e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 9 No 6 Tahun 2022 Hal. : 2094-2103

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

STRATEGI PENGEMBANGAN KAPABILITAS SIBER PERTAHANAN UNTUK MENGHADAPI PEPERANGAN SIBER (STUDI KASUS PADA PUSHANSIBER KEMHAN RI 2020-2021)

Rachmanu Krisnata, Agus H.S. Reksoprodjo, Surryanto Djoko Waluyo

Prodi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan RI

Abstrak

Kemajuan teknologi komunikasi dan informasi serta perkembangan globalisasi telah membawa dampak perubahan di dunia mendorong banyak negara tidak lagi menggunakan cara perang tradisional dan konvensional. Peningkatan terhadap ancaman perang siber berdampak terhadap terjadinya cyber warfare yang mencakup berbagai aspek seperti ideologi, politik, ekonomi, sosial, budaya dan pertahanan nasional. Kemhan memiliki kewajiban mengambil langkah-langkah penting terkait dengan pertahanan siber, baik di dalam lingkungannya sendiri maupun dalam rangka mendukung pertahanan siber nasional. Permasalahan penelitian adalah tentang penanganan peperangan siber dan strategi pengembangan kapabilitas siber pertahanan di Pushansiber. Tujuan penelitian untuk menganalisis penanganan peperangan siber dan strategi pengembangan kapasitas siber pertahanan di Pushansiber Kemhan guna mendukung sistem pertahanan siber nasional. Penelitian dilakukan dengan menggunakan metode kualitatif dengan desain penelitian studi kasus. Data didapatkan dari narasumber secara purposive sampling berdasarkan kepakarannya, terdiri dari pakar di bidang teknologi informatika, pejabat, dan para Analis, serta Operator Siberhan di lingkungan Pushansiber Bainstrahan Kemhan. Hasil penelitian menunjukkan bahwa kapabilitas siber dan pertahanan siber berpengaruh terhadap penanganan peperangan siber. Dimana kapabilitas siber meliputi aset, kemampuan dan proses persiapan. Sedangkan pertahanan siber meliputi kecepatan operasional, inisiatif dan kolaborasi. Pengembangan kapabilitas siber sangat diperlukan untuk mendukung pertahanan siber nasional, untuk itu diperlukan strategi pengembangan kapabilitas siber pertahanan. Kesimpulan bahwa penanganan peperangan siber di Pushansiber belum dapat dijalankan secara maksimal sehingga Pushansiber melakukan strategi pengembangan kapabilitas siber pertahanan dengan pengembangan pada sisi people, process dan technology.

Kata Kunci: Strategi, Kapabilitas siber, Pertahanan siber.

*Correspondence Address : krisnata30@gmail.com
DOI : 10.31604/jips.v9i6.2022.2094-2103

PENDAHULUAN

Kemajuan teknologi komunikasi dan informasi di era perkembangan globalisasi mendorong banyak negara tidak lagi menggunakan cara perang tradisional dan konvensional. Persaingan dan peperangan menjadi semakin kabur dan tanpa batas. Peperangan dan konflik yang terjadi saat ini lebih didominasi kekuatan nirmiliter yang juga dilakukan oleh aktor non-negara (*non-state actor*). Ancaman di ruang siber (*cyberspace*) didominasi oleh aktor non-negara seperti individu *hacker*, komunitas *hacker*, *Non-Government Organization* (NGO), terorisme, kelompok kejahatan terorganisir (*organized criminal groups*) dan sektor swasta seperti *internet companies and carries, security companies* juga dapat mengancam pertahanan dan kedaulatan Negara (Pearlman & Cunningham, 2012).

Peningkatan terhadap ancaman perang siber yang dilakukan baik oleh negara ataupun aktor non-negara (*non-state actor*) berdampak terhadap terjadinya *cyber warfare* atau gangguan *cyber* (*cyber violence*). Berdasarkan laporan *Financial Services Information Sharing and Analysis Center* (FS-ISAC), Indonesia termasuk dalam daftar 10 negara di dunia yang rentan kejahatan teknologi informasi di dunia maya atau *cyber crime*. Laporan FS-ISAC itu dirilis pada kuartal II-2020, di mana Indonesia menduduki peringkat ke-9.

