkan undang-undang yang bersifat mengatur upaya keamanan

siber yang mengaitkan antara pihak-pihak yang perlu memiliki tanggung jawab dalam berbagai upaya dari keamanan siber seperti pemerintah, masyarakat serta pihak swasta masih belum ada. Suatu peraturan yang berisi menyangkut hak dan kewajiban pemerintah, individu, pihak swasta, dan masyarakat dalam kaitannya dengan keamanan siber, aturan pencegahan dan penindakan terhadap penyalahgunaan pemanfaatan siber, serta tata hubungan dan koordinasi antara lembaga-lembaga pemerintah yang terkait, belum diatur secara jelas dan kuat secara hierarki.

Tersebarnya berbagai fungsi siber di beberapa lembaga pemerintah tentunya memerlukan sebuah lembaga yang mampu untuk mengoordinasikan berbagai fungsi siber pada beberapa lembaga pemerintahan. Selain lembaga pemerintahan, konsep baru yang ada pada dunia internasional kini menyatakan perlu terdapatnya kolaborasi antara pemerintah sebagai koordinator serta supervisor dan pihak swasta yang juga ikut memberikan upaya keamanan siber pada infrastruktur yang dimilikinya.

Saat ini kewenangan dalam melaksanakan tugas dan fungsi keamanan siber diberikan kepada Badan Siber dan Sandi Negara (BSSN). Kedudukan BSSN hanya diatur melalui Peraturan Presiden, hal ini tentu kurang kuat dibandingkan dengan lembaga pemerintah yang dibentuk melalui undang-undang. Oleh karena itu dibutuhkan pengaturan secara khusus di dalam undang-undang bagi BSSN dalam menjalankan tugas dan fungsi sebagai koordinator pada khususnya dan keamanan siber di Indonesia pada umumnya.

Tugas BSSN yang sangat bersinggungan dengan kementerian dan lembaga negara lain, misalnya dengan Kementerian Komunikasi dan Informatika dalam penapisan konten negatif ataupun destruktif pada internet dengan mesin sensor. Belum lagi, memburu kejahatan siber (*cyber crime*) yang sudah dilakukan oleh unit *cyber crimes* Mabes Polri. Selain itu dari sisi pertahanan, BSSN akan bersinggungan dengan Kementerian Pertahanan yang sudah memiliki *cyber operation center* (COC). Adanya tugas penanganan insiden

keamanan siber dan diplomasi siber yang dilakukan oleh Kementerian Luar Negeri, penanganan *fraud e-commerce* oleh Kementerian Perindustrian, Kementerian Perdagangan, dan Kemenkominfo; penanggulangan teroris oleh BNPT, operasi intelijen pada ruang siber oleh BIN, kejahatan keuangan dan ekonomi digital oleh PPATK dan KPK. Belum lagi pengamanan infrastruktur kritis yang kini hampir banyak dimiliki oleh pihak swasta.

Keadaan ini membuat BSSN sangat sulit bekerja apabila tugas, fungsi, dan wewenangnya diatur di dalam Peraturan Presiden. Mengingat dalam menjalankan tugas, fungsi dan wewenanganya tersebut, BSSN harus mengkoordinasikan berbagai kementerian dan lembaga negara yang pembentukannya melalui undang-undang. Ditambah lagi perlu adanya kolaborasi antara negara dengan pihak swasta dalam menciptakan iklim yang aman dan nyaman kepada masyarakat pada lingkup keamanan siber. Maka dirasakan Materi dalam Peraturan Presiden tentang BSSN dapat diangkat menjadi materi dalam undang-undang, hal ini dilakukan agar BSSN dapat dengan leluasa melakukan koordinasi dengan kementerian dan lembaga negara serta pihak swasta dalam upaya terkait dengan keamanan siber.

Belum adanya undang-undang yang secara khusus mengatur mengenai keamanan siber dan peraturan perundang-undangan yang ada saat ini masih belum dapat menjawab kebutuhan permasalahan tentang keamanan siber di Indonesia. Oleh karenanya perlu dibentuk undang-undang yang secara khusus lebih komprehensif, tegas dan jelas terkait dengan keamanan siber. Berdasarkan ketiga landasan yang telah dijabarkan baik secara filosofis, sosiologis dan yuridis yang memiliki kesesuaian antara muatan ketentuan pada undang-undang keamanan siber dengan kebutuhan hukum negara Indonesia. Hal ini menunjukan bahwa usulan pengaturan keamanan siber dalam bentuk undang-undang akan efektif dalam sistem hukum nasional. Muatan ketentuan Undang-undang Keamanan Siber dapat bertujuan pada terpenuhinya kebutuhan masyarakat atas sistem hukum

nasional yang baik pada bidang keamanan siber yang menjamin hak, kewajiban dan wewenang yang jelas terhadap para pihak yang terkait. Sehingga pada akhirnya keamanan siber dapat melindungi segala kebutuhan dan kepentingan pihak yang terkait, masyarakat dan negara Indonesia.

BAB V
JANGKAUAN, ARAH PENGATURAN, RUANG LINGKUP MATERI PENGATURAN

A. Sasaran

Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa tujuan Negara adalah melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia. Oleh karena itu dalam lingkup Keamanan Siber atas dasar segala permasalahan yang muncul pada pemanfaatan Siber, perlu upaya-upaya perlindungan Keamanan Siber dengan sasaran seperti:

a) Melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dari bahaya siber.
b) Memajukan kesejahteraan umum dengan mendukung segenap upaya pengembangan perekonomian digital pada aspek pengamanan sarana dan prasarana, dan sumber daya siber nasional.
c) Mencerdaskan kehidupan bangsa melalui pemanfaat siber yang bebas, terbuka, dan bertanggung jawab.
d) Ikut melaksanakan ketertiban dunia dengan berperan bebas aktif di tingkat trans-nasional untuk mengantisipasi bahaya siber yang mengancam perdamaian dunia.

Kesesuaian sasaran dari RUU Keamanan dan Ketahanan Siber dengan tujuan Negara Indonesia seperti yang tercantum dalam Pembukaan Undang-Undang Dasar 1945 kami rasakan menjadi suatu keharusan. Kesesuaian tersebut menunjukan RUU Keamanan dan Ketahanan Siber digali dari nilai-nilai, kebutuhan dan tujuan Negara Indonesia. Sehingga sasaran dari RUU Keamanan dan Ketahanan Siber yang ada tersebut secara tidak

langsung menjadi tujuan dari diselenggarakannya Keamanan Siber di Indonesia.

B. Jangkauan dan Arah Pengaturan

Sejalan dengan sasaran yang akan dituju dari RUU Keamanan dan Ketahanan Siber diatas, arah pengaturan yang terkandung dalam RUU Keamanan dan Ketahanan Siber meliputi ketentuan mengenai penyelengaraan Keamanan Siber Indonesia yang merupakan kolaborasi antara Penyelenggara Keamanan Siber Pemerintah dengan Orang yang dibina dan dikonsolidasi secara efektif dan efisien. Penyelenggaraan Keamanan Siber dilakukan meliputi tata kelola Keamanan Siber yang berupa pendeteksian dan pengidentifikasian ancaman siber dan/atau serangan siber, pemproteksian dari ancaman siber dan/atau serangan siber, penanggulangan dan pemulihan insiden siber dan/atau serangan siber, serta pemantauan dan pengendalian ekosistem Keamanan Siber. Penyelenggaraan Keamanan Siber dapat juga dilakukan dengan diplomasi Keamanan Siber. Ditambah lagi dengan pelayanan Keamanan Siber dengan membentuk Pusat Operasi Keamanan Siber, Pembudayaan Keamanan Siber, dan Sertifikasi Elektronik. Penyelenggaraan Keamanan Siber juga dilakukan dengan penegakan hukum yang berupa dukungan penegakan hukum pidana, penapisan konten, dan penindakan.

