



**DEWAN PERWAKILAN RAKYAT
REPUBLIK INDONESIA**

**RISALAH RAPAT
KOMISI I DPR RI**

Tahun Sidang	: 2021-2022
Masa Persidangan	: III
Jenis Rapat	: Rapat Kerja Komisi I DPR RI dengan Kepala BSSN
Hari, Tanggal	: Kamis, 20 Januari 2022
Pukul	: 10.04 WIB – 13.02 WIB
Sifat Rapat	: Terbuka dilanjutkan tertutup
Tempat	: Ruang Rapat Komisi I DPR RI, Gedung Nusantara II DPR RI, Lantai 1.
Ketua Rapat	: Drs. Utut Adianto, Wakil Ketua Komisi I DPR RI
Sekretaris Rapat	: Sartomo, S.S., M.Si., Kabag Sekretariat Komisi I DPR RI
Acara	: <ol style="list-style-type: none">1. Tindak lanjut Raker Komisi I DPR RI dengan Kepala BSSN tanggal 15 November 2021 terkait dengan usulan untuk segera menerbitkan Perpres mengenai strategi keamanan siber nasional;2. Laporan perkembangan Major Project Penguatan <i>National Security Operation Center (NSOC)-Security Operation Center (SOC)</i> dan Pembentukan <i>Computer Security Incident Response Team (CSIRT)</i>;3. Peningkatan kapasitas SDM dalam rangka penguatan keamanan dan ketahanan siber, penguatan tata kelola keamanan informasi dan pengawasan kepatuhan kepada ketentuan peraturan perundang-undangan;4. Ketersediaan <i>secure hosting</i> aplikasi milik K/L dari berbagai bentuk ancaman dan serangan guna menjaga stabilitas politik, sosial, budaya, dan ekonomi, serta menjaga agar tidak menimbulkan kebingungan dan kepanikan di tengah pandemi Covid-19;5. Upaya langkah strategis dan antisipasi BSSN dalam menghadapi varian baru Covid-19 termasuk penyediaan anggarannya.
Hadir	: PIMPINAN: <ol style="list-style-type: none">1. Meutya Viada Hafid (F-PG)2. Drs. Utut Adianto (F-PDI Perjuangan)3. H. Bambang Kristiono, S.E. (F-Gerindra)4. H. Anton Sukartono Suratno, M.Si. (F-PD)5. Dr. H. Abdul Kharis Almasyhari (F-PKS)

ANGGOTA:

FRAKSI PDI-PERJUANGAN (F-PDIP)

6. Puan Maharani
7. Dede Indra Permana, S.H.
8. Irine Yusiana Roba Putri, S.Sos., MCOMN&MEDIAS
9. Junico BP Siahaan, S.E.
10. Dr. Effendi MS Simbolon, MIPol.
11. Ir. Rudianto Tjen
12. Krisantus Kurniawan, S.IP., M.Si.
13. Dr. H. Hasanuddin, M.M., M.Si.
14. Mayjen TNI Mar. (Purn) Sturman Panjaitan, S.H.
15. Drs. Mukhlis Basri
16. Itet Tridjajati Sumarijanto

FRAKSI PARTAI GOLKAR (F-PG)

17. Dave Akbarshah Fikarno, M.E.
18. Bobby Adhityo Rizaldi, S.E., Ak., M.B.A., C.F.E.
19. I. Lodewijk F. Paulus
20. Nurul Arifin, M.Si.
21. Dr. H. M. Azis Syamsuddin, S.H., S.E., MAF., M.H.
22. Christina Aryani, S.E., S.H., M.H.
23. H. Alex Noerdin

FRAKSI PARTAI GERINDRA (F-GERINDRA)

24. Sugiono
25. Yan Permenas Mandenas, S.Sos., M.Si.
26. Dr. H. Fadli Zon, SS., M.Sc.
27. Rachel Maryam Sayidina
28. Fadhlullah, S.E.
29. R. Imron Amin, S.H., M.H.

FRAKSI PARTAI NASIONAL DEMOKRAT (F-NASDEM)

30. Prananda Surya Paloh
31. Muhammad Farhan
32. Kresna Dewanata Phrosakh
33. Hasbi Anshory, S.E., M.M.
34. Hillary Brigitta Lasut, S.H.

FRAKSI PARTAI KEBANGKITAN BANGSA (F-PKB)

35. Drs. H. Taufiq R. Abdullah
36. Dr. (H.C.) H. A Muhaimin Iskandar, M.Si.
37. Drs. H. M. Syaiful Bahri Anshori, MP.
38. A. Helmy Faishal Zaini
39. H. Bachrudin Nasori, S.Si., M.M.

FRAKSI PARTAI DEMOKRAT (F-PD)

40. Rizki Aulia Rahman Natakusumah
41. Dr. H. Sjarifuddin Hasan, S.E., M.M., M.B.A.
42. H. Darizal Basir, S.Sos., M.B.A.
43. Teuku Riefky Harsya

FRAKSI PARTAI Keadilan Sejahtera (F- PKS)

- 44. Dr. H. Jazuli Juwaini, Lc., M.A.
- 45. H. Sukamta, Ph. D.
- 46. H. Ahmad Syaikh
- 47. Dr. H. Almuzzammil Yusuf, M.Si.

FRAKSI PARTAI Amanat Nasional (F- PAN)

- 48. Ir. Alimin Abdullah
- 49. Ir. H. Ahmad Rizki Sadig, M.Sc.
- 50. Hj. Farah Puteri Nahlia, M.Sc.
- 51. Slamet Ariyadi, S.Psi.

FRAKSI PARTAI Persatuan Pembangunan (F- PPP)

- 52. H. Syaifullah Tamliha, S.Pi., M.S.
- 53. Muhammad Iqbal, S.E., M.Com.

Anggota yang Izin : -

- Undangan : 1. Kepala BSSN RI, Letnan Jenderal TNI (Purn.) Hinsa Siburian.
2. Sektetaris Utama BSSN RI, Syahrul Mubarak, S.Kom. Beserta Jajaran.

Jalannya Rapat:

KETUA RAPAT (DRS. UTUT ADIANTO):

Selamat pagi.

Salam damai sejahtera buat kita semua.

Yang sangat saya hormati teman-teman Anggota Komisi I yang hadir baik fisik maupun virtual, Pak Kepala BSSN Bapak Letjen TNI Purnawirawan Hinsa Siburian beserta seluruh jajaran.

Rasanya walaupun sudah lambat belum terlalu terlambat saya mengucapkan “Selamat Hari Natal” untuk Pak Kepala dan teman-teman yang merayakan dan “Selamat Tahun Baru”, semoga tahun ini jauh lebih baik.

Ibu, Bapak berdasarkan Rapat Bamus tanggal 3 November 2021, saat ini kehadiran maksimal bisa 75%. Kalau sekitar tahun lalu 20% dan seterusnya sekarang sudah 75%. Sebelum saya buka saya mohon izin rapat ini kita menyatakan terbuka. Apa bisa disetujui? Setuju ya, Ibu Itet setuju? Kita nyatakan terbuka untuk umum.

