LEMBAGA KETAHANAN NASIONAL

REPUBLIK INDONESIA

KERJA SAMA KEAMANAN SIBER INDONESIA DENGAN NEGARA LAIN DALAM KERANGKA KETAHANAN NASIONAL

Oleh:

Dr. Sulistyo, S.Si., S.T., M.Si

Nomor Peserta : 65

KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)
PROGRAM PENDIDIKAN REGULER ANGKATAN (PPRA) LXII
LEMHANNAS RI
TAHUN 2021


DHARMMA
TANHANA
MANGRVA

KATA PENGANTAR

Assalammualaikum Wr Wb, salam sejahtera bagi kita semua.

Dengan mengucap rasa syukur dan terimaksih yang sedalam dalamnya kehadirat Allah SWT Tuhan yang Maha Esa. Sehingga penulis sebagai salah satu peserta Program Pendidikan Reguler Angkatan (PPRA) LXII tahun 2021 telah menyelesaikan Kertas Karya Ilmiah Perseorangan (Taskap) dengan judul:

"KERJA SAMA KEAMANAN SIBER INDONESIA DENGAN NEGARA LAIN DALAM KERANGKA KETAHANAN NASIONAL"

Penentuan Tutor dan judul Taskap ini didasarkan oleh Keputusan Gubernur Lembaga Ketahanan Nasional Republik Indonesia Nomor 86 Tahun 2021 tanggal 27 Bulan April tahun 2021 tentang Pengangkatan Tutor Taskap kepada para peserta PPRA LXII tahun 2021 untuk menulis Taskap dengan memilih judul yang telah ditentukan oleh Lemhannas RI.

Penulis menyadari bahwa dalam proses penyelesaian Taskap ini telah melibatkan berbagai pihak, baik secara langsung maupun tidak langsung, perorangan maupun lembaga yang telah memberikan dukungan moril, motivasi dan kontribusi dalam penyelesaian penyusunan Taskap ini. Untuk itu dalam kesempatan yang baik ini, penulis ucapkan terima kasih dan penghargaan yang setinggi-tingginya kepada yang penulis hormati:

Pertama, kepada **Gubernur Lemhannas RI** Bapak Letjen TNI (Pur) Agus Widjojo yang telah memberikan kesempatan kepada Penulis untuk mengikuti PPRA LXII di Lemhannas RI Tahun 2021;

Kedua, juga penulis ucapan terimakasih kepada Pembimbing atau Tutor Taskap Bapak Mayjen TNI Gunung Iskandar dan Bapak Mayjen TNI Mar (Pur) Eddy Oetomo, Tim Penguji Taskap**,** Bapak/Ibu Tajar dan Taprof di Lemhanas serta semua pihak yang telah membantu serta membimbing Taskap ini sampai terselesaikan sesuai waktu dan ketentuan yang dikeluarkan oleh Lemhannas RI;

Ketiga ucapan terimakasih yang setinggi-tingginya juga kami sampaikan kepada Kepala BSSN RI Bapak Letjen TNI (Pur) Hinsa Siburian serta Deputi Bidang Identifikasi dan Deteksi Bapak Irjen Pol Dono Indarto, S.IK, M.H yang telah

memberikan motivasi dan dukungan kepada penulis untuk untuk menempuh pendidikan di Lemhannas guna memajukan organisasi BSSN;

Keempat, penulis sampaikan terimakasih kepada teman-teman se angkatan di Program Pendidikan Reguler Angkatan (PPRA) LXII tahun 2021 serta teman sejawat serta kolega di Badan Siber dan Sandi Negara (BSSN) yang telah memberikan dukungan kepada penulis untuk merampungkan naskah ini;

Kelima yang amat teristimewa dan lebih khusus kepada yang penulis cintai istri tersayang Sulistyowati, SE juga anak anaku Alisha, Atalla dan Arimbi serta Bapak/Ibu Orang Tua penulis yang dengan penuh kesabaran menemani penulis dalam keadaan apapun, serta selalu memberikan semangat untuk menyelesaikan Taskap ini.

Penulis menyadari bahwa penyusunan penulisan Taskap ini masih jauh dari kesempurnaan. Penulis berharap semoga Taskap ini dapat sedikit memberikan manfaat bagi kemajuan Bangsa dan Negara, bagi Lemhannas RI terutama untuk menciptakan pertahanan dan keamanan melalui kedaulatan dan keamanan siber nasional.

Penulis juga berharap Taskap ini dapat memberikan sedikit sumbangsih untuk perkembangan ilmu pengetahuan, khususnya bidang keamanan siber *(cyber security)* serta dapat dijadikan salah satu rujukan bagi penelitian atau penulis karya ilmiah lainnya. Akhir kata penulis berbesar hati apabila para pembaca dapat memberikan kritik, saran dan masukan dan perbaikan dalam rangka proses penulisan dan penelitian berikutnya.

Semoga Allah SWT, Tuhan YME senantiasa memberikan nikmat keberkahan dan bimbingan kepada kita semua dalam melaksanakan tugas dan pengabdian kepada Negara dan Bangsa Indonesia yang kita cintai.

Sekian dan terima kasih. Wassalamualaikum Wr Wb.

Jakarta, 22 Juli 2021
Penulis Taskap

Dr. Sulistyo, S.Si., S.T., M.Si.

LEMBAGA KETAHANAN NASIONAL

REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan dibawah ini:

   Nama : Dr. Sulistyo, S.Si., S.T., M.Si

   Pangkat : Pembina Utama Muda (IV/c)

   Jabatan : Direktur Deteksi Ancaman, Deputi I

   Instansi : Badan Siber dan Sandi Negara (BSSN)

   Alamat : Bumi Dirgantara Permai BN-12 Jatisari Jatiasiah Bekasi

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) ke-LXII tahun 2021 menyatakan dengan sebenarnya bahwa:

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

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

Jakarta, 22 Juli 2021

Penulis Taskap

Dr. Sulistyo, S.Si., S.T., M.Si.

LEMBAGA KETAHANAN NASIONAL

REPUBLIK INDONESIA

LEMBAR PERSETUJUAN TUTOR TASKAP

Yang bertanda tangan dibawah ini Tutor Taskap dari:

Nama : Dr. Sulistyo, S.Si., S.T., M.Si

Peserta : Program Pendidikan Reguler Angkatan (PPRA) ke LXII Tahun 2021

Judul Taskap : **"KERJA SAMA KEAMANAN SIBER INDONESIA DENGAN NEGARA LAIN DALAM KERANGKA KETAHANAN NASIONAL"**

Taskap tersebut di atas telah ditulis "sesuai/~~tidak sesuai~~" dengan Juknis Taskap Peraturan Gubernur Lemhannas RI Nomor 04 Tahun 2021, karena itu "layak/~~tidak layak~~" dan "disetujui/~~tidak disetujui~~" untuk di uji.

"" Coret yang tidak diperlukan.

Jakarta, 23 Juli 2021

Tutor Taskap

Mayjen TNI Gunung Iskandar

DAFTAR ISI

KERJA SAMA KEAMANAN SIBER INDONESIA DENGAN NEGARA LAIN DALAM KERANGKA KETAHANAN NASIONAL

GLOSARIUM
(Daftar Singkatan Kata)

AEC : ASEAN Economic Community

AMCC : *ASEAN* Ministerial Conference on Cybersecurity

ARF : ASEAN Regional Forum

ASC: ASEAN Security Community

ASCC : ASEAN Socio-Cultural Community

BSSN : Badan Siber dan Sandi Negara

CCIC : Cyber Crime Investigation Centre

CIRT : Cyber Insident Response Team

CGI : Cybersecurity Global Index

CII : Critical Information Infrastructures

CISO : Chief Of Information Security Officer

CNAP : Cybersecurity National Action Plan

CNCI : Comprehensive National Cybersecurity Initiative

DDOS : Distributed Denial of Service

DITTIPIDSIBER : Direktorat Tindak Pidana Siber

DUDI : Dunia Usaha dan Dunia Industri

GSoC : Google Summer of Code

IHP : *Indonesia Honeynet Project*

ITE: Informasi dan Transaksi Elektronik

IoT : Internet of things

ITU : International Telecommunication Union

KEMENDAGRI : Kementerian Dalam Negeri

KEMENKOMINFO : Kementerian Komunikasi dan Informatika

KKS : Keamanan dan Ketahanan Siber

KKNI : Kerangka Kualifikasi Nasional Indonesia

NCSI : National Cyber Security Index

OS : operating system

PMSE : Perdagangan Melalui Sistem Elektronik

PPD : Public Private Dialogue

SATBER TNI : Satuan Siber TNI

SKB : Surat Keputusan Bersama

BAB I
PENDAHULUAN

1. Latar belakang

Membahas dimensi ketahanan nasional hari ini tidak terbatas pada bagaimana membangun ketangguhan infrastruktur pertahanan nasional baik itu dari segi personil dan sarana serta prasarana pendukung lainya guna menghadapi dan mengatasi segala ancaman, gangguan, hambatan dan tantangan luar maupun dari dalam negeri yang dapat mengancam eksistensi Bangsa dan Negara Kesatuan Republik Indonesia. Ketahanan Nasional hari ini tengah dihadapkan dalam tantangan terutama di era digital yaitu ketahanan nasional yang menyangkut keamanan siber.

Di tengah hingar-bingar dan perhelatan revolusi industri 4.0 yang telah menempatkan teknologi dan informasi sebagai prioritas, telah memaksa manusia untuk bergantung kepada teknologi digital dalam berbagai aktivitasnya. Kontestasi siber ini muncul bak pisau bermata dua, di satu sisi melahirkan dampak positif dan di sisi lain juga memiliki dampak negatif, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, akan tetapi muncul sebuah paradoks yang menjadi sarana yang efektif untuk melakukan pelanggaran hukum terutama maraknya kejahatan siber yang terjadi akhir-akhir ini terlebih di tengah Pandemi Covid 19.

Richard Clarke (2010) dalam karyanya tentang Cyber War, misalnya, menyarankan bahwa mengukur kekuatan siber harus mencakup: “a) kemampuan dalam menanggulangi pelanggaran siber atau tindak kejahatan siber, b) tingkat ketergantungan siber, dan c) kemampuan pertahanan siber. Perbandingannya antara AS, Rusia, China, Iran, dan Korea Utara menempatkan Amerika sebagai negara terlemah dalam keamanan siber”[1].

Berdasarkan data yang penulis himpun dari beberapa sumber menunjukkan bahwa Badan Siber dan Sandi Negara (BSSN) menyebutkan

[1] R.A. Clarke, R.K. Knake, Cyber War: The Next Threat to National Security and What to Do About It, 2010, p. 147–150

bahwa, sepanjang bulan Januari hingga Agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibanding periode yang sama tahun lalu yang tercatat di kisaran 39 juta.[2]

Selain itu juga seperti data yang disajikan oleh, Kementerian Komunikasi dan Informasi mencatat jumlah pengguna di Indonesia telah mencapai sekitar 132,7 juta orang. Pertumbuhan yang sangat dramatis ini menjadikan keamanan dunia siber di Indonesia menjadi sangat rentan dan terusik oleh pelaku-pelaku tindak kejahatan siber.

Di tengah derasnya aliran digital yang ada pada *cyberspace* diperlukan adanya langkah-langkah strategis dan taktis guna mencegah, menangani dan menindak setiap pelaku kejahatan siber. Terlebih di tengah wabah pandemi Covid-19 ini telah marak aksi-aksi tindak kejahatan siber yang menjadi hidangan di ruang digital kita.[3]

Semua eksponen harus bahu membahu melawan penyebaran tersebut, mulai dari pemerintah dengan membuat perangkat regulasi yang mengatur, Kominfo yang juga menjadi lembaga yang memegang kendali atas distribusi dan kontrol terhadap lalu lintas siber di Indonesia, BSSN, provider dan penyedia platform digital yang memberikan layanan internet dan media sosial hingga masyarakat luas yang menjadi konsumen dari media sosial dan digital.

Sementara itu di satu sisi, data yang dirilis oleh Kemenkominfo (2020) menyebutkan bahwa ada sekitar 800.000 situs di Indonesia yang telah terindikasi sebagai penyebar informasi palsu. Dengan demikian kondisi faktual menunjukkan bahwa internet telah salah dimanfaatkan oleh oknum tertentu untuk keuntungan pribadi dan kelompoknya dengan cara menyebarkan konten-konten negatif yang menimbulkan keresahan dan

---

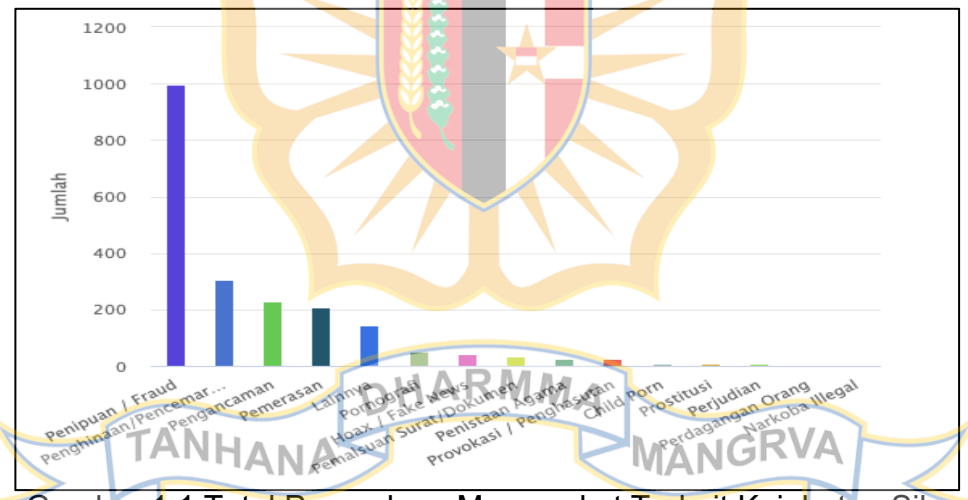
[2] Data ini penulis kutip dari laporan BSSN yang telah dimuat dalam Tekno Kompas dapat dilihat dalam tautan berikut: https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik4-kali-lipat-selama-pandemi.

[3] Siburian, H.K., 2016. Emerging Issue in Cyber Crime: Case Study Cyber Crime in Indonesia. Int. J. Sci. Res. 5, 2013–2016. https://doi.org/10.21275/ART20162818

saling mencurigai di masyarakat yang berbuntut pada konflik sosial baik dalam lingkup kesukuan, etnis, ras, agama ego-ego primordial lainya.

Maraknya serangan siber yang terjadi akhir-akhir ini terutama pada masa pandemi Covid 19 menjadi perhatian serius. Hal ini dikarenakan adanya peningkatan yang signifikan dalam pemanfaatan teknologi informasi dan komunikasi masyarakat karena adanya pemberlakuan social distancing dan juga meningkatnya preferensi masyarakat untuk melakukan aktivitas di ruang virtual. Celah kerentanan siber di Indonesia di masa Pandemi ini banyak dimanfaatkan oleh pihak-pihak tertentu terutama para pelaku kejahatan siber untuk melancarkan serangan siber, seperti malware, phising, SQL *Injection*, Hijacking, dan *Distributed Denial of Service* (DDOS).[4]

Selain data tersebut di atas, data terkait total konten negatif yang bersumber dari laporan masyarakat melalui portal Patrolisiber sebanyak 2.087 total aduan dengan total kerugian mencapai 1,04 Triliun rupiah. Untuk lebih detailnya dapat dilihat dalam grafik berikut ini:



Gambar 1.1 Total Pengaduan Masyarakat Terkait Kejahatan Siber

Data di atas menunjukkan bahwa tindak kejahatan siber yang terlaporkan didominasi oleh tindak kejahatan penipuan/ fraud dengan total laporan mencapai 998 kasus, kejadian disusul kasus penghinaan dan pencemaran nama baik sebanyak 304 kasus. Selain itu juga permasalahan

[4] Tan, Zoe (2020) The state of cybersecurity in the time of COVID-19, https://usa.kaspersky.com/blog/cybersecurity-in-the-time-of-covid/22651/, diakses pada tanggal 5 Mei 2021

serius lainya adalah permasalahan tentang infrastruktur dan regulasi tentang keamanan siber.

Permasalahan infrastruktur terkait dengan terbatasnya sumber daya terutama kebutuhan teknologi yang masih terbatas terutama di wilayah Indonesia yang begitu luas jangkauannya. Keterbatasan infrastruktur ini ternyata juga tidak dibarengi pula dengan peningkatan kapasitas dan sumber daya manusia baik itu dari aparat penegak hukum dan juga masyarakat.[5] Keterbatasan anggota Polri untuk melakukan patroli siber ditambah dengan rendahnya kemampuan mereka dalam menguasai digital forensik masih menjadi persoalan serius.

Meskipun sudah terdapat regulasi yang mengatur tentang keamanan siber, seperti yang tertuang dalam Pasal 94 ayat (1) huruf a Peraturan Pemerintah Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal tersebut menyatakan bahwa peran pemerintah dalam menetapkan strategi keamanan siber nasional merupakan bagian dari strategi keamanan nasional. Untuk itu perlu menjadi payung hukum dan pegangan semua pihak khususnya dalam menjaga ketahanan siber dalam bingkai ketahanan Nasional, agar segala bentuk ancaman tindak kejahatan siber dapat terminimalisir.

Regulasi ini dapat digunakan sebagai acuan dan pijakan bersama bagi seluruh pemangku kepentingan keamanan siber nasional terutama dalam menyusun dan mengembangkan kebijakan keamanan siber di instansi masing-masing. Selain itu, strategi ini diharapkan mampu memicu peningkatan keamanan siber yang akan menumbuhkan potensi ekonomi digital di negara Indonesia sehingga Indonesia dapat menjadi poros negara yang unggul dibidang ekonomi digital di masa mendatang.

Permasalahan lain yang harus menjadi perhatian serius adalah penguatan norma yang ada di ruang siber. Untuk membangun dan

[5] Setiadi, F., Sucahyo, Y.G., Hasibuan, Z.A., 2012. An Overview of the Development Indonesia National Cyber Security. Int. J. Inf. Technol. Comput. Sci. (IJITCS) 6, 106–114. Lihat juga, Prayudi, Y., 2015. A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia 1–8. https://doi.org/10.5815/ijcnis.2015.11.01

melakukan penguatan norma di ruang siber membutuhkan adanya literasi digital yang menekankan pada pembentukan etika dan moral di ruang siber. Ini bertujuan agar semua kalangan menyadari betapa pentingnya norma tersebut dalam menciptakan budaya guna membangun kesadaran kolektif akan ancaman dan gangguan kejahatan siber yang terus meningkat dari waktu ke waktu.

Mengingat pentingnya menjaga keamanan siber sebagai perwujudan ketahanan Nasional, maka diperlukan adanya kerja sama antar negara untuk menjaga keamanan siber. Kerja sama ini dirasa penting karena kejahatan siber dan keamanan siber sebagai trend dalam isu keamanan internasional yang tentu dapat menjadi permasalahan serius di tingkat bilateral maupun regional. Meski sebagian besar ancaman terhadap keamanan siber masih d idominasi oleh aktor non-negara/pemerintah (Hacker, teroris, dan kejahatan terorganisir transnasional), tetapi tidak menutup kemungkinan juga diorganisir oleh satu negara tertentu untuk menyerang negara lain, terutama pada negara-negara yang masih sangat lemah dalam pertahanan sibernya. Oleh karena itu, banyak negara kemudian menaruh perhatian besar pada potensi dampak yang ditimbulkan dari ancaman siber tersebut.

Dalam konteks keamanan siber, sebagian besar pembahasan terkini tentang keamanan siber di era digital sebagian besar berkaitan dengan perlunya pembatasan tertentu dari tindakan pemerintah dalam menangani kejahatan siber yang terdesentralisasi dan dimiliki atau dioperasikan oleh sektor swasta, baik perorangan maupun perusahaan.[6] Artinya pemerintah hanya sebatas memberikan kebijakan serta regulasi dalam upaya untuk melakukan pencegahan, penegakan hukum terhadap para pelaku kejahatan siber.

Seiring dengan perkembangan dan dinamika serta kompleksitas yang muncul dibalik isu kejahatan siber akhir-akhir ini, telah mendorong Pusat

[6] Untuk lebih detailnya dapat dilihat dalam Eriksson, J., & Giacomello, G. (2009). Who Controls the Internet ? Beyond the Obstinacy or Obsolescence of the State. *International Studies Review*, 11, 205–230. https://doi.org/10.1111/j.1468-2486.2008.01841.x

Pengkajian dan Pengembangan Kebijakan (P3K) Kemlu RI untuk menyusun *policy paper* terkait bagaimana membangun kerja sama dalam isu siber dengan negara lain. Adapun landasan dibentuknya *policy paper* tersebut didasarkan pada pertumbuhan pesat Indonesia menuju ekonomi digital yang harus dibarengi dengan upaya-upaya untuk mencegah tindak kejahatan siber. Hal tersebut dapat dilakukan dengan melakukan kerja sama dengan berbagai negara ataupun aktor internasional lainnya, terutama dalam persoalan *capacity building*.

Lebih lanjut, keuntungan yang diperoleh dari kerja sama di bidang siber adalah meskipun infrastruktur siber Indonesia masih tergolong rendah dari negara lain, Indonesia dapat berperan aktif dalam konstelasi siber global dengan mengusung kampanye optimalisasi etika dalam dunia siber yang berupa seruan moral penggunaan teknologi siber yang bertanggung jawab.

Pentingnya kerja sama bilateral antar negara di bidang keamanan siber adalah bertujuan agar pemerintah Indonesia dapat melakukan kerja sama bilateral terkait pengembangan dan pemanfaatan teknologi pertahanan siber bersama seperti latihan simulasi perang siber antara Indonesia dengan negara lain.

Selain itu juga pemerintah Indonesia dapat meningkatkan kemampuan siber yang dimiliki Indonesia saat ini dengan meningkatkan dukungan anggaran dalam rangka peningkatan SDM dan teknologi bidang siber di Indonesia melalui pelatihan dan riset bidang teknologi siber, serta membuat kebijakan ekonomi yang mampu menjadikan industri siber sebagai penggerak pertumbuhan ekonomi nasional.

Sementara dari aspek pengembangan SDM, pemerintah Indonesia dapat meminimalisir ancaman siber dengan meningkatkan kemampuan SDM di Indonesia terkait kemampuan di bidang siber dengan memasukkan kurikulum terkait siber dalam Pendidikan menengah atas dan pendidikan tinggi di Indonesia.

Kendala yang dihadapi dalam kerjasama keamanan siber di ASEAN adalah sebagian besar dari negara anggota ASEAN belum siap untuk terlibat

dalam kerja sama keamanan cyber di tingkat regional, salah satu yang menjadi penyebabnya adalah adanya disparitas perbedaan dalam kemampuan serta penguasaan teknologi komunikasi dan informasi yang masih menghantui. Selain itu juga isu tentang keamanan siber masih belum dianggap sebagai ancaman dan permasalahan serius, atau dalam kata lain masih rendahnya *cyber security awareness* bagi kalangan baik itu pemerintah maupun swasta.

Selain kerja sama eksternal, kerja sama dan sinergitas secara internal juga menjadi sangat penting dilakukan. Yaitu dengan meningkatkan peran serta pemangku kepentingan di bidang keamanan siber eksternal Pemerintah, Swasta maupun Publik dalam pencegahan dan penanggulangan kejahatan siber.

