ANCAMAN SIBER, SEBUAH TANTANGAN PERTAHANAN DI ERA MODERN DALAM PRESPEKTIF PERTAHANAN MATRA LAUT

Jarot Wicaksono
Sekolah Staf dan Komando Angkatan Laut
jwicaksonosh@gmail.com
http://doi.org/10.52307/jmi.v912.171

Abstrak,

Bahaya perang siber menjadi perhatian serius Angkatan Laut negara-negara besar dunia. TNI AL memandang penting hal ini dan melakukan berbagai upaya untuk memperkuat diri terhadap bahaya perang siber, sekaligus memanfaatkan keberadaan siber itu sendiri untuk memperkuat jalur komando dan pengendalian terhadap seluruh jajaran dibawah komandonya melalui *Network Centric Warfare* - NCW. NCW berada di dalam Pusat Komando TNI AL, berkedudukan di Jakarta. Untuk itu berbagai upaya perkuatan atas kemampuan dan keamanan NCW sangat vital untuk terus dilakukan. Diperlukan upaya serius seluruh komponen negara yang peduli pada kemampuan TNI AL menghadapi perang siber yang saat ini sudah mendunia.

Kata Kunci: Perang Siber, *Network Centric Warfare*

Abstract,

The danger of cyber warfare is a serious concern for the navies of the world's major countries. The Indonesian Navy views this as important and has made various efforts to strengthen itself against the dangers of cyber warfare, while at the same time utilizing the existence of cyber itself to strengthen command and control channels for all ranks under its command through Network Centric Warfare - NCW. NCW is at the Indonesian Navy Command Center, located in Jakarta. For this reason, various efforts to strengthen NCW's capabilities and security are very important to continue. Serious efforts are needed from all components of the country who care about the Indonesian Navy's ability to face cyber warfare which is currently global.

Keywords: *Cyber War, Network Centric Warfare*

PENDAHULUAN

Marie O'Neill Sciarrone (mantan Asisten Khusus Presiden Amerika untuk Keamanan Dalam Negeri) menyampaikan, perang siber merupakan sebuah upaya menggunakan ruang siber (media digital) untuk melakukan serangan atas lawan. Pelakunya dapat mewakili sebuah lembaga seperti Pemerintahan atau perorangan.[1] Perang ini berkembang seirama dengan perkembangan teknologi internet. Dengan koneksitas internet ini, seluruh dunia dapat saling terkoneksi untuk kepentingan masing-masing. Serangan melalui media ini, ketika menggunakan sebuah sebuah platform global, dalam hitung detik akan mendera berbagai perangkat secara global selama perangkat dimaksud terkoneksi internet. Serangan siber menjadi pintu konsep peperangan ofensif dan defensif baru sehingga siber menjadi salah satu bagian penting dalam konsep perang terbarukan yang dikenal dengan istilah Perang Generasi ke-5.

Perang generasi ke-5, oleh Daniel H. Abbot digambarkan sebagai bentuk perang dengan penekanan konsepnya pada penggunaan teknologi dan persepsi (pola perang) yang berbeda dari perang generasi ke-4 serta generasi-generasi perang sebelumnya.[2] Medan perang generasi ke-5 dapat terjadi dimanapun, dengan mereka yang terlibat tidak melulu dari fraksi atau kekuatan militer. Kekuatan perang berkembang demikian luas, dapat berupa apa saja (kinetik maupun non-kinetik), dengan sasaran dan tujuan yang sangat luas yang tidak dapat diproyeksi seperti perang konvensional atau bahkan Perang generasi ke-4.[3] Meski belum disepakati secara baku oleh para ahli militer dunia, perang generasi ke-5 telah hadir di sekitar kita. Berdasar terminologi diatas, perang generasi kelima merupakan perang yang merambah pada aksi kinentik dan non-kinetik, rekayasa informasi, *artificial intelligence, cyber attack dan autonomous system* dimana pelakunya dapat dari kalangan mana saja, baik militer maupun non militer.