(RAPAT: SETUJU)

Ibu, Bapak, oh belum saya buka, ini mohon maaf sudah lama nggak memimpin rapat. Dengan ini rapat saya nyatakan dibuka dan terbuka untuk umum.

**(RAPAT DIBUKA PUKUL 10.04 WIB)
(RAPAT DINYATAKAN TERBUKA UNTUK UMUM)
(KETUK PALU: 1X)**

Ibu, Bapak, Rapat Kerja kali ini agendanya ada lima, mohon yang pertama:

- a. Tindak lanjut Raker Komisi I DPR RI dengan Kepala BSSN tanggal 15 November 2021 terkait dengan usulan untuk segera menerbitkan Perpres mengenai Strategi Keamanan Siber Nasional.
- b. Laporan perkembangan *major project* penguatan *National Security Operation Center* (NSOC), *Security Operation Center* dan pembentukan *Computer Security Incident Response Team* atau yang selalu ditayangkan oleh Pak Kepala CSIRT.
- c. Peningkatan kapasitas SDM dalam rangka penguatan keamanan dan ketahanan siber, penguatan tata kelola keamanan informasi dan pengawasan kepatuhan kepada ketentuan peraturan perundang-undangan.
- d. Ketersediaan *secure hosting* aplikasi milik kementerian/lembaga dari berbagai bentuk ancaman dan serangan guna menjaga stabilitas politik, sosial, budaya, dan ekonomi, serta menjaga agar tidak menimbulkan kebingungan dan kepanikan di tengah pandemi Covid-19.
- e. Upaya langkah strategis dan antisipasi BSSN dalam menghadapi varian baru Covid-19 termasuk penyediaan anggarannya.

Apakah agenda kelima ini bisa disetujui? Setuju ya.

(RAPAT: SETUJU)

Selamat datang Pak Lodewijk, beliau sekarang menjadi Wakil Ketua DPR RI. Kalau berdasarkan Undang-Undang Protokol Tahun 2009 beliau setara dengan Presiden Republik

Indonesia. Tetapi yang namanya tentara biasanya orangnya *humble*, ya tetap ke sini rajin bertanya. Beliau pakai ilmu rajin bertanya sesat di jalan, rajin bertanya pangkal pintar, susah bertanya, jarang bertanya sesat di jalan, kalau besar itunya susah jalannya.

Ibu, Bapak sebelum kita mulai ada anggota baru kita, nggak ada ya? Biasanya setiap masa sidang ada anggota baru, nggak ada ya? Nggak ada. Kalau nggak ada anggap lah Bu ltet anggota baru tetapi lama kita. Ibu ltet tadi pagi bercerita “Pak Utut, saya kok capek sekali di Komisi I dari sini ke sini, sini ke sini lagi, *ludrek* saya, padahal saya sudah belajar terus”, memang beliau.

F-PDIP (DR. H. HASANUDDIN, M.M., M.SI.):

Kurang spa barangkali, kurang spa.

KETUA RAPAT (DRS. UTUT ADIANTO):

Beliau *alhamdulillah* usianya sudah 76 tahun. Mudah-mudahan kita bisa mengikuti jejak beliau, karena kalau kita biasanya umur segitu sudah diuruk, dibacain *Al-Fatihah*.

Ibu, Bapak kami persilakan kepada yang terhormat Saudara Kepala BSSN untuk menyampaikan paparannya dan nanti teman-teman memberikan pendalaman. Silakan Pak Kepala.

KEPALA BSSN RI (LETNAN JENDERAL TNI (PURN.) HINSA SIBURIAN):

Terima kasih Bapak Pimpinan Rapat.

Assalamu'alaikum Warahmatullahi Wabarakatuh,
Selamat pagi,
Salam damai untuk kita,
Om swastiastu,
Namo buddhaya,
Salam kebajikan,
Dan salam sehat untuk kita semua.

Yang kami hormati Bapak Pimpinan dan seluruh Anggota Komisi I DPR RI.
Yang kami hormati seluruh peserta rapat.

Pertama-tama izinkan kami menyampaikan rasa hormat dan terima kasih kepada Pimpinan DPR RI atas undangan rapat kerja pada hari ini. Dan sebelumnya juga kami mengucapkan “Selamat Tahun Baru 2022” kepada Ibu, Bapak sekalian. Dan juga kami menyampaikan terima kasih atas Kunjungan Kerja dari Komisi I DPR RI ke BSSN, baik itu ke Batam, baik itu ke Politeknik Siber dan Sandi Negara. Semoga di tahun 2022 ini tentunya kita berharap Covid-19 ini berlalu dan kita dapat melaksanakan tugas pengabdian kita kepada bangsa dan negara dalam keadaan sehat.

Bapak, Ibu yang saya hormati.

Berdasarkan surat Wakil Ketua DPR RI Korpolkam, tanggal 14 Januari 2022 tentang undangan rapat kerja. Rapat kerja pada hari ini akan membahas tema seperti yang sudah

disampaikan oleh Bapak Pimpinan tadi, yaitu progres penyusunan rancangan Perpres tentang Strategi Keamanan Siber Nasional. Kemudian laporan perkembangan *major project* penguatan *National Security Operation Center (NSOC)*, *Security Operation Center (SOC)*, dan pembentukan *Computer Security Incident Response Team (CSIRT)*. Ketiga adalah peningkatan kapasitas SDM dalam rangka penguatan keamanan dan ketahanan siber, penguatan tata kelola keamanan informasi, dan pengawasan kepatuhan kepada ketentuan peraturan perundang-undangan. Kemudian keempat ketersediaan *secure hosting* aplikasi milik K/L dari berbagai bentuk ancaman dan serangan guna menjaga stabilitas politik, sosial, budaya, dan ekonomi, serta menjaga agar tidak menimbulkan kebingungan dan kepanikan di tengah pandemi Covid-19, dan upaya langkah strategis dan antisipasi BSSN dalam menghadapi varian baru Covid-19 termasuk penyediaan anggarannya.

Bapak Pimpinan yang saya hormati.

Kami masuk ke pembahasan pertama, yaitu tema pembahasan yaitu progres penyusunan rancangan Perpres tentang Strategi Keamanan Siber Nasional. Ada slide? Seperti kita ketahui memang dasar dari pembentukan Perpres tentang Strategi ini adalah amanat dari PP 71. PP 71/2019, di mana diamanatkan disitu untuk BSSN menyusun strategi keamanan siber nasional. Dan kami tahun 2020 sudah menindaklanjutinya, karena memang Perpres-nya keluar sudah di akhir 2019, yaitu dengan kami menetapkan Tim Perumus SKSN yang kemudian tim menindaklanjuti dan perumusan draf rancangan peraturan tentang SKSN, internal BSSN.