2. Perumusan Masalah

Di tengah derasnya arus digitalisasi di semua aspek kehidupan yang ada pada *cyberspace* diperlukan adanya langkah-langkah antisipasi strategis dalam rangka mengamankan dan melindungi ruang siber Nasional. Dari tindak pelaku kejahatan siber celah kerentanan siber di Indonesia di masa pandemi ini banyak dimanfaatkan oleh pihak-pihak tertentu terutama para pelaku kejahatan siber untuk melancarkan serangan siber kondisi faktual menunjukkan bahwa pemanfaatan ruang siber nasional telah salah dimanfaatkan oleh oknum tertentu untuk menyebarkan konten-konten negatif yang menimbulkan konflik sosial yang berpengaruh terhadap stabilitas kamtibmas.

Permasalahan-permasalahan yang ada antara lain: 1) infrastruktur, 2) terbatasnya sumber daya,3) peningkatan kapasitas SDM aparat penegak hukum dan masyarakat, 4) regulasi tentang keamanan siber,5) penguatan norma yang ada di ruang siber.

Pentingnya menjaga keamanan siber sebagai perwujudan ketahanan Nasional, maka diperlukan adanya kerja sama antar negara untuk menjaga keamanan siber guna menjaga kedaulatan dalam kerangka ketahanan nasional.

Mengacu pada latar belakang yang telah diuraikan diatas pokok permasalahan yang ingin dibahas pada Taskap ini adalah "*Bagaimana upaya Indonesia dalam menjaga keamanan siber untuk memperkuat ketahanan nasional melalui kerja sama dengan negara lain?"*.

Dari permasalahan utama tersebut kemudian studi ini mencoba membaginya dalam pertanyaan kajian sebagai berikut:

a. Apakah peraturan perundang undangan yang ada sudah mendukung dalam menjaga keamanan siber Nasional
b. Bagaimana kesiapan infra struktur dan SDM dalam membangun sistem keamanan siber Nasional
c. Bagaimana Strategi kerja sama keamanan siber yang akan dilakukan dalam memperkuat ketahanan nasional?

3. Maksud dan Tujuan

a. Maksud dari penulisan Taskap ini adalah untuk memberikan gambaran strategis yang dapat digunakan sebagai bahan kajian terhadap *policy making* guna membangun ketahanan siber di Indonesia. dan membangun Kerja sama Keamanan Siber Indonesia dengan Negara Lain dalam Kerangka Ketahanan Nasional

b. Tujuan, dari Taskap ini adalah untuk memberikan saran strategis masukan dan rekomendasi kepada para pengambil keputusan nasional *(decision maker)* dalam membangun ketahanan siber di Indonesia. Dengan membangun Kerja sama Keamanan Siber Indonesia dengan Negara Lain dalam Kerangka Ketahanan Nasional

4. Ruang Lingkup dan Sistematika

a. Ruang Lingkup.

Ruang lingkup pembahasan dalam Taskap ini akan dibatasi pada persoalan kerja sama Indonesia dengan pemerintah negara-negara lain dalam hal upaya pencegahan dan penanganan kejahatan/ insiden siber, dalam rangka memperkuat ketahanan siber. Studi ini akan membicara kan bagaimana Keamanan siber di Indonesia pada periode tahun 2017

sampai dengan tahun 2021 yang diukur berdasarkan banyaknya serangan siber di Indonesia serta bagaimana tata kelola, pengembangan SDM pada Badan Siber dan Sandi Negara (BSSN) dan berbagai kebijakan nasional yang mempengaruhi kondisi keamanan siber Indonesia serta upaya kerja-sama yang telah dilakukan dengan negara lain. Keamanan siber merupakan bagian dari keamanan nasional yang tentunya mempunyai pengaruh yang kuat bagi Ketahanan Nasional di mana pada saat ini ruang siber merupakan ruang juang yang mengikutsertakan berbagai komponen dalam Negara dalam rangka mewujudkan cita cita nasional.

b. Sistematika.

1) Bab I : Pendahuluan Bab ini diuraikan tentang latar belakang masalah, maksud dan tujuan penelitian, ruang lingkup penelitian dan sistematika dengan teori-teori yang digunakan. metode dan pendekatan yang digunakan; dan definisi istilah kunci yang digunakan dalam Taskap ini.

2) Bab II: Tinjauan Pustaka. Bab ini pertama-tama menjelaskan tentang keamanan siber di Indonesia, Regulasi yang mengatur tentang keamanan siber dan juga kerangka konsep ketahanan nasional, kerja sama keamanan siber yaitu kerja sama bilateral, keamanan nasional, konsep dan teori tentang ketahanan nasional.

3) Bab III: Pembahasan. Bab ini akan menguraikan tentang bagaimana Keamanan siber di Indonesia pada periode tahun 2017 sampai dengan 2019 yang diukur berdasarkan banyaknya serangan siber di Indonesia serta bagaimana tata kelola, pengembangan SDM dan berbagai kebijakan nasional yang mempengaruhi kondisi keamanan siber Indonesia serta upaya kerja sama yang telah dilakukan dengan negara lain. Selain itu juga akan menguraikan tentang sejauh mana upaya pemerintah Indonesia dalam menjaga keamanan siber di Indonesia? Selain itu juga akan mengupas tentang sejauh mana tantangan yang dihadapi dalam menjaga

keamanan siber di Indonesia? Dan juga Bagaimana Strategi kerja sama keamanan siber yang akan dilakukan dalam memperkuat ketahanan nasional?

4) Bab IV: Penutup. Bab ini menjelaskan tentang kesimpulan dan saran dalam rangka meningkatkan keamanan siber dan juga memperkuat ketahanan Nasional

5. Metode dan Pendekatan

Dalam penulisan ini menggunakan metode deskriptif analisis, yaitu suatu metode yang menekankan pada proses penggambaran fakta-fakta yang terungkap di lapangan guna menjawab isu ketahanan Siber. Studi kepustakaan (*library research*) yang digunakan dalam studi ini adalah penelitian kepustakaan (*library research*) sebagai suatu teknik pengumpulan data dengan memanfaatkan berbagai literatur berupa perundang-undangan, buku-buku, jurnal, karya ilmiah, artikel, internet, media massa dan Taskap terdahulu dan sumber lainnya sebagai penunjang data dan fakta yang berkaitan dengan pembahasan.

6. Pengertian.

a. Kerja sama Keamanan Kerja sama Keamanan *(cooperative security)* adalah pendekatan yang dikembangkan oleh Kanada dan Australia pada awal dekade tahun 90-an sebagai cara untuk menemukan format baru dalam pengelolaan keamanan kawasan dalam menjawab perubahan-perubahan kondisi keamanan internasional sebagai dampak dari runtuhnya sistem bipolar dan bubarnya salah satu negara adidaya Uni Soviet. Hal ini dikarenakan pada masa pasca Perang Dingin munculnya sebuah harapan untuk dapat mengelola kondisi keamanan yang tidak hanya sebatas mengantisipasi terjadinya perang, tapi juga dapat membangun nilai-nilai bersama secara internasional dalam mencapai stabilitas perdamaian dan perdamaian dalam jangka Panjang.[7]

[7] Dewitt, D. (1994) Common, Comprehensive and Cooperative Security. The Pacific Review, 7, 1-15. See also, http://dx.doi.org/10.1080/09512749408719067

b. Keamanan nasional Merupakan sesuatu yang nyata di mana pemerintah dapat melakukan tindakan dengan tujuan untuk mengeliminasi kemungkinan ancaman bahaya militer atau juga lebih sering kali dipergunakan untuk mencegah terjadinya instabilitas yang ditimbulkan oleh ancaman. Hal tersebut sangat penting dikarenakan keamanan nasional sangat mempengaruhi keamanan warga negaranya. Keamanan di sini dapat ternilai dari apa yang dirasakan oleh warga negaranya yang ditinjau dari tingkat keamanannya yang meliputi merasakan adanya faktor kestabilan, ketertiban dan ketidak-adaan rasa aman. Singkatnya, keamanan nasional

sering kali diartikan kemampuan negara, untuk bisa melindungi dan mempertahankan warganya.[8]

c. Konsep Keamanan Siber Keamanan siber merujuk pada berbagai bentuk ancaman yang berasal teknologi digital dan komputasi. Sebagaimana semua kajian dalam studi keamanan, gagasan perlindungan sempurna merupakan mitos; hal tersebut juga berlaku bagi *computational-based systems* yang juga memiliki kelemahan. Beberapa pakar dan praktisi menyarankan negara untuk memperkuat infrastruktur digitalnya dan industri nasional. Namun permasalahan keamanan siber tidak hanya menjadi perhatian negara saja, namun juga individu dan korporasi. Kompleksitas adanya aktor non-negara dalam keamanan siber tidak bisa dilepaskan dari karakteristik ruang siber (*cyberspace*) yang merupakan domain baru dan tidak memiliki batasan yang mutlak bagi para aktor untuk berinteraksi dan bertindak.[9]

d. Ketahanan Nasional Menurut Suradinata dan Kaelan, ketahanan nasional adalah suatu kondisi dinamis suatu negara yang memiliki ketangguhan serta mampu mengembangkan kekuatan

---

[8] https://www.un.org/en/chronicle/article/national-security-versus-global-security#:~:text=National%20security%20has%20been%20described,this%20confine%20of%20national%20security. Diakses pada tanggal 5 Mei 2021

[9] Peter J. Denning & Dorothy E. Denning. (2010) The Profession of IT Discussing Cyber Attack. Communcations of the Acm, September 2010, Vol 53, No. 9. See., https://doi.org/10.1145/1810891.1810904, lihat juga. Denning, Dorothy E. (2010). *"Cyber Conflict as an Emergent Social Phenomenon,"* in Thomas J Holt and Bernadette Hlubik Schell (eds), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (Hershey, PA: IGI Global, 2010)

nasional dalam menghadapi dan mengatasi segala macam, gangguan, hambatan, dan tantangan yang datang dari dalam maupun luar negeri, secara langsung maupun tidak langsung, yang dapat membahayakan integritas, identitas, kelangsungan hidup berbangsa, dan bernegara serta perjuangan bangsa dalam menjaga tujuan nasional. Meskipun sebenarnya, konsep ketahanan mempunyai lingkup yang luas, yang salah satunya adalah kapasitas sistem untuk memelihara fungsi dan strukturnya dari perubahan eksternal maupun internal.[10]

[10] L. Carlson G. Bassett, et al (2012). Resilience: theory and application. Argonne National Laboratory. Oak Ridge, p, 11

BAB II
TINJAUAN PUSTAKA

7. Umum

Taskap ini akan melihat berbagai peraturan perundangundangan yang terkait dengan keamanan Nasional dan keamanan siber. Beberapa teori dasar inti dan tinjauan pustaka juga akan diartikulasikan untuk memberikan kerangka teoritis dan dasar logis serta untuk menjawab pertanyaan penelitian yang ada dalam Taskap ini. Di antaranya adalah terkait dengan ancaman keamanan Nasional yang kemungkinan muncul di Indonesia dan bagaimana upaya pemerintah Indonesia dalam menjaga keamanan siber, juga bagaimana tantangan yang dihadapi dalam menjaga keamanan siber di Indonesia serta bagaimana strategi kerja sama keamanan siber yang akan dilakukan dalam memperkuat ketahanan nasional.

Tulisan Ilmiah ini berusaha untuk mengulas kerja sama Indonesia dengan negara-negara lain dalam hal upaya pencegahan dan penanganan kejahatan/ insiden siber, yaitu melalui kerja sama bilateral. Selain kerja sama bilateral, di lingkup regional melalui ASEAN dapat mempertimbangkan beberapa bentuk kerja sama terutama dalam upaya untuk membangun sinergi keamanan siber di wilayah Asia Tenggara. Platform kerja sama dalam lingkup ASEAN dapat memberikan masukan yang bermanfaat untuk membuat platform kerja sama keamanan siber ASEAN di masa depan; Namun untuk isu tersebut ASEAN harus membuat beberapa penyesuaian sehingga platform akan diterima oleh anggota ASEAN[11].

Selain itu juga, dalam Taskap ini berusaha untuk memberikan gambaran secara teoritis terutama terkait dengan bagaimana keamanan siber di Indonesia pada periode tahun 2017 sampai dengan 2021.

[11] Salah satu hasil riset yang memberikan rekomendasi terkait pentingnya platform kerja sama di lingkup ASEAN adalah artikel yang ditulis oleh Rahmat Haryama (2020) yang berjudul *"Asean Cyber Security Platform Kerja sama Keamanan Dunia Cyber Dikawasan ASEAN"*, Peperangan Asimetris, Fakultas Strategi Pertahanan Universitas Pertahanan Indonesia

8. Peraturan Perundang-Undangan

a. Dasar Hukum Pembentukan Badan Siber dan Sandi Negara (BSSN)

Mengingat pentingnya pembentukan lembaga yang menangani ketahanan dan keamanan siber untuk menjamin dan mewujudkan pertahanan siber nasional, pemerintah sebelum membentuk Badan Siber dan Sandi Negara (BSSN) telah memberikan wewenang kepada TNI untuk membentuk Satuan Siber TNI (Satber TNI). Satuan tersebut bertugas menyelenggarakan kegiatan dan operasi siber dilingkungan TNI dalam rangka mendukung tugas pokok TNI yang tertuang dalam Pasal 46A Peraturan Presiden No. 62 Tahun 2016 tentang Susunan Organisasi Tentara Nasional Indonesia[12].

Sementara itu dalam Pasal 23 huruf o Peraturan Kapolri No. 6 Tahun 2017 bahwa pertahanan siber juga menjadi tugas Polri dalam menjalankan fungsinya untuk melakukan pencegahan, penanggulangan dan penegakan hukum pada masyarakat dan lembaga-lembaga lainya. Peraturan Kapolri tersebut kepolisian telah membentuk divisi Teknologi Informasi dan Komunikasi, dan yang lebih khusus adalah Direktorat Tindak Pidana Siber (Dittipidsiber) yang berada dalam naungan Badan Reserse Kriminal Polri. Dittipidsiber bertugas melaksanakan penyelidikan dan penyidikan tindak pidana khusus yang terkait dengan kejahatan siber, tindak pidana informasi dan transaksi elektronik, tindak pidana telekomunikasi termasuk kejahatan transnasional terkait dengan kejahatan siber.[13]

Dasar pembentukan Badan Siber dan Sandi Negara (BSSN) adalah melalui Presiden Republik Indonesia pada tanggal 19 Mei 2017 menandatangani Perpes Nomor 53 tahun 2017 tentang BSSN yang selanjutnya disempurnakan dengan Perpres Nomor 133 tahun 2017 tentang BSSN pada 16 Desember 2017. Dengan demikian fokus penanganan

---

[12] Dokumen tersebut diakses oleh penulis pada tanggal 2 Juni 2021. Mengenai Peraturan Presiden No. 62 Tahun 2016 tersebut dapat diakses dalam tatan berikut ini: https://peraturan.bpk.go.id/Home/Details/40966/perpres-no-62-tahun-2016

[13] Pasal 23 huruf o Peraturan Kapolri No. 6 Tahun 2017, diakses pada tanggal 3 Juni 2021. Terkait dengan dokumen tersebut dapat diakses melalui taurtan berikut ini: https://humas.polri.go.id/download/perkap-no-6-tahun-2017-ttg-susunan-organisasi-dan-tata-kerja-satuan-organisasi-pada-tingkat-mabes-polri/#

kejahatan siber dan keamanan siber juga melekat pada badan negara yang mengurus tentang keamanan siber dan sandi negara yaitu dengan dibentuknya BSSN. Perpres Nomor 133 tahun 2017 tersebut kemudian disempurnakan dan diperbaharui melalui Perpres Nomor 28 Tahun 2021 Tentang Badan Siber dan Sandi Negara.[14] Dalam Peraturan Presiden Nomor 28 tahun 2021 tersebut tugas BSSN adalah melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan. Selain itu juga BSSN juga melakukan identifikasi, deteksi, proteksi, penanggulangan, pemulihan, dan pemantauan insiden keamanan siber dan sandi nasional, serta pengelolaan krisis siber nasional.

Setelah terbitnya Perpres Nomor 28 Tahun 2021 yang bertujuan untuk melakukan penataan organisasi BSSN dalam rangka mewujudkan keamanan, perlindungan, dan kedaulatan siber nasional serta meningkatkan pertumbuhan ekonomi nasional. Perpres tersebut diterbitkan untuk mengoptimalkan pelaksanaan tugas dan fungsi di bidang keamanan siber dan sandi dalam organisasi BSSN sehingga dapat dilakukan dengan lebih efektif dan efisien.

Di dalam Perpres Nomor 28 Tahun 2021 Tentang Badan Siber dan Sandi Negara termuat perumusan dan penetapan kebijakan teknis di bidang keamanan siber. Selain itu juga memuat fungsi BSSN dalam melakukan pelaksanaan kebijakan teknis di bidang tata kelola, manajemen risiko, pengembangan ekosistem, dan pengukuran tingkat kematangan keamanan siber.

b. Regulasi Keamanan Siber

Regulasi tentang keamanan siber mengacu pada beberapa undang-undang, diantaranya adalah: Undang-undang nomor 36 tahun 1999 tentang

[14] Dokumen terkait Peraturan Presiden Nomor 28 tahun 2021 tersebut dapat diakses melalui tautan berkut ini: https://jdih.bssn.go.id/arsip-hukum/perpres-nomor-28-tahun-2021-tentang-badan-siber-dan-sandi-negara.

Telekomunikasi; dalam undang-undang tersebut terutama pada Bab 3 pasal 4 menekankan pada penetapan kebijakan, pengaturan, pengawasan dan pengendalian di bidang telekomunikasi. Lebih spesifik lagi Bab 4 pasal 7 menekankan pada upaya penyelengaraan komunikasi yang bertujuan untuk melindungi kepentingan dan keamanan negara.

Selain itu juga terdapat undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian diubah dengan undang-undang nomor 19 Tahun 2016 UU tersebut banyak membahas bagaimana pengaturan transaksi elektronik, yang mencakup perniagaan elektronik yang mana keamanan siber juga menjadi salah satu hal yang sangat penting untuk dibangun oleh semua lembaga baik dari pemerintah, swasta dan juga masyarakat luas.

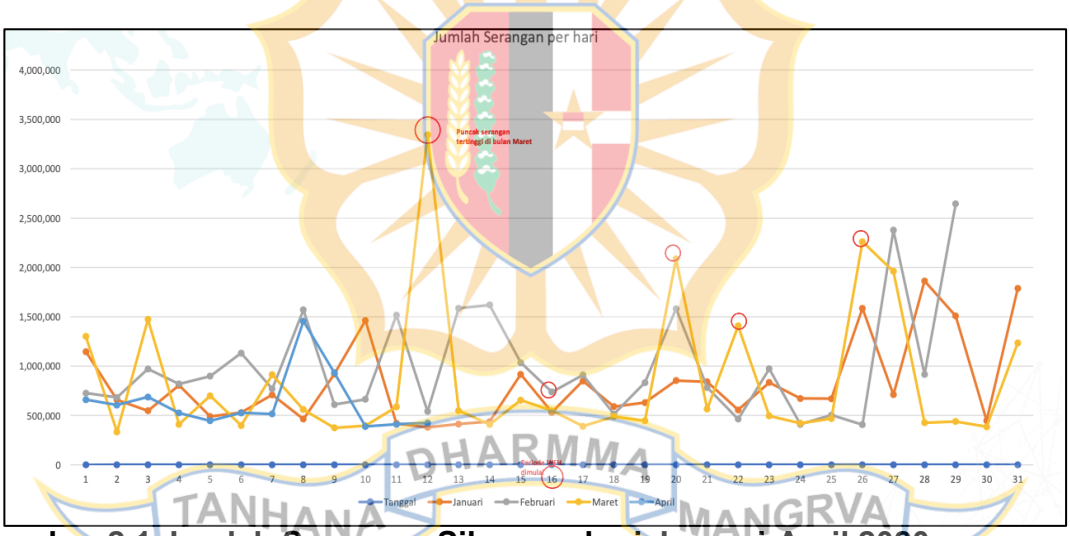
Undang-Undang No. 19 Tahun 2016 yang disahkan pada tanggal 25 November 2015 merupakan solusi konstitusional dari negara dalam rangka membangun etika bagi pengguna media dan juga memberikan kepastian hukum terhadap persoalan-persoalan yang disebabkan oleh lemahnya keamanan dan ketahanan siber terutama yang terkait dengan kejahatan siber. Sesuai dengan sistem hukum Indonesia yang dianut Indonesia yakni *civil law*, maka UU No. 19 Tahun 2016 merupakan peran nyata pemerintah guna memberikan pengaturan bagi kondisi obyektif dimana banyak di media sosial muatan yang melanggar hukum, kesusilaan, pencurian data pribadi, pembobolan situs, pencurian rekening, perjudian online, mengakibatkan kerugian masyarakat dalam Transaksi Elektronik. Keberadaan UU tersebut diharapkan mampu memberikan perlindungan terhadap keadilan, ketertiban umum, dan kepastian hukum pada seluruh pihak baik pemerintah, dunia usaha dan dunia industri (DUDI).

Mengingat pentingnya pertahanan dan keamanan siber, maka ada beberapa regulasi yang juga menekankan pada upaya keamanan siber, salah satunya adalah Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik pada Pasal 61 bagaimana standar

jasa sistem pembayaran dan sistem elektronik harus memenuhi keamanan siber.[15]

9. Data dan Fakta

Tingginya kejahatan siber di Indonesia menjadi perhatian serius dari dunia Internasional, kasus terbaru insiden siber yang terjadi adalah terkait kebocoran data BPJS Kesehatan yang menjadi sorotan media Nasional dan Internasional. Diketahui, sebanyak 279 juta data penduduk Indonesia diduga bocor dan dijual di forum peretas Raid Forums pada tanggal 12 Mei 2021. Juru Bicara Kementerian Komunikasi dan Informatika (Kominfo) Dedy Permadi mengatakan bahwa temuan itu berasal dari analisis yang dilakukan terhadap satu juta sampel data yang dibagikan secara gratis oleh akun bernama Kotz. Ia mengatakan ada 100.002 data penduduk Indonesia yang telah terkonfirmasi dari satu juta data itu. Bahwa 100.002 data pribadi ini diduga kuat berasal dari data BPJS Kesehatan.[16]



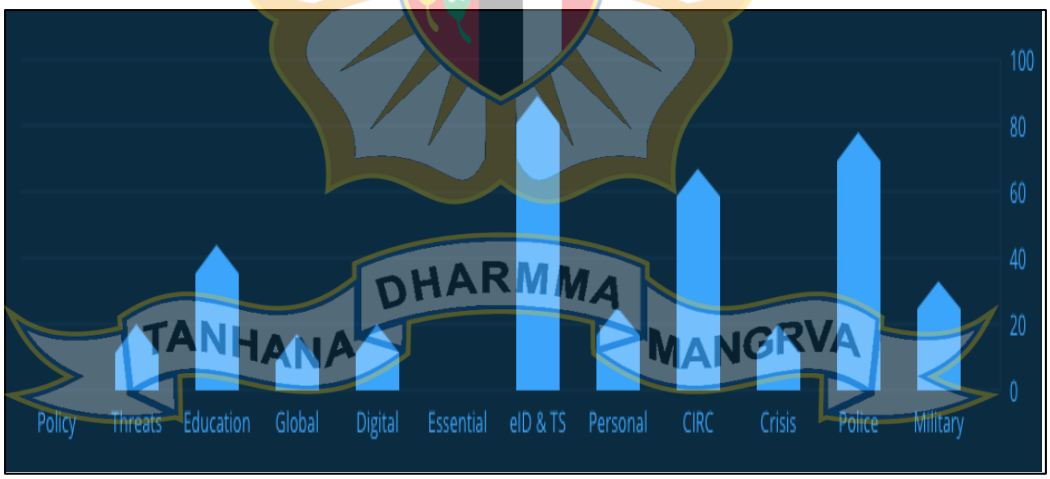
Gambar 2.1 Jumlah Serangan Siber per hari Januari-April 2020
Sumber: BSSN, 2020

[15] Dalam Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik pada Pasal 61 secara lengkap berbunyi: Penyelenggara jasa sistem pembayaran wajib mematuhi standar level keamanan Sistem Elektronik sesuai dengan ketentuan peraturan perundang-undangan. (2) Penetapan standar level keamanan sebagaimana dimaksud pada ayat (1) ditentukan oleh kepala lembaga pemerintah yang menyelenggarakan urusan pemerintahan di bidang keamanan siber dan sandi negara, Gubernur Bank Indonesia, dan/atau Ketua Otoritas Jasa Keuangan.