Dalam melakukan penyelenggaraan Keamanan Siber, perlu otoritas kenegaraan yang berwenang sebagai *focal point* dalam penyelenggaraan Keamanan Siber. Pihak yang ditunjuk mampu dalam melaksanakan hal-hal tersebut adalah Badan Siber dan Sandi Negara yang perlu ditegaskan kedudukan, tugas dan fungsi, wewenang, dan struktur organisasinya. Selain itu terdapat juga pengaturan mengenai sanksi administratif serta ketentuan pidana dari pelanggaran dan kejahatan yang berpotensi terjadi pada lingkup Keamanan Siber.

C. Ruang lingkup materi muatan Undang-Undang

Lingkup Rancangan Undang-Undang atau pengaturan ini akan mengatur mengenai seluruh hal ataupun aspek yang terkait dengan Keamanan Siber. Hal tersebut akan meliputi penyelenggaraan Keamanan Siber, tata kelola Keamanan Siber, pelayanan Keamanan Siber, diplomasi Keamanan Siber, penegakan hukum, dan Badan Siber dan Sandi Negara.

a) Ketentuan Umum

Ketentuan umum berisikan tentang pengertian atau definisi, singkatan atau akronim yang dituangkan dalam batasan pengertian atau definisi, dan/atau hal-hal lain yang bersifat umum yang berlaku bagi pasa atau beberapa pasal berikutnya antara lain ketentuan yang mencerminkan asas, maksud, dan tujuan tanpa dirumuskan tersendiri dalam pasa atau bab. Beberapa istilah beserta batasan pengertian atau definisi yang perlu diakomodasi dalam rancangan Undang-Undang ini, antara lain yaitu:

1. Siber adalah ruang yang bersifat global dan mewadahi aneka ragam kepentingan yang dibentuk dari interaksi antara manusia dengan teknologi informasi, komputerisasi, jaringan komputer, kriptografi, dan/atau kecerdasan buatan.
2. Keamanan dan Ketahanan Siber adalah kondisi dinamis Siber yang meliputi seluruh aspek kehidupan nasional yang terintegrasi, aman, dan tangguh serta mampu mengembangkan kekuatan Siber Indonesia dalam menghadapi segala ancaman Siber terhadap kepentingan Siber Indonesia dan sumber daya yang dikuasai oleh Negara Kesatuan Republik Indonesia.
3. Kepentingan Siber Indonesia adalah keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan kepentingan nasional di berbagai

aspek, baik ideologi, politik, ekonomi, sosial budaya, maupun pertahanan dan keamanan, di ruang Siber.

4. Ancaman Siber adalah segala upaya, kegiatan, dan/atau tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat melemahkan, merugikan, dan/atau menghancurkan Kepentingan Siber Indonesia.
5. Insiden Siber adalah Ancaman Siber yang mengakibatkan sistem elektronik Siber tidak berfungsi sebagaimana mestinya.
6. Serangan Siber adalah Ancaman Siber yang mengakibatkan objek pengamanan Siber menjadi tidak berfungsi, sebagian atau seluruhnya, dan/atau bersifat sementara atau permanen.
7. Objek Pengamanan Siber adalah data, informasi, sarana dan prasarana, serta sumber daya manusia yang mendapat pelindungan dari penyelenggara Keamanan dan Ketahanan Siber.
8. Perimeter Keamanan adalah area dalam lingkup Siber dan non-Siber yang hanya dapat diakses oleh orang yang memiliki izin akses Keamanan dan Ketahanan Siber.
9. Deteksi adalah upaya mengetahui keberadaan, ukuran, dan jarak Ancaman Siber dari Perimeter Keamanan.
10. Identifikasi adalah upaya mengenali dan menganalisis tingkat kebahayaan, penyebab, dan dampak dari suatu Ancaman Siber yang telah dideteksi.
11. Proteksi adalah upaya melindungi Objek Pengamanan Siber dari Ancaman Siber agar kegunaan Objek Pengamanan Siber tidak rusak atau hilang, sebagian atau seluruhnya.
12. Penanggulangan adalah upaya mengatasi, menghilangkan, meminimalisasi dampak, dan/atau mencegah memburuknya dampak dari suatu Insiden Siber atau Serangan Siber yang telah terjadi.

13. Pemulihan adalah upaya memperbaiki dampak buruk atau memulihkan kerugian akibat Insiden Siber atau Serangan Siber dan mengembalikan fungsionalitas Objek Pengamanan Siber.
14. Pemantauan adalah upaya untuk memahami dinamika dan tren yang terkait dengan Insiden Siber atau Serangan Siber dalam rangka merumuskan strategi dan taktik yang efektif dan efisien dalam lingkup Keamanan dan Ketahanan Siber.
15. Pengendalian adalah upaya memelihara dan memperkuat ekosistem Keamanan dan Ketahanan Siber.
16. Akreditasi adalah pengakuan terkait pemenuhan standar khusus di bidang penyelenggaraan pendidikan, pelatihan, dan pengujian kompetensi sumber daya manusia dalam lingkup Keamanan dan Ketahanan Siber.
17. Sertifikat Elektronik adalah sertifikat yang diterbitkan dengan berbasis algoritma kriptografi untuk menjadi penanda atau identitas digital dari orang, komputer, sistem elektronik, data, dokumen elektronik, dan/atau jaringan Siber.
18. Badan Siber dan Sandi Negara, yang selanjutnya disingkat BSSN adalah badan yang melaksanakan urusan pemerintahan dalam bidang Keamanan dan Ketahanan Siber berdasarkan Undang-Undang ini.
19. Pemerintah Pusat adalah Presiden Republik Indonesia yang memegang kekuasaan pemerintahan negara Republik Indonesia yang dibantu oleh Wakil Presiden dan menteri sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
20. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
21. Orang adalah orang perorangan atau badan hukum.

b) Materi yang diatur

1) Asas dan Tujuan RUU Keamanan dan Ketahanan Siber

Penyelengaraan Keamanan dan Ketahanan Siber didasarkan pada asas:

a. kedaulatan;
b. ketepercayaan;
c. profesionalitas;
d. kesiapsiagaan;
e. berdaya saing;
f. kepastian hukum; dan
g. kolaboratif.

Asas-asas yang terdapat dalam RUU Keamanan dan Ketahanan Siber bertujuan untuk merumuskan nilai-nilai dasar yang menjiwai penginterprestasian dan pelaksanaan aturan-aturan dalam RUU Keamanan dan Ketahanan Siber. Asas-asas tersebut merupakan acuan konseptual dalam pelaksanaan diskresi.