Selama wabah covid19, dipastikan angka serangan siber terhadap masyarakat akan melonjak tajam sehingga membutuhkan antisipasi yang segera mungkin. Lebih dari pada sekadar perlindungan dan langkah-langkah pencegahan yang mengandalkan pada kerja Badan Siber Nasional dan Kominfo, upaya untuk melindungi dan menjaga pertahanan siber tentu juga tergantung pada kapabilitas dan infomasi dari berbagai pihak (Sugihartati, 2020). Berdasarkan data *Cybersecurity Threatscape* Q1 2020 menunjukkan bahwa terjadi peningkatan jumlah serangan siber di Indonesia sebesar 22,5% pada kuartal pertama 2020 (Q1 2020) jika dibandingkan dengan kuartal yang sama tahun 2019.

Perang siber bukanlah suatu kabar bohong semata, namun sudah hadir dan mendatangkan sebuah ancaman terhadap keutuhan NKRI. Indonesia telah beberapa kali mengalami perang siber yaitu (Manthovani, 2006), pertama, tahun 1998 melakukan perang siber dengan negara lain terkait masalah sosial politik yang terjadi ketika kerusuhan rasial. Indonesia berperang di ruang siber dengan para *hacker* Taiwan dan China.

Kedua, pada tahun 1999 adanya kerusuhan di dunia maya antara Indonesia dan Portugal terkait masalah Timor Timur. Ketiga, pada tanggal 6 Agustus 2010, produsen *Antivirus Norton* (*Symantec*), mengumumkan bahwa Indonesia berada di peringkat kedua setelah Iran di antara 10 negara yang mengalami serangan worm Stuxnet yang diduga dilakukan oleh Amerika dan Israel sebagai penentang utama program Nuklir Iran. Keempat, perang siber antara Indonesia-Malaysia, para *Hacker* saling menyusup antara kedua negara dalam perang siber tersebut. Kelima, pada kasus penyadapan komunikasi pribadi Presiden Indonesia (Susilo Bambang Yudoyono) dan beberapa pejabat tinggi negara yang dilakukan Australia berdasarkan dokumen yang dibocorkan oleh Edward Snowden mantan kontraktor *National Security Agency* (NSA) dari Amerika.

Menurut laporan *Insikt Group* (2021), divisi riset ancaman perusahaan keamanan siber *Recorded Future*, pada April 2021 melaporkan setidaknya 10 kementerian dan lembaga Indonesia diretas oleh *Mustang Panda*, sekelompok peretas China. *Insikt Group* juga menemukan *PlugX*, *malware Mustang*

Panda, di dalam jaringan pemerintah Indonesia. Pembobolan diduga terjadi sejak Maret 2021. Pakar keamanan siber menganalisis bahwa *Mustang Panda* menggunakan *Ransomware Thanos*.

Serangan siber siber diatas, tidak hanya merugikan individu, masyarakat, melainkan juga pada negara, sehingga berdampak pada terbongkarnya data-data penting negara, data strategis maupun strategi keamanan dan pertahanan negara yang dapat menimbulkan terganggunya ekonomi dan stabilitas negara. Berdasarkan laporan *monitoring* yang dikeluarkan oleh Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) BSSN, mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Pada bulan Januari terpantau 25.224.811 serangan dan pada bulan Februari terjadi 29.188.645 serangan. Pada bulan Maret tercatat 26.423.989 serangan dan pada bulan April sampai dengan tanggal 12 April 2020 telah tercatat 7.576.851 serangan. Jumlah serangan mengalami puncaknya pada tanggal 12 Maret 2020 yang mencapai 3.344.470 serangan.

Ancaman terhadap sistem pertahanan siber tidak lagi dilihat pada masalah teknis keamanan komputer, tetapi mencakup berbagai aspek seperti ideologi, politik, ekonomi, sosial, budaya dan pertahanan nasional. Pada tingkat internasional, baik negara maupun masyarakat internasional harus mengembangkan strategi kooperatif dalam menanggapi perkembangan di dunia siber yang meluas secara internasional, misalnya dengan membuat norma internasional yang menyangkut permasalahan dan ancaman siber (Chotimah, 2019). Strategi implementasi perlindungan terhadap sarana dan prasarana infrastruktur negara dalam pemanfaatan teknologi informatika harus meliputi *Information Security Management System* (ISMS) yaitu suatu pendekatan yang sistematis untuk mengelola dan mengamankan informasi yang bersifat rahasia dan sangat penting dalam organisasi, meliputi aspek Sumber Daya Manusia (*people*), prosedur standar (*process*), dan Sistem Teknologi Informasinya (*technology*).