[16] Ulasan News dari CNN Indonesia tentang "Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat", diakses pada Minggu 6 Juni 2021. Untuk lebih detailnya dapat dilihat pada tautan berikut: https://www.cnnindonesia.com/teknologi/20210606200515-185-650991/kebocoran-data-pribadi-bpjs-kesehatan-bakal-digugat

Berdasarkan laporan dari Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Data yang disampaikan oleh BSSN menunjukan bulan Januari terpantau 25.224.811 serangan dan kemudian pada bulan Februari terekam 29.188.645 serangan lalu kemudian pada bulan Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020 telah tercatat 7.576.851 serangan. Puncak jumlah serangan terjadi pada tanggal 12 Maret 2020 yang mencapai 3.344.470 serangan dan setelah itu jumlah serangan mengalami penurunan yang cukup signifikan saat diberlakukannya kebijakan *work from home* (WFH) di berbagai tempat.[17]

Sementara dari aspek cyber security readiness, berdasarkan data yang disajikan oleh National Cyber Security Index tahun 2020 peringkat Indonesia ada di posisi 77 dengan skor 38,96. Berikut ini adalah grafik yang menunjukan indicator penilaian cyber security index yang disajikan oleh NCSI 2020.



Gambar 2.2 Indicator Penilaian Cyber Security Index 2020

Sumber: National Cyber Security Index tahun 2020

Data yang ada pada grafik di atas menunjukan detail indikator penilaian cyber security index dilihat dari berbagai aspek diantaranya: a) *Cyber security policy development*, nilai persentase ini masih 0%, b) *Cyber threat*

[17] Rilis ini disampaikan oleh BSSN. Untuk lebih detailnya dapat dilihat dalam tautan berikut ini: https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

analysis and information yaitu sebesar 20%, c) *Education and professional development* sebesar 44%, d) *Contribution to global cyber security* sebesar 17%, *e) Protection of digital services* sebesar 20%, f)*Protection of essential services* sebesar *0%,* g)*E-identification and trust services* sebesar 89%, h)*Protection of personal data* sebesar 25%, i) *Cyber incidents response* sebesar 67%, j)*Cyber crisis management* sebesar 20%, k)*Fight against cybercrime* sebesar 78% dan *l)Military cyber operations* sebesar 33%.[18]

Melihat kondisi faktual tersebut di atas menunjukan bahwa keamanan siber menjadi isu yang sentral dan strategis yang memerlukan upaya-upaya kerja sama dan sinergitas baik dari dalam negeri ataupun kerja sama yang bersifat bilateral, regional maupun multilateral dengan didukung oleh kebijakan, strategi, SDM, kekuatan infrastruktur serta pendanaan yang memadai.

10. Kerangka Teoritis

Dalam taskap ini, penulis merumuskan kerangka teoritis yang bertujuan untuk memberikan jawaban atas pertanyaan penelitian yang telah dibahas pada bab 1. Secara umum dalam melihat persoalan tentang keamanan siber di Indonesia, terutama terkait dengan ancaman keamanan Nasional yang kemungkinan muncul di Indonesia dan bagaimana upaya pemerintah Indonesia dalam menjaga keamanan siber serta bagaimana kerja sama keamanan siber yang akan dilakukan dapat memperkuat ketahanan nasional.

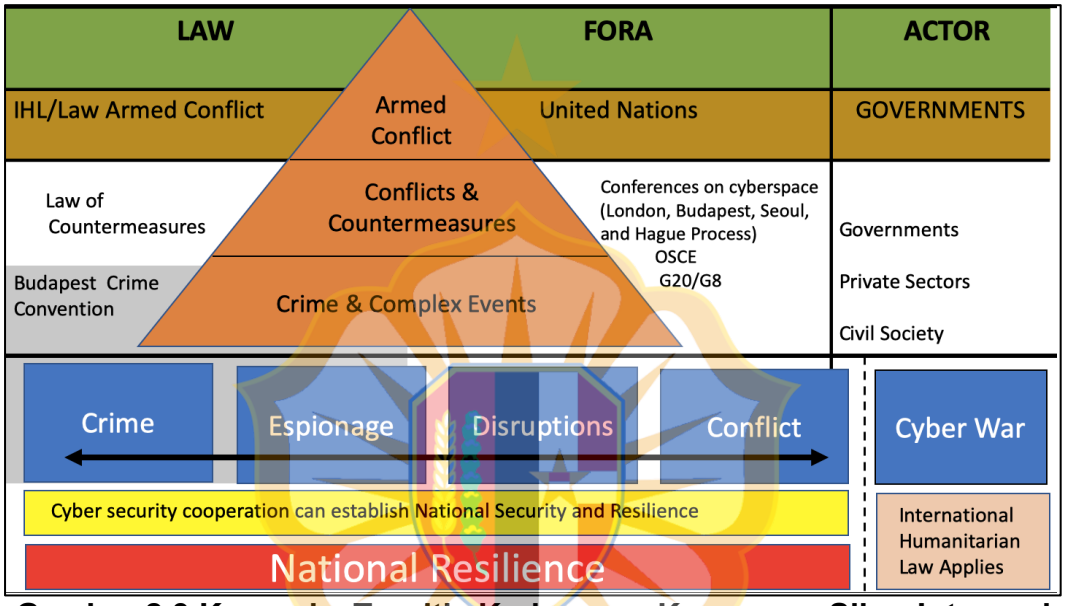
Selain itu juga, kerangka teoritis tersebut digunakan untuk melihat secara sistematis dan logis bagaimana tantangan yang dihadapi dalam menjaga keamanan siber di Indonesia serta bagaimana peraturan dan perundang undangan yang ada sudah mendukung dalam menjaga keamanan siber Nasional.

[18] Mengenai detail laporan National Cyber Security Index tahun 2020 dapat dilihat dalam laporan yang disajikan oleh NCSI dan dapat diunduh pada tautan berikut: https://ncsi.ega.ee/country/id/470/#details

Perspektif yang digunakan dalam melihat keamanan siber di Indonesia adalah aspek norma hukum internasional yang belum terbentuk untuk sehingga kesepakatan bilateral antara kedua negara sangat penting untuk dikedepankan dalam mengatur keamanan siber. Di tingkat global, baik pemerintah maupun aktor non-negara menjadi semakin penting terutama di dalam *cyber space*, dengan kemampuan untuk terlibat dalam kegiatan seperti spionase, dan serangan lintas batas lainnya yang sering disebut sebagai *cyber war*. Secara teoritis sistem hukum internasional berusaha untuk meminta pertanggungjawaban aktor atas tindakan kejahatan siber yang mereka lakukan. Salah satu hasil kesepakatan internasional yang adalah Budapest Convention dimana perjanjian internasional ini merupakan pertama yang berupaya mengatasi kejahatan siber/Internet dan komputer dengan menyelaraskan hukum nasional, meningkatkan teknik investigasi, dan meningkatkan kerja sama antar negara.

Dalam kerangka teoritis ini dapat dilihat bahwa aktor yang juga memegang peranan penting adalah pemerintah dalam hal ini BSSN, aparat penegak hukum Polri harus bersinergi dalam melakukan pencegahan, dan penegakan hukum pada tindak kejahatan siber. Selain beberapa hal tersebut di atas, penulis akan mencoba mengulas tentang strategi keamanan siber Indonesia. Dimana menyangkut beberapa aspek diataranya bagaimana pembentukan organisasi dan tata kelola. Dari sini akan dilihat peran sentral BSSN dengan melakukan langkah-langkah sinergitas beberapa institusi seperti TNI, Polri, DUDI, NGOs serta masyarakat dalam upaya melakukan sosialisasi pencegahan kejahatan siber dan upaya untuk membangun *cyber security awareness*.

Lebih detailnya penulis menyajikan kerangka analisis pada gambar 2.3 yang bertujuan untuk menganalisis persoalan tentang sejauh mana kerja sama internasional mampu mendorong *collaborative action* dan sinergitas dalam menciptakan keamanan siber. Selain itu juga bagaimana peran masing-masing aktor seperti kalangan pemerintah, *private sector*, dan masyarakat umum memiliki peran yang strategis dalam menjaga keamanan siber nasional menuju kedaulatan siber dalam kerangka ketahanan Nasional.



Gambar 2.3 Kerangka Teoritis Kerja sama Keamanan Siber Internasional

Sumber: Andi Wijayanto, 2016, dalam Makalah Keamanan Siber: Kerja sama Internasional, dikembangkan oleh Penulis

11. Keamanan Nasional

Sebelum membahas pada aspek keamanan nasional penulis akan mencoba melihat terminologi keamanan yang memiliki pegertian universal dan beraneka ragam. Ditinjau dari tatarannya, paling tidak dikategorikan sebagai berikut: "(1) *International Security* dan *Global Security* untuk level dunia (2) *National (State) Security* untuk level negara, (3) *Pubic Security (and order)* untuk level masyarakat, dan (4) *Human Security* untuk level individu. Sedangkan berdasarkan aspek ruang dan wilayah konsep

keamanan dibagi menjadi empat bagian yakni keamanan nasional, regional, internasional dan global".[19]

Keamanan nasional merupakan pertanggung jawaban fundamental bagi setiap pemerintah. Tanpa adanya rasa aman, masyarakat tidak akan percaya dengan pemerintah ataupun pada lingkungan di sekitar mereka, masyarakat tidak akan fokus pada pencapaian tujuan hidup mereka atau tujuan yang lebih tinggi dan tujuan dasar mereka serta menyiapkan masa depan mereka. Tanpa adanya keamananan yang menjadi dasar kebutuhan masyarakat, dapat menyebabkan tingginya ketidak percayaan masyarakat terhadap pemerintah.[20]

Terminologi tentang keamanan Nasional tertuang dalam dalam *International Encyclopedia of the Social Sciences* mendefinisikan keamanan sebagai "kemampuan suatu bangsa untuk melindungi nilai-nilai internalnya dari ancaman luar".[21] Keamanan nasional akan diidentifikasi sebagai "keamanan negara"–dengan asumsi bahwa negara tidak lagi menghadapi gugatan atas legitimasinya–maka ia perlu mengandung sedikit-dikitnya tiga komponen: kedaulatan wilayah, lembaga-lembaga negara (termasuk pemerintahan) yang dapat berfungsi sebagaimana mestinya; dan terjaminnya keselamatan, ketertiban serta kesejahteraan masyarakat[22].

Ketika melihat perjalanan sejarah pasca perang dingin, isu tentang keamanan nasional telah mengalami berbagai macam dinamika, pada masa perang dingin isu keamanan nasional terkait pada isu keamanan nasional yang diakibatkan karena adanya dampak yang disebabkan oleh

---

[19] John Baylis, *"International and Global Security in The Post-Cold War Area*, dalam *The Global of World Politic: An Introduction to International Relations Third Edition*, Ed John Baylis dan stave Smith,. New York: Oxford University Press, 2008 hal 300 dan lake and Morgan dalam Buzan, dkk, 2003, hal 10. Penulis mengutipnya dalam Yayan M. Yani, Ian M, Emil M, *"Pengantar Studi Keamanan"*, Intrans Publishing, Malang, 2017, hal 4.

[20] Cynthia A. Watson (2008) dalam *U.S National Security, A Reference Handbook, Second Edition*, (Contemporary world issues), ABC-CLIO, Inc, Santa Barbara, California 93116-1911, pg. 1-2.

[21] International Encyclopedia of the Social Sciences (1968), Volume 11, Editor, David L. Sills, The Macmillan Company & The Free Pres pg. 40.,

[22] Kusnanto Anggoro (2003), *"Keamanan Nasional, Pertahanan Negara, dan Ketertiban Umum"*, Centre for Strategic and International Studies, Jakarta, Makalah Pembanding Seminar Pembangunan Hukum Nasional VIII. diselenggarakan oleh Badan Pembinaan Hukum Nasional, Departemen Kehakiman dan HAM RI Hotel Kartika Plaza, Denpasar, 14 Juli 2003.

peperangan, dengan demikian aspek keamanan militer kala itu menjadi fokus dan agenda besar setiap negara di belahan dunia.

Mely Caballero-Anthony (2004) menyebutkan minimal ada tiga pandangan tentang keamanan, yaitu: “Pandangan pertama adalah yang beranggapan bahwa ruang lingkup keamanan adalah lebih luas daripada semata-mata keamanan militer *(military security).* Pandangan kedua adalah menentang perluasan ruang lingkup daripada keamanan dan lebih cenderung konsisten dengan *status-quo*. Pandangan ketiga tidak saja memperluas cakupan bahwa keamanan adalah lebih luas dari semata-mata ancaman militer dan ancaman negara, namun juga berusaha untuk memperlancar proses pencapaian emansipasi manusia *(human emancipation)”*[23]. Emansipasi manusia bermakna: “pembebasan manusia, baik sebagai individu maupun bagian dari kelompok) dari keterbatasan fisik dan kemanusiaannya yang menghentikan upaya mereka untuk memperoleh kenikmatan dari hal-hal yang sepatutnya mereka dapatkan”.[24]

Keamanan nasional merupakan tanggung jawab yang melekat pada TNI hal tersebut sesuai dengan Undang-Undang Nomor. 34 tahun 2004 tentang TNI yang tertuang dalam pasal 7 ayat (1), di mana tugas pokok TNI adalah menegakkan kedaulatan negara, mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia yang berdasarkan Pancasila dan Undang-Undang Dasar Republik Indonesia Tahun 1945, serta melindungi segenap bangsa dan seluruh tumpah darah Indonesia dari ancaman dan gangguan terhadap keutuhan bangsa dan negara. Upaya untuk mempertahankan kedaulatan NKRI yang bernafaskan Pancasila dan UUD 1945 tidak sebatas pada pemeliharaan, menegakan keamanan dan ketertiban masyarakat saja, kedepan persoalan keamanan nasional akan jauh lembih komples dan semakin berat tantanganya seiring dengan perkembangan teknologi, komunikasi dan informasi.

---

[23] Mely Caballero-Anthony (2004), Non-state regional governance mechanism for economic security: the case of the ASEAN Peoples' Assembly, *The Pacific Review Journals,* Pages 567-585 | Published online: 11 Aug 2006, https://doi.org/10.1080/0951274042000326078

[24] Booth, dalam Ibid 2004.

Sejak tragedi 11 September 2001, bangsa-bangsa di Dunia telah memusatkan perhatian dan sumber dayanya pada isu-isu yang penting bagi keamanan nasional, fokus mereka telah diarahkan pada pencegahan terhadap serangan teroris, terutama serangan yang mungkin menggunakan perangkat penyebaran bahan kimia, biologi, nuklir atau radiologi, atau bom serta senjata pemusnah masal lainya. Para pemimpin dunia juga menyadari bahwa setiap negara rentan terhadap teroris yang akan memanfaatkan strategi serangan terorisme dengan senjata kimia dan senjata pemusnah masal.

Artinya, infrastruktur penting berada dalam risiko dan membutuhkan perlindungan dan kewaspadaan yang terus menerus.[25] Dengan demikian isu keamananan nasional sudah mengarah kepada upaya pencegahan, penanggunalangan dan penanganan tindakan terorisme yang dapat mengancam dan membahayakan kondisi sosial, politik, ekonomi dan juga sektor lainnya.

Seiring dengan berkembangnya teknologi, informasi dan *science*, yang terus bergerak eksponensial, isu tentang keamanan nasional juga mengalami dinamika dan pergeseran yaitu munculnya *cyber war* yang berpotensi memicu konflik di beberapa negara. Sebagai contohnya adalah ketegangan dan konflik yang terjadi antara etnis Rusia yang tinggal di Estonia dan penduduk asli Estonia sendiri telah meningkat sejak negara kecil itu kembali mendeklarasikan kemerdekaannya pada akhir Perang Dingin. Mayoritas orang Estonia berusaha menghilangkan simbol-simbol dari lima dekade yang menindas di mana mereka dipaksa menjadi bagian dari Uni Soviet. Konflik tersebut telah bergeser menuju ruang siber.[26]

Beberapa pandangan tentang pentingnya menjaga keamanan nasional melalui keamanan siber juga pernah dikemukakan oleh beberapa pemimpin dunia, diantaranya Presiden Obama mengeluarkan deklarasi bahwa

---

[25] Cynthia A. Watson (2008) dalam *U.S National Security, A Reference Handbook, Second Edition*, (Contemporary world issues), ABC-CLIO, Inc, Santa Barbara, California 93116-1911, pg.7-8.

[26] Lebih detainya dapat dilihat dalam Dan Constantin Tofan, Maria Lavinia Andrei, Lavinia Mihaela Dinca (2012) dalam *Cyber Security Policy. A methodology for Determining a National Cyber-Security Alert Level*, Informatica Economică vol. 16, no. 2/2012 pg. 103-115.

"ancaman dunia maya adalah salah satu tantangan ekonomi dan keamanan nasional paling serius yang kita hadapi sebagai sebuah bangsa" dan bahwa "kemakmuran ekonomi Amerika di abad ke-21 akan bergantung pada keamanan siber".[27]

Fokus keamanan dan ketahanan siber telah menjadi perhatian serius oleh Kementrian Pertahanan di mana pada tanggal 17 Oktober 2014, Menteri Pertahanan telah menerbitkan buku tentang "Pedoman Pertahanan Siber", dalam buku tersebut telah memuat beberapa hal. Seperti: "pencegahan serangan, pemantauan pengamanan informasi, analisis serangan, sampai pada level serangan balik. Pada dasarnya buku tersebut disusun sebagai lampiran atas Peraturan menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber".[28]

Dengan demikian isu keamanan nasional di era revolusi Industri 4.0 sudah bergeser menuju isu tentang keamanan siber, dimana masing-masing lembaga, badan, unsur dalam negara harus mampu berfikir untuk melakukan *collaborative action*. Terlepas dari penguasaan pengetahuan khusus yang dilakukan oleh negara yang dibutuhkan dalam menciptakan keamanan nasional dengan merancang keamanan siber, dengan demikian dalam domain siber mencegah satu orang atau kelompok untuk menjalankan kendali penuh terhadap sistem siber. Upaya untuk mengurangi ancaman dari kejahatan siber itu mungkin dilakukan dan akan membutuhkan kerja sama internasional.

12. Kerja sama Keamanan

Istilah Kerja sama Keamanan *(cooperative security)* telah menjadi frase populer sejak berakhirnya Perang Dingin. Frase ini biasanya digunakan untuk menggambarkan pendekatan keamanan yang lebih memprioritaskan

[27]"White House: Cybersecurity". whitehouse.gov – via National Archives.

[28] Pedoman Pertahanan Siber menjadi acuan dasar bagi Kementerian Pertahanan/TNI dalam rangka penyelenggaraan pertahanan siber. dapat dibuka dalam tautan berikut: https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf
Dokumen tersebut diakses oleh penulis pada tanggal 2 Juni 2021

perdamaian, tetapi tetap mengedepankan sisi idealisme melalui peningkatan harmoni dan kerja sama internasional.[29]

Kerja sama keamanan *(cooperative security)* biasanya mencakup empat "lingkaran keamanan" yang konsentris dan saling memperkuat: Keamanan Individu, Keamanan Kolektif, Pertahanan Kolektif, dan Mendorong Stabilitas.[30]

Pada dasarnya tujuan utama dari kerja sama keamanan *(cooperative security)* adalah untuk mencegah perang dan meminimalkan sarana untuk agresi. Dengan demikian, Kerja sama keamanan *(cooperative security)* menggantikan inti dari perencanaan keamanan dari bersiap untuk melawan ancaman hingga mencegah munculnya ancaman dari mencegah agresi hingga membuat persiapan untuk itu menjadi lebih sulit. Pada dasarnya kerja sama keamanan *(cooperative security)* lebih mengedepankan pencegahan terjadinya konflik antar negara ketimbang melakukan langkah-langkah diplomasi lainnya yang bersifat penanganan konflik atau peperangan.[31]

Ada beberapa alasan mengapa negara melakukan kerja sama dengan negara lainnya (Wowor, 2008: 34): "*pertama*, dengan alasan untuk meningkatkan kesejahteraan ekonomi dimana banyak negara yang melakukan kerja sama dengan negara lainnya untuk mengurangi biaya yang harus ditanggung negara tersebut dalam memproduksi suatu produk kebutuhan bagi rakyatnya karena adanya keterbatasan sumber daya yang dimiliki negara tersebut; *kedua* , untuk meningkatkan efisiensi yang berkaitan dengan pengurangan biaya; ketiga , karena adanya berbagai masalah yang mengancam keamanan bersama; *keempat*, dalam rangka

---

[29] By Richard Cohen and Michael Mihalka (2001) Cooperative Security: Individual Security to International Stability, George C. Marshall Center for Security Studies, George C. Marshall Center, pg. 1

[30] Ibid, pg. 2

[31] Ashton Carter/William Perry/John D. Steinbrunner., 2000., A New Concept of Cooperative Security; Brookings Institution, Washington D.C. 1992; p. 7 .This definition coincides with the authors earlier distinction between "preventive" and "repressive" instruments of security policy; see H.Vetschera, "International Law and International Security -The Case of Force Control", in: J. Delbrück (ed.), German Yearbook of International Law, vol. 24, Berlin, 1982.

mengurangi dampak negatif yang diakibatkan oleh tindakan-tindakan individual negara yang berakibat terhadap negara lain".

Seiring dengan perubahan tata geopolitik dunia hari ini kerja sama keamanan *(cooperative security)* telah banyak melibatkan dan dilakukan beberapa wilayah regional, salah satunya adalah ASEAN. Pasca perang dingin, ASEAN memprakarsai untuk memajukan kerja sama antara para anggotanya dan kekuatan eksternal, dengan demikian mengembangkan *cooperative security* yaitu dengan menginisiasi dialog keamanan regional yaitu melalui ASEAN Regional Forum (ARF) yang pertama kali diadakan pada tahun 1994 dan ini merupakan inti dari inisiatif ASEAN.[32]

Kerja sama keamanan *(cooperative security)* pada saat sekarang sangat mendesak tidak hanya dalam kerangka keamanan secara umum karena serangan siber termasuk kepada isu keamanan non tradisional. Untuk itulah perlu adanya kerangka pemahaman bersama khususnya bagi negara-negara anggota ASEAN untuk membangun kesadaran bersama terkait bahaya laten ancaman keamanan siber. Untuk menyikapi hal tersebut kerja sama keamanan siber di tingkat ASEAN adalah sebuah keniscayaan. Berdasarkan data yang penulis himpun, pada bulan Mei 2017 yang lalu, dilaporkan bahwa Indonesia, Malaysia, Thailand dan Vietnam telah diserang oleh *ransomware.*[33]

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. Di luar Kawasan ASEAN, beberapa negara yang dari segi kapasitas perekonomian dan teknologi telah maju juga telah memiliki

---

[32] Hiro Katsumata (2009) , *ASEAN's Cooperative Security Enterprise Norms and Interests in the ASEAN Regional Forum*, Palgrave Macmillan in the UK, pg.3

[33] Untuk lebih detailnya dapat dilihat pada tautan berikut:
The Straits Times Asia,Cyber attack: Ransomware cases reported in Asia,
http://www.straitstimes.com/asia/east-asia/cyber-attack-ransomware-cases-reported-in-asia,

Undang-Undang tentang Keamanan Siber secara tersendiri. Diantaranya Russia, Swiss, China, Uni Eropa, Amerika Serikat, dan Jepang[34].