RUU Keamanan dan Ketahan Siber bertujuan untuk:

a. melindungi keutuhan dan kedaulatan negara dari Ancaman Siber;
b. meningkatkan daya saing dan inovasi Siber melalui pemanfaatan Siber yang bebas, terbuka, dan bertanggung jawab;
c. mendukung pengembangan dan pemajuan perekonomian digital pada aspek tata kelola industri Siber, pengamanan sarana dan prasarana, dan sumber daya Siber nasional; dan
d. mengonsolidasikan secara sinergis dan kolaboratif semua unsur yang terlibat dalam penyelenggaraan Keamanan dan Ketahanan Siber untuk mencapai tujuan nasional dan berperan bebas aktif dalam mengantisipasi Ancaman Siber bagi perdamaian dunia.

2) Penyelenggaraan Keamanan dan Ketahanan Siber

Pada penyelenggaraan Keamanan Siber pemerintah selaku otoritas Negara bukan satu-satunya pihak yang bertanggung jawab dalam memelihara dan melindungi Keamanan Siber di Indonesia, melainkan bersama-sama lembaga negara, Pemerintah Pusat, Pemerintah Daerah, dan/atau masyarakat. Sehingga munculnya istilah kolaborasi yang membuat penyelenggaraan Keamanan Siber Indonesia merupakan kolaborasi seluruh komponen Keamanan Siber Nasional.

Penyelenggaraan Keamanan dan Ketahanan Siber harus mengedepankan:

a. pemajuan Kepentingan Siber Indonesia;
b. penghormatan hak asasi manusia;
c. kemandirian dalam inovasi ilmu pengetahuan dan teknologi; dan
d. pemajuan perekonomian nasional.

Komponen Keamanan Siber Nasional tersebut terdiri atas penyelenggara Keamanan Siber Pemerintah dan orang. Secara internasional konsep kolaborasi ini sering disebut sebagai *public private partnership*, dengan upaya Negara bekerja sama atau berkolaborasi dengan pihak swasta, dalam berbagai kegiatan salah satunya adalah melindungi infrastruktur kritis yang ada pada suatu Negara yang dikelola oleh pihak swasta. Kolaborasi tersebut harus dibina dan dikonsolidasikan secara efektif dan efisien agar terwujud satu kesatuan komponen keamanan nasional yang padu dan senantiasa siap siaga untuk melaksanakan fungsi Keamanan Siber. Penyelenggara Keamanan dan Ketahanan Siber pada lembaga negara merupakan tanggung jawab pimpinan lembaga negara yang dilaksanakan oleh kesekretariatan pada lembaga negara.

Penyelenggara Keamanan dan Ketahanan Siber pada Pemerintah Pusat terdiri atas:

a. BSSN;
b. Siber pada Tentara Nasional Indonesia;
c. Siber pada Kepolisian Negara Republik Indonesia;
d. Siber pada Kejaksaan Republik Indonesia;
e. Siber pada Badan Intelijen Negara; dan
f. Siber pada kementerian/lembaga nonkementerian selain huruf a, huruf b, huruf c, huruf d, dan huruf e.

Penyelenggaraan Keamanan dan Ketahanan Siber huruf a sampai dengan huruf e dilaksanakan sesuai dengan lingkup tugas dan fungsi masing-masing berdasarkan ketentuan peraturan perundang-undangan. Penyelenggara Keamanan dan Ketahanan Siber pada Pemerintah Daerah terdiri atas:

a. Siber pada Pemerintah Daerah provinsi; dan
b. Siber pada Pemerintah Daerah kabupaten/kota.

Penyelenggaraan Keamanan dan Ketahanan Siber dilaksanakan secara terbatas untuk Keamanan dan Ketahanan Siber pada lingkup internal organisasinya. Penyelenggaraan Keamanan dan Ketahanan Siber oleh masyarakat terbatas untuk kegiatan sebagai berikut:

a. pelindungan sistem elektronik pada lingkup internal organisasi; dan/atau
b. penyediaan jasa di bidang Keamanan dan Ketahanan Siber.

Koordinasi dan kolaborasi dilakukan oleh BSSN melalui:

a. pertemuan secara rutin;
b. peningkatan kapasitas kelembagaan dan sumber daya manusia;
c. pelaksanaan latihan penanggulangan dan pemulihan;
d. pelaksanaan kegiatan taktis bersama; dan/atau
e. pemberian dukungan teknis dan nonteknis untuk peningkatan kapasitas sarana prasarana, peningkatan kompetensi sumber daya manusia; dan/atau
f. peningkatan jangkauan jejaring kerja sama.

Ketentuan lebih lanjut mengenai koordinasi dan kolaborasi sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dalam Peraturan Pemerintah.....

3) Tata Kelola Keamanan Siber

Pada pelaksanaan fungsi Keamanan Siber terdapat obyek pengamanan yang menjadi fokus perlindungan ancaman/serangan siber yaitu data, informasi, sarana dan pra sarana, dan sumber daya manusia yang terdapat pada Infrastruktur Siber Nasional. Infrastruktur Siber Nasional dapat disusun dalam suatu daftar yang akan dibuat secara bersama-sama oleh Penyelenggara Keamanan Siber dan ditetapkan oleh BSSN. Infrastruktur Siber Nasional tersebut terdiri atas:

(a) infrastruktur informasi kritikal nasional;
(b) infrastruktur sistem informasi atau sistem elektronik Pemerintah dan Pemerintah Daerah;
(c) infrastruktur perekonomian digital nasional; dan
(d) infrastruktur sistem informasi atau sistem elektronik lain sesuai ketentuan perundang-undangan.

Dalam menegaskan macam tindakan yang berpotensi menjadi ancaman untuk dilakukan upaya-upaya dalam Keamanan Siber, maka dalam RUU Keamanan dan Ketahanan Siber perlu disebutkan tentang Ancaman Siber. Ancaman Siber terdiri atas:

a. Insiden Siber yang terjadi dalam Perimeter Keamanan;
b. Serangan Siber terhadap Objek Pengamanan Siber;
c. perangkat lunak yang berbahaya;
d. konten yang mengandung muatan destruktif dan/atau negatif;
e. produk, prototipe produk, rancangan produk, atau invensi yang dapat digunakan sebagai senjata Siber;

f. upaya yang sengaja ditujukan untuk melemahkan, merugikan, dan/atau menghancurkan Kepentingan Siber Indonesia; dan/atau
g. bentuk Ancaman Siber lainnya.

Penyelenggara Keamanan dan Ketahanan Siber wajib melaksanakan mitigasi risiko Ancaman Siber untuk melindungi Objek Pengamanan Siber yang menjadi tanggungjawabnya, dengan cara:

a. membuat salinan dari tiap perangkat lunak yang diperlukan untuk mengoperasikan sistem elektronik;
b. membuat salinan secara berkelanjutan terhadap data pada sistem elektronik untuk digunakan sebagai cadangan;
c. menyimpan salinan sebagaimana dimaksud pada huruf a dan huruf b pada sistem elektronik yang berbeda dengan sumber salinan;
d. mengoperasikan pusat operasi Keamanan dan Ketahanan Siber;
e. mengelola akses dalam Perimeter Keamanan yang menjadi tanggungjawabnya;
f. mengubah secara berkala kode akses ke sistem elektronik;
g. membuat prosedur operasional secara baku tentang mitigasi risiko terhadap Ancaman Siber, serta mensimulasikan prosedur tersebut secara berkala ke sumber daya manusia di lingkup internal organisasi; dan
h. melakukan berbagai upaya mitigasi risiko lainnya sesuai dengan ketentuan sebagaimana dimaksud dalam Undang-Undang ini.