Konsep perang ini menjadi hal baru yang harus diketahui serta dipahami oleh TNI AL selaku kekuatan pertahanan utama negara matra laut. Tentunya agar TNI AL dapat melakukan upaya antisipasi menhadapinya demi tetap tegak serta utuhnya kedaulatan Negara Kesatuan Republik Indonesia (NKRI). Dalam rangka menggali lebih mendalam tentang hal ini,

[1] Sciarone, MON., (2017). *Cyber Warfare: The New Front. The Cataliyst*. Issue Number 6 (springs). https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware. Diakses 15 Agustus 2024. Pukul 09.53 WIB

[2] Abbot, DH., (2010). *The Handbook of 5GW*. Michigan, US : Nimble Books LLC

[3] Schmid, A. (2011). *The Routledge Handbook of Terrorism Research*. Routledge. p.167

maka penelitian dengan judul Perang Siber Dalam Prespektif Pertahanan Matra Laut disusun.

METODOLOGI

Penelitian tentang Perang Siber dalam prespektif pertahanan matra laut disusun melalui metode penelitian kualitatif dimana peneliti menggali data utama dari berbagai literatur yang memiliki tingkat validitas tinggi terhadap objek permasalahan yang ada, baik berdasarkan buku, jurnal hingga sumber lain seperti informasi dari jaringan online. Selanjutnya temuan penelitian dipaparkan dalam naskah yang disusun secara deskriptif analitis demi mendapatkan kesimpulan diakhir penelitian sehingga dapat diperoleh manfaat atasnya.

PEMBAHASAN

Serangan digital menjadi momok dunia seiring perkembangan internet. Di penghujung akhir tahun 90-an, tepatnya pada tahun 1999 periode dimana internet mulai merebak secara global. Dunia dihebohkan dengan kehadiran virus *Melisa*, virus yang kemudian diketahui dibuat David L. Smith seorang programmer computer asal Inggris yang merentas America Online (AOL) sebuah platform digital yang memiliki pengguna global. Memanfaatkan AOL, Melisa menyebar melalui surel (surat elektronik). Pola kerja virus ini menyebabkan kelambatan kerja server, kotak masuk, pola operasional komputer atau perangkat manapun yang terinfeksi. Hingga dinetralisir, Melisa selain menyerang berbagai data base (disinyalir termasuk data base Korps Marinir Amerika). Selama periode serangan, virus Melisa diperkirakan membuat kerugian finansial mencapai $ 80 juta (sekitar 1.301,6 Triliun Rupah).[4] Dengan globalisasi teknologi internet, saat ini dilaporkan bahwa setiap saat, ribuan serangan siber terjadi di dunia maya dengan pola, sasaran, hingga dampak yang beragam, sesuai dengan niat dan tujuan pelakunya.

Menghadapi situasi ini Amerika Serikat sebagai salah satu negara adidaya berupaya melindungi diri dengan membentuk *United States Cyber Command* (US CYBERCOM) di bawah *United States Strategic Command* (US STRATCOM), lembaga ini didirikan tahun 2009 untuk menghadapi ancaman serangan siber terhadap negara mereka. Disamping US CYBERCOM, negeri ini memiliki berbagai komando siber lain di lingkungan militer Amerika, baik yang sudah ada sebelumnya

[4] Stewart E., (2024). Top 10 Biggest Cyber Attacks in History. *Https://em360tech-com.translate.goog/top-10/top-10-most-notorious-cyber-attacks-history?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc* Diakses 15 Agustus 2024. Pukul 11.35 WIB

maupun yang dibentuk kemudian.[5] Setahun sebelum pembentukan US CYBERCOM, organisasi pertahanan Atlantik Utara atau NATO mendirikan *NATO Cooperative Cyber Defense Centre of Excellence* - NATO CCD COE, yang dideklarasi 14 Mei 2008 dan bermarkas di Tallinn, Estonia. NATO CCD COE dibentuk untuk meningkatkan kemampuan negara-negara anggota NATO menghadapi serangan siber.