Guna menangani ancaman siber di ASEAN, pada level bilateral dan regional telah banyak aksi yang dilakukan oleh ASEAN diantarannya, ASEAN ICT Masterplan 2015, The ASEAN Cyber Capacity Programme, *Mactan Cebu Declaration Connected ASEAN: Enabling Aspirations* dan berbagai dokumen lainnya. Namun, sejauh ini aksi yang dilakukan oleh ASEAN dalam menanggulangi ancaman siber masih dalam sebatas pembuatan legal dokumen dan peningkatan kerja sama dalam penegakan hukum. ASEAN masih memerlukan upaya yang lebih komprehensif dan usaha yang lebih nyata dalam menanggulagi ancaman siber dibandingkan hanya sebatas pembuatan dokumen.[35]

13. Cyber Security

Keamanan siber *(cyber security)* telah menjadi masalah sehari-hari yang sering kali ditemui di mana saja, mulai dari adanya berita yang memuat *spam, scam*, penipuan, dan pencurian identitas, hingga berbagai artikel akademis yang membahas isu perang siber, spionase siber, dan pertahanan siber.[36]

Persoalan *cyber security* sering dianggap sebagai persoalan sederhana karena hanya dilihat dari persoalan keamanan jaringan atau keamanan data individu, dimana sebenarnya persoalan keamanan siber dapat menjadi persoalan besar dan rumit, karena berhubungan langsung dengan keamanan negara, masyarakat, bangsa, dan ekonomi baik lingkup nasional maupun internasional.[37]

---

[34] Dikutip dari Naskah Akademik Rancangan Undang-undang Keamanan dan Ketahanan Siber yang di susun oleh DPR RI. Dokumen dapat diunduh pada tautan berikut ini: https://www.dpr.go.id/doksileg/proses1/RJ1-20190617-025848-5506.pdf

[35] James Lewis, "Hidden Arena: Cyber Competition and Conflct in Indo-Pacifi Asia," prepared for the Lowy Institute MacArthur Asia Security Project, March 7, 2013

[36] Dunn-Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: threat Representations with an impact in Cyber-Security Discourse. International Studies Review, 15: pp. 105-122

[37] Hansen, L. & Niessanbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53: pp. 1155-1175

Terminologi keamanan siber dapat dilihat dari dua kata kunci yaitu siber dan keamanan. Berbicara tentang dunia maya (*cyber space*) selalu berkaitan dengan informasi, koneksi (telekomunikasi, jaringan), *gateway* (komputer, perangkat, pengguna), ruangan atau ruang, melibatkan, menggunakan, atau berhubungan dengan komputer, jaringan, internet. Sedangkan keamanan berkaitan dengan perlindungan berbagai aset. Jadi keamanan siber melindungi aset, melindungi komputer, jaringan, program, dan data dari akses yang tidak diinginkan atau tidak sah, perubahan atau penghancuran, melindungi informasi dan sistem dari ancaman keamanan siber[38]

Cyber-security adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna[39].

Cyber-security lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)* informasi. Mekanisme ini harus bisa melindungi informasi baik dari *physical attack* maupun *cyber-attack*. *Cyber-security* merupakan upaya untuk melindungi informasi dari adanya *cyber-attack*, adapun elemen pokok *cyber-security* adalah: Dokumen *security policy, Information infrastructure, Perimeter Defense, Network Monitoring System, System Information and Event Management, Network Security Assessment, Human resource dan security awareness.*

Selain *cyber-security* kelangsungan operasi informasi juga bergantung pada *physical security* yang tentunya berkaitan dengan semua elemen fisik seperti bangunan data center, *disaster recovery system*, dan media

---

[38] Ghernaouti,S. Cybersecurity Guide for Developping Countries. Geneva: International Telecommunication Union, 2009. Pg 28

[39] Edmon Makarim, *Indonesian Legal Framework for Cybersecurity, http://www.nisc.go.jp/security site/campaign/ ajsympo/pdf/lecture2.pdf,*

14. Ketahanan Nasional

Ketahanan Nasional *(national resilience)* merupakan salah satu konsepsi kenegaraan Indonesia. Ketahanan sebuah bangsa pada dasarnya dibutuhkan untuk menjamin serta memperkuat kemampuan bangsa dalam rangka mempertahankan kesatuannya, menghadapi ancaman, gangguan maupun pemanfaatan sumber daya guna memenuhi kebutuhan hidup.[40]

Suradinata (2005: 47) mengemukakan "pengertian Ketahanan Nasional adalah suatu kondisi dinamis suatu bangsa, yang berisi keuletan dan ketangguhan yang mengandung kemampuan mengembangkan kekuatan nasional dalam menghadapi dan mengatasi segala ancaman, gangguan, hambatan dan tantangan baik yang datang dari luar maupun dari dalam negeri, yang langsung maupun tidak langsung membahayakan integritas, identitas kelangsungan hidup bangsa dan negara serta perjuangan dalam mengejar tujuan nasional Indonesia"[41]

Meskipun sebenarnya, konsep ketahanan mempunyai lingkup yang luas, yang salah satunya adalah kapasitas sistem untuk memelihara fungsi dan strukturnya dari perubahan eksternal maupun internal.[42] Sedangkan Suryohadiprojo (1997) menyatakan "Ketahanan Nasional meliputi keamanan nasional dan kesejahteraan nasional yang berarti Ketahanan Nasional sejalan dengan kepentingan nasional".[43]

Oleh karena itu, implementasi Ketahanan Nasional Indonesia dalam proses pembangunan nasional dilakukan melalui 2 pendekatan yaitu pendekatan keamanan digunakan untuk mengembangkan kemampuan dalam melindungi eksistensi serta nilai-nilai luhur yang dimiliki oleh

[40] A. Aco Agus (2015), Jurnal integrasi, Volume 1, Nomor 2, Agustus 2015, Program Studi Pendidikan Ilmpu Pengetahuan Sosial Pasca Sarjana Universitas Negeri Makassar, ISSN: 2443-2822

[41] Suradinata, Ermaya, 2005, Geopoliti dan Geostategik Dalam Mewujudkan Negara Kesatuan Republik Indonesia, Jurnal Ketahanan Nasional No. VI Agustus 2005

[42] L. Carlson G. Bassett, et al (2012). Resilience: theory and application. Argonne National Laboratory. Oak Ridge, p, 11

[43] Suryohadiprojo, Sayidiman, 1997, Ketahanan Nasional Indonesia, Jurnal Ketahanan Nasional No. II 1 April 1997 Program Studi Ketahanan Nasional, PTS UGM, Yogyakarta.

masyarakat, bangsa dan negara terhadap segala ancaman dari dalam maupun dari luar negeri[44]

Pada konteks ini, bangsa Indonesia membutuhkan suatu ketangguhan atas Ketahanan Nasional, yaitu kondisi dinamis bangsa Indonesia yang meliputi segenap aspek kehidupan nasional yang terintegrasi serta berisi keuletan dan ketangguhan yang mengandung kemampuan mengembangkan kekuatan nasional dalam menghadapi dan mengatasi segala tantangan, ancaman, hambatan dan gangguan, baik yang datang dari luar maupun dari dalam, untuk menjamin identitas, integritas, kelangsungan hidup bangsa dan negara, serta perjuangan mencapai tujuan nasionalnya.[45]

Ketahanan Nasional merupakan derivasi dari pembangunan nasional dan keduanya mempunyai hubungan yang bersifat simbiosis mutualistis keberhasilan pembangunan nasional akan dapat meningkatkan Ketahanan Nasional dan sebaliknya Ketahanan Nasional yang tangguh akan lebih mendorong laju pembangunan nasional. Hakekat Ketahanan Nasional adalah keuletan dan ketangguhan yang mengandung kemampuan mengembangkan kekuatan nasional untuk dapat menjamin kelangsungan hidup dan tujuan negara. Hakekat konsepsi Ketahanan Nasional Indonesia adalah “pengaturan dan penyelenggaraan kesejahteraan dan keamanan secara seimbang serasi dan selaras dalam seluruh aspek kehidupan nasional”.[46]

Ketahanan Nasional merupakan salah satu konsepsi politik dari Negara Kesatuan Republik Indonesia. Ketahanan Nasional dapat dikatakan sebagai konsep geostrateginya bangsa Indonesia. Dengan kata lain,

---

[44] A. Aco Agus (2015), Jurnal integrasi, Volume 1, Nomor 2, Agustus 2015, Program Studi Pendidikan Ilmpu Pengetahuan Sosial Pasca Sarjana Universitas Negeri Makassar, ISSN: 2443-2822

[45] Kris Wijoyo Soepandji , Muhammad Farid (2018), Konsep Bela Negara Dalam Perspektif Ketahanan Nasional, *Jurnal Hukum dan Pembangunan Tahun ke-48 No. 3 Juli-September 2018*, Universitas Indonesia, Jurnal Hukum & Pembangunan 48 No. 3 (2018): 436-456 ISSN: 0125-9687 (Cetak) E-ISSN: 2503-1465 (*Online*)

[46] A. Aco Agus (2015), Jurnal integrasi, Volume 1, Nomor 2, Agustus 2015, Program Studi Pendidikan Ilmpu Pengetahuan Sosial Pasca Sarjana Universitas Negeri Makassar, ISSN: 2443-2822

geostrategi bangsa Indonesia diwujudkan melalui konsep ketahanan nasional.

Geostrategi adalah suatu cara atau pendekatan dalam upaya memanfaatkan kondisi lingkungan untuk mewujudkan cita-cita proklamasi dan tujuan nasional. Ketahanan nasional sebagai geostrategi bangsa Indonesia mempunyai pengertian bahwa konsep ketahanan nasional merupakan pendekatan yang digunakan bangsa Indonesia dalam melaksanakan pembangunan dalam rangka mencapai cita-cita dan tujuan nasional. Ketahanan nasional sebagai suatu pendekatan merupakan salah satu pengertian dari konsepsi ketahan nasional itu sendiri[47].

Terdapat tiga perspektif atau sudut pandang terhadap konsepsi ketahanan nasional yakni:

1) Ketahanan Nasional sebagai suatu kondisi. Perspektif ini melihat Ketahanan Nasional sebagai suatu gambaran atas keadaan yang seharusnya dipenuhi.
2) Ketahanan nasional sebagai sebuah pendekatan, metode atau cara dalam menjalankan suatu kegiatan khususnya pembangunan negara.
3) Ketahanan Nasional sebagai suatu doktrin. Ketahanan nasional merupakan salah satu konsepsi khas Indonesia yang berupa ajaran konseptual tentang pengaturan dan penyelenggaraan bernegara.[48]

15. Faktor-Faktor Lingkungan Strategis Yang Berpengaruh-Eksternal

Dalam melihat isu tentang keamanan siber memerlukan sebuah pemikiran yang komprehensif. Pertimbangan tersebut dikarenakan problem keamanan siber menjadi sangat luas dan kompleks. Faktor-faktor eksternal

[47] Kris Wijoyo Soepandji, Muhammad Farid (2018), Konsep Bela Negara Dalam Perspektif Ketahanan Nasional, *Jurnal Hukum dan Pembangunan Tahun ke-48 No. 3 Juli-September 2018*, Universitas Indonesia, Jurnal Hukum & Pembangunan 48 No. 3 (2018): 436-456 ISSN: 0125-9687 (Cetak) E-ISSN: 2503-1465 (*Online*)

[48] Ibid, Kris Wijoyo Soepandji, Muhammad Farid (2018), Konsep Bela Negara Dalam Perspektif Ketahanan Nasional, *Jurnal Hukum dan Pembangunan Tahun ke-48 No. 3 Juli-September 2018*, Universitas Indonesia, Jurnal Hukum & Pembangunan 48 No. 3 (2018): 436-456 ISSN: 0125-9687 (Cetak) E-ISSN: 2503-1465 (*Online*)

seperti: yang *pertama* transformasi teknologi informasi, *kedua* liberalisasi digital ekonomi, *ketiga* persoalan geopolitik.

a. Transformasi Teknologi Informasi

Perkembangan teknologi informasi telah merubah semua aspek kehidupan. Salah satu yang memicu adalah dengan berkembangnya internet yang memberikan kemudahan dan keuntungan bagi masyarakat di seluruh dunia, internet telah mengubah lanskap ekonomi dunia, dan transformasi ini telah berlanjut dengan adanya *Internet of things* (IoT) dalam setiap aktivitas masyarakat.

b. Liberalisasi digital ekonomi

Seperti yang sudah diulas pada pembahasan di atas, bahwa dengan adanya perkembangan teknologi informasi, telah mengarahkan peradaban dunia menuju ekonomi yang berbasis pada digital. Dengan demikian adanya liberalisasi ekonomi digital menjadi sebuah keniscayaan–liberalisasi ekonomi dunia juga secara langsung dipengaruhi oleh perkembangan teknologi, globalisasi, dan perangkat komunikasi digital.

Liberalisasi ekonomi digital merupakan evolusi baru dalam kegiatan ekonomi yang diharapkan dapat memberikan kemudahan bagi setiap kelompok orang atau individu untuk melakukan transaksi secara langsung (yang melibatkan hubungan antara penjual dan pembeli) dan mengurangi biaya transaksi. Masyarakat dapat terhubung melalui platform digital di pasar yang disebut *marketplace*.

Namun di sisi lain liberalisasi ekonomi digital masih memiliki tantangan besar yaitu dari aspek keamanan siber. Salah satu contoh yang bisa kita lihat adalah bagaimana kasus kebocoran data *marketplace* terbesar di Indonesia yaitu Tokopedia. Menurut beberapa sumber pada tanggal 20 maret 2020 Tokopedia dilaporkan mengalami peretasan, bahkan jumlahnya diperkirakan 91 juta akun dan 7 juta akun merchant, tidak lagi 15 juta seperti

diberitakan sebelumnya. Padahal di tahun 2019, Tokopedia mengungkapkan bahwa ada sekitar 91 juta akun aktif di platformnya.[49]

c. Aspek Geopolitik

Aspek geopolitik mempunyai pengaruh yang cukup besar dalam melihat berbagai isu tentang keamanan nasional terutama yang menyangkut keamanan siber. Geopolitik memiliki cakupan multidisipliner, dan meliputi segala aspek ilmu sosial dengan penekanan tertentu terhadap geografi politik, hubungan internasional, aspek teritorial ilmu politik, dan hukum internasional.[50] Selain itu, studi geopolitik meliputi studi hubungan bersama antara kepentingan aktor politik internasional, kepentingan yang terfokus pada wilayah, ruang, elemen geografis, hubungan yang menciptakan sistem geopolitik.[51]

16. Faktor-Faktor Lingkungan Strategis Yang Berpengaruh-Internal

Faktor-faktor lingkungan internal menjadi sangat penting untuk dilihat sebagai pertimbangan dalam merumuskan dan menjawab pertanyaan penelitian yang ada dalam taskap ini. Beberapa aspek internal antara lain: aspek demografi, aspek ideologi, aspek hukum, aspek politik, aspek ekonomi, aspek sosial budaya dan aspek pertahanan dan keamanan.

a. Aspek Demografi

Indonesia saat ini sedang sedang menyongsong bonus demografi, saat ini jumlah penduduk Indonesia sangat besar. Dari Sensus Penduduk 2020 yang dilaksanakan dalam kurun waktu bulan Februari. Kementerian Dalam Negeri (Kemendagri) menyatakan jumlah penduduk Indonesia hingga bulan Desember 2020 mencapai 271.349.889 jiwa (jumlah penduduk Indonesia 2021).

---

[49] Salah satu berita yang mengulas peretasan tersebut adalah CNN, untuk detainya dapat dilihat pada tautan berikut: https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

[50] Geopolitics Journal home page -http://www.tandf.co.uk/journals/titles/14650045.asp

[51] Vladimir Toncea, 2006, "Geopolitical evolution of borders in Danube Basin

b. Aspek Hukum

Aspek hukum memegang peranan sangat penting dalam upaya menjaga keamanan siber dan juga dalam rangka menuju ketahanan nasional, meskipun RUU keamanan siber dan RUU perlindungan data pribadi masih belum disahkan.

Undang-undang dan peraturan-peraturan yang berkaitan dengan keamanan siber di Indonesia telah menjelaskan dan memberikan serta membagi tugas, wewenang dan tanggung jawab kepada beberapa kementrian, TNI dan Polri serta BSSN. Undang-undang yang ada akan menjadi payung hukum bagi upaya pencegahan, penanganan dan penegakan hukum terhadap tindak kejahatan siber.

Adanya regulasi undang-undang dan peraturan-peraturan menjadi penting untuk mencegah ancaman kejahatan siber, untuk itu akan diulas dalam Taskap ini berbagai perundang-undangan yang relevan dan terkait dengan keamanan siber.

c. Aspek ekonomi

Aspek ekonomi menjadi sangat penting untuk dikaji dalam Taskap ini, mengingat Indonesia merupakan negara yang sangat potensial di sektor ekonomi kreatif, pariwisata dan ekonomi digital. Prospek perkembangan ekonomi digital Indonesia memang sangat menjanjikan, karena pada tahun 2019 1,8 juta orang Indonesia sering berbelanja online dan terus meningkat dari tahun ke tahun.

Peluang itu semakin terlihat didorong oleh meningkatnya cakupan pasar dan perilaku konsumtif kelas menengah konsumtif digital masyarakat Indonesia, meskipun marketplace terbesar dunia masih dikuasai oleh China dan AS. Prioritas pemerintah sektor ekonomi digital diproyeksikan sebesar US$ 130 miliar pada tahun 2021 Mengeluarkan beberapa kebijakan yang mendukung Paket Kebijakan Ekonomi dan juga road map ekonomi digital.

Selain itu juga, Total UKM di Indonesia pada tahun 2019 adalah 64.199.606. Penciptaan lapangan kerja baru di UKM dan ini memungkinkan setiap orang untuk memulai bisnis mereka sendiri melalui internet. Angka

terakhir menunjukkan bahwa ada 816.000 UKM di Indonesia, mempekerjakan 7,9 juta orang dan berkontribusi 27% terhadap PDB. Dari total pinjaman bank sebesar Rp 4.136 triliun, UKM mewakili sekitar 16%. Ekspansi perdagangan, jangkau UKM yang lebih luas untuk menjual produk & layanan secara online.

d. Aspek Politik

Lanskap politik di Indonesia memang berjalan sangat dinamis, sejak zaman orde lama, orde baru hingga masa reformasi menunjukan bahwa proses demokrasi di Indonesia masih memiliki kelemahan dan kekurangan. Tetapi setiap pemerintahan memiliki kelebihan dan kekurangan masing-masing. Dalam perkembangan masa reformasi seperti sekarang ini terlebih dengan adanya perubahan IPTEK yang sangat pesat aspek politik nasional setidaknya memberikan pengaruh terhadap pemecahan problem, tantangan dalam rangka mewujudkan Indonesia yang maju, unggul dan sejahtera.

Salah satu aspek politik yang bisa kita lihat adalah, adanya penundaan pengesahan RUU Ketahanan dan Keamanan Siber serta RUU Perlindungan Data Pribadi. Penundaan dari pengesahan tersebut nampaknya dipengaruhi karen factor politik karen rancangan RUU tersebut berhenti pada pembahasan di DPR. Padahal jika kita melihat bahwa rasa aman warga di ranah siber saat ini dinilai sangat mengkhawatirkan.

e. Aspek sosial budaya

Pesatnya perkembangan teknologi digital telah banyak memberikan pengaruh yang cukup signifikan di Indonesia. Adanya revolusi ponsel pintar yang mencapai 28,6% populasi di Indonesia yang menggunakan gawai tersebut pada tahun 2015. Seiring berjalannya waktu, ponsel pintar semakin terjangkau, sehingga meningkatkan penggunaannya dan risiko keamanan data pribadi dan data digitalnya.

Menurut data yang disajikan Kominfo lebih dari setengah populasi di Indonesia atau 56,2% telah menggunakan ponsel pintar pada 2018. Setahun setelahnya, sebanyak 63,3% masyarakat menggunakan ponsel pintar. Diperkirakan pada tahun 2025, setidaknya 89,2% populasi di Indonesia telah

memanfaatkan ponsel pintar. Dalam kurun waktu enam tahun sejak 2019, penetrasi ponsel pintar di tanah air tumbuh 25,9%. Saat ini, ada 170 juta jiwa orang Indonesia yang merupakan pengguna aktif media sosial. Rata-rata dari mereka menghabiskan waktu 3 jam 14 menit di platform jejaring sosial.

f. Aspek pertahanan dan keamanan

Digitalisasi di semua lini kehidupan serta pengembangan teknologi informasi dan komunikasi telah mengubah setiap aspek dalam kehidupan masyarakat modern. Akan muncul persoalan batu ketika ekosistem digital terkoneksi dengan infrastruktur vital, pertahanan negara, kehidupan masyarakat dan bisa membuka peluang untuk inovasi dan pengembangan, maka potensi serangannya pun akan meningkat. Dan cara sebuah negara menjawab berbagai peluang dan resiko yang muncul di dunia siber memainkan sebuah peran penting dalam pertumbuhan dan keamanannya.

Pertahanan dan keamanan Indonesia menjadi sangat penting untuk diimplementasikan. Infrasturktur keamanan siber perlu menjadi perhatian serius oleh pemerintah. Aspek tersebut sangat medasar karene pertahanan dan keamanan negara acap kali berhubungan dengan pertahan dan keamanan Indonesia.


DHARMMA
TANHANA
MANGRVA

BAB III
PEMBAHASAN

17. Umum

Bab ini akan membahas secara rinci keamanan siber di Indonesia pada periode tahun 2017 sampai dengan 2021, yang terdiri dari undang-undang dan peraturan-peraturan terkait dengan keamanan siber nasional, infrastruktur dan pengembangan SDM dan berbagai kebijakan nasional yang mempengaruhi kondisi keamanan siber Indonesia serta upaya kerja sama yang telah dilakukan dengan negara lain.

Selain itu juga akan dibahas berbagai upaya yang dilakukan oleh pemerintah Republik Indonesia dalam menjaga keamanan siber berserta dengan tantangan-tantangan yang dihadapi serta bagaimana strategi kerja sama keamanan siber yang telah dilakukan terutama dalam memperkuat ketahanan Nasional.

Pada bab ini penulis akan mencoba menguraikan keamanan nasional ke dalam kondisi faktual terutama dari aspek keamanan siber. Era revolusi industri 4.0 keamanan siber akan berhubungan dengan sistem pertahanan dan keamanan nasional, terlebih keamanan nasional saat ini mengalami dinamika dan pergeseran yang berpotensi menyulut *cyber war* yang tanpa disadari dapat memicu konflik antar negara, persoalan keamanan nasional kini direpresentasikan juga dengan seberapa kuat sebuah negara menjaga ketahanan siber.

Bab ini juga akan menyoroti tentang faktor-faktor lingkungan strategis yang berpengaruh yaitu faktor eksternal dan faktor internal. Faktor-faktor eksternal seperti: yang *pertama* transformasi teknologi informasi, *kedua* liberalisasi digital ekonomi, *ketiga* persoalan geopolitik.

Sedangkan faktor lingkungan internal antara lain: aspek demografi, aspek ideologi, aspek hukum, aspek politik, aspek ekonomi, aspek sosial budaya dan aspek pertahanan dan keamanan.

