PERLINDUNGAN INFRASTRUKTUR INFORMASI KRITIKAL NASIONAL SEKTOR KETENAGALISTRIKAN DARI ANCAMAN SIBER

CRITICAL NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ON ELECTRICITY SECTOR FROM CYBER THREATS

Khalid S. Robbani[1], Agus H.S. Reksoprodjo[2], Bastari[3]

Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Universitas Pertahanan Indonesia
ksrobbani@gmail.com

Abstrak – Infrastruktur informasi kritikal ketenagalistrikan merupakan bagian dari infrastruktur kritikal ketenagalistrikan yang memanfaatkan TIK sebagai penunjang sistemnya. Maka setiap insiden yang terjadi pada infrastruktur informasi kritikal ketenagalistrikan dapat berdampak selain pada sistem teknisnya, namun juga pada sektor yang lain, pada aspek sosial-ekonomi, bahkan dengan cakupan nasional. Disisi lain, perkembangan ancaman siber yang menyerang TIK juga semakin besar. Hal ini menunjukkan adanya permasalahan yang mendesak untuk menyelenggarakan keamanan siber dalam rangka perlindungan infrastruktur informasi kritikal sektor ketenagalistrikan di level nasional. Maka tujuan penelitian ini menganalisis konsep perlindungan infrastruktur informasi kritikal sektor ketenagalistrikan di Indonesia yang komperehensif dan optimal. Sedangkan pilar keamanan siber di level nasional dinilai dari 5 aspek yaitu legal, teknikal, organisasional, sumber daya manusia, dan kerjasama. Penelitian ini menggunakan metode kualitatif dan pendekatan fenomenologi dengan pengumpulan data dari hasil wawancara terhadap *stakeholder* yang terkait dan studi dokumen. Hasil penelitian menemukan bahwa penyelenggaraan perlindungan tidak berjalan secara komperehensif dan optimal, baik secara legal, teknikal, organisasional, sumber daya manusia, dan kerjasama. Adapun faktor penting yang harus segera ditetapkan di level nasional yaitu kebijakan peraturan, ruang lingkup, dan struktur tata kelola antar *stakeholder* yang terkait. Adapun pada upaya terhadap ancaman siber yaitu penerapan standar keamanan siber dengan sesuai, peningkatan kesadaran karyawan, dan membangun hubungan kerjasama dan kolaborasi, seperti pada forum information-sharing, penelitian dan pengembangan.

Kata Kunci: Ancaman Siber, Infrastruktur Informasi Kritikal Nasional, Keamanan Siber, Ketenagalistrikan, Perlindungan

Abstract *– Critical electricity information infrastructure is part of critical electricity infrastructure that utilizes information and communication technology as a supporting system. So any incidents that occur in the critical electricity information infrastructure can have an impact other than the technical system, but also in other sectors, on the socio-economic aspects, even with national coverage. On the other hand, the development of cyber threats that attack information and communication technology is also getting bigger. This shows that there are pressing issues to carry out cyber security in the context of protecting the critical electricity information infrastructure at a national level. So the purpose of this study is to analyze the concept of protection of critical electricity information infrastructure in Indonesia which is comprehensive and optimal. Whereas the pillars of cyber security at the national level are assessed from 5 aspects namely legal, technical, organizational, capacity building, and cooperation. This study uses a qualitative method with a phenomenological approach by*

[1] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan
[2] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan
[3] Program Studi Strategi Pertahanan Semesta, Fakultas Strategi Pertahanan, Universitas Pertahanan

collecting data from interviews with relevant authorities and document studies. The results indicate that the implementation of protection did not run comprehensively and optimally, both legally, technically, organizationally, capacity building, and cooperation. The important factors that must be immediately determined at the national level are regulatory policies, scope, and governance structures among the relevant authority stakeholders. As for efforts against cyber threats, namely the appropriate application of cyber security standards, increased employee awareness, and building cooperative and collaborative relationships, such as in information-sharing forums, incident-response, or research and development.

Keywords: *Critical National Information Infrastructure, Cybersecurity, Cyberthreat, Electricity, Protection*

Pendahuluan

Dinamika perkembangan lingkungan strategis pada teknologi informasi dan komunikasi (TIK) yang sedemikian pesat mendorong proses globalisasi dengan cepat. TIK menjadi elemen penting dan menyebabkan perubahan pola kehidupan sehari-hari karena menawarkan peningkatan produktifitas, efisiensi, dan efektifitas yang signifikan. Para ahli sering menyebut dimensi jaringan pada TIK dengan istilah *cyberspace* atau ruang siber. Istilah ruang siber digambarkan sebagai sebuah dimensi berupa jaringan teknologi informasi, komunikasi, dan data yang diciptakan manusia untuk menghubungkan jutaan perangkat di dunia ini yang memiliki system pengolah data.[4] Pengaruh teknologi yang telah membentuk ruang siber ini menciptakan dan membawa konektifitas jaringan yang tidak hanya terhadap jaringan komunikasi global manusia, namun juga segala aspek kehidupan masyarakat pada suatu negara.

Seiring perkembangan TIK pula, digitalisasi infrastruktur kritikal yang mengakomodir sektor-sektor penting masyarakat modern semakin meningkat. Maka muncul istilah infrastruktur informasi kritikal untuk menggambarkan totalitas komputer dan perangkat serta jaringan yang terhubung dengan seluruh sistem infrastruktur antara satu dengan yang lainnya secara terpadu dan terintegrasi.[5] Infrastruktur informasi kini mendasari banyak elemen dari infrastruktur kritikal, karena TIK merangkul semua, menghubungkan sistem infrastruktur satu dengan yang lain, dan mengintegrasikannya sehingga

[4] Jason Andress & Steve Winterfeld. Cyber Warfare : Techniques, Tactics, and Tools for Security Practitioners, (USA : Syngress, 2011)

[5] Myriam Dunn & Isabelle Wigert. International CIIP Handbook 2004 (Zurich: ETH Zurich, 2004)

membuat saling terkait dan bergantung. Jika ada insiden sekecil apapun, baik berupa kerusakan atau kegagalan pada infrastruktur informasi, tentu akan mempengaruhi sistem yang lain dan atau akan menjadi resiko yang lebih besar. Hal tersebut dikarenakan setiap kerusakan atau kegagalan pada suatu infrastruktur informasi kritikal dapat berdampak selain pada sistem teknis, namun juga tatanan sosial masyarakat, yang bahkan akan menimbulkan dampak pada skala negara sebab disaat ini kesaling-tergantungan masyarakat yang terjadi jauh lebih besar dan luas.

Salah satu infrastruktur informasi kritikal tersebut adalah bidang energi sector ketenagalistrikan yang sangat vital sebagai kebutuhan pokok pada kehidupan sehari-hari. Secara umum, listik merupakan kebutuhan dasar yang sangat vital dalam pengembangan ekonomi dan kemajuan kesejahteraan social suatu negara. Hal tersebut disebabkan keistimewaan energi listrik yang bisa diubah dari satu bentuk ke bentuk energi lain yang diinginkan. Seperti fenomena *blackout* atau padam total yang terjadi pada awal Agustus 2019 di sebagian besar wilayah Jawa memberi isyarat betapa sangat vitalnya sektor ketenagalistrikan yang efek domino kerusakannya mengganggu sistem transportasi, telekomunikasi, bahkan termasuk pasokan air bersih serta umumnya aktifitas sosial-ekonomi masyarakat. Maka serangan atau gangguan terhadap sektor ketenagalistrikan, bagaimanapun tidak peduli seberapa kecil bentuknya, akan berdampak negatif pada tatanan social-ekonomi masyarakat yang tentu akan menghambat tujuan nasional bangsa Indonesia.