Mitigasi risiko Ancaman Siber dilaksanakan sesuai dengan standar khusus yang ditetapkan oleh BSSN. BSSN

melaksanakan tata kelola dan asesmen terhadap kesesuaian pelaksanaan mitigasi risiko Ancaman Siber.

Setiap penyelenggara Keamanan dan Ketahanan Siber wajib melaksanakan respon Ancaman Siber untuk melindungi Objek Pengamanan Siber yang menjadi tanggungjawabnya.

Respon tersebut dilaksanakan dengan cara:

a. memeriksa keutuhan, ketersediaan, dan fungsionalitas dari Objek Pengamanan Siber yang menjadi tanggungjawabnya pada saat Insiden Siber atau Serangan Siber diketahui;
b. mencatat dan memberitahukan setiap Insiden Siber atau Serangan Siber yang terjadi pada Objek Pengamanan Siber yang menjadi tanggung jawabnya kepada BSSN;
c. melakukan penganalisisan terhadap tingkat kebahayaan dari Insiden Siber atau Serangan Siber yang terjadi pada Objek Pengamanan Siber yang menjadi tanggungjawabnya;
d. melakukan penghapusan perangkat lunak berbahaya dari sistem elektroniknya;
e. menghentikan penggunaan sistem elektronik yang telah terinfeksi Ancaman Siber untuk sementara waktu;
f. melakukan pemutusan hubungan koneksi data dari sistem elektronik ke sistem elektronik lain yang diduga menjadi sumber Ancaman Siber;
g. melaksanakan upaya yang disarankan oleh BSSN agar Insiden Siber atau Serangan Siber yang telah terjadi pada Objek Pengamanan Siber yang menjadi tanggungjawabnya, agar tidak meluas atau berbahaya;
h. melakukan pemberitahuan kepada pengguna sistem elektronik atau pelanggan mengenai respon Ancaman Siber yang telah dilakukan untuk melindungi Objek

Pengamanan Siber yang menjadi tanggung jawabnya; dan/atau

i. melakukan cara lain dalam respon Ancaman Siber sesuai dengan Undang-Undang ini.

Tingkat kebahayaan Ancaman Siber terdiri atas:

a. tidak berbahaya;
b. rendah;
c. sedang; dan
d. tinggi.

Ketentuan mengenai kriteria masing-masing tingkat kebahayaan diatur dalam Peraturan Pemerintah.

Pelaksanaan respon Ancaman Siber wajib mengacu pada standar khusus yang ditetapkan oleh BSSN. BSSN melaksanakan tata kelola dan asesmen terhadap kesesuaian pelaksanaan respon Ancaman Siber

Penyedia jasa di bidang Keamanan dan Ketahanan Siber wajib memiliki izin yang dikeluarkan oleh BSSN, untuk kegiatan usaha sebagai berikut:

a. pengelolaan sistem Keamanan dan Ketahanan Siber;
b. pengujian penetrasi keamanan akses sistem elektronik; dan
c. pembuatan algoritma kriptografi.

Ketentuan mengenai perizinan diatur dalam Peraturan BSSN.

Penyelenggara Keamanan dan Ketahanan Siber wajib memanfaatkan sumber daya manusia yang memiliki kompetensi dalam bidang Keamanan dan Ketahanan Siber, mengacu pada standar khusus yang ditetapkan oleh BSSN. Penyelenggara Keamanan dan Ketahanan Siber dapat menyelenggarakan kegiatan usaha di bidang pendidikan atau pelatihan untuk memenuhi standar. Kegiatan usaha tersebut wajib memiliki akreditasi yang diberikan oleh BSSN.

Untuk meningkatkan kemampuan dan profesionalitas sumber daya manusia, Penyelenggara Keamanan dan Ketahanan Siber yang berasal dari masyarakat dapat berhimpun dan membentuk organisasi profesi di bidang Keamanan dan Ketahanan Siber. Organisasi profesi dapat melakukan penerbitan sertifikat kompetensi profesional kepada sumber daya manusia yang telah memenuhi standar khusus. Penerbitan sertifikat kompetensi profesional hanya dapat dilakukan oleh organisasi profesi yang telah memiliki akreditasi sebagai lembaga sertifikasi profesi. Akreditasi diberikan oleh BSSN berdasarkan rekomendasi dari institusi pembina profesi yang berwenang sesuai dengan ketentuan peraturan perundang-undangan.

Penyelenggara Keamanan dan Ketahanan Siber yang tidak memenuhi standar khusus dikenakan sanksi adminstrasi, yang terdiri atas:

a. teguran;
b. penolakan permohonan izin akses Keamanan dan Ketahanan Siber;
c. pembekuan sementara izin akses Keamanan dan Ketahanan Siber;
d. pencabutan permanen izin akses Keamanan dan Ketahanan Siber;
e. pembekuan sementara izin penyedia jasa;
f. pencabutan permanen izin penyedia jasa;
g. pembekuan atau pemblokiran sementara operasional sistem elektronik;
h. penghentian atau pemblokiran permanen operasional sistem elektronik; dan/atau
i. pengenaan denda administratif.

Penyelenggara Keamanan dan Ketahanan Siber yang tidak menggunakan perangkat Siber tersertifikasi dikenakan sanksi adminstrasi yang terdiri atas:

a. teguran;
b. pembekuan atau pemblokiran sementara operasional sistem elektronik;

c. penghentian atau pemblokiran permanen operasional sistem elektronik; dan/atau
d. pengenaan denda administratif.

Penyedia jasa di bidang Keamanan dan Ketahanan Siber yang tidak mempunyai izin dalam melakukan kegiatan usahanya dikenakan sanksi administrasi yang terdiri atas:

a. teguran;
b. pembekuan atau pemblokiran sementara operasional sistem elektronik;
c. penghentian atau pemblokiran permanen operasional sistem elektronik; dan/atau
d. pengenaan denda administratif.

Penyelenggara Keamanan dan Ketahanan Siber yang menyelenggarakan kegiatan usaha di bidang pendidikan dan pelatihan tetapi tidak mempunyai akreditasi dikenakan sanksi administrasi, yang terdiri atas:

a. teguran;
b. pembekuan atau pemblokiran sementara operasional sistem elektronik;
c. penghentian atau pemblokiran permanen operasional sistem elektronik; dan/atau
d. pengenaan denda administratif.

Organisasi profesi yang menerbitkan sertifikat kompetensi profesi dan tidak mempunyai akreditasi dikenakan sanksi administrasi yang terdiri atas:

a. teguran;
b. pembekuan atau pemblokiran sementara operasional sistem elektronik;
c. penghentian atau pemblokiran permanen operasional sistem elektronik; dan/atau
d. pengenaan denda administratif.