18. Peraturan dan Perundangan-undangan Keamanan Siber Indonesia

Keamanan siber dan ancaman *cyber war* merupakan salah satu bagian penting dalam upaya untuk menjaga kedaulatan negara terutama dalam rangka menciptakan pertahanan dan keamanan nasional. Memang sudah terdapat beberapa peraturan dan perundang-undangan yang dapat menjadi payung hukum dari keamanan siber dan ancaman *cyber war*. Sehingga dengan adanya kerentanan dari aspek regulasi tersebut akan memungkinkan muncul banyak ancaman dan kendala yang akan dihadapi oleh para pemangku kepentingan untuk menegakan ketahanan dan kedaulatan siber nasional.

Sampai saat ini Indonesia belum memiliki regulasi yang mengatur keamanan dan ketahanan siber meski sudah ada UU ITE. RUU Ketahanan dan Keamanan Siber yang sudah di usulkan oleh tim perumus kepada DPR masih belum menemui titik terang, ada beberapa pertimbangan yaitu RUU tersebut yaitu RUU keamanan dan ketahanan siber perlu tetap dilanjutkan untuk dikaji dengan melibatkan partisipasi aktif publik atau *Public Private Dialogue* (PPD) dalam penyusunannya.

Selain itu juga masih memerlukan masukan dari berbagai *stakeholder* seperti para pemerhati serta aktivis dunia siber untuk memperkaya norma-norma dalam produk regulasi itu, selain itu juga diperlukan masukan dari kalangan dunia usaha dan dunia industry, mengingat RUU tersebut juga akan bersinggungan dengan ketahanan siber bagi DUDI. Regulasi yang memayungi ketahanan dan keamanan siber untuk saat ini masih ada pada beberapa undang-undang.

Seperti yang tertuang dalam Undang-undang nomor 36 tahun 1999 tentang Telekomunikasi; dimana pada Bab 3 pasal 4 menekankan pada penetapan kebijakan, pengaturan, pengawasan dan pengendalian di bidang telekomunikasi. Lebih spesifik lagi Bab 4 pasal 7 menekankan pada upaya penyelengaraan komunikasi yang bertujuan untuk melindungi kepentingan dan keamanan negara. Tetapi dalam undang-undang tersebut belum spesifik mengatur tentang bagaimana kebijakan tentang keamanan siber,

belum memuat juga tentang pengaturan yang lebih spesifik terkait pengaturan, pengawasan dan pengendalian dibidang keamanan siber.

Pada tahun 2008 disahkan undang-undang tentang Informasi dan Transaksi Elektronik yaitu Undang-undang No. 11. Dalam regulasi tersebut juga belum memberi penekanan secara khusus tentang sistem keamanan siber dalam undang-undang tersebut lebih mengatur tentang bagaimana menciptakan etika dan komunikasi dalam system informasi dan juga dalam melakukan transaksi elektronik.

Terdapat beberapa alasan mengapa UU ITE masih menjadi payung hukum dalam memecahkan persoalan tentang keamanan siber dan ancaman-ancaman yang muncul dibaliknya, pertimbangan tersebut antara lain:

a. Undang-Undang Nomor 19 Tahun 2016 Jo UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dianggap masih sangat diperlukan, untuk mengantisipasi dan memberi kepastian hukum dunia digital, sehingga tidak akan ada pencabutan UU ITE tersebut dan tidak akan diganti oleh undang-undang ketahanan dan keamanan siber.
b. untuk mengatasi kecenderungan salah tafsir dan tidak sama penerapan, Undang-Undang Nomor 19 Tahun 2016 Jo UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), maka pemerintah membuat pedoman teknis kriteria implementasi yang diwujudkan berupa Surat Keputusan Bersama (SKB) antara tiga pimpinan instansi yaitu Menteri Komunikasi dan Informatika, Jaksa Agung dan Kapolri.
c. terdapat revisi semantik atau revisi terbatas sangat kecil di Undang-Undang Nomor 19 Tahun 2016 Jo UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Revisi ini berupa penambahan frasa dan tambahan di penjelasan UU, seperti penjelasan atau definisi mengenai penistaan, fitnah, keonaran, tetapi lagi-lagi dalam UU tersebut belum secara khusus memberikan kepastian hukum terkait ketahanan dan keamanan siber.

Kepastian hukum terkait dengan keamanan siber juga masih menginduk pada beberapa regulasi lainnya salah satu contohnya adalah Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik pada Pasal 61. Peraturan tersebut berbicara secara umum tentang Perdagangan Melalui Sistem Elektronik (PMSE) tidak mengatur secara spesifik tentang keamanan siber dalam perdagangan, dengan ruang lingkup pihak-pihak yang melakukan transaksi PMSE, persyaratan PMSE, prosedur penyelenggaraanya, dalam peraturan tersebut juga mengatur tentang kaewajiban pelaku usaha, bukti transaksi PMSE, membahas tentang iklan elektronik, penawaran secara elektronik dan komunikasi elektronik serta beberapa ruang lingkup lain tentang perdagangan melalui sistem elektronik.

Peraturan pemerintah nomor 80 tahun 2019 tersebut tidak spesifik memuat tentang keamanan siber, tentang keamanan siber hanya dibahas pada pasal 61 yang sebatas memuat tentang bagaimana standar jasa system pembayaran dan sistem elektronik harus memenuhi keamanan siber. Untuk itu perlu sebuah payung hukum yang benar-benar mengatur tentang keamanan siber dan serangan siber agar kedepan kedaulatan dan ketahanan siber dapat dibangun di Indonesia.

Sejumlah kejahatan siber saat ini tengah mengintai Indonesia, antara lain berupa penjebolan sistem dan pencurian data, hingga penyadapan. Peretasan sistem dan pengambilan data, kejahatan semacam itu banyak mengancam lembaga-lembaga perbankan di Indonesia, karena standarisasi pengamanan sistem di sejumlah bank masih belum berjalan secara maksimal artinya sistem keamanan data dan informasi di lembaga perbankan sering menjadi incaran para pelaku kejahatan siber.

Upaya Pemerintah dan DPR untuk membahas dan mengesahkan RUU keamanan dan ketahanan siber nasional telah dilakukan. Aspek dinamika politik nasional menyebabkan bahwa RUU KKS resmi dibatalkan dan tidak dapat dilanjutkan, dengan alasan tidak memenuhi tata beracara dalam pembuatan legislasi. Alasan tersebut kurang memiliki pijakan argumentasi

dan logika hukum yang kuat apabila dibandingkan dengan kepentingan keamanan nasional dan urgensinya saat ini.

Selain itu, beberapa penolakan dari kalangan LSM juga terjadi, alasan tersebut dikarenakan keberadaan RUU KKS dapat mengancam hak privasi individu dan melanggar hak warga Negara, karena ada kekhawatiran apabila RUU ini disahkan akan memberikan ruang yang sangat besar bagi otoritas untuk melakukan tindakan monitoring dari trafik data dan internet di Indonesia. Padahal dalam RUU tersebut dapat diusulkan pasal yang memuat tentang kerahasiaan data pribadi warga untuk seluruh warga negara Indonesia.

Di lain sisi, kebutuhan akan adanya peraturan perundang-undangan seperti RUU KKS diperlukan untuk menjaga ruang siber guna memenuhi keamanan siber, melindungi lingkungan siber, organisasi, dan aset pengguna. Namun, tampaknya penerapan dan sosialisasi RUU KKS masih belum dapat tersampaikan kepada masyarakat dengan tepat dan belum sesuai dengan lima bidang kerja dari global cyber security, yakni kepastian hukum, teknis dan tindakan prosedural, struktur organisasi, capacity building dan pendidikan pengguna, dan kerja sama internasional. Poin capacity building dan pendidikan pengguna masih belum mampu untuk dicapai karena kurangnya literasi dan pelajaran mengenai ruang siber.

Selain itu, pemahaman mengenai ruang siber dibutuhkan oleh masyarakat guna mencapai tujuan dari keamanan siber, yakni melindungi dan meminimalkan gangguan kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Keberadaan undang-undang untuk mengatur ruang siber dibutuhkan untuk mencegah potensi terjadinya ancaman siber yang lebih besar, terkait dengan kasus serangan siber pada 1 Januari hingga 12 April 2020 yang dicatat oleh BSSN mencapai angka 88.414.296 kasus. Fenomena di mana masyarakat menolak pengesahan RUU KKS ini seakan-akan menunjukkan ketidakpercayaan masyarakat kepada pemerintah, sebaliknya justru mempercayakan data pribadi kepada pihak pengembang aplikasi milik swasta. Oleh sebab itu, adanya pendidikan mengenai ruang siber dibutuhkan oleh masyarakat guna meningkatkan

kewaspadaan dalam aktivitas dalam ruang siber guna mencegah adanya potensi ancaman yang akan terjadi selanjutnya.

Dengan demikian adanya RUU tentang keamanan dan ketahanan siber (KKS) menjadi sangat mendesak untuk segera disahkan, mengingat ancaman cyber warfare saat ini berkembang dari cyber crime yang kini sudah berkembang dalam bentuk-bentuk kejahatan yang disebabkan karena pemanfaatan teknologi internet begitu massif. Berdasarkan fakta kejahatan siber di Indonesia, cyber warfare yang paling sering untuk menjadi sasaran adalah berbagai sistem informasi yang dikeola oleh pemerintah, institusi finansial, provider serta infrastruktur vital lainnya, termasuk di dalamnya sistem pertahanan dan keamanan nasional.

19. Kondisi Kesiapan Infrastruktur dan SDM Keamanan Siber

a. Kesiapan Infrastruktur Keamanan Siber:

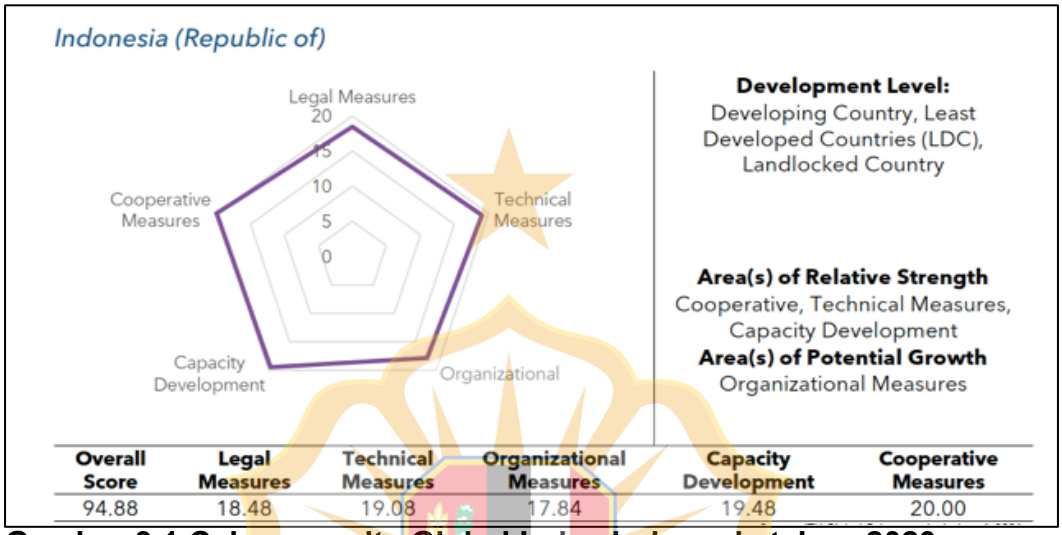
Dari aspek keamanan siber, pemerintah Indonesia sudah melakukan perbaikan terus menerus, indikator ini ditunjukan melalui kenaikan ranking keamanan siber Indonesia yang mengalami peningkatan dari tahun ke tahun. Tahun 2017 berada pada peringkat ke-70 dari 164 negara, tahun 2018 mengalami peningkatan naik 29 peringkat pada posisi ke-41 dari 175 negara di dunia. Tahun 2019 masih diperingkat yang sama yaitu diperingkat 41 dari 175 negara.

Tahun 2020 peringkat keamanan siber global Indonesia mengalami peningkatan yang cukup signifikan. Global Cybersecurity Index (GCI) menyajikan report bahwa Indonesia ada di peringkat ke- 24 dengan jumlah skor GCI 94,88 dari 188 negara. peringkat ini satu peringkat di atas Vietnam dengan skor 94,59 sedangkan Swedia berada di peringkat 26 dengan skor 94,55. Sementara peringkat ke-1 dunia ditempati oleh Amerika dengan skor 100, dan peringkat ke-2 diduduki oleh UK dengan skor 99,54.

Sementara untuk wilayah Asia Pasifik peringkat keamanan siber Indonesia ada di posisi ke-6 ada dibawah India yang ada diperingkat ke-4 dengan skor GCI 97,49 dan Australia diperingkat ke-5 dengan skor 97,45. Sementara untuk peringkat 1 di tingkat Asia Pasifik ditempati oleh Rep Korea

Selatan dan Singapura dengan skor yang sama yaitu 98,52. Pemeringkatan keamanan siber yang dilakukan oleh International Telecommunication Union tahun 2020 berdasarkan pada penilaian kinerja keamanan siber dengan melihat 5 (lima) pilar antara lain: *legal, technical, organizational, capacity development dan cooperative*.

Berikut ini adalah detail skor pemeringkatan GCI Indonesia tahun 2020:



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
94.88	18.48	19.08	17.84	19.48	20.00

Gambar 3.1 Cybersecurity Global Index Indonesia tahun 2020

Sumber: Global Cybersecurity Index 2020, International Telecommunication Union 2021

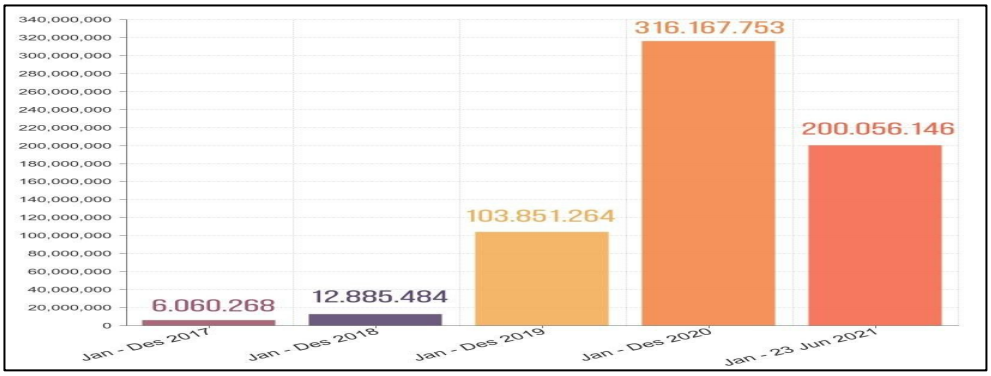
Perkembangan teknologi informasi yang ditunjukkan dengan semakin banyaknya basis data dan transaksi elektronik terutama yang berbasis digital ternyata berbanding lurus dengan jumlah serangan siber di Indonesia.

Selama kurun waktu 1 Januari 2017 sampai dengan 26 Juni 2021 menunjukan bahwa serangan siber yang masuk ke Indonesia berasal dari beberapa negara antara lain India yang menempati posisi tertinggi yaitu dengan jumlah serangan sebesar 122.734.763 serangan. Sedangkan serangan yang berasal dari dalam negeri atau dari Indonesia mencapai 75.894.790 serangan, Irlandia sebesar 68.370.246, serangan, sementara Vietnam sebesar 49.060.550 serangan dan Rusia sebesar 35.401.753 serangan.

Berikut ini data terkait peta serangan siber yang masuk di Indonesia sejak 2017 hingga pertengahan 2021. Data tersebut dapat di akses secara *real time* di situs Honeynet BSSN.

Gambar 3.2 Informasi Peta Serangan Siber di Indonesia 2017 sd 26 Juni 2021 Sumber: https://honeynet.bssn.go.id

Selain dilihat dari peta serangan di atas, tingginya serangan siber juga dapat dilihat dari tahun ke tahun. Laporan yang disajikan oleh Data Honeynet BSSN menunjukan bahwa selama 2017 sampai dengan 23 Juni 2021 total serangan siber ke Indonesia mencapai 639.020.915 serangan. Serangan teringgi tarjadi pada tahun 2020 yaitu sebesar 316.167.753, tahun 2017 sebanyak 6.060.268 serangan, tahun 2018 12.885.484, meningkat pada tahun 2019 sebesar 103.851.264, sedangkan awal Januari 2021 sampai 23 Juni 2021 sebesar 200.056.146 serangan dan kemungkinan akan terus meningkat sampai akhir tahun 2021. Berikut ini penulis sajikan data info grafis serangan siber di Indonesia 2017 sd 23 Juni 2021.



Gambar 3.3 Infografis Serangan Siber di Indonesia 2017 sd 23 Juni 2021. Sumber: https://honeynet.bssn.go.id

Dari data di atas menunjukan bahwa tiap tahun jumlah serangan siber di Indonesia terus mengalami peningkatan yang cukup signifikan, artinya perlu adanya upaya pencegahan dan strategi yang tepat untuk menanggulangi serangan siber. Langkah tersebut dapat dilakukan dengan berbagai pembenahan terutama dari aspek legal, technical, organizational, capacity development dan cooperative.

b. SDM keamanan siber

Secara teknis, peningkatan angka serangan siber tersebut menunjukkan bahwa Indonesia masih kurang siap dalam membangun sistem keamanan siber nasional, baik dari segi infrastruktur dan SDM. Saat ini, Indonesia membutuhkan keamanan siber untuk terus ditingkatkan dalam upaya menghadapi kecanggihan teknologi yang disertai dengan ancamannya. Upaya sosialisasi mengenai ruang dan keamanan siber perlu mencakup hingga ke ranah masyarakat secara umum. Selain itu, pemerintah juga dapat memberikan edukasi kepada mahasiswa sebagai agen penggerak untuk dapat membantu memberikan edukasi mengenai keamanan siber untuk meningkatkan pemahaman dan kesadaran akan potensi ancaman yang hadir dari teknologi internet dalam kehidupan sehari-hari. Keamanan nasional juga perlu memusatkan perhatian kepada infrastruktur guna mencapai pelindungan dan kewaspadaan berkelanjutan di ruang siber. Ancaman siber telah menjadi perhatian dari keamanan nasional karena telah menyerang elemen-elemen negara. Keamanan siber menjadi salah satu kebutuhan penting dalam mencapai keamanan nasional.

Dalam rangka mendukung dan menciptakan system ketahanan dan keamanan siber di Indonesia menuju kedaulatan siber, untuk itu diperlukan adanya kesiapan dan ketersediaan sumber daya manusia baik secara internal kelembagaan dan dukungan SDM dari eksternal lembaga BSSN yang mencukupi sesuai bidang kompetensi. Kondisi objektif saat ini adalah yaitu : **pertama**, sumber daya manusia secara internal yang ada dalam struktur sumber daya manusia pada BSSN masih memerlukan dukungan dan peningkatan serta penguatan masing-masing bidang.

Berdasarkan data yang dihimpun dari BSSN 2020 Jumlah level pipmpinan terdiri dari 3 yaitu terdiri dari 1 orang kepala BSSN, Wakil Kepala ada 1 dan Sekretaris Utama ada 1 orang. Sedangkan jumlah pegawai pada Biro Perencanaan Dan Keuangan, Sekretariat Utama sebanyak 63 pagawai, Jumlah Pegawai Pada Biro Organisasi Dan Sumber Daya Manusia, Sekretariat Utama ada 91 pegawai dan Jumlah Pegawai Pada Biro Tata Usaha, Hukum, Dan Komunikasi Publik, Sekretariat Utama ada 38 pagawai, Jumlah Pegawai Pada Biro Umum, Sekretariat Utama, sehingga total pegawai yang ada pada Sekretariat Utama sebanyak 384.

Jumlah yang ada di level Sekretariat Utama memang sudah mencukupi, kedepan mungkin diperlukan pengembangan dan peningkatan kompetensi secara berkelanjutan agar pegawai yang ada di level ini dapat bekerja secara optimal efektif dan efisien dalam menjalankan tugas dan fungsinya masing-masing.

Di satu sisi yang perlu menjadi catatan adalah perlunya peningkatan baik secara kualitas maupun kuantitas dukungan SDM yang ada di Deputi I yaitu Deputi Bidang Identifikasi Dan Deteksi yang totalnya hanya terdiri dari 96 pegawai, yang terdiri dari 1 Orang Pimpinan Deputi, 21 pegawai pada Direktorat Identifikasi Kerentanan dan Penilaian Risiko Pemerintah. Penambahan jumlah pegawai di bidang ini sangat diperlukan mengingat kerentanan keamanan siber pada sektor pemerintahan sangat tinggi sehingga memerlukan dukungan persolnil atau pegawai. Jumlah Pegawai Pada Direktorat Identifikasi Kerentanan Dan Penilaian Risiko Infrastruktur Informasi Kritikal Nasional sebanyak 22 pegawai, jumlah ini juga perlu

peningkatan dan dukungan personil, agar fungsi operasional dan teknis lainnya dapat berjalan dengan baik. Jumlah Pegawai Pada Direktorat Identifikasi Kerentanan Dan Penilaian Risiko Sektor Ekonomi Digital sebanyak 14 pegawai. Jumlah ini perlu ditingkatkan mengingat kerentanan keamanan siber disektor ekonomi digital juga sangat tinggi sementara potensi Indonesia untuk mengembangkan sektor ekonomi digital sangat potensial untuk bersaing ditingkat dunia internasional.

Dukungan dan peningkatan jumlah SDM di Deputi II Bidang Proteksi sudah cukup memadai saat ini jumlah pegawai di Deputi ini sebanyak 133. Sedangkan di Deputi III Bidang Penanggulangan dan Pemulihan sebanyak 61 pegawai, jumlah ini memerlukan peningkatan kuantitas mengingat penanggulangan kasus serangan siber dan kejahatan siber di Indonesia masih cukup tinggi. Untuk Depiti IV Bidang Pemantauan dan Pengendalian total pegawai sebnyak 80 pegawai, jumlah ini juga perlu evaluasi apakah ketersediaan jumlah pegawai yang ada mempu memenihi tugas dan fungsi bidang ini, mengingat tugas pengendalian informasi investigasi, bahkan digital forensic bidang keamanan siber masih memerlukan jumlah sumber daya manusia yang memadai. Begitu juga penguatan dan penambahan jumlah pegawai yang ada pada Pusat Pengkajian Dan Pengembangan Teknologi Keamanan Informasi, Pegawai Pada Pusat Data Dan Teknologi Informasi Komunikasi, Pegawai Pada Pusat Pendidikan dan Pelatihan perlu dilakukan evaluasi dan pengukuran kinerja melalui *Key Performance Indicator* (KPI) untuk mengetahui efektivitas kinerja dibandingkan dengan alokasi sumberdaya yang ada pada masing-masing bidang;

Selain dari dukungan sumber daya internal, ***kedua*** yang tak kalah penting adalah peran dukungan sumber daya manusia secara eksternal yang dapat melibatkan para pemangku kepentingan bidang keamanan siber diantaranya dari kalangan pelajar/mahaiswa, aktivis bidang siber, kalangan pemerintah, bahkan masyarakat umum. Upaya BSSN untuk merangkul dan melibatkan semua eksponen telah dilakukan melalui program Peta Okupasi Keamanan Siber yang telah dilaksanakan. Pada dasarnya untuk menciptakan SDM unggul dibidang IT dan *cyber security*, Peta Okupasi ini

memetakan berbagai profesi berbasis keahlian terkait keamanan siber berdasarkan standar kompetensi, kualifikasi, level kompetensi nasional dan merupakan bagian dari Peta Okupasi Nasional TIK sebagai cara pandang dan cara bertindak untuk fungsi keamanan siber yang dikembangkan dalam bidang "*IT Security and Compliance*".