Oleh karena itu, jika dilihat dari perspektif aspek pertahanan negara, perkembangan TIK juga mengubah lingkungan keamanan strategis secara signifikan. Ruang siber menjadi salah satu wahana peperangan, yang kemudian diistilahkan dengan peperangan siber, yang digunakan oleh aktor negara maupun non-negara dan menjadi ancaman serius terhadap keamanan suatu negara.[6] Peperangan siber sendiri merupakan bentuk lain dari peperangan informasi yang paling tidak mudah ditebak sebab berada di dunia maya dan

[6] Paulo Shakarian, J. S. Introduction to Cyber-Warfare, A Multidiscipinary Approach, (Waltham: Syngres, 2013)

bersifat fiktif. Sedangkan informasi itu sendiri menjadi salah satu domain peperangan di masa mendatang, selain domain darat, laut, udara, dan ruang angkasa.[7] Artinya aktor negara maupun non-negara akan dapat memanfaatkan ruang siber tersebut untuk melancarkan peperangan yang mengancam kepentingan dan keamanan negara lain. Maka dampak negatif yang ditimbulkan dapat menjadikan situasi dan kondisi kemananan dunia akan lebih mengkhawatirkan disebabkan kejahatan siber yang bersifat tidak mengenal batas ini. Terlebih ketergantungan dalam pemanfaatan sistem, peralatan, dan platform berbasis digital melalui ruang siber diprediksi akan semakin terus membesar sehingga akan semakin besar pula kerentanan terhadap ancaman serangan-serangan asimetris melalui ruang siber tersebut.[8]

Ancaman siber telah menyebabkan kemampuan negara dalam sektor pertahanan nirmiliter khususnya dari aspek *soft-power* dan *smart-power* harus ditingkatkan melalui strategi penangkalan, penindakan, dan pemulihan pertahanan siber dalam rangka mendukung penerapan strategi keamanan siber nasional. Ancaman siber merupakan ancaman aktual dan memerlukan perhatian yang serius. Ruang lingkup, skala, dan dampak serangan siber terhadap infrastruktur kritikal berkembang pesat dan semakin canggih seiring dengan meningkatnya digitalisasi infrastruktur kritikal. Ancaman tersebut bersifat lintas negara berskala regional maupun global sehingga diperlukan penanganan dan tindakan secara kolektif antar kementerian/lembaga di level nasional sebagai bentuk pertahanan negara dengan ruang lingkup yang jelas dan tata kelola yang baik.

Fenomena serangan siber terhadap infrastruktur informasi kritikal terjadi hampir di seluruh dunia. Insiden tersebut antara lain terjadi di Amerika Serkat dan Kanada pada tahun 2013 sampai 2015 yang meyerang lebih dari 50 pembangkit listrik. Diindikasi informasi yang dicuri oleh seorang peretas dari seorang kontraktor mampu masuk kedalam sistem password dan desain kritikal pembangkit listrik. Pada tahun 2003 di Amerika Serikat juga menyerang

[7] Martin C. Libicki, *What is Information Warfare?* (Washington: Institute for National Strategic Studies, 1995)

[8] Rod Thornton, Asymmetric Warfare: Threat and Response in the Twenty- First Century, (UK: Polity Press, 2007)

pembangkit tenaga nuklir yang diserang menggunakan *malware*. Pada tahun 2015 juga terjadi di Ukraina yang menyerang jaringan distribusi listrik diindikasi disebabkan oleh serangan peretas dan mengakibatkan pemadaman 80.000 pelanggan. Pada tahun 2016 juga terjadi di Israel yang menyerang jaringan distribusi listrik dan sektor umum disebabkan oleh seorang karyawan yang lengah yang menyebabkan tertanamnya malware melalui teknik *phising* sehingga menginfeksi dan melumpuhkan komputer. Begitu banyaknya fenomena serangan siber yang menyerang infrastruktur kritikal di seluruh dunia yang menyebabkan kerugian dan kelumpuhan sosial. [9]

Motif serangan siber menjadi semakin beragam, mulai dari faktor ekonomi hingga kebutuhan eksistensi suatu kelompok. Pelaku serangan siber tidak sekadar menandai, membaca, dan mengkopi sasaran, tetapi juga mengubah data dan informasi, melakukan propaganda, maupun hal-hal lain yang dapat merusak infrastruktur kritikal suatu negara. Maka fenomena kemunculan ancaman serangan siber, sangat mungkin menuntut intervensi campur tangan negara dalam pengelolaannya.

Pemerintah Indonesia dalam rangka memberikan isyarat terhadap perhatiannya pada ruang siber, telah menetapkan kebijakan keamanan siber nasional. Kebijakan tersebut dirasakan setelah munculnya Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara sebagaimana telah diubah dengan Peraturan Presiden Republik Indonesia No. 133 Tahun 2017. Dalam Perpres tersebut, Badan Siber dan Sandi Negara atau BSSN diberi kewenangan dalam pelaksanaan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber di level nasional.

Dalam perpres tersebut juga dinyatakan bahwa BSSN memiliki tugas dalam menyelenggarakan fungsi keamanan siber pada infrastruktur informasi kritikal nasional (IIKN). Secara tidak langsung, melalui perpres tersebut, menempatkan BSSN sebagai lembaga yang sangat strategis dalam rangka

[9] World Energy Council. *World energy Perspectives | 2016*, (United Kingdom: www.worldenergy.org, 2016)

menyelenggarakan pertahanan nirmiliter terhadap ancaman serangan-serangan asimetris melalui ruang siber, termasuk pada IIKN sektor ketenagalistrikan.

Maka dua hal penting yang menjadi pembenaran bagi pemerintah dalam hal ini BSSN, untuk melakukan intervensi campur tangan, termasuk pada IIKN sektor ketenagalistrikan adalah terancamnya sisi keamanan siber dan sekaligus menjadi ancaman bagi pertahanan keamanan dan perekonomian nasional. Maka sejauh apa tindakan nyata pemerintah pada sistem yang menggabungkan komponen fisik dan siber, sehingga dapat memungkinkan terciptanya keamanan siber pada IIKN. Berdasarkan permasalahan diatas, peneliti mengangkat tema perlindungan IIKN sektor ketenagalistrikan. Fokus penelitian ini adalah bagaimana perlindungan IIKN sektor ketenagalistrikan yang optimal secara umum dan khususnya upaya terhadap ancaman siber di Indonesia.

Metode Penelitian

Penelitian tentang perlindungan IIKN sektor ketenagalistrikan dari ancaman siber dilakukan dengan menggunakan metode penelitian kualitatif dan pendekatan fenomenologi. Metode tersebut digunakan karena dinilai mampu menguraikan pemaknaan dan penyikapan negara terhadap fenomena pada perlindungan IIKN di Indonesia. Maka agar pemaknaan dan penyikapan terhadap fenomena tersebut terarah dan jelas, peneliti menggunakan *purposive sampling* dalam menentukan subjek penelitan sebagai partisipan yang memiliki kaitan erat dan terlibat langsung dengan fenomena yang dikaji.