Dalam proses penyusunan pada tanggal 8 sampai 16 Agustus 2020, BSSN mengundang pakar dan narasumber, baik dari jajaran Pemerintah, akademisi, pelaku usaha, maupun komunitas untuk mendapatkan saran dan masukan terkait Rancangan Peraturan Presiden SKSN yang sedang disusun. Pada tanggal 16 Oktober 2020 dilaksanakan *legal drafting* strategi keamanan siber nasional. Kemudian selanjutnya untuk memperdalam substansi dan menggali masukan serta informasi, maka dilakukan *focus group discussion* pada tanggal 21 Oktober 2020. Dan pada tanggal 4 sampai 6 November 2020 dilakukan diskusi publik dengan *stakeholder* SKSN dan penyusunan SKSN dalam bentuk buku.

Sebagai rangkaian kegiatan dari penyusunan rencana Perpres SKSN ini oleh internal BSSN diselenggarakan simposium sebagai salah satu bentuk sosialisasi dan uji publik terhadap rencana Perpres SKSN yang telah disusun. Simposium pertama dilaksanakan pada tanggal 7 Desember 2020 di Bali dan simposium kedua dilaksanakan pada tanggal 11 Desember 2020 di Yogyakarta.

Kemudian tahun 2021, pada tahun 2021 BSSN menindaklanjuti kegiatan penyusunan rancangan perpres dengan mengirim surat permohonan izin prakarsa kepada Bapak Presiden terkait penyusunan Rancangan Peraturan Presiden tentang SKSN pada tanggal 28 Mei 2021. Yang kemudian surat izin prakarsa penyusunan rancangan Perpres SKSN tersebut terbit pada 15 Desember 2021. Memang agak cukup lama baru keluar izinnya. Kemudian sesuai dengan surat Menteri Sekretaris Negara B1019/M/D1HK03.00/12/2021.

Kemudian kami tindak lanjuti terus karena ini memang waktunya tinggal beberapa minggu tapi kami tetap koordinasi, sehingga terus dilaksanakan kegiatan. Dan dilaksanakan kegiatan rapat panitia antar kementerian, yang pertama pada tanggal 20 Desember 2021. Rapat panitia ini kemudian diwakili oleh 19 instansi Pemerintah yang ditetapkan dalam sebuah surat keputusan. Kemudian dalam rapat tersebut dihadiri oleh Kemenkopolhukam, Kemenhan, Kemendagri, Kemlu, Kemsetneg, Seskab, Kemenkumham, Kemenkominfo, Kemenperin, Kemendikbud Ristek, Kemenpan RB, Kemen PPN/Bappenas, Kemen BUMN, Kemen PPPA, TNI/Polri, dan BIN, BPS, dan BRIN.

Kemudian dilakukan rapat kedua PAK pembahasan kerangka Perpres pada batang tubuh SKSN pada 28 Desember 2021. Dan tahun 2022 ini juga sudah dilaksanakan rapat PAK tanggal 13 Januari 2022 kemarin, dalam rangka membahas batang tubuh hingga pasal 9 dan pasal 18. Selanjutnya direncanakan tanggal 28 Januari ini akan dilaksanakan rapat PAK keempat yang akan membahas kelanjutan dan bahan pengaturan manajemen krisis siber nasional.

Bapak Pimpinan dan hadirin yang kami hormati.

Sampai di situ kondisi dan kemajuan pembahasannya. Kami berharap dan berkoordinasi terus dengan instansi terkait, sehingga ini harus kalau bisa paling lambat pertengahan tahun ini sudah ditandatangani oleh Bapak Presiden.

Kemudian Bapak Pimpinan dan hadirin yang kami hormati.

Kami izin menjelaskan sedikit tentang strategi ini. Jadi strategi keamanan siber nasional disusun sebagai acuan bersama seluruh pemangku kepentingan keamanan siber nasional dalam rangka mengembangkan kebijakan keamanan siber di instansi masing-masing. SKSN ini disusun selaras dengan nilai-nilai dasar kehidupan berbangsa dan bernegara yang berlandaskan ideologi Pancasila sebagai falsafah hidup, *culture* strategis, dan dasar kekuatan bangsa.

Strategi keamanan siber nasional merupakan rumusan arah kebijakan nasional dalam menggunakan seluruh sumber daya siber nasional untuk mewujudkan keamanan siber guna mempertahankan dan memajukan kepentingan nasional keamanan siber Indonesia, yaitu yang adaptif dan inovatif untuk melindungi seluruh lapisan yang ada di ruang siber. Sebagaimana kita ketahui ruang siber itu terdiri dari 3 lapisan, fisik, lapisan sosial, dan manusianya.

Kemudian, *next* kami lanjutkan. Adapun visi dari SKSN ini adalah terwujudnya keamanan ruang siber nasional untuk mewujudkan visi Pemerintah Indonesia Maju yang berdaulat, mandiri, dan berkepribadian berlandaskan gotong royong. Misi SKSN RI adalah upaya strategis yang harus dilaksanakan secara aktif dan berkesinambungan oleh bangsa Indonesia di tingkat nasional dan global guna mencapai visi SKSN RI. Ada 4 misi yang di dalamnya, yaitu menjamin keamanan ruang siber dan sistem informasi nasional serta melindungi seluruh rakyat, tumpah darah Indonesia, dan nilai-nilai kehidupan bangsa. Kemudian melindungi ekosistem perekonomian digital nasional demi tergapainya pertumbuhan dan inovasi, membina kekuatan dan kemampuan keamanan siber Indonesia yang handal dan berdaya tangkal, memajukan kepentingan nasional keamanan siber Indonesia, dan mendukung terciptanya ruang siber global yang terbuka, aman, stabil, dan bertanggungjawab.

Strategi keamanan siber nasional bertujuan untuk menjadi acuan pemangku kepentingan untuk mewujudkan keamanan siber nasional dalam rangka mencapai stabilitas keamanan dan peningkatan perekonomian nasional, serta mewujudkan kekuatan dan kapabilitas siber.

Kemudian landasannya tentu kita menggunakan landasan hukum nasional yang adaptif dan *compatible* dalam upaya mewujudkan keamanan siber nasional, kemudian dibutuhkan totalitas dan keutuhan sumber daya keamanan siber nasional, kemudian sinergitas antara kementerian/lembaga Pemerintah dan kemitraan antar pemangku kepentingan. Pemangku kepentingan dalam strategi ini terdiri dari, penyelenggara negara tentu dalam hal ini Pemerintah dan DPR, dan yang lainnya, kemudian pelaku usaha, akademisi, dan komunitas.

Dan fokus area kerja dari strategi ini meliputi bagaimana tata kelolanya, kemudian kesiapsiagaan dan ketahanan, kemudian perlindungan infrastruktur informasi vital nasional, kemudian manajemen resiko dalam keamanan siber nasional, kemudian kemandirian

kriptografi. Jadi kemandirian kriptografi ini memang menjadi dari dulu *core* bisnis BSSN. Dan intinya dari keamanan siber antara lain adalah bagaimana kita memiliki kemandirian dalam bidang kriptografi, inti dari keamanan. Kemudian pengembangan kemampuan dan kapasitas serta peningkatan kewaspadaan. Kemudian legislasi dan regulasi, ini juga sedang kita usahakan dan tentu bekerjasama dengan semua pihak. Kemudian kerja sama internasional. Jadi inilah fokus area yang ada di strategis siber nasional.