Peta Okupasi Keamanan Siber Nasional memetakan berbagai profesi berbasis keahlian terkait keamanan siber berdasarkan standar kompetensi, kualifikasi dan level kompetensi nasional. Peta tersebut disusun dengan tujuan memberikan kejelasan kepada tenaga kerja, akademisi dan industri mengenai definisi tugas, kompetensi, wewenang, dan karir di bidang keamanan siber. Peta Okupasi Keamanan Siber Nasional nantinya akan diturunkan menjadi berbagai dokumen standar kompetensi kerja nasional Indonesia.

SDM yang diperlukan adalah SDM yang berintegritas, nasionalis, berorientasi hasil, tanggap terhadap setiap risiko keamanan, dan mampu menjadi agen-agen yang menumbuhkan *security awareness* di lingkungannya. Peta okupasi adalah dokumen yang memuat pemetaan okupasi-okupasi di suatu bidang atau sektor berdasarkan standar kompetensi, kualifikasi dan level kompetensi nasional.

Peta Okupasi Keamanan Siber merupakan bagian yang tidak terpisah dari Peta Okupasi Nasional TIK yang disusun dalam Kerangka Kualifikasi Nasional Indonesia (KKNI). Peta Okupasi memetakan berbagai jenis jabatan, okupasi, dan profesi yang terdapat pada bidang Keamanan Siber.

Peta Okupasi Nasional Keamanan Siber, diharapkan dapat menjadi rujukan dalam pengembangan standar kompetensi, penyelenggaraan aktivitas sertifikasi kompetensi berbasisi skema okupasi, pengembangan kurikulum Pendidikan, pemetaan profil kebutuhan dan ketersediaan, serta pembuatan berbagai modul berbasis kompetensi.

Beberapa kompetensi yang memerlukan sertifikasi bidang keamanan siber dimulai dari level puncak di bidang keamanan siber seperti: *Chief Information Of Security Officer*, *Chief Of Information Security Officer (Ciso)*,

Cyber Risks Specialist, Cryptographic Engineer, ICT Security Product Lead, Evaluator, Threat Hunter, Penetration Tester, Cybersecurity Governance Officer, Digital Forensic Analyst, Cybersecurity Administrator dan masih banyak lagi jenis kompetensi yang lain.[52]

Keamanan Siber tidak akan terwujud tanpa adanya SDM yang mumpuni dalam pelaksanaannya. Ekosistem pengembangan SDM di bidang Keamanan Siber akan sulit terwujud tanpa adanya standar kompetensi dan pemetaan okupasinya. Karenanya, sebagai Instansi Pemerintah yang melaksanakan fungsi Keamanan Siber, Badan Siber dan Sandi Negara (BSSN) melakukan inisiatif untuk merumuskan Peta Okupasi Nasional Keamanan Siber. Dengan demikian inisiasi Peta Okupasi Nasional Keamanan Siber merupakan ikhtiar untuk membangun dan menciptakan ekosistem keamanan siber Indonesia yang tangguh dari aspek SDM yang berasal dari eksternal dan melibatkan berbagai eksponen.

20. Strategi Kerja sama Bilateral Keamanan Siber

Kerja sama keamanan siber yang telah dilakukan oleh pemerintah Indonesia merupakan bagian dari upaya untuk membangun pertahanan siber nasional, juga sebagai upaya untuk terlibat aktif dalam menjaga sistem keamanan siber di tingkat regional maupun internasional. Kerja sama dibidang keamanan siber menjadi sangat penting dan mendesak untuk dilakukan seluruh negara-negara dibelahan dunia terutama di era revolusi industri 4.0 dan *internet of Things* (IoT).

Payung hukum pelaksanaan kerja sama RI dengan negara lain merujuk kepada Undang-undang Republik Indonesia Nomor 37 Tahun 1999 tentang hubungan luar negeri. Di mana hubungan luar negeri dan politik luar negeri didasarkan pada pancasila, undang-undang dasar 1945, dan menganut prinsip bebas aktif yang diabdikan untuk kepentingan nasional. Politik Luar Negeri dilaksanakan melalui diplomasi yang kreatif, aktif, dan

[52] Untuk lebih detailnya mengenai kompetensi-kompetensi yang dilakukan beberapa sertifikasi bidang keamanan siber yang ada dalam Peta Okupasi Keamanan Siber dapat dilihat dalam panduan Peta Okupasi Keamanan Siber yang dapat diakses pada tautan berikut: https://bssn.go.id/peta-okupasi-nasional-keamanan-siber/

antisipatif, tidak sekedar rutin dan reaktif, teguh dalam prinsip dan pendirian, serta rasional dan luwes dalam pendekatan.

Selain itu juga terdapat Undang-undang Nomor 24 Tahun 2000 tentang Perjanjian Internasional. Di mana Pemerintah Republik Indonesia membuat perjanjian internasional dengan satu negara atau lebih, organisasi internasional, atau subjek hukum internasional lain berdasarkan kesepakatan, dan para pihak berkewajiban untuk melaksanakan perjanjian tersebut dengan iktikad baik. Dalam pembuatan perjanjian internasional, Pemerintah Republik Indonesia berpedoman pada kepentingan nasional dan berdasarkan prinsip-prinsip persamaan kedudukan, saling menguntungkan, dan memperhatikan, baik hukum nasional maupun hukum internasional yang berlaku. Dua payung hukum tersebut cukup penting untuk dipedomani dalam menjalin kerjasama keamanan siber baik yang bersifat bilateral maupun multirateral .

Salah satu kerja sama bidang keamanan siber yang mencatat perubahan besar di bidang keamanan siber adalah Council of Europe's Convention on Cybercrime (2001), yaitu kerja sama internasional pertama yang membahas kejahatan siber secara mendalam, bahkan konvensi ini menetapkan defenisi, tipologi serta batasan mengenai kejahatan siber, konvensi ini ditandatangani oleh 49 negara, empat diantaranya berada diluar Eropa seperti, Amerika Serikat, Jepang, Afrika Selatan dan juga Kanada. Sebanyak 39 negara telah meratifikasi konvensi ini, Belgia merupakan negara terakhir yang meratifikasi perjanjian ini pada tahun 2012, dan dua negara ikut sebagai peserta tambahan yaitu Australia pada tahun 2012 dan Republik Dominika pada tahun 2013 (Council of Europe Treaty Office, 2013).[53] Perjanjian yang ditulis secara komprehensif ini dapat menjadi acuan ASEAN dalam upaya mempersiapkan dan juga mensosialisasikan rancangan kerja sama ini diantara para anggota ASEAN sebelum bekerja

[53] Rahmat Haryama (2020) yang berjudul *"Asean Cyber Security Platform Kerja sama Keamanan Dunia Cyber Dikawasan ASEAN"*, Peperangan Asimetris, Fakultas Strategi Pertahanan Universitas Pertahanan Indonesia

dalam sebuah kerangka kerja nyata mengenai kerja samana keamanan siber.[54]

Seiring dengan adanya perkembangan zaman, Barrinha dan Renard menyebutkan bahwa diplomasi bukan hanya aktivitas yang melibatkan hubungan antar negara semata, tetapi juga melibatkan sejumlah aktor seperti regional dan international organisation, perusahaan multinasional, *sub-national actors*, *advocacy networks*, maupun individu yang berpengaruh.[55] Lebih jauh, Barrinha dan Renard juga menyebutkan bahwa konsep diplomasi meluas pada kebijakan baru yang kemudian masuk ke area politik yang belum dipetakan seperti negosiasi iklim hingga meluas ke dalam isu-isu siber.[56]

Pada saat ini, negara-negara anggota ASEAN telah berupaya untuk saling mendukung serta memperkuat dalam menjaga keamanan siber di wilayah Asia Tenggara. Upaya bersama ini tercetus dalam *ASEAN Ministerial Conference on Cybersecurity* (AMCC) yang merupakan Konferensi Tingkat Menteri ASEAN ke-5 yang membahas isu keamanan siber regional Asia Tenggara. Pertemuan AMCC merupakan rangkaian dari *Singapore International Cyber Week* (SICW) yang dilaksanakan selama lima hari mulai dari 5-9 Oktober 2020. Kegiatan ini diikuti oleh perwakilan dari sepuluh negara ASEAN di antaranya Indonesia, Brunei, Kamboja, Laos, Malaysia, Myanmar, Filipina, Singapura, Thailand dan Vietnam. Pada dasarnya poin penting dari pertemuan ini, yaitu adanya komitmen bersama seluruh negara anggota ASEAN untuk memperkuat sinergitas dan kolaborasi penyelenggaraan keamanan siber melalui berbagai kerja sama di tingkat regional maupun internasional, meskipun di dalam implementasinya kesepakatan tersebut sulit untuk dilaksanakan mengingat perbedaan

---

[54] Ibid

[55] Hidayat Chusnul Chotimah (2019), Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency, Ilmu Hubungan Internasional, Universitas Teknologi Yogyakarta, Politica Vol. 10 No. 2 November 2019, doi: https://doi.org/10.22212/jp.v10i1.1447

[56] Barrinha A, Renard T. Cyber-diplomacy: the making of an International society in the digital age. Global Affairs; (2017): 1-12. https://doi.org/10.1080/23340460.2017.1414924, Retrieved from http://www.tandfonline.

kapabilitas keamanan siber setiap negara ASEAN seperti terlihat di dalam index GCI . Pada pertemuan tersebut Kepala BSSN Hinsa Siburian, juga menyatakan bahwa Indonesia siap berkolaborasi dengan negara manapun untuk menjaga keamanan siber.[57] . Selain dalam lingkup regional ASEAN Indonesia sudah menandatangani kerja sama bilateral keamanan siber dengan Amerika Serikat, Belanda, Inggris Raya, Australia dan Tiongkok (**lampiran A taskap**). Berkaitan dengan kerja sama keamanan siber tersebut setidaknya dipedomani oleh beberapa pengertian tentang konsep Kerja sama keamanan (*Cooperative security*), lebih jauh diartikan oleh Mihalka sebagai keinginan dari negara-negara untuk bersama-sama memecahkan atau menyelesaikan suatu permasalahan bersama. Secara sederhana, Mihalka menggambarkan kerjasama dimana negara-negara bekerjasama untuk mengatasi ancaman dan tantangan yang bukan berasal dari aktor negara (ancaman non-tradisional). Menurutnya, konsep ini membedakan pemahaman antara kerjasama keamanan *(collective security)* atau ancaman bersama *(common security)* yang berkembang pada masa PD I, PD II serta Perang Dingin (Mihalka, 2005:114).

Pendapat terkait konsep *cooperative security* ini juga dikemukakan oleh mantan Menlu Australia, Gareth Evans pada era 1990-an, yang menyatakan bahwa konsep tersebut sebenarnya berkembang dari gagasan-gagasan tentang *collective security, common security* maupun *collective defense*. Perbedaannya, *common security* dan *collective security* berbicara mengenai komitmen negara-negara untuk mempertahankan diri dari ancaman, melalui kerjasama yang lebih difokuskan pada bidang militer. Sedangkan *cooperative security* justru melakukan kerjasama untuk isu-isu yang lebih multidimensional. *Cooperative security* ini merupakan bagian dari *comprehensive security,* sehingga penanganannya pun tidak selalu dengan penggunaan kekuatan militer (Evans, 1993:15-16). Di samping itu, ada tiga prinsip yang menaungi konsep *cooperative security* ini. Hal ini disebutkan oleh Amitav Acharya dan David Dewitt, yakni (Acharya, 2005) yaitu : ***pertama*** Inklusivitas, baik itu partisipannya maupun

[57] https://www.itworks.id/33493/negara-asean-sepakat-saling-kerja sama-perkuat-keamanan-siber.html

subyek yang menjadi masalah bersama. Dengan adanya perluasan pemahaman tentang keamanan maka masalah keamanan itu tidak lagi terbatas hanya pada masalah-masalah tradisional dan ancaman militer, tetapi juga meluas kepada masalah-masalah non-tradisional, seperti lingkungan, ekologi, dan fenomena demografis dan isu ancaman siber juga masuk kedalamnya; ***kedua*** Peningkatan dialog, dimana konsultasi reguler di antara para aktor dan partisipan akan memungkinkan kerjasama yang terjalin menjadi lebih formal, dan bisa diterapkan hingga ke level para pengambil keputusan; ***ketiga*** Masalah keamanan tidak lagi merupakan tanggung jawab satu negara yang kemudian bertindak secara unilateral, melainkan membutuhkan kerjasama dari aktor-aktor baik itu intra-negara, inter-negara maupun internasional.

Senada dengan pendapat Amitav, Gareth Evans juga menyebutkan ciri-ciri dari *cooperative security*. Menurutnya, kerjasama keamanan seperti ini lebih menekankan kepada strategi penjaminan daripada penangkalan dan inklusif daripada eksklusif. Selain itu, sifatnya pun tidak mengikat dalam hal keanggotaa dan lebih memilih kerjasama multilateral daripada bilateral. Lebih jauh lagi, *cooperative security* tidak menggunakan penyelesaian secara militer dan meski berasumsi negara adalah aktor utama dalam sistem keamanan, namun juga mengakui bahwa aktor non negara juga dapat berperan di dalamnya. Selanjutnya, sistem ini tidak membutuhkan pembentukan institusi keamanan yang formal, meski juga tidak menolaknya, dan di atas semua itu, *cooperative security* menekankan pada budaya dialog atas dasar multilateral (Evans, 1993:16).

Konsep *Cooperative Security* ini juga telah diadopsi oleh Indonesia, seperti kerjasama keamanan siber antara Indonesia dengan Australia **(lampiran A Taskap).** Melalui MOU keamanan siber RI dan Australia yang telah disepakati, kedua pemerintah juga menyatakan keinginannya untuk terus dan secara berkala mengadakan konsultasi dan dialog di semua level, termasuk di tingkat pemerintah. Konsultasi ini diperlukan untuk membuat dan mengambil kebijakan dalam menjaga dan menciptakan keamanan nasional serta keamanan bersama di ruang siber. Pelaksanaan dialog ini,

sekaligus juga membuktikan adanya upaya bersama dan bukan tindakan unilateral dalam menyelesaikan masalah keamanan siber bersama.

Berdasarkan analisis di atas, untuk mendukung keamanan siber nasional dalam kerangka ketahanan nasional yang tangguh, maka diperlukan peningkatan kerja sama bilateral dengan negara lain baik dalam lingkup regional ASEAN maupun internasional dengan memperhatikan faktor geopolitik, potensi sumber serangan siber dan tingkat kerawanan siber yang berasal dari luar Indonesia. Poin-poin kesepakatan kerjasama keamanan siber yang tertuang dalam MoU (*memorandum of understanding*) antara Indonesia dengan negara lain harus dapat ditindaklanjuti dan dilakukan evaluasi secara periodik dalam rangka keberlangsungan kerja sama yang saling menguntungkan antar negara pihak. Kerja sama bilateral perlu diprioritaskan menjadi pilihan mengingat kerja sama multilateral di bidang keamanan siber masih mencari bentuk untuk membangun norma keamanan siber yang mengikat antar negara di forum Internasional maupun forum regional ASEAN.

21. Langkah-langkah Strategis dalam Menjaga Keamanan Siber Nasional

Dalam menyusun Strategi Keamanan Siber Nasional (SKSN), BSSN yang menjadi *leading sektor* untuk pelaksanaan. Strategi ini akan menjadi acuan bersama seluruh pemangku kepentingan keamanan siber nasional dalam menyusun dan mengembangkan kebijakan keamanan siber di instansi masing-masing. Strategi yang disusun dalam menjaga keamanan siber nasional dirumuskan sesuai dengan visi BSSN, yaitu "*Menjadi institusi tepercaya dalam menjaga keamanan Siber dan Sandi Negara dengan menyinergikan berbagai pemangku kepentingan untuk ikut serta mewujudkan keamanan nasional dan meningkatkan pertumbuhan ekonomi nasional.*"

Dalam visi tersebut, dapat dituangkan secara kongkrit dalam misi BSSN yang lebih spesifik dan terukur diantaranya adalah: pertama, menjamin keamanan informasi di sektor pemerintah, infrastruktur informasi kritikal nasional, dan ekonomi digital dalam mewujudkan keamanan nasional dan meningkatkan pertumbuhan ekonomi nasional; kedua , membangun

dan menerapkan tata kelola keamanan siber dan sandi yang komprehensif; ketiga, membangun kemandirian teknologi keamanan siber dan sandi dengan mendorong tumbuhnya industri dalam negeri di bidang keamanan siber dan sandi; keempat, membangun, mengoordinasikan, mengolaborasikan, dan mengoperasionalkan sistem identifikasi, deteksi, mitigasi, manajemen krisis, penanggulangan, dan pemulihan terhadap ancaman, insiden, dan/atau serangan siber dan sandi; kelima, membangun budaya keamanan siber sebagai tatanan nilai budaya yang melekat dengan mendorong tumbuhnya budaya penggunaan internet yang aman dan nyaman oleh setiap warga negara Indonesia; keenam, menyediakan dan mengoptimalkan sumber daya keamanan siber dan sandi melalui proses pembelajaran dan peningkatan kualitas yang berkelanjutan dengan didukung manajemen perkantoran secara transparan dan akuntabel.

Dengan demikian untuk mengimplementasikan visi dan misi BSSN untuk menjamin keaman siber baik di institusi pemerintahan, swasta dan juga infrastruktur kritikal nasional serta untuk meningkatkan kinerja ekonomi digital dalam rangka mewujudkan keamanan nasional dilakukan strategi keamanan siber nasional yang terdiri dari:

Pertama, melakukan *joint research* dan literasi keamanan siber. Salah satu upaya yang dilakukan adalah melakukan join research dan literasi keamanan siber pada masyarakat dalam menyerap informasi serta menyelaraskannya dengan nilai-nilai budaya, agama, dan adat-istiadat kita yang menjunjung tinggi nilai-nilai harmonis. Hal ini sangat penting karena dengan adanya literasi dan edukasi kepada seluruh masyarakat dan pemangku kepentingan akan tumbuh *awareness* terhadap ancaman siber, atau setidaknya mengurangi terjadinya tindak kejahatan siber yang dapat mengancam persatuan dan kesatuan bangsa salah satunya adalah adanya ancaman hoax dan ujaran;

Kedua kerja sama dalam penyelenggaraan kegiatan sosialisasi, workshop dan forum ilmiah yang berkaitan dengan keamanan siber. Banyak kegiatan yang telah dilakukan oleh BSSN yang merupakan leading sektor di bidang keamanan siber di Indonesia. Umumnya kegiatan tersebut diawali

dengan penyelenggaraan sosialisasi secara massif dari kampus ke kampus, lembaga pemerintahan, asosiasi, hingga perusahaan-perusahaan yang tertarik dan membutuhkan informasi dan juga pengetahuan terkait *cyber security*. Dalam hal ini, rencana untuk ekspansi kegiatan sosialisasi perlu untuk diperluas hingga ke seluruh lapisan masyarakat terkait dengan penggunaan teknologi berbasis siber yang semakin meluas. Pengetahuan mengenai ruang siber dibutuhkan oleh masyarakat karena kehadiran teknologi yang saat ini telah menjadi bagian dariaktivitas sehari-hari manusia. Tindakan ini dapat membantu untuk meningkatkankesadaran masyarakat, sehingga tidak hanya sekadar melihat manfaat yangdapat diperoleh dari internet, melainkan juga mencegah terjadinya tindakancaman dan kejahatan yang muncul melalui ruang siber;

Ketiga kerja sama peningkatan dan pengembangan kompetensi sumber daya manusia serta penyelenggaraan pendidikan dan pelatihan. Strategi peningkatan dan pengembangan kompetensi telah dilakukan oleh BSSN dengan menggandeng beberapa stakeholder. BSSN bersama Pemerintah Daerah dan dunia pendidikan menyepakati kerja sama dalam penggunaan Sertifikat Elektronik. Kerja sama ini merupakan bentuk dukungan aspek keamanan dalam penyelenggaraan sistem elektronik milik instansi pemerintah melalui pemanfaatan sertifikat elektronik. BSSN telah bekerja sama dengan beberapa Pemerintah Pusat dan Pemerintah Daerah;

Keempat strategi pre-emtif dalam mengurangi atau menghindari tindak kejahatan siber dan serangan siber. Langkah preemtif sangat diperlukan dalam mencegah serangan siber dan tindak kejahatan siber di era revolusi industri 4.0 menjadi sangat fundamental untuk dioptimalkan sebagai bentuk perisai dalam menangkal dengan menciptakan harmonisasi di masyarakat, memberikan pemahaman dan kesadaran kepada pemerintah, kalangan dunia usaha dan dunia industri serta masyarakat luar agar lebih *aware* akan tindak kejahatan siber dan juga serangan siber.

Kelima Strategi pencegahan tindak kejahatan siber. Strategi yang perlu dilakukan untuk melakukan pencegahan tindakan serangan siber dan

kejahatan siber peran pemimpin dalam lembaga seperti BSSN, Kominfo, Polri, TNI, Intelijen menjadi sangat penting. Peran seorang pemimpin dibutuhkan untuk menggerakan, memberikan arahan serta memberi motivasi juga merencanakan langkah dan strategi penanganan serangan dan kejahatan siber benar-benar sangat krusial.

Keenam Strategi penegakan hukum di bidang siber. Upaya penegakan hukum untuk tindak kejahatan siber sudah dilakukan, akan tetapi pada saat melakukan penegakan hukum masih ada kendala yang dialami. Salah satunya adalah aspek apparat penegak hukum yang masih memerlukan penguatan pengetahuan dan kecakapan dibidang *cyber crime*. Kondisi obyektif penegak hukum di Indonesia masih mengalami kesulitan dalam menghadapi maraknya tidak pidana *cybercrime*. Hal ini disebabkan karena masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet), di samping itu aparat penegak hukum di daerah-daerah pun belum siap dalam mengantisipasi maraknya kejahatan siber ini karena masih banyak aparat penegak hukum yang belum memiliki kompetensi khusus dibidang keamanan siber, salah satunya adalah kemampuan dalam melakukan digital forensik.

Selain langkah-langkah strategis di atas, untuk menjaga keamanan siber diperlukan penguatan dan kesiapan infrastruktur serta SDM dalam membangun sistem keamanan siber Nasional untuk itu dapat dianalisis berdasarkan faktor strategis lingkungan eksternal dan internal. Dari **faktor eksternal**, dapat dibagi menjadi transformasi teknologi informasi, liberalisasi digital ekonomi, dan persoalan geopolitik, yaitu :

Pertama, dalam tranformasi teknologi informasi, dapat diketahui bahwa di era globalisasi ini, teknologi telah berada dalam kehidupan sehari-hari manusia. Transformasi ini tidak hanya sekadar menjadi fasilitas yang dapat digunakan untuk membantu aktivitas manusia, namun juga dapat menjadi pusat arus informasi yang membentuk *big data*. Penggunaan internet oleh masyarakat akan menghadapi ancaman risiko keamanan siber apabila tidak dapat dicegah sejak dini;

Kedua, liberalisasi digital ekonomi telah menjadikan kegiatan perekonomian bergantung pada penggunaan teknologi. Peralihan aktivitas dari konvensional menuju modern dengan teknologi internet menciptakan konsep transaksi pasar secara digital, yaitu *e-commerce*. Evolusi pasar ini juga menunjukkan perkembangan pesat di Indonesia karena aktivitas dan penggunaan teknologi yang mudah, cepat, dan murah. Di lain sisi, liberalisasi digital ekonomi juga berpotensi memunculkan ancaman siber, seperti kasus kebocoran data dari salah satu *market place* di Indonesia, yaitu Tokopedia;

Ketiga, aspek geopolitik yang menyulitkan dalam penindaklanjutan terhadap serangan siber. Ruang siber telah menciptakan kondisi di mana batas antar negara menjadi semakin pudar. Seseorang dapat mengakses berita dari negara lain secara mudah dan cepat. Keterbukaan akses informasi tersebut dapat menjadi ancaman serius yang dapat mengancam aktor mana pun, mulai dari pemerintah hingga individu.