Penerapan pertahanan siber merupakan prioritas bagi negara dan semua instansi terkait. Kemhan dan TNI memiliki kewajiban mengambil langkah-langkah penting terkait dengan pertahanan siber, baik di dalam lingkungannya sendiri maupun dalam rangka mendukung pertahanan siber nasional. Hal ini sesuai tugas pokok Pertahanan Siber yaitu untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan negara. Mengingat luasnya bidang pertahanan siber, guna membangun *sense of defence* dalam bidang keamanan siber di sektor pertahanan telah dikeluarkan Permenhan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Kementerian Pertahanan Republik Indonesia (Kemhan RI) dalam menjaminan keamanan pertahanan siber, pada tahun 2017 membentuk Pusat Pertahahan Siber (Pushansiber) yang mempunyai tugas melaksanakan tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber (Permenhan Nomor 14 tahun 2019 pasal 1176).

Pembentukan Pushansiber terbilang masih sangat baru. Bila melihat pendekatan yang sistematis untuk mengelola dan mengamankan informasi yang bersifat rahasia dan sangat penting dalam organisasi, meliputi aspek *people, process* dan *technology*, Pushansiber telah memiliki ketiga aspek tersebut, tetapi dengan segala keterbatasan dan permasalahannya. Pada aspek Sumber Daya Manusia (*people*), Pushansiber belum dapat memenuhi kualitas dan kuantitas personelnya. Kemudian untuk aspek prosedur standar (*process*),

regulasi yang digunakan oleh Pushansiber adalah Permenhan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan dan Permenhan Nomor 14 Tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan. Sedangkan untuk aspek Sistem Teknologi Informasinya (*technology*), Pushansiber belum menjalankan teknologi ISO 27001. Pertahanan siber merupakan bidang yang sangat khusus di mana ketrampilan dan keahlian harus terus dipelihara dan dikembangkan untuk memastikan pertahanan yang efektif terhadap aset, fasilitas dan infrastruktur penting negara. Teknik-teknik yang digunakan oleh penyerang siber yang selalu berubah secara cepat, sehingga ketika terjadi suatu serangan, sistem pertahanan siber harus siap untuk segera merespon dengan cepat dan tepat terhadap serangan yang terjadi.

Untuk dapat menjalankan tugas dalam hal pertahanan siber di lingkungan Kemhan maupun dalam rangka mendukung sistem siber nasional, maka Pushansiber perlu mengembangkan kapabilitas dari tiga aspek yaitu *people*, *procces*, dan *technology*. Bagaimana personil yang dimiliki, proses yang berlangsung saat ini dan teknologi yang digunakan. Melihat berbagai kasus serangan siber yang terjadi beberapa tahun terakhir menurut hasil survei, penelitian maupun pantauan beberapa lembaga terkait, menunjukkan Indonesia sangat rentan terhadap serangan siber yang menyerang berbagai kepentingan negara dan masyarakat, baik di bidang ekonomi, pemerintahan, pertahanan dan keamanan nasional, ditambah dengan permasalahan yang ada di Pushansiber dari aspek *people*, *procces* dan *technology*. Kemhan dalam hal ini Pushansiber terus berupaya meningkatkan kapabilitas pertahanan siber untuk menghadapi serangan siber guna mendukung sistem pertahanan siber nasional. Berdasarkan permasalahan diatas, maka pertanyaan penelitian yang perlu dijawab adalah bagaimana penanganan peperangan siber dan strategi pengembangan kapabilitas siber pertahanan di Pushansiber?

METODE PENELITIAN.

Metode penelitian yang digunakan dalam kegiatan penelitian ini yaitu dengan metode penelitian kualitatif dengan teknik pengumpulan data melalui studi pustaka dan wawancara mendalam dengan metode *purpossive sampling* kepada pakar di bidang teknologi informatika, pejabat, dan para Analis, serta Operator Siberhan Pushansiber Kemhan. Menurut Sugiyono (2018) pada metode penelitian kualitatif terdapat beberapa desain penelitian diantaranya adalah fenomenologi, *grounded theory*, studi kasus, etnografi dan penelitian tindakan. Desain penelitian sangat menentukan sebagai suatu strategi dalam mencapai tujuan penelitian. Dalam penelitian ini, peneliti menggunakan metode penelitian kualitatif dengan pendekatan studi kasus. Penelitian dilaksanakan di Pushansiber Kemhan yang berlokasi di Komplek Perkantoran Kemhan Pondok Labu Jakarta Selatan.