Kemudian yang berikutnya kepada Bapak Pimpinan dan hadirin yang kami hormati. Kami laporkan perkembangan *major project* penguatan *National Security Operation Center* (NSOC), *Security Operation Center* (SOC), dan pembentukan *Computer Security Incident Response Team*.

Kami laporkan RPJPN Tahun 2020-2024 ditetapkan melalui Peraturan Presiden sebagaimana kita ketahui salah satu *major project* dalam RPJPN yang terkait BSSN adalah penguatan *National Security Operation Center*, *Security Operation Center* (SOC), dan pembentukan *Computer Security Incident Response Team*. Pemerintah telah memberikan panduan atas manfaat dari proyek tersebut, yaitu menurunnya insiden serangan siber, meningkatnya kemampuan bersama *multi stakeholder* keamanan siber dalam melakukan deteksi dini serangan ancaman siber, kemudian meningkatnya pelayanan *multi stakeholder* keamanan siber melalui pusat informasi terpadu bagi masyarakat, dan meningkatnya integrasi dan *sharing* informasi antar *stakeholder* terkait, baik Pemerintah, swasta, komunitas siber lainnya.

Perlu kami sampaikan di sini NSOC merupakan bagian dari upaya nasional dalam upaya mengorkestrasi aktivitas perlindungan, pencegahan, mitigasi, dan pemulihan insiden serangan siber untuk meningkatkan postur keamanan dan ketahanan siber di tingkat nasional. Informasi yang diperoleh dari proses integrasi dalam NSOC ini menjadi salah satu sumber informasi yang diperlukan dalam upaya mewujudkan *cyber security situational awareness*.

Tujuan dan manfaat NSOC adalah sebagai mekanisme deteksi dini serangan siber di tingkat nasional, memperoleh gambaran menyeluruh mengenai kondisi keamanan siber Indonesia, membantu proses tanggap insiden yang lebih cepat, mencegah meluasnya dampak serangan, prediksi serangan siber di masa depan sebagai data acuan dalam menentukan strategi nasional keamanan siber, membangun keamanan ruang siber Indonesia yang lebih aman dan tahan, membantu proses penegakan hukum, serta atribusi pelaku kejahatan siber, membangun kapabilitas sumber daya manusia Indonesia di bidang keamanan siber.

Bapak Pimpinan dan hadirin yang kami hormati.

Sedangkan SOC merupakan tim yang terorganisir dan memiliki kemampuan yang mumpuni untuk melakukan *monitoring* secara berkelanjutan dan meningkatkan postur keamanan di level organisasi dengan melakukan pendeteksian analisa dan tanggap insiden, menggunakan bantuan teknologi serta proses dan prosedur yang terdefinisi dengan baik. Idealnya setiap pemangku kepentingan, baik kementerian/lembaga, pemerintah daerah, sektor IIP, *e-commerce*, dan lain-lainnya memiliki SOC melakukan *monitoring* di level organisasinya masing-masing.

Tujuan dan manfaat SOC ini adalah sebagai mekanisme deteksi dini serangan siber di level organisasi, memperoleh gambaran menyeluruh mengenai kondisi keamanan siber di level organisasi, membantu proses tanggap insiden yang lebih cepat, mencegah meluasnya dampak serangan.

Kami laporkan pembangunan dari NSOC kita, *next* slidenya. Karena pembangunannya dimulai tahun 2019. Jadi kami coba menjelaskan mulai dari cakupan *traffic* ISP, kemudian kementerian/lembaga, lokus, dan teknologi kapasitasnya mulai tahun 2019, 2020, sampai dengan 2021. Tahun 2019 cakupan *traffic* kita adalah 80 *giga byte* per second, kemudian ISP

atau NAP yang dimonitor adalah Moratel Cybernet Indonesia, Biznet Network, Indonesia Internet Exchange Jakarta.

Kemudian kementerian/lembaga, institusi yang didukung *monitoring* BSSN, antara lain internal NSOC sendiri, Mahkamah Agung, Mahkamah Konstitusi, Kementerian Kesehatan, Sekretaris Kabinet, Direktorat Jenderal Kependudukan dan Pencatatan Sipil, Direktorat Jenderal Pemasyarakatan, Diskominfo Provinsi Jawa Barat. Kemudian locus ISP Jakarta, 7 kementerian/lembaga Jakarta, 1 Pemerintah Provinsi Jawa Barat.

Kemudian teknologi dan kapasitas atau teknologi yang mendukung kegiatan ini adalah kita bangun sistem *monitoring* ancaman siber di IIX, sistem *monitoring* keamanan siber di IPN, kementerian/lembaga, *threat intelligence platform*, sistem manajemen kerentanan, *world application security testing system*, *vulnerability assessment lab*, *digital forensic lab*, *information war campaign*, *social network analytic*, *big data analytic*, sistem pengaduan.

Kemudian di tahun 2020 kita cakupan 50 *giga byte*, karena memang ini kaitannya dengan pemotongan anggaran. Jadi waktu itu memang kita menggunakan yang anggaran yang ada, cakupannya 50 yang kita bangun 50 *giga byte per second*, *traffic* pada 5 NAP, XL, CBN, Lintas Arta, Telkom, Indosat, yang melewati EX.

Kemudian *cloud security protection* pada dukungan Pemilukada, KPU, Mahkamah Konstitusi, dan di BSSN sendiri. *Cloud security protection* untuk dukungan layanan publik KSP, kemudian BP-POM. Kemudian locus, IIX Jakarta, 6 kementerian/lembaga Jakarta, kemudian teknologi yang kita bangun di tahun 2020 adalah *network security monitoring*, sensor dan *sandbox*, *cloud security protection*, *threat intelligent platform*, *system sein holding malicious traffic* di Jakarta, sistem agregasi *traffic*, dan sistem gerbang *traffic* Jakarta.

Kemudian di tahun 2021 kita membangun ini anggarannya lumayan lebih banyak dari 2020 sehingga kita bisa cakupan *traffic* yang kita bangun adalah 1 *tera byte per second* plus 50 *giga byte*. Kemudian ISP atau NAP yang kita pasang adalah Telkom Internet Gateway, Indonesia Internet Exchange Surabaya, kemudian kementerian/lembaga, yaitu piloting penerapan *open sources sensor* Dinas Kominfo Yogyakarta. Kemudian locusnya International Gateway Batam, dan IIX Surabaya.

Teknologi yang kita bangun di tahun 2021 adalah *network security monitoring* berkapasitas tinggi, sensor dan *sandbox*, *threat attribution engine*, sistem agregasi *traffic*, *cyber threat intelligence bids*, sistem penelusuran kejahatan siber di *dark web*, sistem *calling malicious traffic* di Surabaya, dan sistem gerbang *traffic* Surabaya.

