KEBIJAKAN *CYBER DEFEND* INDONESIA DALAM RANGKA MENANGANI *INTERNATIONAL CYBER THREATS*

Mohammad Makbul[1], Mahsun Ismail[2], Nur Hidayat[3], Sri Sulastri[4]

[1]Fakultas Sosial dan Ilmu Politik Universitas Jenderal Soedirman

[2,3,4]Dosen Fakultas Hukum Universitas Madura

Jl. Profesor DR. HR Boenyamin No.708 Kabupaten Banyumas

makbulisme@gmail.com

Abstrak

Semakin berkembangnya teknologi informasi melahirkan fenomena baru yang disebut dengan ancaman dunia siber *(Cyber Threats)* yang dapat mengganggu stabilitas suatu negara baik negara yang memiliki index pertahanan siber yang rendah maupun tinggi. *Cyber Threat* merupakan tindakan kejahatan yang dilakukan oleh seseorang atau individu dengan memanfaatkan kelemahan dari sistem teknologi. Pemerintah dalam skala global dituntut untuk membangun ekosistem pertahanan siber *(Cyber Defend)* yang terstruktur. Indonesia sampai saat ini masih belum memiliki undang-undang pertahanan siber sehingga penanganan kasus kejahatan siber masih menggunakan kebijakan alternatif. Model analisis dalam penelitian ini menggunakan model penelitian kualitatif-deskriptif. langkah yang harus dilakukan pemerintah adalah dengan melakukan percepatan dalam pengesahan terhadap undang-undang siber, membangun komunikasi baik dengan negara-negara yang memiliki pertahanan siber yang kuat serta memberdayakan masyarakat agar memiliki *Cyber Awareness*

Kata kunci: Pertahanan Siber, Ancaman Dunia Siber

Abstract

The development of information technology has given birth to a new phenomenon called cyber threats which can disrupt the stability of a country, whether it is a country with a low or high cyber defense index. Cyber Threat is a crime committed by a person or individuals by exploiting the weaknesses of the technological system. Governments on a global scale are required to build a structured cyber defense ecosystem. Until now, Indonesia still does not have a cyber defense law so that the handling of cybercrime cases still uses alternative policies. The analysis model in this study uses a qualitative-descriptive research model. The steps that the government must take are accelerating the ratification of cyber laws, building good communication with countries that have strong cyber defenses and empowering people to have cyber awareness.

Keyword: *Cyber Defend, Cyber Threats*

Pendahuluan

Perkembangan teknologi informasi saat ini sangat mempengaruhi perkembangan setiap negara dalam segala sektor. Aktivitas hubungan internasional saat ini mulai menghadirkan kecanggihan teknologi informasi sebagai media penghubung antara negara satu dengan negara lain. Cepatnya perkembangan teknologi informasi membuat pergeseran yang sangat signifikan terhadap pertahanan sebuah negara. Pada saat ini ancaman dalam bidang pertahanan sebuah negara tidak lagi hanya bersifat fisik, hadirnya teknologi informasi menghadirkan ancaman baru yang biasa dikenal sebagai ancaman siber. Kejahatan dunia maya atau *cybercrime* dilakukan oleh

seseorang yang memiliki kemampuan dalam bidang *Hacking* melalui berbagai cara yang salah satunya adalah sabotase siber/*Cyber Sabotage.*[1]

Pada umumnya serangan *cyber* yang dilakukan pada suatu negara memiliki berbagai tujuan diantaranya adalah mempengaruhi ekonomi negara tersebut agar mengalami keterlambatan ekonomi dan bertujuan untuk mengambil data atau informasi penting guna mengancam negara tersebut bahkan dalam beberapa kasus data atau informasi yang didapat dijual-belikan kepada negara atau organisasi lewat *Dark Web.* Menurut Maurer & Nelson (2021) menyatakan bahwa actor yang telibat dari serangan siber terutama dalam lembaga keuangan tidak hanya dilakukan oleh pribadi atau kelompok semata, tetapi tidak jarang dalam beberapa kasus Tindakan penyerangan dilakukan atau didukung oleh negara atau kelompok tertentu yang memiliki kepentingan.[2]