Teknik pengumpulan data yang digunakan menggunakan metode wawancara mendalam untuk mendapatkan data primer yang valid. Selanjutnya pengumpulan data digunakan dengan studi dokumen dengan mengumpulkan dokumen tertulis. Sedangkan untuk pemeriksaan keabsahan data digunakan triangulasi sumber dan teknik, yaitu pengecekan data yang divalidasi dengan sumber dan teknik yang berbeda.

Adapun teknik analisa data yang dilakukan menggunakan teknik Miles dan Huberman. Dalam teknik tersebut, dilakukan proses mencari dan menyusun secara sistematis data yang diperoleh selama pengumpulan data dengan kondensasi data, kemudian data disajikan secara berulang menyesuaikan hasil dari kondensasi data dengan naratif dan

beberapa gambar untuk memudahkan. Dan terakhir melakukan kesimpulan atau verifikasi terhadap data akhir.

Hasil dan Pembahasan

Penelitian ini membahas sejauh mana pemerintah Indonesia menetapkan dan menjalankan kebijakan perlindungan IIKN sektor ketenagalistrikan. Terdapat 5 aspek yang dijadikan sebagai pokok utama berdasarkan pilar keamanan siber global yang dikeluarkan oleh ITU UN pada tahun 2018.[10] 5 aspek tersebut antara lain: legal, organisasional, kerjasama, teknikal, dan pembangunan kapasitas.

Aspek Legal

Secara legal belum ada peraturan yang spesifik mengatur terkait perlindungan IIKN di Indonesia. BSSN masih bertumpu pada Peraturan Presiden Nomor 53 Tahun 2017 yang telah diperbaharui pada Nomor 133 Tahun 2017 tentang Badan Siber dan Sandi Negara. Namun peraturan tersebut belum mendetail dan mampu mengakomodasi pada kebijakan perlindungan IIKN. Sebelumnya sudah ada regulasi yang mengatur terkait keamanan infrastruktur kritikal dalam Peraturan Menteri Energi dan Sumber Daya Mineral RI Nomor 48 Tahun 2018 tentang Penetapan Objek Vital Nasional Bidang Energi dan Sumber Daya Mineral, namun dalam regulasi tersebut tidak membahas aspek siber. Sedangkan pada sisi siber, keberadaan kebijakan yang menjadi dasar hukum di Indonesia hanya bertumpu pada Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun dinilai belum mampu untuk mengakomodasi perlindungan IIKN karena hanya membahas aspek transaksional.

Aspek Organisasional

Selama ini, eksistensi kebijakan yang membahas aspek organisasional secara nasional masih berdasar pada kebijakan keamanan siber secara umum dan belum spesifik menjurus kepada perlindungan IIKN. Pedoman dan dukungan yang diperlukan dalam perlindungan IIKN juga tidak ada. Akibat dari tidak adanya kebijakan dan/ atau pedoman struktur dan tata kelola mengakibatkan perlindungan IIKN tidak berjalan optimal.

[10] International Telecommunication Union. *Global Cybersecurity Index*, (Geneva: ITU Publications, 2019)

Padahal idealnya ada keterlibatan yang sangat kuat dari pemerintah dan/atau regulator sektor pada IIKN untuk mempertimbangkan situasi, kondisi, ukuran, dan kemampuan pada setiap pemilik dan/atau pelaksana penyelenggara IIKN. Sehingga tidak semua dibebankan pada BSSN dan keberjalanan secara organisasional menjadi lebih optimal. Disamping itu, akibat yang ditimbulkan adalah tidak adanya pola koordinasi yang jelas antar *stakeholder*. Selama ini keberjalanan penerapan perlindungan IIKN secara organisasional masih bersifat reaktif dan sporadis.

Aspek Kerjasama

Konsep kemitraan dan kerjasama yang dilakukan belum berjalan dengan maksimal karena pola hubungan kerjasama yang dijalin masih parsial dan pada beberapa hubungan kerjasama yang sudah diinisiasi, tidak berjalan dengan baik. Konsep kemitraan dan kerjasama yang dibangun seharusnya menyentuh pada partisipasi forum internasional, lintas sektor, kemitraan dengan sektor swasta. Kemitraan dan kerjasama yang dibangun juga terkait *information-sharing*, tanggap bencana atau *incident response*, penelitian dan pengembangan, serta penerapan *best-practice* dengan lembaga lain terkait keamanan siber.

Aspek Teknikal

Aspek teknikal pada keamanan siber yang digunakan diukur berdasarkan kematangan keberadaan lembaga dan kerangka kerja teknis dalam mengatasi keamanan siber. Fungsi teknis keamanan siber di tingkat penyelenggara atau pelaksana IIKN sektor ketenagalistrikan diambil alih oleh *Security Operation Centre* (SOC) yang berada dibawah Divisi Sistem dan Teknologi Informasi PLN yang terpusat di PLN pusat. SOC memiliki karyawan yang selalu dipantau terkait kapasitas pengetahuan dan kapabilitas kemampuan dalam menghadapi ancaman siber. Tim SOC bekerja selama 24 jam full secara tim dan dalam 7 hari.

Selanjutnya kerangka kerja penerapan standarisasi keamanan siber yang digunakan sesuai dokumen adalah panduan standar penerapan manajemen teknologi informasi menggunakan kerangka kerja COBIT (*Control Objectives for Information and related Technology*). Adopsi keamanan siber dengan pendekatan berbasis risiko tersebut diselenggarakan dan diprioritaskan sesuai dengan dampak dan frekuensi ancaman yang terjadi. Infrastruktur

informasi kritikal di sektor ketenagalistrikan dengan dampak risiko terbesar pertama adalah sistem SCADA (*Supervisory Control and Data Acquisition*). Sistem SCADA merupakan sistem pada tenaga listrik yang berfungsi memonitor, mengontrol, dan mengakuisisi data serta informasi listrik secara real-time. PLN menggunakan sistem SCADA pada pembangkit, pengatur beban, dan transmisi.

Aspek Pembangunan Kapasitas

Aspek pembangunan kapasitas difokuskan pada faktor sumber daya manusia. Adapun sumber daya manusia pada keamanan siber diukur berdasarkan kematangan program peningkatan kesadaran, penelitian, pengembangan, pendidikan, dan pelatihan, serta sertifikasi para profesional. Program pendidikan dan pelatihan yang dijalankan seputar pembangunan kesadaran menjadi prioritas di PLN saat ini. Adapun sumber daya manusia yang menangani keamanan sibernya, PLN telah berinisiatif untuk mendorong para karyawan operasional untuk melakukan peningkatan pengetahuan dan kemampuan. Peningkatan kemampuan dilakukan dengan pelatihan *penetration testing* untuk internal atau pelatihan-

Gambar 1. Ruang Lingkup Perlindungan IIKN Sektor Ketenagalistrikan
Sumber: diolah peneliti, 2020

pelatihan yang serupa, serta mendorong agar mengikuti sertifikasi keamanan siber untuk level profesional.