Kami bisa menjelaskan sedikit tentang peta *monitoring* keamanan siber yang sampai dengan tahun 2021 ini yang kita bangun, yaitu 3 sensor international Gateway, kemudian 8 sensor K/L seperti yang kami jelaskan tadi, kemudian 18 sensor ISP, NAP, kemudian instansi mitra honeynet. Jadi di samping itu juga kita ada membangun kerja sama dengan lembaga dan perguruan tinggi, yaitu mitra honeynet untuk memonitor kemungkinan ancaman, di antaranya 20 provinsi, 58 pemerintah, 9 IIPM, dan 13 akademi. Jadi contohnya seperti di Syiah Kuala Banda Aceh, kemudian di Yogyakarta kita kerja sama dengan perguruan tinggi yang tersebut.

Bapak Pimpinan dan hadirin yang kami hormati.

Kami izin sedikit menjelaskan hasil dari apa yang kami sampaikan tadi pembangunan itu sehingga kita dapat memonitor, antara lain terutama memang kaitannya dengan kemungkinan ancaman. Kalau kita lihat di slide, yang kita catat di pusat operasi keamanan siber nasional itu 1.652.521.839 anomali *traffic* pada tahun 2021 periode Januari sampai dengan Desember 2021. Dan kalau kita lihat di data juga 3 sektor peretasan situs di Indonesia, yaitu kasus peretasan situs pendidikan tinggi, situs swasta, dan situs pemerintah.

Kemudian klasifikasi anomali *traffic* yang kita monitor dari alat tadi adalah anomali *traffic* Indonesia sepanjang tahun 2021 didominasi oleh aktivitas *malware*. Hal ini menunjukkan bahwa salah satu tantangan di dalam proses transformasi digital ini adalah bagaimana membangun kesadaran keamanan kepada seluruh pemangku kepentingan. Mengingat tingginya presentase aktivitas anomali berupa *malware* merupakan indikasi bahwa aktivitas pengguna di internet dibayangi oleh ancaman akan infeksi maupun pencurian informasi yang mungkin saja dilakukan melalui infeksi *malware* tersebut.

Dan rekapitulasi notifikasi, tentunya kami dari pusat operasi keamanan siber nasional, setiap anomali yang ada di *stakeholder* di lembaga itu langsung pada saat itu juga kita notifikasi kepada mereka. Memang ini juga menjadi tantangan kita, karena apa? dari sekian banyak notifikasi yang kita berikan, kita boleh lihat di grafik ya total notifikasi yang sudah diberikan tahun 2021 ini ada 2.258 kita sampaikan kepada *stakeholder* yang bersangkutan hasil *monitoring* kita di Ragunan. Memang hanya 8,5% dari total notifikasi yang dibalas dan ditindaklanjuti. Ini ada memang masalah kesadaran dari *stakeholder* untuk menindaklanjutinya. Ini tantangan tersendiri memang untuk kita.

Kemudian kami laporkan masalah *Computer Security Incident Response Team*, ini kelanjutan dari *National CSIRT* dan SOC tadi *Security Operation Center*, kemudian CSIRT. Ini kita bangun seperti yang tertera di slide di mana diketahui bahwa *Computer Security Incident Response Team* merupakan organisasi atau tim yang bertanggungjawab untuk menerima, meninjau, dan menanggapi laporan aktifitas insiden keamanan siber dengan fungsi memberikan layanan reaktif, yaitu koordinasi insiden, *triage incident*, resolusi insiden. Kemudian memberikan layanan proaktif, mempublikasikan informasi kerawanan, keamanan, dan teknologi, audit keamanan informasi, kemudian memberikan layanan peningkatan kualitas keamanan, konsultasi, *cyber drill*, pelatihan, dan *workshop*.

Ibu, Bapak sekalian yang kami hormati.

Kalau kita lihat *next* slidennya, yang kita akan bentuk tentunya sesuai dengan RPJPN, yaitu dari tahun 2020 sampai 2024 itu 131 *Computer Security Incident Response Team* yang harus kita bangun di semua lembaga. Dan ini sudah kita mulai di tahun 2020 sesuai dengan program tersebut, yaitu 15 kementerian/lembaga dan daerah, instansi pusat, seperti yang tertera di slide, tahun 2020 itu 15 kementerian tersebut antara lain instansi pusat. Kemensetneg, Kemenlu, Kemenkeu, Kemendikbud, dan KSP. Kemudian Pemerintah Provinsi DKI Jakarta, Jawa Barat, Jawa Tengah, Jawa Timur, DIY, Kepulauan Riau, Sumbar, Kalsel, Gorontalo, NTB.

Kemudian di tahun 2021 walaupun situasinya Covid kita tetap bisa melaksanakan sesuai target yang diberikan kepada kita, yaitu 39 kementerian/lembaga dan daerah. Antara lain instansi pusat, BSSN sendiri, BSN, DPD RI, Batan, BPPT, Kemen ESDM, Kemenhub, Ombudsman, LIPI, Kemen Kominfo, Lapan, PPATK, Kemendag, Kementan, LKPP, Bappenas, BP-POM, BPS, BKN, LAN, Kejagung, Kemenkes, Kemenko Perekonomian, Kemhan, dan BEJ.

Kemudian provinsi yang sudah kita *launching* CSIRT di tahun 2020, antara lain Bali, Bengkulu, Jambi, Papua Barat, Babel, Sumsel, Sulbar, Maluku, kemudian Banten, Riau, Sulsel, Kalteng, Kaltim, dan Papua. Di Tahun 2022 ini kita akan bangun 32 di kementerian/lembaga dan pusat. Kemudian di tahun 2023 di 36 K/L, dan tahun 2024 di 10 K/L dan daerah.

Inilah program sampai saat ini sesuai dengan yang ditugaskan oleh Bappenas ke BSSN, kami masih *on the track*. Dan justru sebenarnya hasil evaluasi kami di lapangan ini perlu ditingkatkan, karena masalah keamanan hanya di 131 ini belum masuk kabupaten/kota dan swasta yang lain. Ini juga kami sedang berkoordinasi supaya bisa lebih dipercepat.

Bapak Pimpinan dan Ibu, Bapak Anggota Komisi I DPR RI yang kami hormati.

Kami lanjut ke tema pembahasan ketiga, yaitu peningkatan kapasitas SDM dalam rangka penguatan keamanan dan ketahanan siber, penguatan tata kelola keamanan informasi, dan pengawasan kepatuhan kepada ketentuan peraturan perundang-undangan. Program BSSN dalam peningkatan ini adalah, satu merumuskan standarisasi SDM, bicara SDM memang harus kita menyusun merumuskan standar dari SDM *cyber security*, yaitu sektor Pemerintah, yaitu kamus kompetensi bidang keamanan siber, dua, standar kompetensi jabatan fungsi, sandiman, dan manggala informatika. Kemudian sektor non pemerintah, peta okupasi, 4 SKKNI, SOC, audit keamanan informasi, uji keamanan siber, dan digital forensik.