Penyelenggara Keamanan dan Ketahanan Siber yang dijatuhi sanksi administrasi berhak mengajukan upaya

pembelaan, yang ketentuan lebih lanjutnya diatur dalam Peraturan Pemerintah.

Setiap Orang yang dirugikan akibat dari penyelenggaraan fungsi dan/atau kegiatan Keamanan dan Ketahanan Siber dapat mengajukan permohonan rehabilitasi, kompensasi, dan/atau restitusi sesuai dengan ketentuan peraturan perundang-undangan.

Penyelenggara Keamanan dan Ketahanan Siber dapat menggunakan jasa asuransi Siber yang diselenggarakan oleh pelaku usaha perasuransian Indonesia, untuk mempertanggungkan risiko kerugian akibat Insiden Siber atau Serangan Siber

Pelaku usaha jasa asuransi Siber wajib memiliki sumber daya manusia yang kompeten dalam bidang Keamanan dan Ketahanan Siber, yang sekurang-kurangnya meliputi:

a. penilai risiko (*underwriter*) Siber*;* dan
b. penilai kerugian Siber.

Sumber daya manusia yang kompeten dibuktikan dengan sertifikat kompetensi yang dikeluarkan oleh BSSN yang pengaturannya diatur dalam Peraturan BSSN.

4) Pelayanan Keamanan dan Ketahanan Siber

Pelayananan Keamanan Siber merupakan salah satu yang menjadi lingkup dalam penyelenggaraan Keamanan Siber dalam RUU Keamanan dan Ketahanan Siber. Pelayanan Keamanan Siber dilakukan demi kesiapan dalam menghadapi insiden siber atau serangan siber, meningkatkan kualitas pengelolaan risiko dari pemanfaatan Siber yang dekstruktif dan negatif, serta upaya menjamin Keamanan Siber. Sehingga diharapkan bila suatu saat terjadi insiden siber atau serangan siber, baik upaya preventif, penanggulangan dan pemulihan

dapat dilakukan dengan cepat, dan kerugian pun bisa diminimalisir.

Insiden siber yang timbul terjadi harus mendapatkan wadah atau pusat yang berfungsi sebagai tempat untuk melakukan penanggulangan dan pemulihan oleh para Penyelenggara Keamanan Siber. Hal ini dilakukan dengan membentuk Pusat Operasi Keamanan Siber yang wajib dibentuk oleh setiap Penyelenggara Keamanan Siber.

Ketentuan mengenai Pusat Operasi Keamanan Siber dikecualikan bagi Pusat operasi Keamanan dan Ketahanan Siber yang diselenggarakan oleh pelaku usaha mikro, kecil, menengah, dan koperasi. Pusat operasi Keamanan dan Ketahanan Siber nasional diselenggarakan oleh BSSN.

Pusat Operasi Keamanan Siber tersebut memberikan layanan yang terdiri dari:

(a) pengoperasian narahubung atau pusat kontak untuk pelaporan dugaan tentang akan atau telah terjadinya insiden siber dan/atau serangan siber;
(b) pemrosesan laporan dugaan insiden siber dan/atau serangan siber untuk ditindaklanjuti oleh Penyelenggara Keamanan Siber; dan
(c) pemberian informasi mengenai status perkembangan dari laporan dugaan insiden siber dan/atau serangan siber kepada pelapor.

Wadah atau pusat yang berfungsi sebagai tempat untuk penanggulangan dan pemulihan dari insiden siber tersebut yaitu Pusat Operasi Keamanan Siber, juga perlu dibuat secara nasional yang diselenggarakan oleh BSSN sebagai *focal point* dalam bidang Keamanan Siber. Pusat Operasi Keamanan Siber yang dibentuk oleh masing-masing penyelenggara Keamanan Siber, wajib berkolaborasi dan berkoordinasi dengan Pusat Operasi Keamanan Siber Nasional.

Masih dalam Pelayanan Keamanan Siber, dalam rangka meningkatkan kualitas pengelolaan risiko dari pemanfaatan Siber yang bersifat destruktif dan negatif, maka setiap Penyelenggara Keamanan Siber melakukan upaya pembudayaan Keamanan Siber. Hal ini dilakukan sebagai upaya preventif atau pencegahan dan proteksi dari pemanfaatan siber yang bersifat destruktif dan/atau negatif yang akan berujung pada insiden siber atau serangan siber, sehingga perlu adanya upaya pembudayaan Keamanan Siber. Upaya pembudayaan Keamanan Siber tersebut seperti:

(a) pengelolaan informasi dan dokumentasi terkait Keamanan Siber;
(b) pelaksanaan kegiatan promosi, bimbingan teknis, dan lokakarya untuk semakin meningkatkan literasi dan kesadaran masyarakat terhadap Keamanan Siber; dan
(c) Pemberian penghargaan kepada setiap Orang yang telah berpartisipasi dalam mewujudkan tujuan penyelenggaraan Keamanan dan Ketahanan Siber.

Terakhir pada Pelayanan Keamanan Siber, terdapat upaya yang dapat dilakukan untuk menjamin Keamanan Siber. Upaya tersebut adalah kewajiban menerapkan Sertifikasi Elektronik oleh setiap Penyelenggara Keamanan Siber dalam sistem informasi atau sistem elektroniknya. Hal ini masuk dalam pengaturan Keamanan Siber untuk menegaskan bahwa perlunya upaya yang dilakukan untuk menjadi perlindungan Keamanan Siber terhadap berbagai infrastruktur siber yang dimiliki oleh Penyelenggara Keamanan Siber, sehingga sistem informasi atau sistem elektroniknya dari masing-masing Penyelenggara Keamanan Siber perlu menerapkan Sertifikasi Elektronik.

5) Diplomasi Siber

Pada upaya penyelenggaraan Keamanan Siber, lingkup penyelenggaraan Keamanan Siber termasuk juga pada Diplomasi Siber. Melihat secara lebih luas bahwa lingkup siber sendiri bersifat internasional maka dalam usaha memajukan Kepentingan Siber Indonesia perlu adanya upaya Diplomasi Siber baik dengan melakukan penelitian, perumusan kebijakan, kerjasama, maupun peran aktif Negara Indonesia dalam dunia internasional.

Dengan begitu dikatakan Diplomasi Siber merupakan serangkaian upaya dengan menggunakan metode dan cara diplomatik untuk memajukan Kepentingan Siber Indonesia di tingkat internasional dan turut serta dalam menjaga perdamaian dunia. Dalam upaya Diplomasi Siber tersebut dilakukan oleh BSSN yang berkolaborasi dan berkoordinasi dengan Kementerian yang bertanggung jawab dalam urusan luar negeri. Kementerian tersebut dalam rangka mengefektifkan pelaksanaan diplomasi Siber:

a. mengusulkan kepada Presiden pengangkatan duta besar yang khusus menangani hubungan diplomatik di bidang Keamanan dan Ketahanan Siber; dan
b. menetapkan jabatan atase Keamanan dan Ketahanan Siber pada perwakilan diplomatik tertentu.