Terhadap dunia militer dengan pelaku disinyalir merupakan membawa misi sebuah negara yang tercatat adalah *Stuxnet* (kuat dugaan dibuat oleh Amerika dan Israel). Stuxnet dibuat secara khusus yang menargetkan sasaran pada sistem kontrol pengawasan dan akuisisi data (SCADA) milik Iran dipenghujung tahun 2010.[6] Menyerang melalui sistem operasional komputer yang menngunakan *Microsoft Windows*, virus ini memberikan perintah spesifik pada perangkat lunak *Siemens Step7* yang mengendalikan sentrifus pada program nuklir Iran. Stuxnet membuat ribuan mesin sentrifus Iran kemudian berotasi melebihi ambang batas dan merusak keseluruhan sistem. Mesin ini (sentrifus) sangat penting bagi program nuklir Iran karena sentrifus membantu proses pembentukan Uranium U-235 sebagai bahan baku fisil. Untuk mendapatkan uranium U-235 Iran harus merubah Uranium di alam yang merupakan U-238 menjadi U-235. Untuk itu, diperlukan sentrifus untuk memisahkan isotop tertentu demi mencapai U-235 melalui gaya sentrifugal sehingga isotop yang tidak dibutuhkan dapat dipisahkan dari Uranium, mengkreasi Uranum U-235. Kerusakan sentrifus ini membuat kegagalan produksi U-235 oleh Iran.[7] Sumber tertentu menyebutkan, dampak dari serangan ini membuat program nuklir Iran mengalami stagnansi selama beberapa tahun.

Dalam perkembangannya, serangan siber saat ini menjadi komponen berbahaya. Baik terhadap pribadi, kelompok masyarakat lebih luas dan menjangkau negara hingga lingkungan global. Penyebab utama karena serangan siber tidak dapat dilihat secara visual atau fisik, menyerang sisi lemah diri melalui media internet. Penggunaan internet secara meluas merupakan sarana ideal bagi serangan siber. Pada 2023, Indonesia menurut

[5] Soewardi, BA., (2013). *Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia.* Majalah Direktorat Jenderal Potensi Pertahanan Kementerian Pertahanan RI, Edisi Maret, hal 31 – 35

[6] Kushner, D. (2013). *The Real Story of Stuxnet,* IEEE Spectrum. Volume **50** Nomor. 3. Hal 48–53

[7] Josh Fruhlinger, J. (2022). *Stuxnet Explained: The First Known Cyberweapon. Https*://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html. Diakses 15 Agustus 2024. Pukul 11.50 WIB

Kaspersky (sebuah perusahaan yang digital) mengalami 97,465 serangan *phishing* finansial, 16,4 juta insiden lokal, 11,7 juta serangan RDP, dan 97,226 deteksi *ransomware*, hal ini disampaikan Dony Koesmandarin, Enterprise Group Manager Kaspersky untuk Indonesia (3 Juni 2024).[8] Bagi Wakil Menteri Komunikasi dan informasi RI - Wamenkominfo Nezar Patria, dampak ketergantungan pada teknologi digital menyebabkan kasus keamanan siber mengalami peningkatan signifikan dengan peningkatan mencapai lebih 77% pada tahun 2023.[9]

"***Life Free or Die Hard***," sebuah film produksi Holywood tahun 2007 yang dibintangi banyak bintang besar seperti Bruce Willis, Justin Long, Timothy Olyphant, Cliff Curtis, Maggie Q menggambarkan serangan siber terstruktur yang menyebabkan penghentian total kemampuan sebuah negeri Adidaya dengan memanfaatkan sistem digital canggih yang dimiliki oleh negara itu sendiri. Dalam film ini digambarkan betapa serangan siber menyebabkan seluruh akses infrastruktur, telekomunikasi hingga data penting negara dapat dikuasai sekelompok teoris yang memiliki tujuan dan kepentingan tertentu dipimpin seorang mantan analis Departemen Pertahanan AS bernama Thomas Gabriel (Olyphant). Para teroris memulai kampanye serangan dengan melakukan penawaran lomba kepada hacker global dengan tema upaya melumpuhkan sistem suatu negara yang dinamakan **Fire Sale**. Para hacker tanpa sadar kemudian menjadi bagian terorisme dan membuat kekacauan masiv. Film *Life Free or Die Hard* dibuat berdasar sebuah artikel yang ditulis John Carlin, seorang jurnalis dan penulis Inggris untuk majalah Wired tentang bahaya serangan siber dengan judul "A Farewell to Arms".Meski di penghujung film dikisahkan bahwa pada akhirnya upaya pihak teroris itu mengalami kegagalan, namun film ini menjadi sebuah pembelajaran penting tentang bahaya strategis serangan siber.