Adapun subyek dalam penelitian adalah informan yang mampu memberikan informasi mengenai "pengembangan kapabilitas siber pertahanan di Pushansiber Kemhan untuk menghadapi peperangan siber", dengan obyek penelitian adalah Penanganan peperangan siber dan strategi pengembangan kapabilitas siber pertahanan di Pushansiber.

HASIL DAN PEMBAHASAN.

Pusat Pertahanan Siber (Pushansiber) Badan Instalasi Strategis Pertahanan (Bainstrahan) Kementerian Pertahanan adalah salah satu sub satuan kerja di Kemhan yang disahkan dalam

Peraturan Menteri Pertahanan (Permenhan) RI Nomor 14 Tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan. Dalam Permenhan tersebut, Pushansiber merupakan unsur pelaksana tugas dan fungsi Bainstrahan Kemhan yang dipimpin oleh Kepala Pusat Pertahanan Siber (Kapushan Siber) yang bertugas melaksanakan tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber.

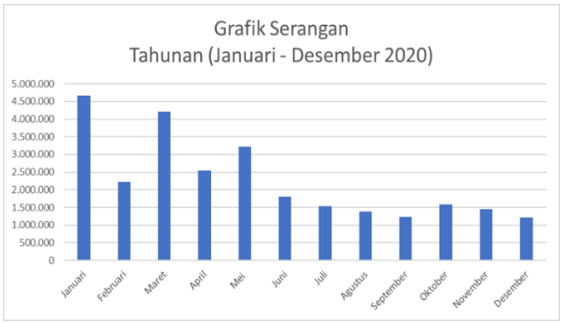
Data yang diperoleh saat melaksanakan penelitian di Pushansiber, peneliti representasikan dalam berbagai bentuk. Wawancara dengan beberapa pemangku kepentingan, peneliti catat dalam bentuk transkrip, sementara beberapa kejadian serangan siber dalam bentuk file elektronik. Kemudian informasi tentang sumber daya yang dimiliki baik pada sisi *people, process* dan *technology*, peneiliti peroleh baik dalam bentuk keterangan-keterangan hasil wawancara maupun dalam bentuk dokumen dan file elektronik. Selain itu peneliti juga memperoleh informasi tentang kondisi Pushansiber melalui dokumentasi dan studi pustaka.

Penanganan Peperangan Siber.

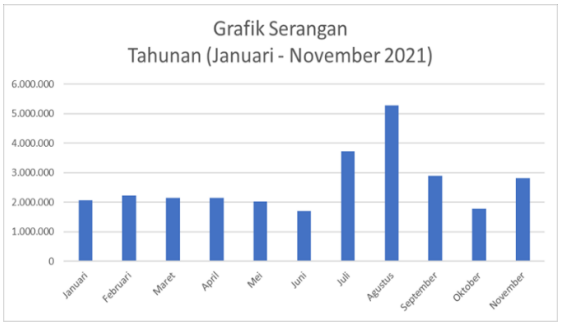
Keberadaan Pushansiber sebagai bagian dari Kementerian Pertahanan tidak dapat terlepas dari berbagai ancaman di bidang siber, baik itu kegiatan intelijen, *hackers*, kriminal, maupun penyalahgunaan teknologi. Ancaman yang menjadi suatu serangan dapat menjadi sebuah gangguan siber dan perang siber. Untuk memastikan adanya pertahanan siber yang kokoh dan handal, Pushansiber melakukan upaya-upaya dalam mencegah dan penanganan serangan

Sebagai upaya penanganan, Pushansiber memiliki sensor-sensor yang dipasang di tujuh titik yaitu Salemba, Cawang, Tugu Tani, Bintaro, Sentul, Merdeka Barat dan Pondok Labu. Tahun 2016 dipasang lagi sensor di tempat yang sama di tujuh titik dengan fungsi yang hampir sama hanya berbeda *Engine*-nya. Sejak 2016 sampai dengan tahun 2021 belum ada revitalisasi. Berarti sejak 2016 sudah 6 tahun belum ada revitalisasi.

Jika melihat tingkat serangan dan berbagai serangan yang terjadi di Pushansiber pada periode tahun 2020 dan 2021, maka diperlukan penanganan yang cepat dan tepat, sehingga dapat menghindari segala dampak kerugian baik materiil maupun non matriil. Tingkat serangan dapat dilihat seperti pada gambar dibawah ini:



Gambar 1. Serangan Siber tahun 2020.
Sumber: Pushansiber, 2020.