Selanjutnya, upaya Diplomasi Siber yang dilakukan antara lain:

a. berpartisipasi dalam menciptakan, merumuskan, memajukan usulan atau inisiatif konsep, norma, perilaku, dan panduan internasional dalam Keamanan dan Ketahanan Siber secara bilateral, regional, atau multilateral;
b. berpartisipasi dalam kegiatan pemecahan masalah Keamanan dan Ketahanan Siber di fora bilateral, regional, atau multilateral;

c. berpartisipasi dalam pengadministrasian rezim internasional di bidang Keamanan dan Ketahanan Siber di tingkat regional atau multilateral;
d. menjalin kemitraan, kerja sama, dan hubungan timbal balik dengan berbagai negara dan/atau organisasi internasional untuk meningkatkan ketahanan Siber nasional, untuk mencegah penyalahgunaan Siber, dan/atau meningkatkan kesadaran tentang aneka macam konsep dan tata pengelolaan Siber di dunia;
e. mendorong negara kawasan untuk meningkatkan kapasitas Keamanan dan Ketahanan Siber dan menegakkan sistem bersama untuk saling berbagi informasi situasional tentang kerentanan, ancaman, dan peristiwa Keamanan dan Ketahanan Siber;
f. menyelenggarakan kegiatan, pertemuan, atau lokakarya untuk mendiseminasikan konsep dan/atau kebijakan Keamanan dan Ketahanan Siber Indonesia ke negara lain; dan
g. upaya lain sesuai dengan ketentuan peraturan perundang-undangan dan/atau hukum internasional.

6) Penegakan Hukum

Dalam Penyelenggaraan Keamanan Siber, upaya penegakan hukum menjadi suatu yang sangat penting untuk mendapatkan perhatian. Penegakan hukum dalam RUU Keamanan dan Ketahanan Siber termasuk seperti pada dukungan penegakan hukum pidana, penapisan konten, serta penindakan. Dalam rangka penegakan hukum pidana, pada lingkup keamanan siber berpotensi timbul kerumitan sehingga perlu pihak yang kiranya kompeten membuat terangnya suatu kasus pada proses penegakan hukum pidana. Hal ini menjadi kompetensi BSSN sebagai *focal point* dalam urusan Keamanan Siber.

Sehingga BSSN dapat memberikan dukungan pada penegakan hukum pidana termasuk pada proses penyelidikan, penyidikan, dan pembuktian di persidangan. Penjabaran lebih lanjut dalam upaya pemberian dukungan penegakan hukum pidana oleh BSSN akan dijelaskan pada bagian setelah ini, dan ketentuan teknis prosedur operasional dari pemberian dukungan penegakan hukum pidana akan diatur lebih lanjut oleh BSSN.

Upaya penegakan hukum perlu juga menegaskan, upaya menghindari potensi adanya insiden siber atau serangan siber. Hal tesebut dilakukan demi mendukung terwujudnya pemanfaatan siber secara aman dan positif. Maka upaya yang dapat dilakukan adalah dengan melakukan penapisan terhadap konten yang bersifat desktruktif dan negatif pada ruang siber. Prosedur operasional dari penapisan konten tersebut akan diatur lebih lanjut oleh BSSN, yang bertujuan untuk menjelaskan bagaimana teknis mengenai prosedur operasional penapisan konten melalui ketentuan yang dibuat BSSN tersebut.

Dalam rangka penegakan hukum terkait pelanggaran dari ketentuan-ketentuan yang muncul dalam RUU Keamanan dan Ketahanan Siber, BSSN dapat melakukan penindakan terhadap orang yang terbukti bersalah melakukan pelanggaran. Penindakan yang dapat dilakukan oleh BSSN yaitu:

(a) penjatuhan sanksi administratif;
(b) pelimpahan hasil investigasi ke pejabat yang berwenang dalam bidang penyidikan tindak pidana;
(c) pengajuan gugatan ganti kerugian; dan/atau
(d) tindakan lain yang sesuai dengan ketentuan perundang-undangan.

Dalam rangka proses penegakan hukum, BSSN memberikan dukungan pada proses pemeriksaan perkara perdata dan pidana. Dukungan pada proses pemeriksaan perkara perdata dilakukan pada tahap pembuktian di persidangan. Dukungan pada proses pemeriksaan perkara pidana dilakukan pada tahap penyelidikan, penyidikan, dan/atau pembuktian di persidangan. Pelaksanaan mengenai pemberian dukungan

7) Badan Siber dan Sandi Negara

Dalam rangka melaksanakan urusan Keamanan Siber, BSSN memiliki kedudukan di bawah dan bertanggung jawab kepada Presiden Republik Indonesia. BSSN sebagai *focal point* dalam melaksanakan kekuasaan pemerintahan di bidang Keamanan Siber. BSSN memiliki tugas menyelenggarakan urusan pemerintahan di bidang Keamanan Siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur pemangku kepentingan yang terkait dengan Keamanan dan Ketahanan Siber, serta melakukan pengawasan pengunaan produk persandian dan penyelenggaraan persandian negara.

Selain itu BSSN juga menyelenggarakan fungsi:

a. tata Kelola Keamanan dan Ketahanan Siber;
b. pelayanan Keamanan dan Ketahanan Siber;
c. diplomasi Siber;
d. dukungan penegakan hukum; dan
e. pembinaan dalam penyelenggaraan Sertifikasi Elektronik.

Dalam rangka menyelenggarakan urusan Keamanan Siber, BSSN memiliki wewenang yiatu:

a. membentuk dan memberlakukan peraturan, standar khusus, dan/atau prosedur operasional di bidang Keamanan dan Ketahanan Siber secara nasional;
b. merumuskan kerangka strategis dan kerangka teknis Keamanan dan Ketahanan Siber;
c. melaksanakan upaya perwujudan Keamanan dan Ketahanan Siber Indonesia di dalam dan di luar negeri;
d. menetapkan Perimeter Keamanan;
e. memberikan, membekukan, atau mencabut izin, sertifikasi, atau akreditasi dalam lingkup Keamanan dan Ketahanan Siber;
f. melakukan investigasi, penindakan dan pengenaan sanksi administrasi;
g. melakukan asesmen, pengujian, penetrasi keamanan akses sistem elektronik, dan/atau audit Keamanan dan Ketahanan Siber; dan
h. memberikan dukungan dalam proses penegakan hukum pidana dan perdata.

Dalam rangka mendukung proses penegakan hukum pidana, BSSN melakukan:

a. penganalisisan bukti digital;
b. pemberian keterangan ahli di bidang forensik digital; dan/atau
c. pemberian dukungan teknis keamanan siber dalam tahap penyelidikan dan penyidikan.