Menurut *International Monetary Fund (IMF)* terdapat beberapa aktor dibalik serangan siber dunia. Pertama, warga negara atau grup yang disponsori negara *(Nation-state or state sponsored groups)* yang dilakukan atas dasar geopolitik atau ideologi, tujuannya untuk menciptakan disrupsi, destruksi, dan keuntungan finansial (*financial gain).* Kedua, *Cybercriminal's* yang dilakukan hanya untuk mendapatkan *enrichment* serta bertujuan untuk melakukan pencurian *(Theft)* dan *financial gain.* Ketiga, grup teroris, *hacktivist, dan Insider threats* serangan siber dilakukan dengan motivasi ideologi dan ketidakpuasan *(discontent),* kelompok ketiga ini memiliki tujuan untuk melakukan pengrusakan atau disrupsi.

Salah satu negara yang pernah terkena *cybercrime* adalah Australia. Pada saat itu alasan Autralia mendapat serangan karena penggunaan teknologi menjadi kemudi dalam menggerakkan ekonomi Autralia. Dampak serangan tersebut membuat Autralia mengalami kerugian ekonomi dan hilangnya data-data penting milik pemerintah. Menanggapi hal tersebut pemerintah Autralia pada tahun 2016 mulai memperbarui kebijakan *Cyber Security* nya. Berbagai inisiatif dilakukan

[1] Anjani Firman, F. (2018). *Kebijakan Pertahanan Cyber Estonia Dalam Merespon Tindakan Cyber Sabotage Oleh Rusia Kepada Estonia*. Universitas Komputer Indonesia

[2] Maurer, T., & Nelson, A. (2021). The global cyber threat. *Finance \& Development, February 2020*, 24–27

diantaranya mendirikan badan keamanan siber serta menjalin hubungan regional dan internasional sebagai upaya prefentif dalam menangkal serangan siber yang mungkin akan kembali terjadi.[3]

Indonesia pada tahun 2013 pernah menggeser Cina sebagai negara yang paling banyak terkena serangan siber. Menurut data Kementrian Komunikasi dan Informasi (Kominfo) pada tahun 2010-2013 kasus serangan siber telah mencapai 36,7 juta insiden. data tersebut terus mengalami kenaikan setiap tahun. Pada saat pandemic virus Covid-19 dimana sebagian besar masyarakat mulai menggunakan akses internet sebagai media untuk melakukan aktivitas akibat dampak dari pembatasan kegiatan masyarakat. Hal tersebut mengakibatnya lonjakan kasus serangan siber meningkat pesat. Menurut laporan Pusat Operasi Keamanan Siber Nasional (Pusopkamsinas) BSSN pada sepanjang tahun 2020 tercatat sebanyak 495,3 juta kasus serangan *cyber* dengan tujuan mencuri data dan infomasi melalui *Malware.*

Pada dasarnya yang menjadi target utama para penjahat *cyber* adalah lembaga keuangan atau Bank yang ada di negara sasaran. Banyak data pribadi dan data keuangan masyarakat yang dengan sangat mudah untuk dibobol. Menurut Wicaksana (2020) menyatakan bahwa mudahnya data keuangan masyarakat diretas adalah lemahnya *Security Awareness* masyarakat dalam melindungi data pribadinya terutama data dalam bidang keuangan. Sehingga hal tersebut memperluas kesempatan penjahat siber dalam melakukan aksinya. Bahkan Inggris Raya dan Malaysia yang sudah memiliki pertahan siber yang kuat masih belum mampu membendung intensitas serangan siber terutama pada saat pandemic Covid-19. Rendahnya *Security Awareness* masyarakat merupakan dampak dari aktivitas masyarakat dalam mengkases internet sebagai media mempermudah pekerjaan.[4]

Kasus serangan siber paling banyak adalah dalam bidang keamanan data pribadi masyatakat. Hal ini diakibatkan karena masih lemahnya regulasi pemerintah untuk melindungi hal tersebut. Sampai saat ini kebijakan pertahanan siber di Indonesia masih belum ada, pemerintah

[3] Putro, Z. P. P. (2022). *Perumusan Kebijakan Pertahanan Siber Rusia Dalam Menghadapi Ancaman Siber Global Pasca Serangan Siber Rusia Terhadap Estonia (Estonian Cyber Attack 2007) Melalui Rezim Tallinn Manual*. Universitas Pembangunan Nasional Veteran Jakarta.