Gambar 2. Serangan Siber tahun 2021
Sumber: Pushansiber, 2021.

Seperti pada gambar 1, terlihat bahwa serangan yang terjadi setiap bulannya diatas 1 juta serangan. Sedangkan pada tahun 2021, terjadi peningkatan setiap bulannya. Dalam penanganan peperangan siber perlu diketahui kapabilitas dan pertahanan siber yang dimiliki oleh Pushansiber. Menurut Farzan Kolini dan Lech Janczewski (2015), kapabilitas siber

dikelompokkan dalam tiga kelompok yaitu aset, kemampuan dan proses persiapan. Terkait dengan meningkatnya ancaman siber yang semakin komplek, maka diperlukan kapabilitas siber yang kuat dan handal untuk dapat menangani serangan siber dan untuk menghindari kerugian-kerugian yang ditimbulkan baik non materiil maupun materiil.

Bila dibandingkan dengan tingkat serangan yang terjadi pada tahun 2020 dan 2021 dengan kapabilitas siber Pushansiber, berdasarkan informasi dari narasumber bahwa aset yang dimiliki Pushansiber saat ini untuk penanganan peperangan siber adalah SDM yang mengawaki tugas dan fungsi Pushansiber belum sesuai dengan Daftar Susunan Personel (DSP), itupun baru Sebagian kecil yang memiliki sertifikat *Offensive Security Certified Professional* (OSCP) sertifikat *Certified Ethical Hacker* (CEH). Kemudian aset peralatan (teknologi) yang digunakan Pushansiber belum dapat menjalankan standarisasi ISO 27001. ISO 27001 sudah menjadi ikon tentang pengelolaan risiko *information security* yang berlaku di seluruh dunia. Belum berjalannya standar ISO 27001 dikarenakan banyak *tools* yang tidak ber-*license* (*free*) sehingga belum bisa dilakukan *update* dan peralatan yang belum di *maintenance*. Ini terjadi karena keterbatasan anggaran yang diterima oleh Pushansiber.

Kemudian untuk kemampuan, Pushansiber memiliki kemampuan dalam mendeteksi *traffic*, menganalisa serangan, kemampuan Identifikasi, deteksi, proteksi, *respons* dan pemulihan, meskipun kemampuan yang ada saat ini terus menurun karena terdapat kendala dan permasalahan pada aset peralatan yang dimiliki. Sedangkan untuk proses persiapan, Pushansiber melakukan perencanaan tanggap insiden dengan telah di *Launching*-nya *Computer Security Incident Response Team* (CSIRT) pada 8 Desember 2021, menyiapkan regulasi yang *update* dengan melakukan revisi regulasi yaitu Peraturan Menteri Pertahanan Nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber.

Selain kapabilitas siber, pertahanan siber juga berperan dalam penanganan peperangan siber yang menjadi ancaman. Sesuai dengan konsep pertahanan siber dari *cybertalk* (2020), pada suatu organisasi siber, respon yang dapat dilakukan ketika terjadi serangan siber adalah kecepatan operasional, belajar inisiatif dan kolaborasi. Berbicara tentang penanganan, kecepatan operasional adalah merupakan hal penting dalam deteksi dan respons serangan. Pushansiber selalu menyusun laporan harian dari data-data tangkapan yang dihasilkan oleh sensor-sensor yang berada di tujuh titik Satker Kemhan. Hasil dari tangkapan pelanggaran siber kemudian dianalisa oleh beberapa tim dari Laboratorium *Monitoring*, Laboratorium *Malware* maupun Laboratorium Forensik dan dilaporkan kepada pimpinan untuk memperoleh penanganan dalam sebuah rekomendasi. dDlam menghadapi serangan siber, diperlukan analisis terhadap eskalasi ancaman dan gradasi dalam menghadapi serangan siber.

Inisiatif yang dilakukan Pushansiber dalam penanganan peperangan siber adalah dengan selalu berkoordinasi dengan cara memberikan dan membagikan informasi bila terjadi insiden serangan kepada *Stakeholder* KL di bidang siber untuk memberikan peringatan ancaman dan untuk mengantisipasi serta menghindari serangan serupa kepada instansi lainnya. Cara ini mampu menjaga dan menghindari serangan serupa, sehingga dapat memberikan perencanaan, komunikasi dan evaluasi strategi penanganan kepada masing-masing instansi siber untuk lebih menambah keamanan siber dalam melindungi data, informasi maupun sistemnya masing-masing.