Dukungan proses penegakan hukum pidana dilaksanakan oleh BSSN apabila ada permintaan tertulis dari penyelidik, penyidik, dan/atau penuntut umum kepada BSSN, sedangkan dukungan proses penegakan hukum perdata dilaksanakan oleh BSSN apabila ada permintaan secara tertulis oleh pengadilan. Pelaksanaan dukungan penegakan pidana dan dan perdata oleh BSSN

dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Selain wewenangan yang telah disebutkan, BSSN dalam urusan Keamanan Siber juga memiliki wewenang dalam melaksanakan Deteksi, Identifikasi, Proteksi, Penanggulangan, Pemulihan, Pemantauan, dan Pengendalian pada Obyek Pengamanan Siber. Wewenang melaksanakan Deteksi dilakukan BSSN dengan kegiatan seperti:

a. Deteksi Ancaman Siber pada lalu lintas data;
b. Deteksi Ancaman Siber terkait perilaku sosio-kultural;
c. Deteksi potensi Ancaman Siber;
d. intelijen sinyal;
e. asesmen, pengujian, dan penetrasi keamanan akses sistem elektronik untuk menemukan kerentanan dan celah keamanan terkait Infrastruktur Siber Nasional;
f. Pemberian izin untuk kegiatan penelitian dan pengujian kekuatan Keamanan dan Ketahanan Siber; dan
g. kegiatan Deteksi lain sesuai dengan ketentuan peraturan perundang-undangan.

Dalam rangka melaksanakan Identifikasi sebagaimana dimaksud dalam 44, BSSN melakukan kegiatan:

a. Identifikasi Ancaman Siber pada lalu lintas data;
b. Identifikasi Ancaman Siber terkait perilaku sosio-kultural;
c. Identifikasi potensi Ancaman Siber;
d. Penganalisisan hasil intelijen sinyal;
e. penganalisisan hasil asesmen, pengujian, dan penetrasi keamanan akses sistem elektronik terkait Infrastruktur Siber nasional;
f. Pemberian izin untuk kegiatan penelitian dan pengujian kekuatan Keamanan dan Ketahanan Siber; dan

g. kegiatan Identifikasi lain sesuai dengan ketentuan peraturan perundang-undangan.

Pelaksanaan proteksi oleh BSSN dilakukan dengan kegiatan seperti:

a. tata kelola terhadap pemanfaatan algoritma kriptografi;
b. penerbitan Sertifikat Elektronik pada infrastruktur Siber nasional;
c. pelindungan jaringan Siber intra penyelenggara Keamanan dan Ketahanan Siber;
d. pengauditan pelaksanaan standar keamanan;
e. perencanaan kebutuhan peralatan persandian negara;
f. pemeliharaan peralatan persandian negara;
g. pengelolaan kunci sistem sandi yang digunakan untuk persandian negara;
h. pelindungan keamanan gelombang frekuensi atau sinyal;
i. kontra penginderaan;
j. pengelolaan hibah; dan
k. pembinaan komunitas Keamanan dan Ketahanan Siber.

Dalam melaksanakan Penanggulangan, BSSN melakukan kegiatan seperti:

a. pengelolaan sentra informasi untuk penanggulangan Ancaman Siber;
b. pengonsolidasian upaya untuk penanggulangan Ancaman Siber; dan
c. pengonsolidasian aneka upaya penanggulangan untuk menjaga keberlanjutan operasional dari infrastruktur Siber nasional.

Dalam rangka melaksanakan Pemulihan sebagaimana dimaksud dalam Pasal 44, BSSN melakukan kegiatan:

a. penyebarluasan informasi untuk meningkatkan kesadaran Keamanan dan Ketahanan Siber;

b. pelaksanaan investigasi untuk mengupayakan pemulihan terhadap kerugian atau kehilangan yang terjadi pada Infrastruktur Siber Nasional; dan
c. pelaksanaan tindak lanjut hasil investigasi melalui upaya administratif dan/atau upaya pemulihan kerugian lain sesuatu dengan perundang-undangan.

Dalam rangka melaksanakan Pemantauan sebagaimana dimaksud dalam Pasal 44, BSSN melakukan kegiatan:

a. tata kelola terhadap data dan informasi terkait cara terjadinya Insiden Siber atau Serangan Siber yang telah terjadi di seluruh dunia;
b. tata kelola terhadap data dan informasi terkait dampak dari Insiden Siber atau Serangan Siber yang telah terjadi di seluruh dunia; dan
c. penelaahan terhadap data dan informasi terkait Insiden Siber atau Serangan Siber untuk merumuskan strategi dan taktik terbaik dalam merespon berbagai perkembangan Ancaman Siber yang ditujukan kepada Negara Kesatuan Republik Indonesia.

Dalam rangka melaksanakan Pengendalian sebagaimana dimaksud dalam Pasal 44, BSSN melakukan kegiatan:

a. perizinan penyedia jasa di bidang Keamanan dan Ketahanan Siber;
b. pensertifikasian perangkat Siber yang disediakan untuk digunakan pada infrastruktur Siber nasional;
c. pensertifikasian penilai risiko (*underwriter*) Siber dan penilai kerugian Siber;
d. pengakreditasian lembaga pendidikan dan pelatihan di bidang Keamanan dan Ketahanan Siber; dan
e. pengakreditasian lembaga sertifikasi profesi di bidang Keamanan dan Ketahanan Siber.

Sebelumnya telah dijelaskan bahwa munculnya insiden Keamanan Siber suatu Negara akan mengganggu sendi-sendi kehidupan masyarakat pada Negara tersebut. Insiden siber yang timbul dari serangan siber yang merugikan tersebut tidak jarang pula ditemukan berpotensi menimbulkan keadaan perang pada suatu Negara baik dengan *state actor* maupun *non-state actor*. Dalam memaksimalkan kinerja dari BSSN, perlu struktur organisasi yang mendukung BSSN melaksanakan tugas, fungsi dan wewenangnya sebagai institusi yang memegang kekuasaan pemerintahan di bidang Keamanan Siber. Struktur organisasi BSSN terdiri atas:

a. Kepala;
b. Wakil Kepala;
c. Sekretariat Utama;
d. deputi;
e. inspektorat utama; dan
f. pusat dan/atau unit kerja lain menurut aturan dan ketetapan yang berlaku.

Dari urutan stuktur organisasi tersebut, BSSN dipimpin oleh seorang kepala dan dibantu oleh seorang wakil kepala, yang pengangkatan dan pemberhentiannya ditetapkan dengan Keputusan Presiden. Kepala BSSN diberikan hak keuangan dan fasilitas setingkat dengan menteri, begitupun Wakil Kepala BSSN juga diberikan hak keuangan dan fasilitas setingkat wakil menteri.

Dalam rangka efektifitas dan efisiensi pelaksanaan koordinasi dan kolaborasi dengan Pemerintah Daerah, BSSN membentuk kantor perwakilan, yang susunan organisasi dan tata laksana dari kantor perwakilan ditetapkan oleh BSSN. Dalam rangka pemenuhan kebutuhan sumber daya manusia untuk pelaksanaan tugas, fungsi, wewenang, dan kegiatan BSSN dalam

lingkup Keamanan dan Ketahanan Siber, BSSN menyelenggarakan pendidikan kedinasan, yang susunan organisasi dan tata laksana dari pendidikan kedinasan ditetapkan oleh BSSN.