Perlindungan Infrastruktur Informasi Kritikal Sektor Ketenagalistrikan dari Ancaman Siber

Ada beberapa pokok poin yang menjadi sangat vital dan harus diprioritaskan. Hal prioritas yang diajukan menjadi pokok yang berdampak pada poin masalah yang lainnya dalam rangka tata kelola perlindungan IIKN yang lebih optimal.

Prioritas I: Penetapan Ruang Lingkup

Penetapan ruang lingkup dari perlindungan IIKN bertujuan agar jelas cakupan perlindungan tersebut. Berdasarkan kajian yang dilakukan terhadap 4 dokumen keamanan siber pada infrastruktur informasi kritikal, yaitu Forum ASEAN-Japan, ITU UN, ENISA EU, dan CISA US.[11][12][13][14] Maka ada 8 aspek penting yang menjadi ruang lingkup perlindungan IIKN seperti pada Gambar 1.

Prioritas II: Penguatan Legislasi dan Regulasi

Sebagai negara hukum, aspek legal dapat menentukan pemberian kewenangan terhadap penyelenggaraan sebuah pemerintahan.[15] Dalam perspektif keamanan siber, aspek legal ditujukan untuk menyelaraskan praktik keamanan siber, baik di tingkat sektoral, nasional, regional, dan internasional. Disamping itu dapat digunakan untuk menetapkan pondasi standar dasar perilaku minimum yang dibangun dan membentuk mekanisme peran dan tanggung jawab dasar, baik pada aspek keamanan siber praktikal maupun tindakan hukum siber kriminal. Dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber, salah satu aspek kerangka kerja penyelenggaraan keamanan siber agar implementasi keamanan siber dapat berjalan secara optimal dan berkeseinambungan serta dapat diukur kinerjanya adalah aspek legal.

---

11 ASEAN-JAPAN Summit. CIIP Guidelines Ver. 3.0 (Tokyo: The 9th ASEAN-Japan Information Security Policy Meeting, 2016)

12 International Telecommunication Union, Guide Developing A National Cybersecurity Strategy (Geneva: Place des Nations, 2018)

13 ENISA, Stocktaking, Analysis, and Recommendations on the Protection of CIIs (Europe Union: European Union Agency For Network And Information Security, 2016)

14 CISA, A Guide to Critical Infrastructure Security and Resilience (United States: Cybersecurity and Infrastructure Security Agency, 2019)

15 Siallagan Haposan, Penerapan Prinsip Negara Hukum di Indonesia, (Sosiohumaniora, Volume 18 No. 2, 2016) hal. 122 - 128.

Sebagai landasan legal, kebijakan legislasi dan/atau regulasi diperlukan agar sesuai dengan penyelenggaraan tata kelola pemerintahan yang baik sehingga mampu menjadi pondasi dasar penerapan keamanan siber pada instansi pemerintah. Belum adanya kekuatan hukum yang mengatur kebijakan perlindungan IIKN membuat proses terjaminnya keamanan siber menjadi lama. Penetapan kebijakan legal baik berupa undang-undang atau peraturan yang berkaitan tentang perlindungan infrastruktur informasi kritikal menjadi prioritas utama saat ini disebabkan Republik Indonesia menganut negara hukum.

Adapun bentuk kebijakan legal keamanan siber harus mencakup skala tertinggi dalam rangka melaksanakan penyelenggaraan kekuasaan pemerintahan di level nasional. Peraturan tersebut kedepannya dapat mencakup lintas sektor dan/atau lintas kementerian/lembaga. Maka menurut Undang-Undang Republik Indonesia Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan jenis kebijakan legal terkait perlindungan IIKN yang diinisiasi paling tidak harus berupa Peraturan Presiden atau Peraturan yang lebih tinggi status hukumnya.

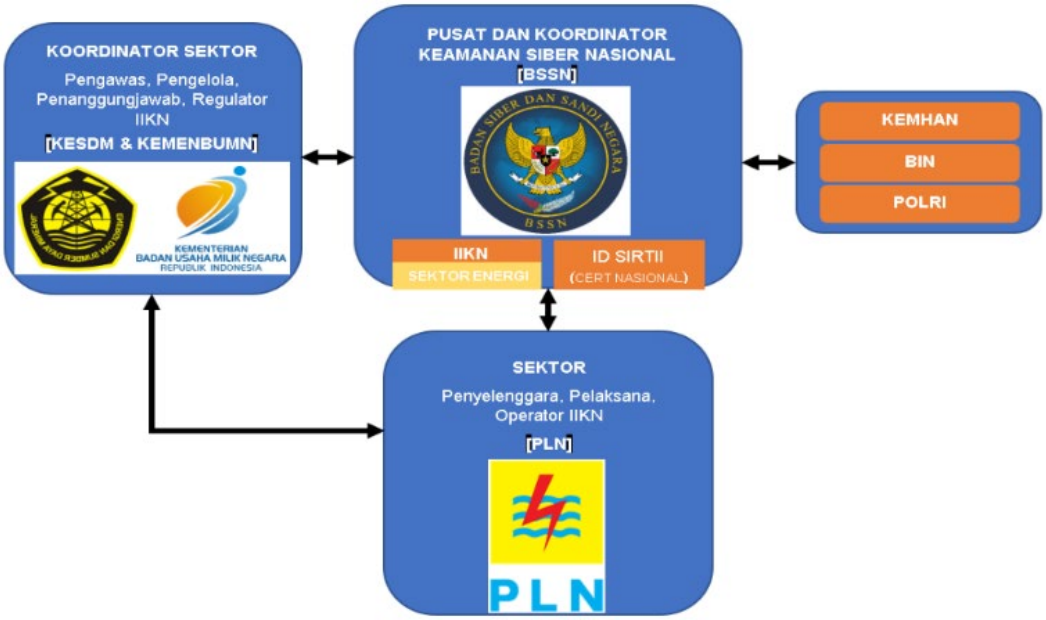
Prioritas III: Penguatan Skema Organisasi Tata Kelola

Dalam rangka perlindungan IIKN secara komperehensif dibutuhkan strategi yang memberikan penguatan pada struktur tata kelola, peran, dan tanggung jawab seluruh *stakeholder*. Dalam pengembangan keamanan siber, tanpa strategi nasional, model tata kelola, dan badan yang bertanggungjawab, upaya di berbagai sektor menjadi kontraproduktif.[16] Sehingga bentuk evaluasi terhadap aspek organisasional harus didasarkan pada penguatan keberadaan lembaga dan strategi yang dijalankan oleh lembaga tersebut dalam rangka pengembangan keamanan siber di tingkat nasional.

Pemenuhan tugas instansi pemerintah sebagai upaya pemerintah atas perlindungan keamanan secara komperehensif dan integratif.[17] Perlindungan IIKN yang efektif dan efisien mensyaratkan para *stakeholder* memiliki

[16] International Telecommunication Union. *Global Cybersecurity Index*, (Geneva: ITU Publications, 2019)

[17] Don C. Smith. Enhancing Cybersecurity in The Energy Sector: A Critical Priority (Journal of Energy & Natural Resources Law, 2018) hal. 373-380



Gambar 2. Skema Organisasi Tata Kelola Perlindungan IIKN Sektor Ketenagalistrikan di Indonesia
Sumber: diolah peneliti, 2020

peran dan tanggung jawab yang jelas. Disamping itu, juga dituntut untuk membangun mekanisme koordinasi diantara *stakeholder* tersebut. Hal penting yang pertama harus dilakukan sebagai bentuk penguatan organisasi adalah mengindetifikasi seluruh *stakeholder* yang terkait dengan IIKN yang dalam penelitian ini fokus pada sektor energi ketenegalistrikan.