Bagaimana pertahanan matra laut negara sahabat memaknai serangan siber?

Hingga saat ini, belum ada satupun negara yang mampu menjamin dirinya bebas dari serangan siber. Terhadap serangan siber, banyak negara *concern*

[8] CNN Indonesia (2024). *Indonesia Digempur 6 Juta Ancaman Siber di Awal 2024, Cek Modusnya*. https://www.cnnindonesia.com/teknologi/20240603103200-185-1105033/indonesia-digempur-6-juta-ancaman-siber-di-awal-2024-cek-modusnya. Diakses 15 Agustus 2024. Pukul 12.00 WIB

[9] Siaran Pers No. 243/Hm/Kominfo/03/2024. *Ancaman Siber Meningkat, Wamenkominfo Tekankan Pelindungan Data Pribadi*. https://www.kominfo.go.id/content/detail/55668/siaran-pers-no-243hmkominfo032024-tentang-ancaman-siber-meningkat-wamenkominfo-tekankan-pelindungan-data-pribadi/0/siaran_pers. Diakses 15 Agustus 2024. Pukul 12.25 WIB

padanya dan pro aktif menghadapi. Untuk pertahanan matra laut terhadap ancaman siber, US Navy (AL Amerika) saat ini memiliki *The U.S. Fleet Cyber Command.* Organisasi ini bernaung dibawah Armada ke-10 (*United States Tenth Fleet*) yang diaktifkan kembali oleh Angkatan Laut Amerika seiring dengan terbentuknya *The U.S. Fleet Cyber Command.* Sejak resmi diaktifkan kembali pada tanggal 29 Januari 2010, *The U.S. Fleet Cyber Command* terus berkembang hingga saat ini menjadi organisasi yang tidak saja bersifat defensive, melaikan juga memiliki komponen serang militer berupa pasukan operasional yang terdiri lebih dari 16.000 personel (dengan komposisi berasal dari militer profesional, tenaga ahli sipil hingga komponen cadangan) yang di organisir dalam 27 Komando Aktif, 40 unit Pasukan Misi Siber, dan 27 Komando Cadangan yang disebar di seluruh dunia. *The U.S. Fleet Cyber Command* saat ini memiliki tugas cukup kompleks di berepa bidang mulai dari operasi jaringan informasi, operasi siber ofensif dan defensif, operasi ruang angkasa, dan intelijen sinyal.[10]

Singapura menjadi negara kawasan Asia Tenggara terdepan yang concern terhadap kerentanan keamanan siber. *the Cyber Security Agency of Singapore* (CSA) atau Badan Keamanan Siber Singapura didirikan sebagai implementasi Rancangan Undang-Undang Keamanan Siber Singapura (*Cybersecurity Act*) berhasil dirumuskan pada 5 Februari 2018 dan mendapatkan persetujuan Presiden Singapura tanggal 2 Maret 2018.[11] Organisasi ini kemudian membentuk *the Singapore Computer Emergency Response Team* (SingCERT). Bertugas melaksanakan berbagai hal terkait siber yang antaranya deteksi, resolusi, dan pencegahan insiden-insiden serangan siber. Hingga saat ini SingCERT berhasil melakukan berbagai upaya keamanan siber dan melakukan broadcast tentang peringatan-peringatan, masukan-masukan dan *security patches*; SingCERT juga secara aktif melaksanakan seminar dan lokakarya; dan berkolaborasi dengan badan-badan CERT lainnya untuk menanggapi insiden keamanan siber sekaligus memberikan penerangan kepada oraganisasi pemerintahan di lingkungan negara mereka tentang bahaya siber.[12]

Bagaimana dengan TNI Angkatan Laut?