Dalam rangka pelaksanaan Keamanan Siber pada penyelenggaraan pemerintahan berbasis elektronik, BSSN menyelenggarakan layanan penerbitan Sertifikat Elektronik, yang meliputi:

a. pengelolaan penerbitan Sertifikat Elektronik berbasis algoritma kriptografi untuk pembuatan tanda tangan elektronik dan pengautentikasian identitas Orang;
b. pengelolaan penerbitan Sertifikat Elektronik berbasis algoritma kriptografi untuk pembuatan tanda tangan elektronik dan pengautentikasian komputer atau sistem elektronik;
c. pengelolaan penerbitan Sertifikat Elektronik berbasis algoritma kriptografi untuk pembuatan tanda tangan elektronik dan pengautentikasian jaringan komputer atau jaringan siber; dan
d. pengelolaan penerbitan Sertifikat Elektronik berbasis algoritma kriptografi untuk pembuatan tanda tangan elektronik dan pengautentikasian data atau dokumen elektronik.

Layanan penerbitan Sertifikat Elektronik dapat diberikan kepada pihak di luar Sistem Pemerintahan Berbasis Elektronik apabila terdapat permintaan. Susunan organisasi dan tata laksana layanan penerbitan Sertifikat Elektronik ditetapkan oleh BSSN. Untuk lebih lanjut melengkapi mengenai stuktur, organisasi, dan tata kerja dari BSSN akan berada dan diatur dalam Peraturan Presiden.

Penyelenggaraan Keamanan dan Ketahanan Siber dalam keadaan perang dilakukan di bawah kendali

langsung Presiden dengan mendapat persetujuan Dewan Perwakilan Rakyat.

8) Pendanaan Dan Pengadaan

Pendanaan untuk penyelenggaraan Keamanan dan Ketahanan Siber bersumber dari:

a. Anggaran Pendapatan dan Belanja Negara;
b. anggaran pendapatan dan belanja daerah;
c. dana pengembangan Keamanan dan Ketahanan Siber nasional;
d. hibah; dan/atau
e. sumber pendanaan lain yang sah dan tidak mengikat menurut ketentuan peraturan perundang-undangan.

Yang dimaksud dengan Hibah dapat berupa:

a. uang;
b. barang;
c. fasilitas;
d. peralatan; dan/atau
e. jasa.

Hibah uang dimasukkan dalam dana pengembangan Keamanan dan Ketahanan Siber nasional dan dikelola oleh BSSN, yang hasilnya digunakan untuk:

a. pengembangan sumber daya manusia;
b. penelitian;
c. pemberian penghargaan; dan/atau
d. dana cadangan untuk mengantisipasi keperluan kontijensi atas terjadinya Insiden Siber dan/atau Serangan Siber.

Ketentuan lebih lanjut tentang pengelolaan dana pengembangan Keamanan dan Ketahanan Siber nasional diatur dalam Peraturan Pemerintah.

Hibah barang, fasilitas, peralatan, dan/atau jasa dikelola oleh BSSN, yang digunakan untuk peningkatan

kemampuan penyelenggaraan Keamanan dan Ketahanan Siber nasional. Ketentuan lebih lanjut tentang pengelolaan hibah barang, fasilitas, peralatan, dan/atau jasa diatur dalam Peraturan BSSN.

Pemerintah Pusat dan Pemerintah Daerah wajib mengalokasikan dana penyelenggaraan Keamanan dan Ketahanan Siber dalam Anggaran Pendapatan dan Belanja Negara dan Anggaran Pendapatan dan Belanja Daerah, yang diperuntukkan bagi:

a. pengembangan sumber daya manusia; dan
b. pembangunan dan/atau penguatan perangkat dan infrastruktur Keamanan dan Ketahanan Siber.

Ketentuan lebih lanjut mengenai pengalokasian dan peruntukan Dana penyelenggaraan Keamanan dan Ketahanan Siber diatur dalam Peraturan Pemerintah.

Pembangunan dan/atau penguatan perangkat dan infrastruktur Keamanan dan Ketahanan Siber wajib memenuhi ketentuan 50% (lima puluh persen) tingkat komponen dalam negeri dan diterapkan masing-masing untuk pengadaan perangkat keras dan/atau perangkat lunak, serta dilaksanakan oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang perindustrian dan berkoordinasi dengan BSSN. Ketentuan lebih lanjut tentang pemenuhan 50% (lima puluh persen) tingkat komponen dalam negeri diatur dalam Peraturan Pemerintah.

Pengadaan perangkat keras dan perangkat lunak dalam keadaan tertentu dapat dilakukan dengan cara penunjukan langsung atau pengadaan langsung.

Penunjukan langsung atau pengadaan langsung dalam keadaan tertentu dilakukan dalam hal:

a. penanganan darurat untuk keamanan dan keselamatan masyarakat;

b. pekerjaan yang kompleks dan hanya dapat dilaksanakan oleh penyedia jasa di bidang Keamanan dan Ketahanan Siber yang sangat terbatas atau hanya dapat dilakukan oleh pemegang hak;
c. pekerjaan yang perlu dirahasiakan yang menyangkut keamanan dan keselamatan negara; dan/atau
d. pekerjaan yang berskala kecil.

Penunjukan langsung atau pengadaan langsung dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

9) Larangan

Setiap Orang dilarang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang mengakibatkan infrastruktur Siber Nasional terganggu dan/atau tidak bekerja sebagaimana mestinya.

Setiap Orang dilarang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, mendistribusikan, atau menyediakan perangkat yang dirancang atau dikembangkan secara khusus untuk memfasilitasi tindakan apapun yang mengakibatkan infrastruktur Siber Nasional terganggu dan/atau tidak bekerja sebagaimana mestinya.

10) Ketentuan Pidana

Penerapan sanksi pidana diharapkan mampu memberikan efek jera pada mereka yang melakukan pelanggaran terhadap ketentuan yang ada dalam rancangan undang-undang ini. Pengenaan sanksi pidana dalam RUU Keamanan dan Ketahanan Siber:

a. Setiap Orang yang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang mengakibatkan infrastruktur Siber Nasional terganggu

dan/atau tidak bekerja sebagaimana mestinya, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah) berdasarkan tingkat kerusakan yang ditimbulkan.

b. Setiap Orang yang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, mendistribusikan, atau menyediakan perangkat yang dirancang atau dikembangkan secara khusus untuk memfasilitasi tindakan apapun yang mengakibatkan infrastruktur Siber Nasional terganggu dan/atau tidak bekerja sebagaimana mestinya, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah) berdasarkan tingkat kerusakan yang ditimbulkan.

Ketentuan pidana di atas tidak berlaku kepada setiap Orang yang melakukan penelitian dan/atau pengujian, serta harus terdaftar dan memiliki izin dari BSSN, terhadap kekuatan dari Keamanan dan Ketahanan Siber pada infrastruktur Siber nasional. Ketentuan mengenai tata cara penelitian, pengujian, pendaftaran, dan pemberian izin diatur dalam Peraturan BSSN.

11) Ketentuan Peralihan

Pada saat Undang-Undang ini mulai berlaku, semua peraturan perundang-undangan yang mengatur mengenai Keamanan dan Ketahanan Siber dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Undang-Undang ini.

Organisasi atau badan yang merupakan unsur penyelenggaraan Keamanan dan Ketahanan Siber yang sudah ada tetap berlaku sampai dengan diubah atau

diganti dengan organisasi atau badan baru berdasarkan ketentuan dalam Undang-Undang ini.

BSSN wajib menyesuaikan dengan ketentuan Undang-Undang ini, paling lama 2 (dua) tahun terhitung sejak Undang-Undang ini berlaku.