Selanjutnya adalah **faktor internal** yang terdiri dari aspek demografi, hukum, politik, ekonomi, sosial budaya, dan pertahanan dan keamanan, yaitu: **Pertama**, dari aspek demografi dapat terlihat bahwa Indonesia menghadapi bonus demografi dengan didominasi oleh generasi Y dan Z. Kedua generasi tersebut cenderung lebih terbuka dan paham mengenai penggunaan teknologi. Internet telah menjadi kehidupan sehari-hari dari generasi Y dan Z tersebut. Namun, kurangnya edukasi mengenai ruang dan keamanan siber dapat berpotensi menyebabkan penggunaan internet secara tidak aman;

Kedua, aspek hukum yang terjadi di Indonesia saat ini sedang menghadapi pro kontra mengenai RUU KKS. Di tengah peningkatan penggunaan internet yang pesat ini, masyarakat membutuhkan adanya peraturan yang tidak hanya sekadar mengatur aktivitas mereka di ruang siber, melainkan juga menjaga data dan privasi dari serangan siber;

Ketiga, secara aspek politik, Indonesia tidak hanya mengalami pro kontra mengenai pengesahan RUU KKS, melainkan juga kejahatan siber yang sering terjadi ketika menghadapi persoalan politik dengan aktivitas

black campaign, ujaran kebencian, dan hoaks. Ketegangan antar pendukung pasangan calon politik yang disalurkan dengan kejahatan siber dapat merusak persatuan dan kesatuan Nasional;

Keempat, dari aspek ekonomi, masyarakat Indonesia telah lebih terbuka dalam penggunaan teknologi digital sebagai wadah dalam kegiatan jual beli. Kemudahan, kecepatan, dan biaya yang cenderung lebih murah meningkatkan aktivitas dan menjadi lapangan kerja baru bagi masyarakat;

Kelima, aspek sosial budaya dapat terlihat dari peningkatan angka penggunaan teknologi digital yang meningkat, bahkan mencapai setengah populasi Indonesia. Harga ponsel pintar yang semakin terjangkau dan ketersediaan layanan internet yang meluas mendorong kemudahan bagi masyarakat dalam mengakses internet. Penggunaan teknologi telah menjadi salah satu rutinitas masyarakat sehari-hari;

Keenam, dari aspek pertahanan dan keamanan, dapat diketahui bahwa peningkatan teknologi internet dan berbagai manfaat yang dapat diperoleh secara tidak langsung juga akan meningkatkan potensi munculnya ancaman dan risiko siber. Dalam hal ini, Negara dapat memaksimalkan penggunaan internet oleh masyarakatnya yang diikut dengan infrastruktur dan SDM guna mencapai keamanan siber dan mencegah serangan siber, baik dari dalam atau luar negeri. Saat ini, ruang siber telah menjadi perhatian yang penting guna menjaga pertahanan dan keamanan Indonesia dari tindak kejahatan siber.

Oleh karena itu dalam menghadapi tingginya serangan siber ke Indonesia maka negara memerlukan infrastruktur dan kesiapan SDM di bidang keamanan siber yang kompeten dan memiliki kualifikasi unggul dalam mendeteksi dini dan cegah dini beragam ancaman siber yang dapat mengancam NKRI. Apabila tidak dipersiapkan sejak dini untuk melakukan proteksi dan membentengi diri menghadapi ancaman berbagi ancaman siber dari dunia luar, dan tidak dapat mempersiapkan diri dalam menghadapi potensi *cyber warfare* maka akan berdampak pada sistem pertahanan dan keamanan Nasional Indonesia yang secara langsung akan melemahkan Ketahanan Nasional

BAB IV
PENUTUP

22. Simpulan

Keamanan siber dan ancaman *cyber war* merupakan salah satu bagian penting dalam upaya untuk menjaga kedaulatan negara terutama dalam rangka menciptakan pertahanan dan keamanan Nasional. Untuk menjaga kedaulatan dan ketahanan siber diperlukan regulasi, perundang-undangan serta kebijakan yang dapat menjadi payung hukum dari sistem keamanan siber. Selain itu juga diperlukan dukungan infrastruktur, sumber daya manusia, strategi yang tepat serta penguatan norma yang ada di ruang siber.

Fokus taskap ini adalah adalah "*Bagaimana upaya Indonesia dalam menjaga keamanan siber untuk memperkuat ketahanan nasional melalui kerja sama dengan negara lain?"*. Kemudian studi ini mencoba membaginya pertanyaan kajian sebagai berikut: Apakah peraturan perundang undangan yang ada sudah mendukung dalam menjaga keamanan siber Nasional?; Bagaimana kesiapan infrastruktur dan SDM dalam membangun sistem keamanan siber Nasional?; Bagaimana Strategi kerja sama keamanan siber yang akan dilakukan dalam memperkuat ketahanan nasional?

Analisis dan temuan yang ada dalam Taskap ini antara lain sebagai berikut: Melalui analisis dan peraturan perundang-undangan keamanan siber Indonesia bahwa sampai saat ini Indonesia belum memiliki regulasi yang mengatur keamanan dan ketahanan siber meski sudah ada UU ITE (Undang-Undang Nomor 19 Tahun 2016 Jo UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik). Keamanan siber masih menginduk pada beberapa regulasi lainya salah satu contohnya adalah Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

Upaya yang dilakukan pemerintah dalam hal ini BSSN yang bertindak sebagai *leading sector* untuk menjaga ketahanan dan keamanan siber sudah dilakukan sejak tahun 2018 yaitu dengan mengembangkan

infrastruktur keamanan siber, sistem deteksi dini ancaman siber yaitu melakukan bekerja sama dengan *Indonesia Honeynet Project (IHP).*

Melalui analisis yang ada bahwa sumber daya manusia secara internal yang ada dalam struktur sumber daya manusia pada BSSN masih memerlukan dukungan dan peningkatan serta penguatan masing-masing bidang. Selain itu juga yang tak kalah penting adalah peran dukungan sumber daya manusia secara eksternal yang dapat melibatkan para pemangku kepentingan bidang keamanan siber diantaranya dari kalangan pelajar/mahaiswa, aktivis bidang siber, kalangan pemerintah, bahkan masyarakat umum. Upaya BSSN untuk merangkul dan melibatkan semua eksponen telah dilakukan melalui program Peta Okupasi Keamanan Siber.

Melalui analisis tantangan keamanan siber Indonesia menunjukan bahwa secara pemeringkatan yang ada dalam *Global Cybersecurity Index* posisi Indonesia terus mengalami peningkatan dari tahun ketahun, tahun 2020, Indonesia ada di peringkat ke- 24 dengan jumlah skor CGI 94,88 dari 188 negara. Akan tetapi jumlah serangan siber juga terus mengalami peningkatan, selama 2017 sampai dengan 23 Juni 2021 total serangan siber ke Indonesia mencapai 639.020.915 serangan.

Melalui analisis strategi keamanan siber nasional, beberapa strategi BSSN dan pemangku kepentingan lainnya telah melakukan *join research* dan literasi keamanan siber. Hal itu dilakukan melalui penyelenggaraan sosialisasi, workshop dan forum ilmiah dengan melibatkan kampus, lembaga pemerintahan, asosiasi, perusahaan dan pemangku kepentingan lainya terkait dengan urgensi keamanan siber. BSSN dalam megembangkan SDM dilakukan melalui penyelenggaraan pendidikan dan pelatihan. Dalam lingkup Nasional telah dilaksanakan program unggulan BSSN yaitu peta okupasi keamanan siber nasional. Telah dilaksanakan strategi pre-emtif dalam mengurangi atau menghindari tindak kejahatan siber dan serangan siber dan juga telah dilakukan upaya pencegahan tindak kejahatan siber. Selain itu juga telah dilakukan upaya penegakan hukum dibidang siber.

Melalui analisis kerja sama keamanan siber menunjukan bahwa, kerja sama keamanan siber telah dilakukan oleh pemerintah Indonesia

merupakan bagian dari upaya untuk membangun pertahanan siber nasional. Kerja sama bilateral tersebut telah dilakukan dengan beberapa negara antara lain: dengan melakukan kerja sama bilateral keamanan siber dengan Australia, Belanda, Inggris Raya, Amerika dan Tiongkok. Kerja sama tersebut dilakukan dengan mempertimbangkan geopolitik Internasional, di mana BSSN sebagai koordinator Keamanan Siber Nasional melakukan kerja sama bilateral dengan negara-negara penting dan berpengaruh untuk menjaga keseimbangan dan netralitas Indoensia dalam dalam rangka menguatkan Ketahanan Nasional.

23. Rekomendasi

Melihat temuan dari karya tulis ini, beberapa rekomendasi diajukan sebagai tindak lanjut dari Taskap ini:

a. Pemerintah bersama DPR RI perlu segara untuk membahas dan mengesahkan RUU keamanan dan ketahanan siber. Sebelum RUU tersebut disahkan terlebih dahulu perlu adanya kajian secara komprehensif dengan melibatkan partisipasi aktif publik atau *Public Private Dialogue (PPD)* dalam penyusunannya yaitu dengan merangkul akademisi, para professional dan expert di bidang keamanan siber, dari kalangan pebisnis, perusahaan teknologi, pemerintah, dan juga para pihak yang memiliki kemampuan teknis terkemuka yang berasal dari luar pemerintah, industri komersial, dan pemangku kepentingan serta masyarakat untuk membuat rekomendasi penting tentang bagaimana menggunakan solusi teknis baru dan praktik terbaik di bidang siberr untuk membangun keamanan siber nasional yang unggul.
b. Perlu adanya dukungan infrastruktur teknologi dan modernisasi IT khususnya bidang keamanan siber dan juga perlu adanya investasi untuk membangun pengembangan kapasitas mengenai masalah keamanan siber terkait dengan perlindungan infrastruktur informasi vital, manajemen keamanan data, perlindungan informasi pribadi dan respon ancaman siber.
c. Perlu adanya harmonisasi dan konvergensi antara lembaga-lembaga terkait dan pemangku kepentingan di bidang keamanan siber agar

strategi dan langkah-langkah keamanan siber dapat diimplemtasikan dan berjalan secara tersruktur dan massif. Seperti contohnya adalah Pemerintah menugaskan Kementerian Pendidikan, Kebudayaan dan Ristek untuk mendukung program riset unggulan di bidang keamanan siber dan program Peta Okupasi Keamanan Siber Nasional.

d. Pemerintah Republik Indonesia perlu meningkatkan kapasitas finansial terutama untuk mendukung aparat penegak hukum untuk meningkatkan kompetensinya di bidang keamanan siber. Salah satu contohnya adalah peningkatan kompetensi penegakan hukum di bidang *computer/digital forensic* untuk Polri dari tingkat mabes hingga polres, dengan BSSN sebagai leading sektor yang mengawal program tersebut.
e. Kerja sama keamanan siber bilateral dengan negara lain perlu terus dilakukan mengingat semakin tingginya serangan siber yang berasal dari negara besar seperti India dan Russia sesuai data dari Honeynet BSSN. Kerja sama keamanan siber yang telah dilakukan dengan tiap negara perlu terus dirawat melalui pelaksanaan dari poin-poin kerja sama yang telah disepakati serta secara periodik dilakukan evaluasi bersama di antara negara pihak.

DAFTAR PUSTAKA

A. Aco Agus (2015), Jurnal integrasi, Volume 1, Nomor 2, Agustus 2015, Program Studi Pendidikan Ilmpu Pengetahuan Sosial Pasca Sarjana Universitas Negeri Makassar, ISSN: 2443-2822

Anggoro., Kusnanto .,2003, *"Keamanan Nasional, Pertahanan Negara, dan Ketertiban Umum"*, Centre for Strategic and International Studies, Jakarta, Makalah Pembanding Seminar Pembangunan Hukum Nasional VIII. diselenggarakan oleh Badan Pembinaan Hukum Nasional, Departemen Kehakiman dan HAM RI Hotel Kartika Plaza, Denpasar, 14 Juli 2003

Barrinha A, Renard T. Cyber-diplomacy: the making of an International society in the digital age. Global Affairs; (2017): 1-12. https://doi.org/10.1080/23340460.2017.1414924, Retrieved from http://www.tandfonline

Buku Putih Pertahanan Indonesia 2014, Kementerian Pertahanan Republik Indonesia

Carter, Ashton., Perry., William /John D. Steinbrunner., 2000., A New Concept of Cooperative Security; Brookings Institution, Washington D.C. 1992; p. 7 .This definition coincides with the authors earlier distinction between "preventive" and "repressive" instruments of security policy; see H.Vetschera, "International Law and International Security -The Case of Force Control", in: J. Delbrück (ed.), German Yearbook of International Law, vol. 24, Berlin, 1982.

Clarke, Richard A and Knake, Robert.., 2010. *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins e-books, ISBN:9780061992391, 0061992399.

Cohen, Richard and Mihalka, Michael., 2001., *Cooperative Security: Individual Security to International Stability*, George C. Marshall Center for Security Studies, George C. Marshall Center

Chusnul Chotimah (2019), Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency, Ilmu Hubungan Internasional, Universitas Teknologi

Yogyakarta, Politica Vol. 10 No. 2 November 2019, doi: https://doi.org/10.22212/jp.v10i1.1447

Cynthia A. Watson (2008) dalam *U.S National Security, A Reference Handbook*, Second Edition, (Contemporary world issues), ABC-CLIO, Inc, Santa Barbara, California 93116-1911, pg. 1-2.

Denning, Dorothy E. 2010. *"Cyber Conflict as an Emergent Social Phenomenon,"* in Thomas J Holt and Bernadette Hlubik Schell (eds), Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (Hershey, PA: IGI Global, 2010)

Denning. Peter J. & Dorothy E. Denning. (2010) *The Profession of IT Discussing Cyber Attack. Communcations of the Acm*, September 2010, Vol 53, No. 9. See., https://doi.org/10.1145/1810891.1810904

Dewitt, D. 1994 *Common, Comprehensive and Cooperative Security. The Pacific Review*, 7, 1-15. See also, http://dx.doi.org/10.1080/09512749408719067

Dunn-Cavelty, M. (2013). *From Cyber-Bombs to Political Fallout: threat Representations with an impact in Cyber-Security Discourse*. International Studies Review, 15: pp. 105-122

Eriksson., & Giacomello, G., 2009. *Who Controls the Internet ? Beyond the Obstinacy or Obsolescence of the State. International Studies Review*, 11, 205–230. https://doi.org/10.1111/j.1468-2486.2008.01841.x

Ghernaouti,S. 2009., *Cybersecurity Guide for Developping Countries. Geneva: International Telecommunication Union*, 2009. Pg 28

Hansen, L. & Niessanbaum, H. (2009). *Digital Disaster, Cyber Security, and the Copenhagen School*. International Studies Quarterly, 53: pp. 1155-1175

Haryama., Rahmat, 2020. ASEAN Cyber Security Platform Kerja sama Keamanan Dunia Cyber Dikawasan ASEAN. Peperangan Asimetris, Fakultas Strategi Pertahanan Universitas Pertahanan Indonesia

H.K.Siburian,., 2016. *Emerging Issue in Cyber Crime: Case Study Cyber Crime in Indonesia*. Int. J. Sci. Res. 5, 2013–2016. https://doi.org/10.21275/ART20162818

International Encyclopedia of the Social Sciences (1968), Volume 11, Editor, David L. Sills, The Macmillan Company & The Free Pres pg. 40

John Baylis, *"International and Global Security in The Post-Cold War Area, dalam The Global of World Politic: An Introduction to International Relations*., Third Edition, Ed John Baylis dan stave Smith,. New York: Oxford University Press, 2008 hal 300 dan lake and Morgan dalam Buzan, dkk, 2003, hal 10. Penulis mengutipnya dalam Yayan M. Yani, Ian M, Emil M, "Pengantar Studi Keamanan", Intrans Publishing, Malang, 2017, hal 4.

Katsumata, Hiro (2009) , *ASEAN's Cooperative Security Enterprise Norms and Interests in the ASEAN Regional Forum*, Palgrave Macmillan in the UK,

Kris Wijoyo Soepandji , Muhammad Farid (2018), *Konsep Bela Negara Dalam Perspektif Ketahanan Nasional,* Jurnal Hukum dan Pembangunan Tahun ke-48 No. 3 Juli-September 2018, Universitas Indonesia, Jurnal Hukum & Pembangunan 48 No. 3 (2018): 436-456 ISSN: 0125-9687 (Cetak) E-ISSN: 2503-1465 (Online)

Laurell, Christofer; Sandström, Christian (December 2017). "*The sharing economy in social media: Analyzing tensions between market and non-market logics".* Technological Forecasting and Social Change. 125: 58–65

Laporan Tahunan 2018 Honeynet Project BSSN-IHP, ISSN 2655-8467 Volume 1 Tahun 2018. Laporan tersebut dapat diakses pada: https://bssn.go.id/wpcontent/uploads/2019/02/Laporan-Tahunan-Honeynet-Project-BSSN_IHP-2018.pdf

Laporan Tahunan 2019 Honeynet Project BSSN-IHP, ISSN 2655-8467 Volume 1 Tahun 2019. Laporan tersebut dapat diakses pada tautan berikut: https://cloud.bssn.go.id/s/MNropQrMbsQFmS6#pdfviewer

Laporan Tahunan 2020 Honeynet Project BSSN-IHP, ISSN 2655-8467 Volume 1 Tahun 2020. Laporan tersebut dapat diakses pada tautan berikut: https://cloud.bssn.go.id/s/q5Hx6ifSj86cKnA#pdfviewer

L. Carlson G. Bassett, et al (2012). *Resilience: theory and application. Argonne National Laboratory*. Oak Ridge, p, 11

Lewis, James, 2013., *"Hidden Arena: Cyber Competition and Conflct in Indo-Pacifi Asia,"* prepared for the Lowy Institute MacArthur Asia Security Project, March 7, 2013

Maria Lavinia Andrei, Lavinia Mihaela Dinca (2012) dalam *Cyber Security Policy. A methodology for Determining a National Cyber-Security Alert Level*, Informatica Economică vol. 16, no. 2/2012 pg. 103-115

Masyarakat ASEAN, 2014., *"Kerja sama ASEAN-Australia semakin Meningkat"*, Masyarakat ASEAN Edisi 6, 2014, p 11

Matthew Fraser (2009) Geopolitics; An entirely new form of virtual weaponry is transforming the dynamics of geopolitics, Spain's International Image and Public Opinion ARI 144/2009 Date: 14/10/2009, URL: http://biblioteca.ribei.org/id/eprint/1721/1/ARI-144-2009-I.pdf

Mely Caballero-Anthony (2004), Non-state regional governance mechanism for economic security: the case of the ASEAN Peoples' Assembly, *The Pacific Review Journals,* Pages 567-585 | Published online: 11 Aug 2006, https://doi.org/10.1080/09512740420003260 78

Mohadib (2018), *Prospek dan Tantangan Komunitas Politik Keamanan ASEAN*, Jurnal Kajian Lemhannas RI Edisi 35 September 2018, hal 35-48

Peta Okupasi Keamanan Siber dapat dilihat dalam panduan Peta Okupasi Keamanan Siber yang dapat diakses pada tautan berikut: https://bssn.go.id/peta-okupasi-nasional-keamanan-siber/

Peta Kemampuan Siber Beberapa Negara Hasil Operasi Infrastruktur Ti Dan Siber Luar Negeri, BSSN 2020

Putranti *et.al* (2020), *Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah*, Jurnal Ketahanan Nasional Vol. 26, No. 3, Desember 2020, Hal 359-379 DOI:http://dx.doi.org/ 10.22146/jkn.57322, ISSN:0853-9340(Print), ISSN:2527-9688(Online), Online sejak 28 Desember 2015 di :http://jurnal.ugm.ac.id/JKN

Rebecca Slayton (2017) International Security, Vol. 41, No. 3 (Winter 2016/17), pp. 72–109, doi:10.1162/ISEC_a_00267

Rifkin, J. 2014. *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*. New York: St. Martin's Press.

Rollins, John, and Henning. Anna C. 2009. *Comprehensive National Cybersecurity Initiative Legal Authorities and Policy Considerations*. Washington, D.C.: Congressional Research Service,

Sang-Yun Lee and Hong-Joo Yoon (2019) "A Study on the 4th Industrial Revolution and E-Government Security Strategy In Terms of the Cyber Security Technology of Intelligent Government", Journal of the KIECS. pp. 369-376, vol. 14, no. 2, Apr. 30. 2019, t. 94, pISSN 1975-8170 | eISSN 2288-2189 http://dx.doi.org/10.13067/JKIECS.2019.14.2.369

Setiadi, F., Sucahyo, Y.G., Hasibuan, Z.A., 2012. *An Overview of the Development Indonesia National Cyber Security*. Int. J. Inf. Technol. Comput. Sci. (IJITCS) 6, 106–114. Lihat juga, Prayudi, Y., 2015. A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia 1–8. https://doi.org/10.5815/ijcnis.2015.11.01

Suradinata, Ermaya, 2005, *Geopoliti dan Geostategik Dalam Mewujudkan Negara Kesatuan Republik Indonesia*, Jurnal Ketahanan Nasional No. VI Agustus 2005

Suryohadiprojo, Sayidiman, 1997, Ketahanan Nasional Indonesia, Jurnal Ketahanan Nasional No. II 1 April 1997 Program Studi Ketahanan Nasional, PTS UGM, Yogyakarta.

Varkey Foundation (2017) *Generation Z: Global Citizenship Survey What The World's The Young Feel and Think*, pg. 14.


DHARMMA
TANHANA
MANGRVA

Sumber dari Internet

News dari CNN Indonesia tentang “Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat”, diakses pada Minggu 6 Juni 2021. Untuk lebih detailnya dapat dilihat pada tautan berikut: https://www.cnnindonesia.com/teknologi/20210606200515-185-650991/kebocoran-data-pribadi-bpjs-kesehatan-bakal-digugat

New York Times, 4 September 2019, "The Secret History of the Push to Strike Iran Hawks in Israel and America Have Spent More than a Decade Agitating for War Against the Islamic Republic’s Nuclear Program. Will Trump Finally Deliver?"

Naskah Akademik Rancangan Undang-undang Keamanan dan Ketahanan Siber yang di susun oleh DPR RI. Dokumen dapat diunduh pada tautan berikut ini: https://www.dpr.go.id/doksileg/proses1/RJ1-20190617-025848-5506.pdf

N. Perlroth, M Scott and S. Frenkel, “Cyberattack Hits Ukraine Then Spreads Internationally”, The New York Times, pada tautan brikut: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf

Indonesian Defense University, Technology Perscpetive: National Cyber Security, http://binkorpspelaut.tnial.mil.id/index.php?option=com_docman&task=doc_download&gid=6&Itemid=22.