Sejak masa kepemimpinan Kepala Staf TNI Angkatan Laut - Kasal Laksamana TNI (Purn) Yudo Margono, Pusat Komando

[10] United States Navy, Chief of Naval Operations (2009). F*leet Cyber Command/Commander Tenth Fleet Implementation Plan*. (Memorandum)

[11] Cyber Security Agency. (2018). *Cybersecurity Act.* https://www.csa.gov.sg/legislation/cybersecurity-act. Diakses 15 Agustus 2024. Pukul 20.30 wib

[12] Ibid.

Dan Pengendalian TNI Angkatan Laut (Puskodal) melakukan berbagai upaya peningkatan kemampuan dengan memanfaatkan teknologi internet, salah satunya adalah membangun *Network Centric Warfare* – NCW. NCW didefinisi sebagai sebuah pola operasi militer dengan dukungan piranti mumpuni di bidang informasi yang unggul dari entitas yang memiliki pengetahuan efektif tentang medan yang dihadapi sehingga meningkatkan daya gempur, koneksitas, hingga pengambilan keputusan dengan lebih cepat dan akurat. Entitas ini berada di sebuah pusat komando yang atas keberadaannya mampu mengkomando dan melakukan kontrol secara *real time*. Kondisi ini membuat serangan yang dibangun menjadi lebih mematikan dengan daya getar tinggi akibat akurasi dan kecepatan serang, pembangunan sebuah NCW seiring dengan kemampuan ofensifnya, memberi peluang kemampuan pertahanan menjadi jauh lebih baik.[13] Untuk mencapai apa yang diharapkan Laksamana Yudo Margono kala itu, TNI AL melakukan berbagai hal seperti revitalisasi hardware, revitalisasi software, revitalisasi organisasi serta revitalisasi sumber daya manusia (SDM).

Menggunakan *System Performance Readiness and Tactical Analysis* (SPARTAN) sebuah aplikasi yang digagas oleh salah satu putra terbaik TNI AL, Laksamana Pertama TNI Arif Badrudin, M.Mgt.Stud. kala beliau menjabat sebagai Kapuskodal, proyek revitalisasi ini dilakukan Puskodal. Revitalisasi pada Puskodal akhirnya membuat komunikasi Markas Besar TNI AL - Mabesal dengan satuan bawah menjadi lebih mudah. Melalui SPARTAN, berbagai Fitur *Chat, Voice* dan Pesan Singkat (KRI dapat menerima berita/perintah dari Puskodal secara *real time* dari Puskodal/Armada), Fitur *Tracking* Unsur (pantauan dislokasi unsur KRI secara real time dijajaran Puskodal), Fitur *Risk Scoring* (sistem deteksi dan alert pelanggaran dilaut secara otomatis), Fitur Visualisasi (*long range camera CSS*), *Fitur Geofencing* AIS (giat perairan Indonesia) serta Fitur *Distress Signal* dapat dideteksi Puskodal TNI AL dan dikomunikasi kepada satuan bawah terkait.[14] SPARTAN juga mampu menindak lanjut setiap data yang diterima secara lebih efektif dengan kemampuan lebih terhadap berbagai perubahan dinamis lingkungan atas data yang diterima. Dari piranti SPARTAN, membuat terjadinya sinkronisasi data

[13] Alberts DS., Garstka JJ., dan Stein FP., (1999). *Network-Centered Warfare: Alerting and Exploiting Information Advantage*. Londonn, UK : CCRP

[14] Indodefense (2022). *KSAL Terima Laporan Perkembangan Program Revitalisasi Puskodal. https://indonesiadefense.com/ksal-terima-laporan-perkembangan-program-revitalisasi-puskodal/*

intelijen, pengawasan, dan pengintaian (ISR), yang meningkatkan kewaspadaan situasional sehingga dapat dilakukan langkah antisipasi efektif atas setiap perubahan dinamika lingkungan strategis sendiri, regional hingga global.