Kemudian menyusun regulasi, kemudian regulasi pengembangan kompetensi, yaitu pelatihan kami sudah menyusun Perban BSSN Nomor 5 Tahun 2021 tentang Pelatihan Keamanan Siber dan Persandian, 3 pedoman penyelenggaraan pelatihan fungsional sandiman, pelatihan teknis dasar persandian, pelatihan SNI, ISO, IEC 270001. Kemudian sertifikasi, Perban Nomor 7 Tahun 2020 tentang Pemberian Rekomendasi dan Pemberian Registrasi Lembaga Sertifikasi Profesi Bidang Keamanan, kemudian Perban tentang Pedoman Peningkatan Kapasitas SDM.

Kemudian melakukan literasi. Melakukan literasi, kampanye literasi tahun, kalau kita mulai tahun 2018 memang dimulai literasi sudah 21 kota dengan total peserta 12.525 orang. Kemudian kita menyusun buku literasi 4 buku, literasi pengendalian informasi di 5 kota, kemudian quote *goes to school* 2 kota, kemudian melaksanakan *monitoring* dan evaluasi.

Pemberian penghargaan SDM, kemudian pendaftaran tenaga ahli, kemudian pemuktahiran data, kemudian pelaporan lembaga sertifikasi profesi teregistrasi, akreditasi lembaga Diklat, Pemerintah penyelenggara Diklat Sandi, contohnya ini yang di BAIS, pusat pendidikan BAIS yang di Bogor, kemudian melaksanakan evaluasi SDM.

Kemudian yang kelima, memfasilitasi sertifikasi SDM, LPS teregister, LSP UBJ, kemudian LSP yang telah mendapat rekomendasi 4 LSP, BPPTIK, TII, TIK global, dan UMP. Kemudian LSP sedang proses rekomendasi ada dua, LPS IPAD dan multimatic.

Kemudian pengembangan kompetensi, pelatihan keamanan siber sebanyak 161 orang, pelatihan SPBE sebanyak 200 orang, kemudian pelatihan CSIRT sebanyak 160 orang. Dan ke depan, dan tahun ini memang kami akan lebih fokus di bidang pelatihan ini dari semua CSIRT yang sudah kita bangun kita sudah programkan mereka akan kita latih, kita tingkatkan kemampuan mereka.

Bapak Pimpinan dan hadirin yang kami hormati.

Ada masih terkait dengan masalah poin yang ketiga ini, kami menambahkan di sini menginformasikan kaitannya dengan layanan tanda tangan elektronik. Sampai dengan tahun ini 2021 jumlah *hit* transaksi tanda tangan elektronik per tanggal Desember 2021 sudah 76.277.949. Kemudian jumlah rata-rata sertifikat elektronik yang diterbitkan itu 4.000 per bulan, kemudian total perjanjian kerja, kerja sama, kita sudah kerja sama dengan artinya kerja sama ini kita mendukung tanda tangan elektronik lembaga tersebut 111 instansi pusat dan BUMN, kemudian 289 instansi daerah dan universitas, jadi sudah ada 400. Kemudian sertifikat elektronik yang sudah dikeluarkan 169.619 dan total aplikasi terintegrasi 550. Ini untuk mendukung juga masing-masing lembaga tersebut.

Kemudian kami lanjutkan evaluasi kematangan keamanan siber. Hasil penilaian evaluasi kematangan keamanan siber kementerian/lembaga dan daerah tahun 2020-2021. Memang belum semua lembaga itu bisa kita laksanakan evaluasi, tapi kita pilih untuk mewakili dan tentu ruang lingkup penilaian kematangan keamanan siber suatu lembaga atau organisasi

dilihat dari tata kelolanya, kemudian identifikasi, kemudian proteksinya, kemudian deteksinya bagaimana, responnya bagaimana.

Hasil penilaian evaluasi kematangan keamanan siber tahun 2020-2021 kalau kita lihat di sini persentase yang telah diukur tingkat kematangan sibernya ada 11,22%, kemudian persentase Pemda yang telah diukur tingkat kematangan keamanan sibernya 38,24%. Kalau kita lihat di grafik yang tertinggi itu adalah Kementerian Keuangan. Ini memang tidak terlepas dari memang kami juga lihat secara fisik ya mereka punya data center sendiri, dia tidak pinjam, tidak istilahnya nitip datanya ke pusat data yang swasta. Jadi itu antara lain dan terlihat memang di sini kementerian, atau lembaga, atau provinsi yang *care* mereka benar-benar masalah *security cyber*-nya bisa terlihat dari grafik tersebut, antara lain Jabar, Yogyakarta, kemudian KSP, kemudian juga Sumsel termasuk tinggi.

Ibu, Bapak sekalian yang saya hormati.

Kami izin masuk ke tema pembahasan berikutnya, yaitu ketersediaan *secure hosting* aplikasi milik kementerian/lembaga dari berbagai bentuk dan ancaman dan serangan guna menjaga stabilitas politik sosial, budaya, dan ekonomi, serta menjaga agar tidak menimbulkan kebingungan dan kepanikan di tengah pandemi Covid-19.

Bapak Pimpinan dan hadirin yang kami hormati.

Kami laporkan di sini *secure hosting* aplikasi yang ada di BSSN yang kita amankan, yaitu tentunya pertama adalah KRISNA Bappenas. Sistem Kolaborasi Perencanaan dan Informasi Kinerja Anggaran (KRISNA). Kemudian SPBE sendiri dalam hal ini Kemenpan RB yang bertanggungjawab, aplikasi sebagai sarana untuk mengumpulkan data SPBE milik seluruh kementerian/lembaga dan pemerintah daerah, serta sebagai salah satu sarana dalam hal sosialisasi terkait program SPBE.

Kemudian di Kemenko Polhukam, dari Kemenko Polhukam yang kami amankan atau *hosting* adalah sistem penanganan perkara tindak pidana secara terpadu berbasis teknologi informasi. Kemudian kami juga melayani Jaringan Komunikasi Sandi Nasional (JKSN), sistem komunikasi dan informasi ekstranet Kementerian Luar Negeri sampai saat ini, kemudian KSP, kemudian jaringan di TNI, jaringan komunikasi mereka. Sebagai contoh ini *secure infrastruktur high and availability*, sistem data base penanganan perkara tindak pidana terpadu berbasis teknologi informasi SPPTI.

Keterlibatan BSSN dalam SPPTI ini adalah *penyedia secure infrastructure high and availability* SPPTI untuk mendukung aparat penegak hukum, termasuk di Kejaksaan, kemudian Kepolisian, Kehakiman, melakukan percepatan pertukaran penanganan perkara yang aman dan akuntabel, penerapan enkripsi pada dokumen penanganan perkara rahasia yang ditangani oleh badan-badan tersebut. Sebagai contoh *secure infrastruktur high and availability*, sistem data base penanganan perkara tindak pidana terpadu berbasis teknologi seperti yang tertera di slide. Jadi walaupun diambil orang memang mereka, *next*, tidak akan bisa karena sudah terenkripsi.