Respon yang dilakukan dalam menghadapi serangan dalam penanganan serangan siber pada situasi dan kondisi pertahanan siber yang lemah, hanya bisa dihadapi dengan kekuatan pertahanan yang dibangun melalui kolaborasi dari berbagai elemen dan komponen maupun organisasi siber yang ada dalam negara. Pushansiber menyadari pentingnya kolaborasi untuk mendukung pertahanan siber yang semakin menurun karena kendala-kendala yang ada di Pushansiber. Pushansiber melakukan kerja sama dan menjalin komunikasi serta *networking* dengan lembaga atau Badan pemerintah bidang siber, Satsiber TNI dan Angkatan maupun dengan komunitas *Underground* termasuk kerja sama bidang siber dengan Perguruan Tinggi.

Strategi Pengembangan Kapabilitas.

Pengembangan kapabilitas siber pertahanan sangat diperlukan dalam mendukung pertahanan siber. Untuk bisa mencapai hal tersebut tentunya diperlukan suatu strategi yang tepat dalam mencapai strategi pengembangannya. Dihadapkan dengan tingginya tingkat serangan, Pushansiber harus mengembangkan kapabilitas siber pertahanan untuk dapat melindungi semua data-data maupun informasi penting khususnya di Kementerian Pertahanan dan dapat mendukung sistem pertahanan siber nasional.

Menurut ahli strategi Carl Von Clausewitz (1874), menjelaskan tiga unsur yang digunakan sebagai kunci keberhasilan perumusan suatu strategi yaitu pertama *Ends*, merupakan sasaran atau tujuan yang ingin dicapai dari strategi tersebut. Kedua, *Means* merupakan sumber daya yang dibutuhkan dalam merumuskan strategi atau dengan kata lain bahwa *means* merupakan sumber daya yang digunakan dan dikerahkan untuk mencapai sasaran atau tujuan dari strategi. Ketiga, *Ways* yaitu cara-cara atau metode yang digunakan dalam mencapai sasaran atau tujuan dari strategi.

Sesuai informasi narasumber bahwa strategi pengembangan kapabilitas siber pertahanan memiliki tujuan (*ends*) untuk memiliki kapabilitas dan pertahanan siber yang kuat serta menjadi daya tangkal yang handal terhadap serangan siber terhadap infrastruktur kritis nasional. Guna mencapai tujuan tersebut, diperlukan sumber daya yang akan digunakan. Sumber daya yang digunakan adalah *people*, *process* dan *technology*. Sumber daya yang dimiliki oleh Pushansiber saat ini belum mampu mendukung secara maksimal dalam mencapai tujuan strategi pengembangan kapabilitas siber pertahanan di Pushansiber.

Diperlukan cara (*ways*) yang tepat dalam pengembangan kapabilitas pertahanan siber dihadapkan dengan sejumlah serangan yang semakin kompleks. Cara-cara yang dilakukan oleh Pushansiber untuk mencapai tujuan strategi pengembangan kapabilitas siber pertahanan adalah melalui Pendidikan dan pelatihan terhadap personelnya, melakukan komunikasi, menjalin *networking*, kerjasama dan kolaborasi dengan *stakeholder* pemerintah, Satsiber TNI dan Angkatan, komunitas *Underground* dan Perguruan Tinggi.

Pushansiber harus banyak belajar dari badan atau Lembaga pertahanan siber negara lain yang lebih dulu berhasil mengembangkan kapabilitas sibernya. Setiap negara pasti mempunyai ekosistem pertahanan sibernya masing-masing. Ekosistem tersebut hendaknya perlu digambarkan dan ditetapkan agar diketahui secara pasti komponen-komponen apa yang ada di dalamnya dan bagaimana hubungan satu komponen dengan lainnya saling berelasi dan berinteraksi, sehingga tidak terjadi tumpang tindih peran.

Strategi pengembangan kapabilitas siber pertahanan

Pushansiber dilakukan dengan mengembangkan pada tiga sisi utama yaitu pada sisi *people*, *process* dan *technology*. Untuk SDM (*people*), Pushansiber berusaha terus mencetak SDM handalnya dengan pelatihan, pendidikan maupun kursus untuk bisa diakui secara internasional dan memiliki profesionalitas yang handal untuk kemampuan siber dengan memiliki sertifikat OSCP maupun CEH.