Pelibatan *stakeholder* pada perlindungan IIKN sektor ketenagalistrikan yang tertata bertujuan agar tidak ada ego sektoral dan/atau tidak ada yang merasa geraknya tersekat dan/atau melimpahkan semua tanggungjawab hanya kepada satu pihak sehingga *stakeholder* khususnya di level pemerintahan memiliki mekanisme dan porsinya masing-masing dalam menangani perlindungan IIKN. kolaborasi antar organisasi *stakeholder* adalah faktor penting untuk keberhasilan dalam mengimplementasikan inisiatif dan program terkait penanganan perlindungan IIKN. [18]

Jika *stakeholder* tersebut dipetakan dan dikaitkan pada sektor ketenagalistrikan di Indonesia, maka rancangan sebagai berikut:

1. Koordinator keamanan siber nasional.
2. Koordinator sektor (regulator, pengawas, dan pengatur operator sektor IIKN).
3. Sektor – operator (penyelenggara dan pelaksana IIKN).

[18] Rossella Mattioli, Dr. Cedric Levy-Bencheton. Methodologies for the Identification of Critical Information Infrastructure Asset and Services (Koln: ENISA, 2014)

4. Kementerian/ lembaga terkait (pertahanan, intelijen, tindak pidana)

Berdasarkan Gambar 2. maka ada beberapa kementerian/ lembaga sebagai *stakeholder* yang memiliki peran dan tanggung jawab pada perlindungan IIKN sektor ketenagalistrikan di Indonesia. Kementerian/ lembaga tersebut dapat dijabarkan sebagai berikut:

1. Badan Siber dan Sandi Negara (BSSN)

Koordinator keamanan siber sesuai Peraturan Presiden Nomor 53 Tahun 2017 adalah BSSN. Dalam peraturan tersebut BSSN bukan hanya berwenang dalam merumuskan dan melaksanakan kebijakan teknis, namun juga dalam fungsi koordinasi penanganan siber. Maka BSSN harus mampu menjadi *leading sector* dan lembaga yang paling bertanggung jawab terhadap keamanan siber secara nasional. Dalam peraturan tersebut BSSN mempunyai tugas dalam pelaksanaan keamanan siber secra efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber. Maka jika dihadapkan pada perlindungan IIKN di Indonesia, BSSN menjadi pusat dan koordinator keamanan siber nasional yang melakukan fungsi perlindungan secara komperehensif.

BSSN mempunyai peran dan tanggung jawab secara proporsional pada seluruh aspek ruang lingkup perlindungan IIKN, mulai dari menetapkan peraturan legislasi dan regulasi terkait keamanan siber secara nasional, melakukan inisiasi sekaligus menjadi koordinator pada skema tata kelola keamanan siber nasional, menjalankan fungsi pusat sekaligus fasilitator *information-sharing stakeholder* lintas sektor, menetapkan pedoman standar penerapan keamanan siber, pedoman manajemen risiko keamanan siber, pedoman penanganan insiden atau tanggap bencana siber, pedoman upaya untuk pemulihan pasca insiden siber, menetapkan program pembangunan kesadaran masyarakat, menjalankan program peningkatan pengetahuan dan kemampuan, termasuk didalamnya sertifikasi terhadap karyawan profesional, dan terakhir melakukan inisiasi kerjasama antar negara *govt-to-govt*, dan/atau antar *stakeholder* lintas sektor, dan/atau antara *public-private*, dan/atau dengan lembaga penelitian, pengembangan, serta akademisi/pakar terkait keamanan siber pada IIKN secara

umum, dan secara khusus pada penelitian ini di sektor ketenagalistrikan.

2. Kementerian Energi dan Sumber Daya Mineral (KemenESDM) dan Kementerian Badan Usaha Milik Negara (KemenBUMN)

Kementerian sektor terkait selaku koordinator sektor, dalam hal ini KemenESDM dan KemenBUMN, memiliki tanggung jawab terhadap pengawasan keberjalanan sub-sektor atau pelaksana dan penyelenggara IIKN. Secara sederhananya kementerian terkait mengemban tugas secara legal untuk menjadi penanggungjawab sektor terkait. KemenESDM dalam Undang-Undang Republik Indonesia Nomor 30 Tahun 2009 tentang Ketenagalistrikan ditetapkan sebagai kementerian yang diberi kewenangan untuk menetapkan pedoman penyusunan rencana umum ketenagalistrikan. Maka KemenESDM dalam rangka perlindungan IIKN dinilai berwenang untuk menetapkan kebijakan regulasi terkait keamanan siber si sektor ketenagalistrikan. Sedangkan KemenBUMN dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2003 tentang Badan Usaha Milik Negara ditetapkan sebagai kementerian yang ditunjuk dan/atau diberi kuasa ntuk mewakili pemerintah pemegang saham negara pada Persero, dalam hal ini PLN. Maka ada kepentingan yang KemenBUMN dalam menjaga aset keuntungan bisnis pada IIKN sektor ketenagalistrikan.

Sedangkan perlindungan IIKN ditujukan untuk melindungi segala macam potensi bahaya dan ancaman yang menyerang IIKN, salah satunya untuk melindungi keberlangsungan bisnis. Dari uraian undang-undang diatas maka koordinator sektor memiliki peran dan tanggung jawab dalam menetapkan kebijakan regulasi sektor, melakukan pengawasan terhadap penerapan keamanan siber di instansi penyelenggara dan pelaksana sektor.

3. Perseroan Terbatas Perusahaan Listrik Negara

Dalam Undang-Undang Republik Indonesia Nomor 30 Tahun 2009 tentang Ketenagalistrikan disebutkan bahwa PT Perusahaan Listrik Negara (Persero) sebagai badan usaha milik negara yang dianggap telah memiliki izin usaha penyediaan tenaga listrik. Sedangkan dalam rangka pembangunan ketenagalistrikan dalam undang-undang tersebut disebutkan menganut asas salah satunya adalah keamanan dan keselamatan. Dari dasar tersebut dapat

dinyatakan bahwa PLN memiliki tanggung jawab sebagai pelaksana dan penyelenggara utama usaha penyediaan tenaga listrik, termasuk didalamnya untuk aspek keamanan dan keselamatannya.

Sedangkan dari sisi keberjalanan bisnis, disebutkan dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2003 tentang Badan Usaha Milik Negara dijelaskan bahwa PLN yang berstatus persero merupakan Badan Usaha Milik Negara. Disamping itu, dalam undang-undang tersebut disebutkan bahwa BUMN didirikan dengan maksud dan tujuan untuk perkembangan ekonomi, pemenuhan hajat hidup orang banyak, keuntungan bisnis negara, sehingga segala macam perlindungan terhadap infrastruktur BUMN tersebut, termasuk infrastruktur informasi, harus diselenggarakan dengan optimal dan efisien.

Maka PLN memiliki tanggungjawab sebagai pelaksana dan penyelenggara utama keamanan siber dalam rangka perlindungan IIKN sektor ketenagalistrikan secara optimal dan efisien.