[4] Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *22*(2), 143–158

masih menggunakan kebijakan alternatif yang tentunya kebijakan tersebut tidak mampu untuk mengkover banyaknya insiden kejahatan siber. Saat ini pemerintah hanya mengguakan UU KUHP, UU ITE, UU Perbankan, UU Telekomunikasi, UU Perlidungan Konsumen, dll. Tentunya kebijakan tersebut tidak spesifik dalam menangani sulitnya kasus kejahatan siber, sehingga dalam menangani kasus kejahatan siber akan cenderung lamban.

Sampai saat ini pemerintah indonesia masih belum membuat kebijakan pertahanan siber atau *cyber defend policy*. Padahal jika dilihat dari atas *(take the view from above)* hanya Indonesia yang dari keanggotaan ASEAN yang masih belum memiliki kebijakan pertahanan siber. padahal pemerintah sebagai pelindung public memiliki kewajiban dalam membangun, memelihara data-data public baik data pribadi maupun data keuangan milik masyarakat serta melindungi privasi masyarakat dari ancaman kejahatan siber baik ancaman regional maupun ancaman internasional.

METODE

Model analisis dalam penelitian ini menggunakan model penelitian kualitatif-deskriptif. Model penelitian kualitatif merupakan strategi penelitian dengan melakukan pendekatan terhadap data, partisipasi, serta pengalaman. Alat penelitian yang digunakan dalam penelitian ini adalah study pustaka *(Library Studies)* yaitu mendalami dan mempelajari berbagai literatur yang berhubungan dengan kebijakan pertahanan siber *(Cyber Defend)* terhadap ancaman kejahatan siber internasional.

Global Policy dan Ancaman Siber Internasional Terhadap Suatu Negara

Konsep global policy cakupan masalahnya tidak lagi mengenal batas. Adanya global policy merupakan gerakan penyatuan pemimpin-pemimpin politik dalam bekerjasama untuk menyelesaikan masalah-masalah di negara yang bersangkutan. Gerakan ini biasanya melibatkan lembaga-lembaga internasional misalnya PBB, Mahkamah Internasinal, serta bank dunia. Meskipun sistem hubungan politik global saat ini tidak terintegrasi, hubungan antara rezim pemerintahan global yang berbeda tetap penting, dan tidak ada bentuk organisasi yang dominan

dalam sistem ini. wajar secara birokrasi. Artinya, memiliki aturan, terikat oleh hukum, dan wajar. Model ini ada di semua sistem politik kontemporer dan menyediakan kerangka kerja untuk transisi dari kedaulatan klasik ke kedaulatan internasional liberal. Inilah yang disebut oleh David Held sebagai Rezim Kedaulatan Kedua.

Untuk mencapai perlindungan global yang lebih efektif terutama dalam sector sistem keuangan terhadap ancaman dunia maya, Carnegie Endowment di *International Peace* merilis sebuah laporan pada November 2020 berjudul "*International Strategy to Better Protect the Global Financial System against Cyber Threats*." Dikembangkan bekerja sama dengan Forum Ekonomi Dunia, laporan tersebut merekomendasikan tindakan spesifik untuk mengurangi fragmentasi dengan mendorong lebih banyak kolaborasi, baik secara internasional dan di antara lembaga pemerintah, perusahaan keuangan, dan perusahaan teknologi.[5]

Dalam konteks *Cyber Defend* PBB sebagai otoritas tertinggi lembaga internasional mengeluarkan beberapa kebijakan dalam hal penanganan *Cybercrime* (kejahatan dunia maya). Resolusi Kongres PBB VIII/1990 mengenai "*Computer-related crime*" mengajukan beberapa kebijakan antara lain:

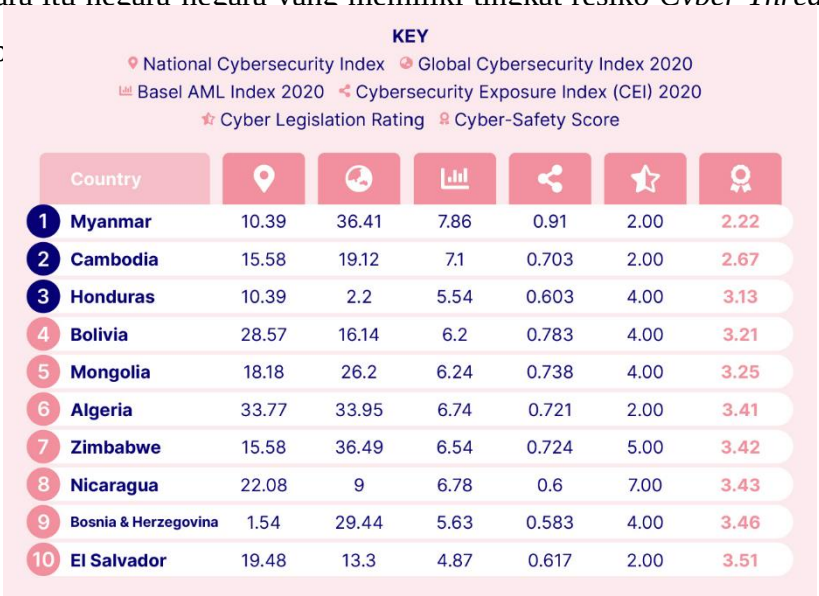
- Melakukan modernisasi hukum pidana materiil dan hukum acara pidana;
- Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
- Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan, dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer;
- Mengimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cybercrime*.
- Memperluas *"rule of ethics*" dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika.[6]

Dalam ranah global ancaman *Cyber Threat* masih menghantui individu, kelompok, bahkan pemerintahan global secara keseluruhan. *Center for Strategic & International Studies* (CSIS)

[5] Maurer, T., & Nelson, A. (2021). The global cyber threat. *Finance \& Development*, *February 2020*, 24–27.
[6] Bahiej, A., & Tahir, A. T. A. (2012). Kebijakan Penanggulangan Kejahatan Studi Terhadap Resolusi Kongres PBB VIII/1990 Tentang Computer-Related Crime. *Asy-Syir'ah: Jurnal Ilmu Syari'ah Dan Hukum*, *46*(2)

melacak serangan siber terhadap badan pemerintah, lembaga pertahanan, dan perusahaan teknologi tinggi, serta kejahatan ekonomi mengakibatkan kerugian setidaknya $1 juta (satu juta dollar). Data CSIS menunjukkan bahwa 105 dari serangan ini terjadi pada 2019, dan statistic mencatat serangan siber meningkat 400% dari level mulai dari tahun 2009.[7]

Sementara itu negara-negara yang memiliki tingkat resiko *Cyber Threat* tertinggi terlihat dalam gambar b



Country						
1 Myanmar	10.39	36.41	7.86	0.91	2.00	2.22
2 Cambodia	15.58	19.12	7.1	0.703	2.00	2.67
3 Honduras	10.39	2.2	5.54	0.603	4.00	3.13
4 Bolivia	28.57	16.14	6.2	0.783	4.00	3.21
5 Mongolia	18.18	26.2	6.24	0.738	4.00	3.25
6 Algeria	33.77	33.95	6.74	0.721	2.00	3.41
7 Zimbabwe	15.58	36.49	6.54	0.724	5.00	3.42
8 Nicaragua	22.08	9	6.78	0.6	7.00	3.43
9 Bosnia & Herzegovina	1.54	29.44	5.63	0.583	4.00	3.46
10 El Salvador	19.48	13.3	4.87	0.617	2.00	3.51

Gambar 1: Negra-negara dengan resiko *Cyber Threat* tertinggi
Sumber: *https://seon.io/resources/global-cybercrime-report/*