Selanjutnya peran BSSN dalam penanganan ancaman siber pada aplikasi penanganan Covid-19. Ini kami laporkan, ini agak ramai memang kemarin datanya Kementerian Kesehatan itu bocor atau kita lihat diperjualbelikan di *dark web*. Jadi memang banyak pertanyaan, itu PeduliLindungi atau tidak. Jadi yang bocor itu bukan PeduliLindungi. Jadi rupanya di kementerian itu masing-masing Dirjen itu punya sendiri sistemnya. Jadi kemarin itu, itu belum masuk ke BSSN. Jadi karena kita fokus untuk mengamankan PeduliLindungi.

Jadi peran BSSN dalam penanganan ancaman siber pada hanya aplikasi penanganan Covid terutama PeduliLindungi adalah menilai keamanan dan menyusun rancangan pengamanan data. Pada tanggal 23 sampai 26 Agustus 2021 BSSN melakukan penilaian keamanan *security assessment* pada aplikasi PeduliLindungi, Silacak, Tcare, dan *new all record* Kemenkes, serta menyusun rancangan pengamanan data dan aplikasi terkait Covid-19.

Kemudian kedua, *monitoring* kinerja sistem keamanan. Bersama dengan Kementerian Kominfo, PT. Telkom, PT. Lintas Arta, melakukan *monitoring* kinerja sistem keamanan, baik dari sisi infrastruktur, maupun dari sisi aplikasi melalui penggunaan *dashboard* berbagi pakai. Kemudian merekomendasikan implementasi teknik keamanan. Merekomendasikan kepada Kementerian Kominfo dan Kemenkes untuk mengimplementasikan teknik keamanan aplikasi berbasis web dan jaringan pada aplikasi PeduliLindungi dalam upaya menangkal serangan yang mungkin terjadi.

Kemudian *monitoring anomaly traffic*. Melaksanakan *monitoring anomaly traffic* terhadap aplikasi PeduliLindungi yang disimpan pada pusat data nasional sementara Kementerian Kominfo ini kemarin memang menjadi fokus kita juga, kita pasang sensor sehingga PeduliLindungi bisa kita monitor dari Ragunan, dari pusat operasi keamanan siber.

Kemudian melakukan uji kelaikan pada tanggal 17 sampai 24 September 2021, BSSN melakukan uji kelaikan dengan hasil Telkom dapat menggunakan *backup cloud* bagi aplikasi PeduliLindungi dengan menindaklanjuti rekomendasi keamanan oleh BSSN, kemudian menyimpan data cadang. BSSN menyimpan 2,98 juta data terkait Covid-19 dan menyimpan data cadangan tersebut di BSSN Ragunan.

Ada beberapa kendala dalam penanganan aplikasi PeduliLindungi, tapi ini tetap kita coba untuk menyelesaikan. Jadi memang PeduliLindungi dari awalnya itu tidak mulus juga, banyak kendala tapi kendala-kendala tersebut dapat kita atasi. Misalnya di tanggal 5 dan 6 September 2021 waktu gangguan, terjadi gangguan, kemudian gangguan adalah akses PeduliLindungi lambat dikarenakan terdapat gangguan koneksi ke server, kemudian penyebab infrastruktur tidak memadai. Kami memberikan saran melakukan pengaturan dan perangkat jaringan dan perangkat keamanan jaringan.

Kemudian 7 September 2021 terjadi lagi gangguan, sebagian layanan aplikasi PeduliLindungi ini terganggu, penyebabnya adalah infrastruktur tidak memadai. Kemudian kami melakukan pembatasan akses pada segmentasi alamat IP penyerang. Kemudian tanggal 8 September gangguan lagi, kemudian aplikasi PeduliLindungi tidak dapat diakses. Ini penyebabnya adalah tingginya *traffic* pada pusat data nasional sementara dan adanya kendala pada perangkat keamanan jaringan. Kemudian kami sudah membantu mereka memberi saran meng-*update brainware* dan *restart* perangkat keamanan.

Kemudian 15 September 2021 gangguan lagi aplikasi PeduliLindungi mengalami gangguan akses, tingginya *traffic* pada PDNS, kemudian kami melakukan pembatasan akses dan pemindahan perangkat keamanan jaringan. Jadi memang PeduliLindungi ya mudah-mudahan sampai saat ini ke depan juga tetap bisa kita amankan, karena sudah menjadi kepentingan nasional di situ. Dan kita tetap bekerja sampai saat ini untuk membantu dari sisi keamanannya.

Bapak Pimpinan dan Ibu, Bapak Anggota Komisi I yang kami hormati.

Kami masuk ke tema pembahasan kelima, yaitu upaya langkah strategis dan antisipasi BSSN dalam menghadapi varian Covid-19 termasuk penyediaan anggarannya. Tentunya ini sebenarnya kami sudah lakukan sejak awal dan sampai saat ini juga tetap kita lakukan, yaitu upaya-upaya tersebut mengikuti kebijakan Pemerintah tentunya, pengaturan WFO, bekerja dari kantor maupun dari rumah, sesuai dengan level PPKM. Jadi kami masuk, Ragunan itu

masuk Jakarta, sedangkan Sawangan itu masuk Jawa Barat. Jadi kami mengikuti apa kebijakan dari pemerintah daerah atau nasional.

Kemudian kedua, melaksanakan vaksinasi pegawai, taruna, keluarga pegawai, seluruh pegawai BSSN telah melaksanakan vaksin pertama dan kedua. Jadi kami waktu itu kami sisihkan anggaran dari yang ada, kita melaksanakan vaksin sudah dua kali untuk semua, nanti kita sedang berkoordinasi ini bagaimana bisa untuk *booster* yang ketiga.

Kemudian melakukan upaya pencegahan Covid-19 bagi pegawai BSSN, membentuk tim Satgas, pengaturan internal penerapan protokol kesehatan, melakukan edukasi, bekerja sama dengan rumah sakit setempat, konsultasi dan *monitoring* kesehatan *online*, *screening test*, pengukuran suhu, *swab test*, ini sarana kita lengkapi. Kemudian tes Covid-19 untuk kegiatan kedinasan, setiap mau melaksanakan kegiatan memang cukup tinggi, karena kita tetap melaksanakan kegiatan, misalnya peluncuran *launching* dari CSIRT misalnya.

Kemudian memberikan disinfektan secara rutin, pemberian vitamin dan suplemen, melaksanakan senam rutin. Jadi BSSN tetap melaksanakan senam Selasa, Jumat, tapi dengan protokol kesehatan. Kemudian Korpri Peduli Covid, kemudian melakukan *tracing*, kemudian menyiapkan sarana dan prasarana untuk mendukung pelaksanaan tugas, menyediakan aplikasi *video conferene* untuk kegiatan secara *daring*. Jadi kami rapat setiap saat bisa dilakukan karena memang kami mempunyai dua sarana *video conference*.