4. Kementerian Pertahanan

Kementerian Pertahanan dalam Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara disebutkan memiliki kewenangan dalam penetapan kebijakan tentang penyelenggaraan pertahanan negara berdasarkan kebijakan umum yang ditetapkan Presiden. Dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber, menyatakan bahwa perhatian pertahanan siber secara khusus diberikan pada sektor yang mengelola infratruktur kritikal nasional salah satunya energi, dimana gangguan sistem elektronik pada sektor tersebut dapat menyebabkan kerugian ekonomi, turunnya tingkat kepercayaan masyarakat pada pemerintah, terganggunya ketertiban umum. Sehingga dari risiko tersebut menjadi bahan pertimbangan terkait kebutuhan akan pertahanan siber yang kuat di Indonesia.

5. Badan Intelijen Negara

Pada rumusan Peraturan Presiden Nomor 73 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Nomor 90 Tahun 2012 tentang Badan Intelijen Negara menyatakan bahwa Badan Intelijen Negara memiliki penambahan Deputi Bidang Intelijen Siber atau selanjutnya disebut Deputi VI Badan Intelijen Negara. Deputi VI merupakan unsur pelaksana

dari Badan Intelijen Negara di bidang intelijen negara. Deputi VI memiliki tugas dalam pelaksanaan perumusan kebijakan dan kegiatan dan/atau operasi intelijen siber. Deputi VI dalam melaksanakan tugas tersebut, menyelenggarakan fungsi antara lain: penyusunan rencana kegiatan dan/atau operasi intelijen siber; pelaksanaan, pengoordinasian, pengendalian, kegiatan dan/atau operasi intelijen siber; dan terakhir melakukan penyusunan laporan intelijen siber.

6. Kepolisian Republik Indonesia

Kepolisian Republik Indonesia memiliki kewenangan dalam penanganan kejahatan siber di Indonesia. Pengaturan tidak pidana siber yang menjadi tanggung jawab Kepolisian Republik Indonesia diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Prioritas IV: Upaya Perlindungan IIKN terhadap Ancaman Siber

1. Identifikasi dan deteksi Potensi Ancaman Siber

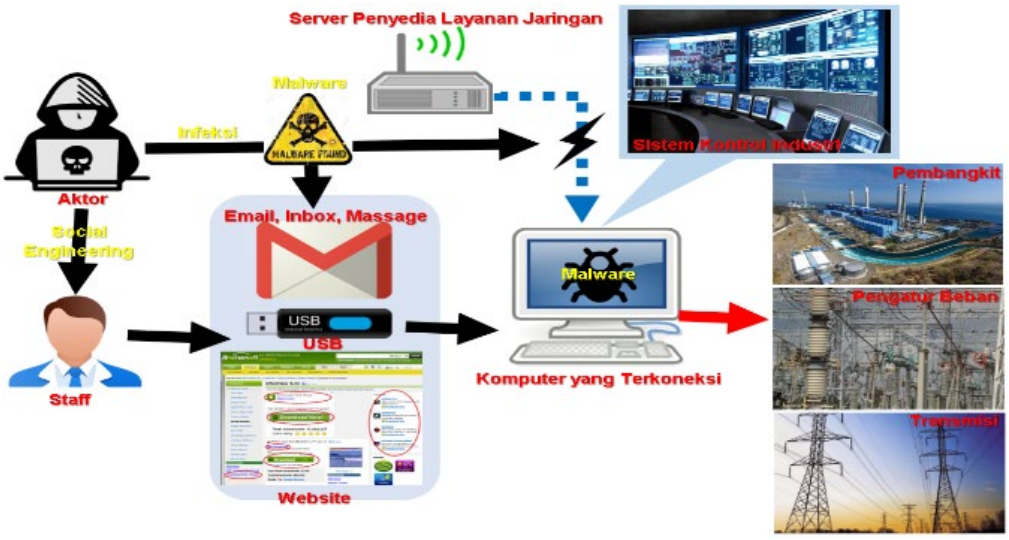
Langkah pertama dalam upaya perlindungan IIKN terhadap ancaman siber tersebut adalah dengan mengidentifikasi dan mendeteksi potensi ancaman siber yang mungkin menjadi

Gambar 3. Klasifikasi Aktor, Bentuk, dan Motif Ancaman Siber
Sumber: diolah peneliti, 2020

sumber risiko keamanan siber dan dapat mempengaruhi bahkan menyerang infrastruktur informasi kritikal. Adapun potensi ancaman siber dapat diidentifikasi dari aktor yang melakukan, motif yang dilakukan, dan bentuk serangan. Hal tersebut dikarenakan pada setiap aktor dan/atau bentuk dan/atau motif potensi ancaman siber memiliki penanganan yang berbeda-beda. Meski pendekatan yang dibangun sama-sama menggunakan pendekatan berbasis risiko. Maka jika dipetakan menurut aktor, bentuk dan motif ancaman siber, dapat diklasifikan seperti pada Gambar 3.

2. Mengidentifikasi dan Mendeteksi Infrastruktur Informasi Kritikal

Langkah kedua dalam upaya perlindungan IIKN sektor ketenagalistrikan adalah dengan mengidentifikasi dan mendeteksi seluruh infrastruktur informasi kritikal yang rentan terhadap ancaman siber. Infrastruktur informasi kritikal bukan hanya terkait keamanan sistem informasi, namun keamanan siber secara keseluruhan, termasuk efek keamanan siber pada dimensi fisik, dunia maya, dan manusia, termasuk untuk organisasi yang mengandalkan teknologi, baik teknologi informasi, sistem kontrol industri, sistem fisik cyber, dan Internet of Things (IoT). [19] Maka dalam mengidentifikasi dan mendeteksi infrastruktur informasi kritikal pada sektor ketenagalistrikan,



Gambar 4. Alur Potensi Serangan Siber pada IIKN Sektor Ketenagalistrikan di Indonesia
Sumber: diolah peneliti, 2020

[19] Eric Luiijf. Good Practice Guide on Critical Information Infrastructure Protection for Governmental policy-makers (Netherlands: Global Forum on Cyber Expertise Meridian, 2016)

maka harus dilihat secara umum pada teknologi yang digunakan, proses yang dijalankan, dan sumber daya manusia yang mengoperasikan.

Bentuk identifikasi dan deteksi pertama dapat dilakukan dengan penilaian risiko terhadap fungsi detail pada infrastruktur informasi yang dikategorikan sangat kritikal. Jika melihat PLN, maka penggunaan sistem SCADA pada operasional teknisnya menjadi ancaman yang paling besar. Sistem SCADA merupakan sistem yang diserang oleh para peretas saat terjadinnya insiden siber di sektor kelistrikan yang menyebabkan *blackout* di Ukraina.

Seringnya PLN mendapat serangan berupa *spamming* atau *phising* yang memungkinkan jebakan *malware*. Disisi lain bahwa sumber penyebab insiden terbesar adalah dari internal perusahaan sendiri karena kesadaran terhadap keamanan siber yang perlu ditingkatkan dan masih kurangnya sumber daya manusia di unit cabang, artinya operator keamanan siber di lapangan belum seluruhnya dan sepenuhnya sesuai dengan standar. Maka, PLN sepenuhnya sangat berpeluang mendapat serangan ancaman siber.