Berdasarkan gambar tersebut terlihat bahwa Myanmar, Kamboja, dan Honduras menjadi negara dalam urutan tiga besar sebagai negara yang memiliki resiko serangan siber *(Cyber Threat)* tertinggi. Myanmar adalah negara terburuk untuk keamanan internet *(Internet Safety)*, dengan skor hanya 2,22 pada Indeks Keamanan Dunia Maya. Myanmar mendapat skor buruk secara keseluruhan, terutama dalam hal undang-undang, karena hampir tidak ada yang diberlakukan untuk menghalangi penjahat dunia maya. Di tempat kedua adalah Kamboja, yang memperoleh Skor Keamanan Cyber 2,67 secara keseluruhan. Negara Asia Tenggara lainnya dengan keamanan internet yang buruk, Kamboja memiliki kinerja yang sedikit lebih baik daripada Myanmar dalam

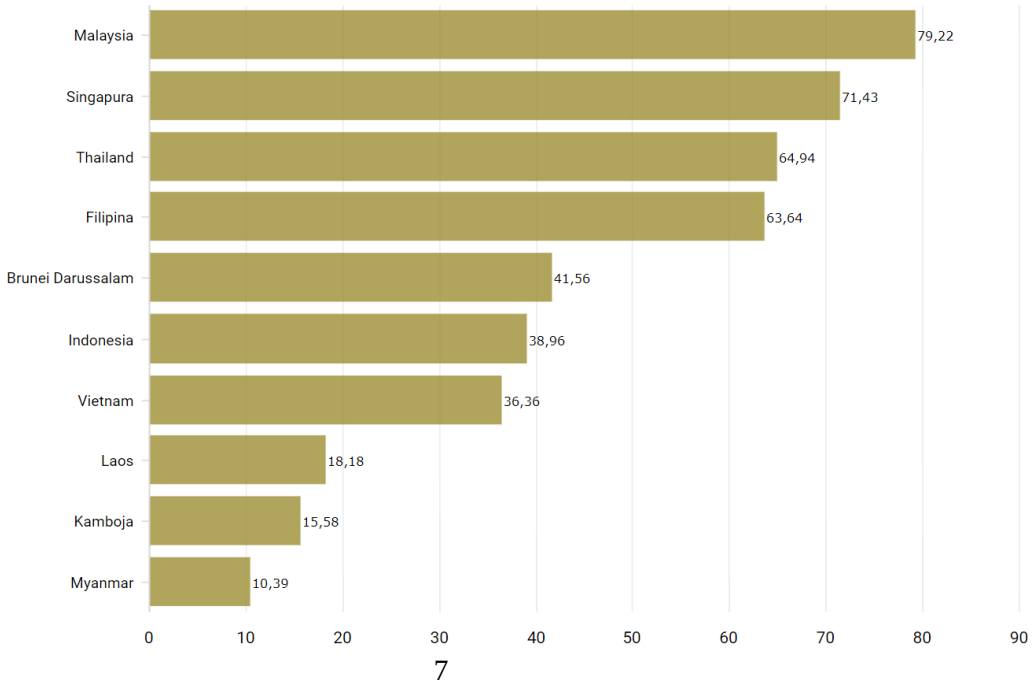
[7] Varga, G. (2020). *Global Cybercrime Report: Which Countries Are Most at Risk?* Ttps://Seon.Io. ttps://seon.io/resources/global-cybercrime-report/

setiap metrik selain Indeks Keamanan Siber Global. Honduras menempati posisi ketiga dengan skor 3,13. Negara Amerika Tengah ini mendapat skor paling rendah pada *Global Cybersecurity Index* dari negara manapun di Amerika Tengah, sementara berkinerja buruk di semua bidang lainnya. Namun, Honduras tampil dua kali lebih baik dari Myanmar dan Kamboja dalam hal undang-undang anti-kejahatan dunia maya.

Ancaman serangan siber dalam skala internasional tidak hanya menjadi ancaman besar bagi negara-negara yang memiliki index keamanan siber paling rendah, akan tetapi negara-negara besar pun seperti Amerika Serikat pun tidak luput menjadi sasaran kejahatan siber. Ancaman siber *(Cyber Threats)* telah menjadi masalah utama bagi bisnis di AS. Aktivitas seperti menggunakan *ransomware* serangan yang dilakukan bertujuan untuk memeras uang dari organisasi atau membocorkan informasi pribadi pelanggan dan karyawan. Pada tahun 2019, diperkirakan bahwa penipuan merugikan ekonomi global sebesar $5,127 triliun per tahun, tanpa ada yang menunjukkan bahwa angka ini tidak akan terus meningkat.[8]