Kemudian pada sisi regulasi (*process*), Pushansiber akan merevisi Peraturan Menteri Pertahanan Nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber yang dijadikan pedoman oleh Pushansiber. Negara maju yang memiliki pertahanan siber yang kuat, mempunyai regulasi yang lengkap yang berada pada seluruh domain dalam sistem peringkat perundang-undangannya. Jadi untuk dapat melakukan pengembangan kapabilitas pertahanan siber yang kuat, regulasi yang terkait dengannya harus berada pada seluruh tata urutan peraturan perundang-undangan, paling tidak terdapat pada domain Undang-Undang (UU), Peraturan Pemerintah (PP), Keputusan Presiden (Keppres), dan Peraturan atau Keputusan Menteri (Kepmen/Permen).

Saat ini yang terjadi di Indonesia baru memiliki satu kebijakan terkait dengan pertahanan siber yang berada pada tingkat Peraturan Menteri (Permenhan Nomor 82 tahun 2014). Pada tingkatan regulasi yang lebih tinggi masih bergantung pada kebijakan umum di bidang siber, bukan spesifik berada dalam domain pertahanan siber. Kebijakan umum yang dimaksud adalah Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). UU ITE ini telah mengalami beberapa kali perubahan sebagai jawaban terhadap dinamika perkembangan jaman. Permasalahannya bahwa UU ini hanya mengatur masalah seputar informasi dan transaksi elektronik, yang berada pada domain ancaman kejahatan siber bukan pertahanan siber.

Pada sisi teknologi (*technology*), Pushansiber akan melakukan *update* teknologi, mengganti beberapa peralatan dengan yang baru, serta melakukan *maintenance* terhadap *tools* maupun peralatan yang ada. Teknologi merupakan piranti atau perangkat yang dibutuhkan dalam pengembangan kapabilitas pertahanan siber. Selain pada sisi *people, process* dan *technology*, strategi pengembangan kapabilitas siber pertahanan yang dilakukan adalah dengan kerja sama dan kolaborasi dengan berbagai *stakeholder* siber baik pemerintah, Perguruan Tinggi maupun dengan komunitas siber lainnya (komunitas *underground*). Diluncurkannya CSIRT Kemhan juga merupakan strategi Pushansiber untuk pengembangan kapabilitas siber pertahanan.

Hal ini didukung dengan dikeluarkannya Keputusan Menteri Pertahanan (Kepmenhan) Nomor: Kep/821/M/VII/2021 tentang Penetapan Tim Tanggap Insiden Siber di lingkungan Kementerian Pertahanan, dengan konstituennya adalah lintas sektor. Pushansiber sebagai kepala CSIRT dan memiliki sub CSIRT yaitu Bagdatin ditiap-tiap Satker di Kemhan. Satker-Satker harus menjadi konstituen atau bagian dari penanggulangan siber.

SIMPULAN.

Strategi pengembangan kapabilitas siber pertahanan tentunya mempengaruhi efektifitas dan kemampuan dalam penanganan peperangan siber yang terjadi dengan skala yang terus meningkat dan kompleks. Hal ini disebabkan karena kapabilitas siber merupakan sesuatu yang dianggap menjadi hal yang utama dalam suatu penanganan serangan siber. Dari penelitian dan pembahasan yang

telah dilakukan dapat diambil kesimpulan sebagai berikut:

1. Penanganan peperangan siber di Pushansiber belum dapat dilaksanakan secara maksimal. Hal ini disebabkan karena permasalahan pada kapabilitas siber yang dimiliki oleh Pushansiber meliputi aset, kemampuan dan proses persiapan belum sepenuhnya dapat terpenuhi. Selain itu pertahanan siber meliputi kecepatan operasional, inisiatif dan kolaborasi belum sepenuhnya dapat dilaksanakan dengan tepat karena kendala pada teknologi yang digunakan Pushansiber saat ini.
2. Strategi yang dilakukan oleh Pushansiber dalam pengembangan kapabilitas siber guna mendukung sistem pertahanan siber nasional adalah pada sisi *people* dengan melakukan pelatihan dan pendidikan personelnya baik level nasional maupun internasional, pada sisi *process* dengan merevisi pedoman pertahanan siber dan pada sisi *technology* dengan melakukan *update* dan *maintenance* untuk peralatannya sesuai dengan anggaran yang ada. Selain itu strategi pengembangan kapabilitas siber yang dilaksanakan oleh Pushansiber adalah dengan *Launching Computer Security Incident Response Team* (CSIRT) sehingga Pushansiber memiliki sub CSIRT yaitu Bagdatin ditiap-tiap Satker di Kemhan yang menjadi konstituen atau bagian dari penanggulangan siber. Bekerja sama dengan komunitas siber baik pemerintah maupun Perguruan Tinggi dan *networking* dengan komunitas *Underground* yang dapat menjadi agen-agen Pushansiber yang setiap saat bisa membantu Pushansiber bila diperlukan.