Indonesia Alami 205 Juta Serangan Siber Sepanjang 2017” yang dimuat dalam Liputan 6.com. untuk lebih detailnya dapat dilihat dalam https://www.liputan6.com/tekno/read/3203987/indonesia-alami-205-juta-serangan-siber-sepanjang-2017

Katadata.co.id dengan Judul “Nasib Indonesia di Tengah "Perang Dingin" Teknologi Kecerdasan Buatan” Penulis: Desy Setyowati.: https://katadata.co.id/desysetyowati/digital/60477c5e83a7c/nasib-indonesia-di-tengah-perang-dingin-teknologi-kecerdasan-buatan

Policy Brief Recommendation: Cyber Security and Defence Policy of Indonesia. https://www.researchgate.net/publication/326155837_Policy_Brief_Recommendation_Cyber_Security_and_Defence_Policy_of_Indonesia

Siaran Pers pers yang disampaikan oleh Menko Bidang Perekonomian No. HM.4.6/30/SET.M.EKON.2.3/03/2020 tanggal 10 Maret 2020 di Jakarta. Untuk artikel lengkap dapat diunduh dalam link berikut: https://www.ekon.go.id/publikasi/detail/178/indonesia-belanda-sepakat-perkuat-kerja-sama-perdagangan-investasi-hingga-pariwisata

The Straits Times Asia,Cyber attack: Ransomware cases reported in Asia, http://www.straitstimes.com/asia/east-asia/cyber-attack-ransomware-cases-reported-in-asia,

Edmon Makarim, Indonesian Legal Framework for Cybersecurity, http://www.nisc.go.jp/security site/campaign/ ajsympo/pdf/lecture2.pdf,

: https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

Geopolitics Journal home page - http://www.tandf.co.uk/journals/titles/14650045.asp

https://bssn.go.id/badan-siber-dan-sandi-negara-dan-universitas-swiss-german-tandatangani-perjanjian-kerja sama-implementasi-honeypot-sebagai-sensor-deteksi-malware/

https://www.itworks.id/33493/negara-asean-sepakat-saling-kerja sama-perkuat-keamanan-siber.html

https://obamawhitehouse.archives.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know

Lampiran A : LIST Kerjasama Bilateral Keamanan Siber Indonesia

I. I. Kerja sama Bilateral keamanan siber dengan Australia

Indonesia melalui Kementerian Luar Negeri dan Badan Siber dan Sandi Negara serta Australia melalui Kementerian Luar Negeri Australia serta *Cyber Affairs Department of Foreign Affairs and Trade* sepakat melakukan kolaborasi untuk mencapai *cyber security system* dimana kedua negara berkomitmen untuk membangun internet yang aman bagi kedua negara. Penandatanganan nota kesepahaman dimulai pada tahun 2017 di Canberra sebagai awal mulainya kerja sama di bidang *cyber security*.

Pada *Cyber Policy Dialogue 2018* antara Indonesia-Australia dirumuskan kerja sama kedua belah pihak untuk bersepakat dalam hal penenganan keamanan siber dan isiden siber untuk kepantingan pertahanan dan keamanan kedua negara. Isi dalam kerja sama tersebut memuat tentang berbagi informasi mengenai hukum dan peraturan perundang-undangan, strategi siber nasional dan kebijakan, serta prosedur manajemen penanganan insiden siber.

Kedua belah pihak juga bersepakat akan berkonsultasi dan berkoordinasi dalam hal respon insiden siber dan informasi ancaman siber, khususnya ketika insiden siber tersebut memiliki dampak langsung kepada Indonesia dan Australia. Selain itu kedua belah pihak akan berbagi pandangan, pengalaman, pembelajaran, dan praktik terbaik mengenai bidang siber.

II. II. Kerja sama Bilateral keamanan siber dengan dengan Amerika

Kerja sama keamanan siber antara Indonesia dengan Amerika ditunjukan dengan penandatanganan *Letter of Intent* (LoI) di Jakarta pada 28 September 2018. Acara penandatanganan LoI tersebut dihadiri oleh Perwakilan dari Kementerian/Lembaga terkait, antara lain, yaitu Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan; Badan Siber dan Sandi Negara; Kepolisian Republik Indonesia; dan unit/satuan kerja terkait di Kementerian Luar Negeri.

LoI tersebut menjadi kerangka kerja untuk memajukan kerja sama dan pembangunan kapasitas ruang siber dan keamanan siber nasional serta memperkuat kelembagaan Badan Siber dan Sandi Negara (BSSN) sebagai pelaksana tugas dan pengkonsolidasi keamanan siber nasional.

Beberapa area kerja sama yang diatur dalam ruang lingkup LoI tersebut meliputi: diskusi tentang pengembangan strategi ruang siber nasional Kemampuan manajemen insiden nasional; kapasitas dan kerja sama penanggulangan kejahatan siber; kemitraan dengan banyak pemangku kepentingan; penggalakan kesadaran akan keamanan siber; dan kerja sama di berbagai forum kawasan sesuai kebutuhan.

III. III. **Kerja sama Bilateral keamanan siber dengan Belanda**

Kerja sama keamanan siber menjadi sangat penting bagi kedua negara, mengingat banyak invrastruktur vital yang terkait dengan keamanan system informasi dan teknologi yang harus dilindungi dari serangan siber agar akslerasi ekonomi digital semakin cepat. Untuk itu kedua negara, telah ditandatangani *Letter of Intent* di bidang kerja sama siber oleh Kepala BSSN dan Menteri Luar Negeri Belanda pada hari ini, 3 Juli 2018 di Kementerian Luar Negeri Republik Indonesia disaksikan Menteri Luar Negeri Republik Indonesia, setelah sebelumnya pada bulan Juni, BSSN mengadakan pertemuan dengan perwakilan Belanda di kantor BSSN.[58]

Penandatangan *Letter of Intent* ini merupakan langkah awal dan bentuk komitmen Indonesia dan Belanda seperti misalnya dalam berbagi informasi dalam bidang hukum, kebijakan nasional dan strategi kebijakan manajemen yang terkait dengan ranah siber, pertukaran sudut pandang, pengalaman, pembelajaran dan penerapan terbaik terkait ranah siber dan penguatan kapasitas dan perbantuan kelembagaan dan pengembangan teknologi di bidang keamanan siber melalui jaringan dan program pelatihan dan

[58] https://bssn.go.id/penandatangan-letter-of-intent-kerja_sama-bidang-keamanan-siber-kepala-bssn-dengan-menlu-belanda/

pendidikan, pertukaran kunjungan kenegaraan, analisis dan studi lapangan, seminar dan konferensi.[59]

Pertemuan ke-1 Dialog Keamanan Siber Indonesia-Belanda merupakan tindak lanjut dari *Letter of Intent*(*LoI*) antara BSSN dengan Kementerian Luar Negeri Kerajaan Belanda dalam rangka meningkatkan kerja sama bilateral ranah siber yang telah terselenggara pada tanggal 3 Juli 2018.[60] Bentuk kongkrit dari kerjasam tersbut akan dilaksanakan dengan program lanjutan yaitu program Beasiswa Pelatihan Stuned V *Tailor Made Training* (TMT) dengan Tema *Evidence-Based Cybersecurity Policy Making Training Program*. Pelatihan rencananya dilaksanakan secara *offline* di Indonesia pada bulan Agustus 2021.

Harapan dari adanya dialog tersebut adalah memberikan kontribusi yang nyata bagi kemajuan *cybersecurity*, penurunan serangan siber, serta turut menciptakan stabilitas dan perdamaian pada kedua negara, untuk kawasan dan bahkan untuk dunia internasional.

Selain itu juga dalam dialog tersebut juga antara Indonesia-Belanda dapat bertukar informasi mengenai progress upaya konsensus hukum siber internasional yang sampai dengan saat ini masih dalam tahap pembahasan pada sidang *United Nations Group of Governmental Experts (GGE) – Open-Ended Working Group (OEWG)*.

IV. IV. Kerja sama Bilateral keamanan siber dengan Inggris Raya

Republik Indonesia mengisiasi kerja sama di sektor keamanan siber. Pada hari Selasa 14 Agustus 2018 di Kantor Kementerian Luar Negeri, Jakarta Pusat. Pemerintah Republik Indonesia telah menandatangani nota kesepahaman *(Memorandum of Understanding)* dengan pemerintah Inggris Raya dalam hal kerja sama di bidang keamanan siber *(cyber security).*

---

[59] Ibid

[60] https://bssn.go.id/tingkatkan-kerja sama-bilateral-bssn-gelar-the-1st-cybersecurity-dialogue-indonesia-belanda/

Pokok-pokok yang tertuang dalam kerja sama di bidang keamanan siber yang meliputi:[61]

1) Implementasi dan Pengembangan Strategi Keamanan Siber Nasional

Indonesia dan Inggris Raya sepakat untuk menyelenggarakan pertukaran informasi dalam penyusunan kebijakan keamanan siber nasional dan penerapannya. Kerja sama ini diharapkan dapat memberikan kontribusi dalam penyusunan norma dan standar berperilaku global di ranah siber dimana saat ini menjadi perhatian dunia.

2) Pengelolaan Insiden Siber

Substansi kerja sama ini dikhususkan untuk melakukan langkah tindak dalam penanganan insiden siber yang salah satunya adalah dengan melakukan pertukaran *point of contact* masing-masing negara sebagai pintu awal koordinasi. Pertukaran *point of contact* ini berfungsi sebagai mekanisme konsultasi dan koordinasi ketika terjadi insiden siber baik secara global maupun di negara masing-masing untuk saling menemukenali bentuk serangan, hal ini dapat memudahkan untuk menyusun solusi bersama.

3) Kejahatan Siber

Ranah *cybercrime* atau kejahatan siber dan penegakan hukum saat ini berada di Kepolisian Republik Indonesia. Namun, poin inti kerja sama ini adalah join exercise dalam upaya penguatan kapasitas di bidang cyber forensics dan kemampuan investigasi barang bukti digital di mana tugas ini diemban oleh salah satu Deputi di BSSN.

4) Pelatihan dan Kampanye Kesadaran Keamanan Siber

Indonesia dan Inggris Raya akan saling bertukar pengalaman dalam mengkampanyekan kesadaran keamanan informasi dan siber untuk masyarakat, serta mengedukasi masyarakat tentang nilai infomasi dan dampak penyalahgunaannya. Sedangkan dalam hal pelatihan, BSSN akan

---

61 https://bssn.go.id/bssn-tandatangani-nota-kesepahaman-kerja sama-di-bidang-keamanan-siber-dengan-pemerintah-inggris-raya/

menjalin kerja sama teknis untuk meningkatkan keterampilan dan keahlian SDM siber untuk mencapai ketahanan ranah siber Indonesia yang kuat.

5) Peningkatan Kapasitas

Bersama Inggris Raya, pemerintah Indonesia akan mengggalakan kerja sama riset dengan akademisi di kedua negara dalam mendukung perkembangan riset di tanah air khususnya bidang keamanan siber. Selain itu, melalui poin kerja sama ini pemerintah Indonesia dengan Inggris Raya bisa menjalin kerja sama di bidang industri siber yang tentunya dikonsolidasikan melalui BSSN.

Dalam kerja sama tersebut, BSSN sebagai wakil dari Indonesia memegang teguh sikap-sikap sebegai berikut:[62] *pertama*,dalam menyelenggarakan kerja sama luar negeri, BSSN tetap memegang politik bebas aktif termasuk kerja sama di bidang keamanan siber; *kedua*, untuk itu, sikap BSSN terhadap kerja sama dengan Inggris Raya adalah tetap mengedepankan prinsip terbuka, kesetaraan, keberimbangan dan saling menguntungkan antar kedua belah pihak serta tetap menghormati hukum yang berlaku di internal masing-masing pihak; ketiga, dalam menyusun kerja sama ini, Indonesia tidak menempatkan diri sebagai pihak penerima saja tetapi juga sebagai pihak yang mampu mandiri dan berkontribusi aktif dalam prinsip kesamaan posisi di ranah siber; *keempat*, Negara Inggris Raya merupakan mitra strategis Indonesia di wilayah Eropa dan juga di beberapa forum internasional.

V. **Kerja sama Bilateral keamanan siber dengan Republik Rakyat Tiongkok**

Kerja sama Leamanansiber RI-Tiongkok kedua negara ini ditunjukkan dengan penandatangan MoU Pada tanggal 12 Januari 2021 bentuk kerja sama keamanan siber tersebut terdiri dari bidang-bidang sebagai berikut:

1) Mendorong pertukaran informasi mengenai system regulasi terkait tata kelola ruang siber yang dapat mencakup pertkukaran dalam hal

[62] Ibid

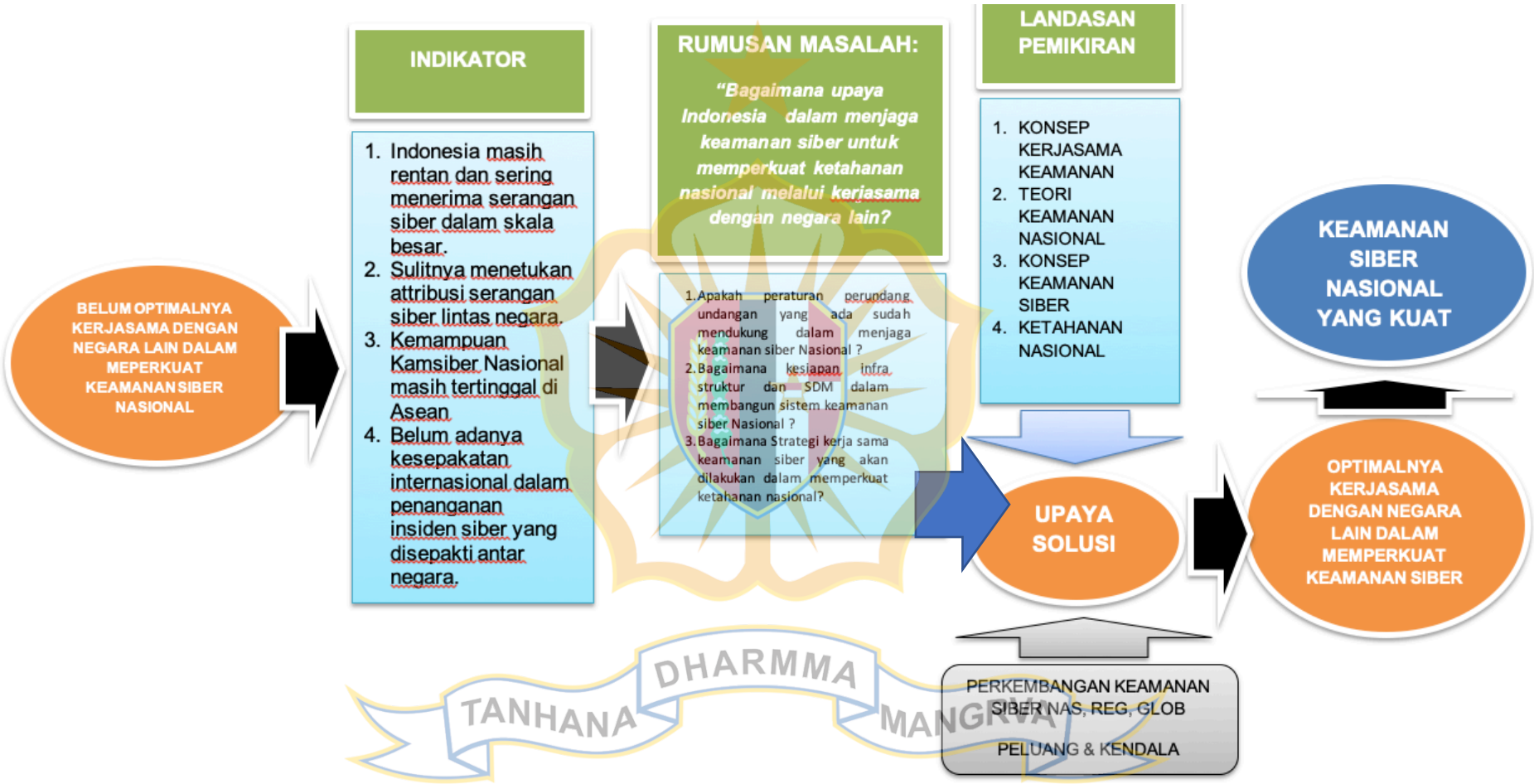
hukum dan perundang-undangan, regulasi, dan kebijakan manajemen terkait ruang siber;

2) Berbagi pandangan, pengalaman, pembelajaran dan praktik terbaik tentang pelindungan infrastruktur informasi vital, respons ancaman siber, dan kerja sama di masing-masing pihak;
3) Melaksanakan dan memfasilitasi dialog tentang isu keamanan siber antara pemerintah, institusi, akademisi, industry komersial, dan pemangku kepentingan terkait lainya serta mendorong rasa saling percaya dan kerja sama dibidang keamanan data;
4) Mendorong dan mengkoordinasikan kunjungan para pakar keamanan siber antara Indonesia dengan Tiongkok termasuk antar instansi pemerintah, akademisi, industry komersial, dan pemangku kepentingan terkait lainya melalui program dialog siber, konfrensi, symposium, kursus dan seminar;
5) Memfasilitasi pertukaran dan program pelatihan tentang teknologi dan metode pertahanan ruang siber diantara para pemangku kepentingan yang terkait, sebagaimana disepekati para pihak;
6) Mendorong kerja sama dalam pengembangan kapasitas mengenai masalah keamanan siber terkait dengan perlindungan infrastruktur informasi vital, manajemen keamanan data, perlindungan informasi pribadi dan respon ancaman siber;
7) Area kerja sama lainnya dibidang keamanan siber yang disepakati Bersama oleh para pihak;

LAMPIRAN B – ALUR PIKIR

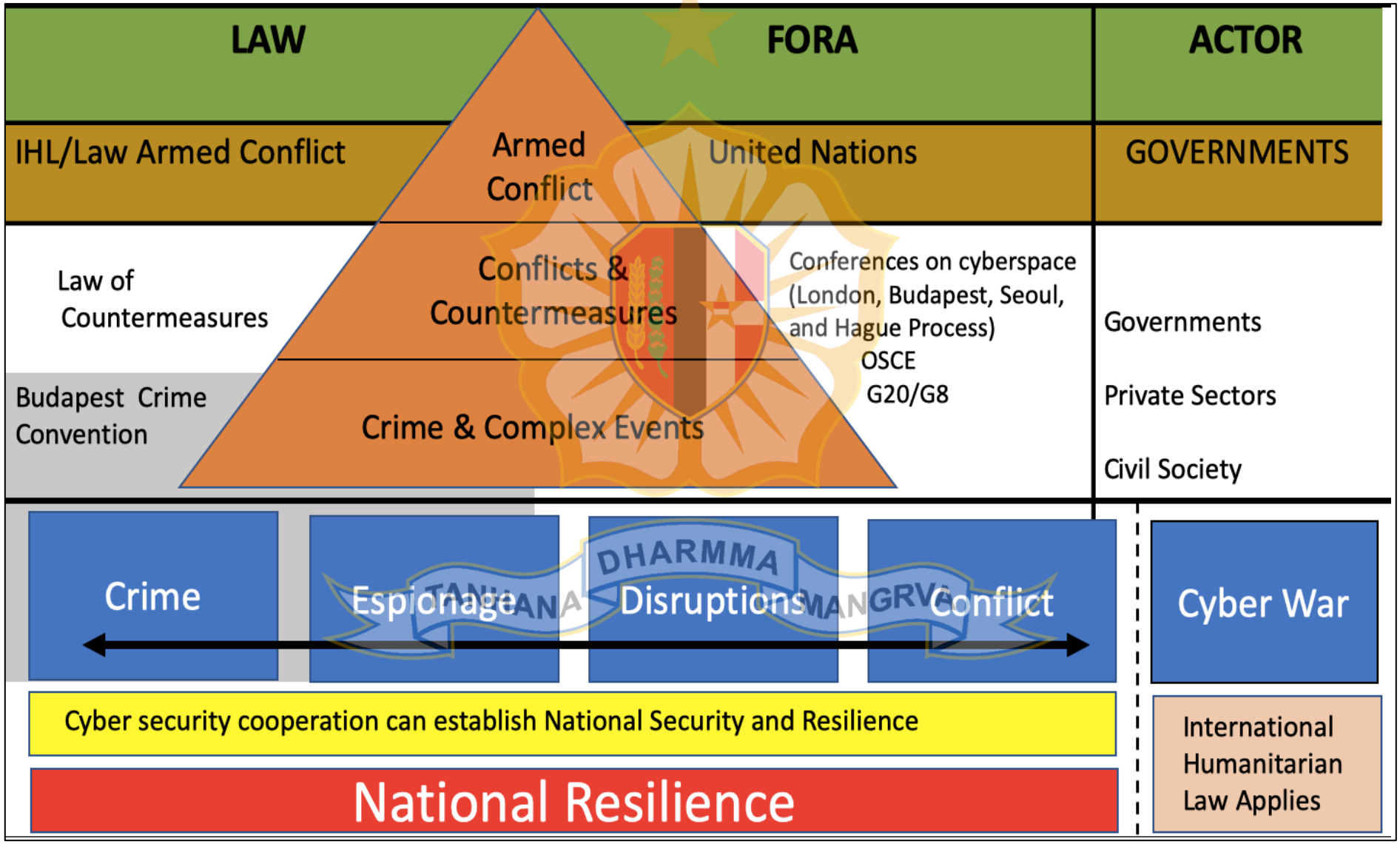
"KERJA SAMA KEAMANAN SIBER INDONESIA DENGAN NEGARA LAIN DALAM KERANGKA KETAHANAN NASIONAL"

==========



LAMPIRAN C – KERANGKA TEORITIS

"KERJA SAMA KEAMANAN SIBER INDONESIA DENGAN NEGARA LAIN DALAM KERANGKA KETAHANAN NASIONAL"



LAMPIRAN D – RIWAYAT HIDUP

Nama	:	**Dr. Sulistyo, S.Si., S.T., M.Si**
Tempat/ Tanggal Lahir	:	Jakarta, 11 Oktober 1972
NIP	:	19721011 199212 1 001
Pangkat/ TMT	:	Pembina Utama Muda (IV/c)
Jabatan	:	Direktur Deteksi Ancaman, Deputi I BSSN
Alamat Rumah	:	Bumi Dirgantara Permai Bn-12 Bekasi

Riwayat Pendidikan

- 1985 : SDN 11 PT Grogol Utara
- 1988 : SMPN 16 Jakarta Selatan
- 1991 : SMAN 29 Jakarta Selatan
- 1994 : Akademi Sandi Negara (D-III)
- 1999 : Statistika Terapan Universitas Terbuka (S-1)
- 2003 : Teknik Elektro Institut Teknologi Indonesia (S-1)
- 2014 : Kajian Stratejik Intelijen Universitas Indonesia (S2)
- 2020 : FISIP Hubungan Internasional Universitas Padjajaran (S-3)

Riwayat Jabatan :

- 1994 – 2004 : Staf Puskaji Kripto Dan Sistem Sandi
- 2005 – 2007 : Staf Puskom Kemlu
- 2007 – 2011 : Sandiman KBRI Washington DC
- 2012 – 2017 : Kasubdit Analisis Teknik Sandi, Deputi II Lembaga Sandi Negara
- 2017 - 2018 : Plt. Kepala Direktorat Analisis Sinyal, Deputi II Lemsaneg
- 2018 – sekarang : Direktur Deteksi Ancaman, Deputi I BSSN

Penghargaan yang Diterima :

- 2003 : Dharma Persandian X Tahun Lembaga Sandi Negara
- 2003 : Satya Lencana Karya Satya X Tahun Presiden RI
- 2013 : Dharma Persandian XX Tahun Lembaga Sandi Negara
- 2013 : Satya Lencana Karya Satya XX Tahun Presiden RI
- 2017 : Kenaikan Pangkat Pilihan (Prestasi Luar Biasa)

Karya Ilmiah

1. 2019 : Smart Honeypot : Optimalisasi Honeynet Project Yang Lebih Efektif dan Efisien
2. 2019 : Efisiensi Monitoring Honeypot dengan Menggunakan Visualisasi dan Otomatisasi Laporan Log Serangan
3. 2019 : Design Integrated Honeypot Untuk Deteksi Dan Identifikasi Serangan Siber
4. 2019 : Honeynet-Based Threat Sharing Platform