Langkah Kebijakan Indonesia Dalam Merespon Ancaman siber *(Cyber Threats)*

Jika dibandingkan dengan negara-negara lain dikawasan Asia, menurut data *Nasional Cyber Security Index* (NCSI) Indonesia menempati urutan ke-6:



[8] Cavelty, M. I
debate. *Journa*

Gambar 2: persentase keamanan siber di ASIA
Sumber: *https://databoks.katadata.co.id*

Berdasarkan gambar tersebut membuktikan bahwa Indonesia sebagai negara yang secara statistik berada diatas Filipina dan Brunei Darussalam, dalam konteks keamanan siber masih kalah.

Sampai saat ini Indoensia belum mempunyai kebijakan yang secara spesifik mengatur tentang *Cyber Defend* atau pertahanan siber, dan masih menggunakan kebijakan alternatif yang tentunya belum efektif dalam menangkal *Cyber Threat.* Kebijakan yang digunakan Indonesia saat ini adalah UU KUHP, UU ITE, UU Perbankan, UU Telekomunikasi, UU Perlidungan Konsumen, UU kependudukan, UU Hak Asasi Manusia, UU Administrasi Kependudukan, UU Keterbukaan Informasi Publik, UU Kesehatan, PP No. 71 Tahun 2019 dan Permen Kominfo No. 20 Tahun 2016. Regulasi ini tidak besifat spesifik sehingga pemerintah kesulitan dalam mengambil Tindakan prefentif maupaun tindakan represif guna menangkal *Cyber Threat.*

Pada dasarnya munculnya *Cybercrime* melalui penggunaan internet dengan cara melakukan *Cyber-attack* dengan menggunakan virus yang dikirim melalui computer yang menggunakan infrastruktur sistem telekomunikasi. Maka berdasarkan data diatas maka perlu dilakukan langkah-langkah berikut:

a) Diperlukan percepatan dalam pembuatan peraturan perundang-undangan tentang pertahanan siber *(Cyber Defend)*

Solusi guna menghadapi ancaman serangan siber dalam sektor publik, pemerintahan dan swasta salah satunya adalah memiliki undang-undang yang menangani berbagai jenis serangan siber baik serangan dari dalam maupun serangan internasional. Undang-undang keamanan siber harus melindungi infrastruktur penting dari serangan siber, dan harus diatur oleh undang-undang terpisah tentang keamanan siber. Koordinasi ini harus dilakukan dengan cara yang sejalan dengan undang-undang lainnya. Indonesia seharusnya memiliki platform tersendiri yang dapat membantu koordinasi kerja sama lintas sektor terkait isu siber, baik itu di sektor pemerintah, swasta, maupun publik. Kejahatan siber adalah masalah yang harus ditangani dalam peraturan yang mencakup jenis

kejahatan siber tertentu dan mampu untuk menanganinya. Ini termasuk aktivitas seperti peretasan dan penipuan online. Ini juga melibatkan kerja sama dengan penegak hukum di negara lain untuk memerangi kejahatan ini.

b) Perlu dibangun sebuah ekosistem yang mampu menciptakan keamanan siber

Di era normal baru, serangan siber menjadi semakin kompleks dan meluas. Artinya, pemerintah perlu bekerja sama untuk berkoordinasi dan bersinergi antara berbagai elemen penanganan siber, seperti *Cybercrime* Polri, Kementerian Komunikasi dan Informatika, Badan Intelijen Negara (BIN), dan elemen keamanan siber di berbagai sektor industri. Masih ada ego sektoral yang ada di Indonesia dalam penanganan siber, sehingga kasus penipuan online dan pembobolan data pribadi masih terjadi. Seharusnya Indonesia harus belajar dari Malaysia yang sudah membangun pusat koordinasi dan komando siber nasional (NC4). NC4 yang dibangun Malaysia memiliki berbagai unit yang menangani *Critical National Information Infrastructure* (CNNI). CNNI memiliki tanggung jawab untuk melakukan pelaporan, menyebarkan informasi, serta memiliki wewenang untuk mengambil tindakan untuk melindungi sistem TIK yang bersifat vital. Unsur-unsur yang terdapat di CNNI terdiri dari badan publik dan swasta. Selain itu Indonesia juga dapat belajar dari Inggris Raya serta negara-negara Eropa lainnya dengan membangun organisasi independen non-profit, di Inggris Raya organisasi ini diberi nama *Information Sharing and Analysis Centers* (ISACs).[9]