Kemudian menyediakan pembelajaran secara *online* bagi Politeknik Siber dan Sandi, dan Pusat Pengembangan SDM. Jadi pembelajaran di Politeknik Siber dan Pusat Pengembangan Sumber Daya Pusdiklat BSSN, kami sudah menyiapkan juga secara *online*. Dan masing-masing mahasiswa dan peserta pelatihan itu, kita menyediakan satu anak satu orang. Jadi sebelum Covid memang ada dua orang di satu kamar, tapi dengan waktu yang ada ini kami mengupayakan ruangan yang ada untuk setiap mahasiswa maupun peserta pelatihan itu di satu ruangan. Dan di situ kita pasang sarannya untuk mereka bisa mengikuti pelajaran.

Kemudian mengamankan data pemerintah, dalam hal ini kami sampaikan tadi mengamankan data terkait Covid-19, yaitu Kemenkes punya. Kemudian melakukan audit keamanan aplikasi terkait penanganan Covid-19 PeduliLindungi. Kemudian kami telah menyiapkan pusat data tertentu untuk menyimpan rekam cadang elektronik, ini juga sesuai dengan PP 71. Jadi mudah-mudahan di bulan Maret data-data yang strategis, seperti Dukcapil karena mereka memang sesuai PP 71 harus membuat rekap cadangnya dan itu harus disimpan di kita. Mudah-mudahan bulan Maret data-data tersebut sudah bisa kita simpan di pusat data tertentu ini sesuai dengan amanat PP 71.

Bapak Pimpinan dan Ibu, Bapak, hadirin yang saya hormati.

Itulah yang bisa kami sampaikan, tentu dalam penyampaian ini masih belum lengkap. Dan kami mohon arahan, mohon masukan untuk apa yang kami kerjakan ini tentunya untuk bisa lebih baik ke depan selanjutnya. Saya sampaikan terima kasih.

Kami kembalikan kepada Bapak Pimpinan. Terima kasih.

KETUA RAPAT (DRS. UTUT ADIANTO):

Terima kasih Pak Kepala.

Sebelum kita mulai karena banyak yang baru, ada baiknya saya perkenalkan supaya teman-teman tahu. Di sebelah kiri doktor Edit Prima ini Plt. Deputi IV Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata. Kemudian Pak Hasto Prastowo, ini orangnya

Deputi III Plt, ini banyak Plt, yang ini kursinya cor-coran nggak pernah tergoyangkan Syahrul Mubarak, ini kursinya cor-coran ini, nggak ada yang berani goyang-goyang, Sekretaris Utama BSSN. Kemudian kalau Pak Hinsa semua orang sudah kenal, terutama Pak Luhut kenal baik. Kemudian Inspektur Jenderal Polisi Dono Indarto, ini semasa saya SMA ada juga Dono Indarto Kepala Basarnas, tapi kalau nggak salah beliau Marsekal Madya namanya persis, ini polisi inspektur jenderal belum pensiun. Kemudian sebelah kanan Brigjen TNI Ferdinand Mahulette Plt. Deputi II Bidang Operasi Keamanan dan Siber.

Ibu, Bapak mohon izin nanti kalau tayangan kalau bisa agak digedein dikit Pak, ini kecil, Pak Utut tulisannya kecil nggak kelihatan. Pak Dominggus itu lain kali kalau tayangan lebih gede, bukan angka yang tulis-tulisan tadi itu. Terus kemudian mohon juga kita lain kali dikasih penjelasan juga, karena ini terlalu detail teknis kita nggak paham. Jadi dibiasakan jangan “mata satu di negara buta raja”. Jadi Bapak matanya satu, kita buta, Bapak jadi raja. Dibiasain Bapak juga memberitahu kita apa itu *cyber threat intelligent service* apa itu *dark web*, apa itu *sinkhole malicious traffic*, dan seterusnya itukan bahasa teknis. Kalau Pak Utut kasih tahu *zugzwang* dicatur ya nggak ada yang tahu. *Zugzwang* adalah apabila melangkah posisinya jelek dikasih contoh, kan begitu. Jadi jangan sampai “mata satu di negara buta raja”.

Kemudian Ibu, Bapak itu kelima yang sudah disampaikan untuk me-*refresh* ingatan kita bahwa APBN teman-teman yang di depan ini tahun ke tahun menurun. Di 2019 Rp2,3 triliun, Pak Hinsa sudah di situ ya.

KEPALA BSSN RI (LETNAN JENDERAL TNI (PURN.) HINSA SIBURIAN):

Pertengahan.

KETUA RAPAT (DRS. UTUT ADIANTO):

Kemudian 2020 turun 2 triliun 206, ada Perpres Covid turun jadi 1 triliun 300, kemudian ada Perpres lagi Nomor 72, jadi ini nggak ada APBNP jadi dipotong langsung Pak Rudi Tjen oleh *world best finance minister*, tinggal 1 triliun 62 miliar. Dan yang terakhir 2020, 1 triliun 700, yang sekarang tinggal 554 miliar, begitu ya Pak, bener ya. Artinya Bapak tadi memuji keuangannya Kementerian Keuangan paling bagus katanya, coba saja tuh yang ahli *hack* siapa Hasto Prastowo tadi coba di-*hack*, biar kaing-kaing baru ke sini, kan gitu.

Ini bukan ngajarin jahat, artinya Bapak-bapak ini tidak dalam *top of mind*-nya *madam world best finance minister*. Itu lima, mohon silakan, oh ini sudah ada yang nanya.

KEPALA BSSN RI (LETNAN JENDERAL TNI (PURN.) HINSA SIBURIAN):

Yang terhormat Bapak Pimpinan dan Ibu, Bapak Anggota Komisi I DPR RI.

Kami menyampaikan terima kasih atas segala masukan, dukungan. Dan semuanya itu mendorong kami tentunya untuk lebih bisa berinovasi, berbuat yang terbaik. Dan memang permasalahan keamanan siber ini yang saat ini juga BSSN sedang atau masih baru, tentu kita harus kerja keras. Ini yang kami selalu sampaikan kepada seluruh anggota. Tuntutan masyarakat terhadap situasi keamanan ruang siber yang begitu luar biasa. Dan pada saat ini juga kami menyampaikan terima kasih sekali lagi atas semua masukan. Dan itu semua menjadi dorongan untuk kami bisa berbuat yang terbaik tentunya. Demikian yang ingin kami sampaikan.

Terima kasih, kami akhiri.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.
Selamat siang,
Om Shanti Shanti Shanti Om,
Salam sehat untuk kita semua.

KETUA RAPAT (DRS. UTUT ADIANTO):

Dengan mengucapkan syukur *Alhamdulillah*, puji syukur kepada Tuhan Yang Maha Esa, dengan ini Rapat Kerja dengan Badan Siber dan Sandi Negara kami nyatakan ditutup.

(KETOK PALU: 3 KALI)

Semoga niat baik kita selalu diberi kemudahan oleh Yang Maha Kuasa dan semoga kerja-kerja keras kita menjadi bagian dari ibadah kita.

Billahi Taufiq Walhidayah,
Wassalamu'alaikum Warahmatullahi Wabarakatuh.

(RAPAT DITUTUP PUKUL 13.04 WIB)

Jakarta, 20 Januari 2022
a.n Ketua Rapat
SEKRETARIS RAPAT,

SARTOMO, S.S., M.Si.
NIP. 196808111996031001