DAFTAR PUSTAKA

Alistair Haskett. (2016). "*Australian Govermenet Releases Its Cyber Security Strategy*". Australia: Herbert Smith Freehills.

Andress, J. and S. Winterfeld. (2011). *Cyber warfare: techniques, tactics and tools for security practitioners*, Elsevier.

Arikunto,Suharsimi. (2006). Prosedur Penelitian (Suatu Pendekatan Praktik). Rineka Cipta.

Badan Siber dan Sandi Negara. (2019). Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019.

Carl Von Clausewitz. (1874). *On War. Oxford University Press.*

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. Politica.

Clarke, Richard, and Robert Knake. (2010). *Cyber War: The Next Threat to National Security And What To Do About It*.

D.A.N. Dustri, D.A.N. Aspek, and H. Yang. (2014). "Mengenal dan Mengantasipasi Kegiatan *Cybercrime* pada Aktifitas *Online* Sehari-hari dalam Pendidikan, Pemerintahan, dan Industri dan Aspek Hukum Yang Berlaku.," Snikom.

Danim, Sudarwan. (2002). Menjadi Peneliti Kualitatif. Bandung: CV. Pustaka Setia.

Edmon Makarim. (2019), Indonesian *Legal Framework for Cybersecurity. Retrieved* from http://www.nisc.go.jp/security-site/ campaign/ajsympo/pdf/ lecture2.pdf.

Farzan Kolini & Lech Janczewski. (2015). *Cyber Defense Capability Model*: *A*

Foundation Taxonomy, International Conference on Information Resources Management. The University of Auckland.

ISACA (2014) *Cybersecurity Fundamentals* USA.

ISO, B. (2012) "BS ISO/IEC 27032:2012 *Information Technology Guideline for Cybersecurity."British Standards Institute*, London.

ITU. (2017). *Global Cybersecurity Index 2017. International Telecommunication Unit./*

Jordan, F. and G. Hallingstad. (2011) "*Towards Multi-National Capability Development in Cyber Defense." Information & Security: An International Journal,* (27)1, pp. 81-89.

Manthovani, R. (2006). Problematika dan Solusi Penanganan Kejahatan *Cyber* Di Indonesia. PT. MALIBU. Retrieved from **Error! Hyperlink reference not valid.**

NIST (2014) *National Institute of Standards and Technology, U.S. Department of Commerce*.

Pearlman, W., & Cunningham, K. G. (2012). *Nonstate Actors, Fragmentation, and Conflict Processes. Journal of Conflict Resolution*, 56(1), 3–15. Retrieved from https://doi.org/10.1177/ 00220027 11429669.

Perpres No.53. (2017, Mei 19). Peraturan Presiden No.53 tahun 2017 tentang Badan Siber dan Sandi Negara.

Peraturan Menteri Pertahanan Nomor 57 Tahun 2014 tentang Pedoman Strategis Pertahanan Nirmiliter.

Permenhan Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.

Permenkominfo No.5. (2017, Januari 24). Peraturan Menteri Komunikasi Republik Indonesia tentang Perubahan keempat atas Peraturan Menteri Komunikasi dan Informatika No.26 tahun 2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Intern.

Sugihartati, R. (2020, May). Ancaman *Cyber Crime* di Tengah Wabah Covid-19. Media Indonesia, 1. https://mediaindonesia.com/ opini/310180/ancaman-cyber-crime-di-tengah-wabah-covid-19. Diakses pada 20 Juli 2021.

Sugiyono. (2018). Metode Penelitian Kuantitatif, Kualitatif dan R & D. Bandung: Alfabeta.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, pasal 30 ayat 1, 2, dan 5 tentang Pertahanan dan Keamanan Negara.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.

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

Undang-Undang RI Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 25 Tahun 2009 Tentang Pelayanan Publik.

Undang-Undang No.19 tahun 2016 Tentang Perubahan Atas Undang-Undang No.11 tahun 2008 Tentang Informasi dan transaksi Elektronik. President Republik Indonesia