c) Meningkatkan kapasitas SDM dan *Security Awareness* tentang keamanan siber

Dalam hal ini pemerintah melalui BSSN, Kementerian Kominfo, Bank Indonesia, serta lembaga-lembaga pemerintah terkait harus melakukan literasi dan sosialisasi kepada masyarakat baik secara langsung ataupun melalui *webinar* atau iklan layanan masyarakat lainnya guna meningkatkan *security awareness* masyarakat terutama dalam sektor keuangan, sehingga masyarakat dapat secara mandiri melindungi data-data pribadi pada tingkat awal. Selain itu BSSN diharuskan membangun komunikasi, koordinasi, memfasilitasi, serta memberikan pendampingan kepada berbagai perusahaan dalam segala sektor dalam rangka meningkatkan standar keamanan sistem informasi dan jaringan mereka. Pemerintah juga dapat melibatkan sumberdaya manusia

[9] Europa, E. (2022). *Information Sharing and Analysis Centers (ISACs)*. Www.Enisa.Europa.Eu. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

yang dalam hal ini adalah generasi millennial dengan memberikan berbagai pelatihan terstruktur dalam bidang keamanan siber.

Penutup

Ancaman dunia siber *(Cyber Threat)* saat ini sudah menjadi ancaman global, tidak melihat siapa negara apapun baik yang memiliki pertahan siber *(Cyber Defend)* yang kuat atau tidak. serangan siber biasanya dilakukan oleh individua tau kelompok yang memiliki tujuan dalam mengacaukan sistem suatu negara baik ekonomi dan sosial. Indonesia sendiri belum memiliki kebijakan yang komprehensif dalam menanggapi serangan siber, sehingga Indonesia cenderung akan menjadi sasaran empuk para pelaku kejahatan siber. Tentunya ini merupakan sebuah masalah public yang harus diurus oleh negara. Untuk itu langkah yang harus dilakukan pemerintah adalah dengan melakukan percepatan dalam pengesahan terhadap undang-undang siber, membangun komunikasi baik dengan negara-negara yang memiliki pertahanan siber yang kuat misalnya Canada, jerman, dan amerika serikat, dan yang terakhir memberdayakan masyarakat agar memiliki *Cyber Awareness* sehingga membantu pemerintah dalam melindungi data pribadinya.

Daftar Pustaka

Anjani Firman, F. (2018). *Kebijakan Pertahanan Cyber Estonia Dalam Merespon Tindakan Cyber Sabotage Oleh Rusia Kepada Estonia*. Universitas Komputer Indonesia.

Bahiej, A., & Tahir, A. T. A. (2012). Kebijakan Penanggulangan Kejahatan Studi Terhadap Resolusi Kongres PBB VIII/1990 Tentang Computer-Related Crime. *Asy-Syir'ah: Jurnal Ilmu Syari'ah Dan Hukum*, *46*(2).

Cavelty, M. D. (2008). Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*, *4*(1), 19–36.

Europa, E. (2022). *Information Sharing and Analysis Centers (ISACs)*. Www.Enisa.Europa.Eu. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

Maurer, T., & Nelson, A. (2021). The global cyber threat. *Finance \& Development*, *February 2020*, 24–27.

Putro, Z. P. P. (2022). *Perumusan Kebijakan Pertahanan Siber Rusia Dalam Menghadapi Ancaman Siber Global Pasca Serangan Siber Rusia Terhadap Estonia (Estonian Cyber Attack 2007) Melalui Rezim Tallinn Manual*. Universitas Pembangunan Nasional Veteran Jakarta.

Varga, G. (2020). *Global Cybercrime Report: Which Countries Are Most at Risk?* Ttps://Seon.Io. ttps://seon.io/resources/global-cybercrime-report/

Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *22*(2), 143–158.