Peneliti mencoba membentuk pola antara potensi ancaman serangan yang ada dengan kelemahan yang dimiliki oleh PLN. Peneliti hanya memberikan satu skema kasus yang kemungkinan menjadi penyebab paling banyak dan paling besar. Berikut gambaran alur bagaimana potensi malware yang disebar melalui *spamming* dan/atau *phising* dapat disebarkan dan sukses masuk dalam akses sistem kontrol industri ketenagalistrikan karena kelemahan kesadaran dan/atau kemampuan karyawan PLN pada Gambar 4.

3. Melakukan Upaya Perlindungan, Penanggulangan, dan Pemulihan

Mekanisme yang dibangun dalam rangka perlindungan, penanggulangan, dan pemulihan infrastruktur informasi kritikal adalah pengembangaan terhadap metodologi berbasis risiko yang menyesuaikan perkembangan ancaman infrastruktur kritikal yang tidak hanya seputar teknikal seperti menggunakan kerangka kerja manajemen risiko pada keamanan siber, namun juga aspek yang lainnya. Hal yang dimaksudkan seperti kesadaran keamanan, kepercayaan hubungan kerjasama, mengetahui sistem proses yang berjalanan, dan membangun

information-sharing antar pemangku kebijakan. [20]

Maka upaya perlindungan terhadap IIKN dari ancaman siber dapat dilakukan dengan menetapkan kebijakan penerapan standar keamanan siber yang sejalan dengan kebijakan perlindungan IIKN, membangun kapasitas dan kapabalitas sumber daya manusia, serta menguatkan hubungan kerjasama dan kolaborasi.

4. Menetapkan kebijakan penerapan standar keamanan siber

Penetapan kebijakan penerapan standar keamanan siber menjadi prioritas dari sisi teknikal dan operasional. Namun yang menjadi penekanan adalah pada pengawasan, pemantauan, dan evaluasi penerapan standar keamanan siber. Melakukan pemantauan dan evaluasi berkala pada setiap sumber risiko, baik dari ancaman siber eksternal maupun internal pada teknologi yang digunakan, proses yang berjalan, dan sumber daya manusia yang mengoperasikan. Selanjutnya dibutuhkan juga untuk membangun langkah-langkah mitigasi yang disesuaikan berbasis risiko yang ditimbulkan. Langkah-langkah mitigasi dilakukan untuk mencegah insiden siber yang semakin meluas, mengurangi dampak yang terjadi, dan tentunya untuk menyelesaikan insiden tersebut. Dan terakhir mengevaluasi efektifitas penerapan keamanan siber saat dan pasca insiden terjadi, termasuk manajemen dan kemampuan tanggap bencana atau incident response, perencanaan pemulihan.

5. Membangun Kapasitas dan Kapabilitas Sumber Daya Manusia

Aspek pembangunan kapasitas ditujukan pada sumber daya manusia yang menjadi aset utama karena mempunyai peranan sangat penting dalam keamanan siber. Pembangunan kapasitas sumber daya manusia sangat penting untuk meningkatkan kesadaran, pengetahuan, dan kemampuan dalam rangka mengatasi permasalahan keamanan siber yang komperehensif. Terkadang instansi besar dan/atau kementerian/lembaga berinvestasi secara besar-besaran dalam pengembangan teknologi hanya untuk melindungi infrastruktur sistem teknologi saja.

[20] Solomon Karchefsky. *Toward a Safer Tomorrow: Cybersecurity and Critical Infrastructure,* (The Palgrave Handbook of Managing Continuous Business Transformation,2016) hal. 335-352

Namun pada aspek sumber daya manusia sebagai operator atau pelaksana sistem tidak diperhatikan. Pertahanan infrastruktur informasi kritikal yang bersifat perimeter saja tidak mampu mempertahankan sistem. Sebagian besar kesalahan sistem adalah pada kesalahan manusia.[21] Maka memberikan perhatian khusus aspek manusia untuk membangun kontrol keamanan siber dapat secara signifikan mengurangi resiko. Hasil perlindungan infrastruktur informasi kritikal yang optimal, efektif, dan efisien sangat memerlukan dukungan tenaga kerja sumber daya manusia dalam suatu penyelenggaraan keamanan siber di lingkungan infrastruktur kritikal. Jika tenaga kerja sumber daya manusia tidak memiliki pemahaman standar keamanan siber minimal dan/atau memegang peranan penting sebagai operator bagian-bagian kritikal infrastruktur informasi namun tidak memiliki kemampuan standar keamanan siber minimal, maka jaminan keamanan siber dengan infrastruktur sistem teknologi, seperti menggunakan antivirus, firewall, atau sistem deteksi tidak akan berjalan dengan optimal. Bahkan dapat dikatakan bahwa meski dengan adanya teknologi yang diperbaharui pun, dan/atau standar prosedur keamanan, dan/atau bagian yang bertanggungjawab pun belum akan mencapai keamanan siber yang optimal tanpa peningkatan kapasitas sumber daya manusia terkait keamanan siber.

Maka bentuk pembangunan kapasitas yang fokus pada sumber daya manusia dapat dilakukan, antara lain:

a. Program peningkatan kesadaran untuk karyawan,
b. Program peningkatan kapasitas dan kapabilitas untuk operator,
c. Program sertfikasi untuk profesional maupun lembaga.

6. Menguatkan Hubungan Kerjasama dan Kolaborasi

Penguatan kerjasama menjadi hal penting yang harus menjadi prioritas. Hal yang mendasari penguatan kerjasama adalah tantangan pada ancaman yang menyerang IIKN, khususnya ancaman siber yang semakin canggih dan persebarannya cepat. Maka dibutuhkan kerjasama dan kolaborasi baik dalam rangka *information-sharing* dan/atau tanggap bencana lintas sektor, atau penelitian dan pengembangan terkait perkembangan teknologi siber.

[21] Leandros A. Maglaras. *Cyber Security of Critical Infrastructures,* (The Korean Institute of Communication and Information Sciences, ICT Express 4, 2018) hal. 42-45

Hubungan kerjasama dan kolaborasi juga sebaiknya dijalin terkait *best practice* atau pedoman keamanan siber yang diterapkan oleh instansi lainnya. Inisiasi kerjasama dapat dilakukan antar negara atau govt-to-govt, dan/atau antar *stakeholder* lintas sektor, dan/atau antar instansi publik dan swasta, dan/atau dengan lembaga penelitian, pengembangan, serta akademisi terkait keamanan siber pada IIKN secara umum, dan secara khusus pada penelitian ini sektor ketenagalistrikan.

Kesimpulan Rekomendasi dan Pembatasan

Perlindungan IIKN pada sektor ketenagalistrikan di Indonesia harus menjadi salah satu titik fokus bagi *stakeholder* lintas sektor di Indonesia sebab belum berjalan secara optimal. Adapun faktor yang menyebabkan belum berjalan secara optimal adalah legal, organisasional, dan kerjasama. Faktor legal yaitu belum adanya peraturan spesifik yang mengatur kebijakan perlindungan IIKN secara umum, dan khususnya sektor ketenagalistrikan. Faktor organisasional yaitu tidak ada kebijakan dan/atau pedoman struktur organisasi dan tata kelola serta tidak adanya pola koordinasi yang jelas antar *stakeholder*. Dan pada faktor kerjasama sudah terbangun, namun dinilai tidak optimal dan masih parsial.

Maka dalam rangka optimalisasi perlindungan IIKN sektor ketenagalistrikan hal pertama yang dilakukan adalah identifikasi dan menetapkan seluruh ruang lingkup yang menjadi bentuk perlindungan IIKN. Kedua penguatan legislasi dan/atau regulasi menjadi prioritas di dalam konteks Indonesia sebagai negara hukum. Dan yang ketiga secara organisasional melakukan penguatan skema organisasi tata kelola khususnya terkait peran dan tanggung jawab serta koordinasi antar *stakeholder*.

Upaya perlindungan IIKN sektor ketenagalistrikan dari ancaman siber di Indonesia selama ini sudah berjalan, namun belum berjalan maksimal. Upaya tersebut dilihat dari faktor teknikal dan pembangunan kapasitas. Adapun faktor teknikal berupa penerapan standar keamanan siber yang dijalankan beserta tim teknis yang bertanggung jawab pada penerapan tersebut. Sedangkan faktor pengembangan kapasitas fokus pada sumber daya manusia yaitu dengan peningkatan kesadaran, pengetahuan, dan kemampuan sumber daya manusia.

Bentuk upaya teknikal yaitu identifikasi dan deteksi ancaman. Kedua identifikasi dan deteksi infrastrutur informasi yang kritikal. Dan dalam upaya perlindungan, penanggulangan, dan pemulihan, selain menerapkan kerangka kerja keamanan siber, juga menguatkan aspek sumber daya manusia, yaitu peningkatan kesadaran, pengetahuan, dan kemampuan. Disamping itu, juga menguatkan hubungan kerjasama dan kolaborasi baik terkait *information-sharing*, tanggap bencana, penelitian dan pengembangan, serta *best-practice* yang digunakan oleh instansi lain pada keamanan siber.

Rekomendasi dari pembahasan hasil penelitian antara lain, yaitu perlindungan IIKN sektor ketenagalistrikan masih membutuhkan pembahasan dan kajian lebih mendalam terutama pada setiap 8 pokok ruang lingkup perlindungan yang diusulkan. Kajian tersebut diharapkan dapat diterapkan pada sektor lainnya dan disesuaikan *stakeholder* yang terlibat serta upaya yang dilakukan terhadap ancaman siber. Untuk penelitian selanjutnya diharapkan ada kajian lebih mendalam terkait struktur organisasi dan tata kelola BSSN yang menggunakan pembagian deputi berdasarkan kerangka kerja keamanan siber dengan pembagian berdasarkan *end-to-end* pada setiap sektor.

Bagi *stakeholder* perlindungan IIKN, khususnya BSSN yang diberi kewenangan dalam kebijakan keamanan siber nasional, diharapkan untuk memprioritaskan agenda penetapan kebijakan legislasi dan/atau regulasi yang membahas perlindungan infrastruktur informasi kritikal secara komperehensif yang mencakup 8 aspek ruang lingkup. Selanjutnya membangun struktur organisasi dan tata kelola perlindungan IIKN sektor ketenagalistrikan terutama pada bentuk peran dan tanggungjawab serta koordinasi antara koordinator kemanan siber nasional, BSSN; koordinator sektor, KemenBUMN dan KemenESDM; operator pelaksana dan penyelenggara utama, PLN; serta kementerian/ lembaga terkait.

Bagi PLN diharapkan menguatkan upaya dalam rangka perlindungan IIKN sektor ketenagalistrikan dari ancaman siber dengan membangun lingkungan dan budaya keamanan siber serta menguatkan hubungan kerjasama. Membangun lingkungan dan budaya keamanan siber khususnya pada 3 hal yaitu, kesadaran, pengetahuan, dan kemampuan. Melakukan inisiasi dengan

menguatkan kerjasama baik tekait forum *information-sharing*, forum tanggap bencana siber, penelitian dan perkembangan teknologi siber, dan/atau *best-practice*/ pedoman keamanan siber yang diterapkan.

Daftar Pustaka

Buku

ASEAN-JAPAN Summit. (2016). CIIP Guidelines Ver. 3.0. Tokyo: The 9th ASEAN-Japan Information Security Policy Meeting.

CISA. (2019). A Guide to Critical Infrastructure Security and Resilience. United States: Cybersecurity and Infrastructure Security Agency.

Dunn, M., & Wigert, I. (2004). International CIIP Handbook 2004. Zurich: Eidgenossische Technische Hochschule Zurich Swiss Federal Institute of Technology Zurich.

ENISA. (2016). Stocktaking, Analysis, and Recommendations on the Protection of CIIs. Europe Union: European Union Agency For Network And Information Security.

International Telecommunication Union. (2018). Guide Developing A National Cybersecurity Strategy. Geneva: Place des Nations

International Telecommunication Union. (2019). Global Cybersecurity Index 2018. Geneva: ITU Publications.

Andress, Jason & Winterfeld, Steve. (2011). Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners. USA: Syngress.

Libicki, M. C. (1995). What is Information Warfare? Washington, DC: Institute for National Strategic Studies, National Defense University.

Luiijf, E. (2016). Good Practice Guide on Critical Information Infrastructure Protection for Governmental policy-makers. Netherlands: Global Forum on Cyber Expertise Meridian.

Thornton, R. (2007). Asymmetric Warfare: Threat and Response in the Twenty- First Century. UK: Polity Press.

Jurnal

World Economy Council. (2016). World energy Perspectives | 2016. United Kingdom: www.worldenergy.org.

Maglaras, Leandros A. (2018). Cyber Security of Critical Infrastructures. The Korean Institute of Communication and Information Sciences, ICT Express 4, 42-45.

Shakarian J.S, Paulo (2013). Introduction to Cyber-Warfare, A Multidiscipinary Approach. Waltham: Syngress, Elsevier.

Mattioli, Rossella & Levy-Bencheton, Cedric (2014). Methodologies for the Identification of Critical Information Infrastructure Asset and Services. Koln: ENISA

Haposan, Siallagan. (2016). Penerapan Prinsip Negara Hukum di Indonesia. Sosiohumaniora, Volume 18 No. 2 Juli 2016, 122 - 128.

Smith, D. C. (2018). Enhancing Cybersecurity in The Energy Sector: A Critical Priority. Journal of Energy & Natural Resources Law, 373-380

Karchefsky, Solomon. (2016). Toward a Safer Tomorrow: Cybersecurity and Critical Infrastructure. The Palgrave Handbook of Managing Continuous Business Transformation, 335-352.

Peraturan

Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Peraturan Menteri Energi dan Sumber Daya Mineral RI Nomor 48 Tahun 2018 tentang Penetapan Objek Vital Nasional Bidang Energi dan Sumber Daya Mineral.

Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Peraturan Presiden Republik Indonesia No. 133 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Peraturan Presiden Nomor 73 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Nomor 90 Tahun 2012 tentang Badan Intelijen Negara.

Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2003 tentang Badan Usaha Milik Negara.

Undang-Undang Republik Indonesia Nomor 30 Tahun 2009 tentang Ketenagalistrikan.

Undang-Undang Republik Indonesia Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.

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