Gambar 1. Prinsip Kerja NCW
Sumber:
https://defence360officials.blogspot.com/2016/12/network-centric-warfare-capabilities.html

Konsep NCW untuk kawasan Asia juga telah diaplikasi lebih jauh oleh Angkatan Laut India. India membuat kemajuan besar dalam jaringan Komando, Kontrol dan Komunikasi dengan mengembangkan kemampuan NCW mereka. Saat ini seluruh kapal milik Angkatan Laut India terkoneksi dalam satu pola manajemen tempur yang membuat sistem kesenjataan mereka (kapal-kapal milik Angkatan Laut India) menjadi hampir sepenuhnya full otomatis, sehingga membantu percepatan waktu reaksi unsur kapal di jajaran armada mereka.[15] Untuk keamanan jaringan, India melakukan pembangunan proyek jaringan komunikasi mandiri oleh perusahaan strategis dalam negeri dengan meluncurkan berbagai satelit militer produksi dalam negeri. Hal ini memberikan Angkatan Laut India keunggulan pertahanan digital yang setara dengan angkatan-angkatan laut terbaik milik negara-negara dengan kekuatan Matra Laut yang besar di dunia.

Kasal Laksamana TNI Muhammad Ali, seperti pendahulunya sangat concern terhadap ancaman siber, pada saat penutupan Pendidikan Reguler Sekolah Staf dan Komando Angkatan Laut Angkatan ke-61 beliau menyampaikan ,"Dihadapkan dengan ancaman siber, maka pengembangan dan pemanfaatan teknologi informasi menjadi suatu keharusan dan upaya strategis dalam membentengi negara dari ancaman hibrida yang berkembang semakin kompleks di era modern".[16] Keamanan jaringan termasuk menghadapi ancaman siber, menjadi perangkat vital yang hingga saat ini masih diupaya oleh TNI AL. Atas hal ini, Profesor Onno W

[15] Kumar, CN., (2020). *Network Centric Warfare and Emerging Communication Technologies.* https://dras.in/network-centric-warfare-and-emerging-communication-technologies/. Diakses 15 Agustus 2024. Pukul 21.00 wib

[16] Arsilan, R (2023). KSAL Muhammad Ali Beberkan 5 Strategi untuk Hadapi Perang Hibrida di Era Modern. Viva.co.id. https://www.viva.co.id/militer/militer-indonesia/1650123-ksal-muhammad-ali-beberkan-5-strategi-untuk-hadapi-perang-hibrida-di-era-modern. Diakses 15 Agustus 2024. Pukul 21.30 WIB

Purbo seorang Ilmuwan dan pakar di bidang teknologi informasi, dalam *Foccus Gorup Discusion* (FGD) Sekoal 2024 menyampaikan usulan perkuatan dan penggunaan satelit dalam negeri, dalam hal ini produk industri atau lembaga penelitian milik negara seperti misalnya LAPAN sebagai penyusun jalur komunikasi digital terbatas untuk kewasgiatan masing-masing, termasuk komponen pertahanan negara seperti TNI AL.

Bagi Onno, sejalan dengan Kasal Laksamana TNI Muhammad Ali, hal ini penting dilakukan demi menjamin keamanan jalur komunikasi antara NCW yang berada di Puskodal TNI AL dengan seluruh jajaran di bawah komando TNI AL dimanapun berada. Salah satu yang ditawarkan oleh beliau adalah penguatan satelit LAPAN A5. LAPAN A5 sangat layak dipertimbangkan karena satelit ini, selain memiliki kemampuan penyalur komunikasi juga dilengkapi berbagai fitur canggih salah satunya adalah *Synthetic Aperture Radar* (SAR), sebuah bentuk radar yang dapat membuat gambar objek dua dimensi atau tiga dimensi, seperti landscape.[17] Satelit ini juga menjadi bagian dari konstelasi yang terdiri dari sekitar delapan atau sembilan satelit produksi dalam negeri yang dapat mengirimkan data ke pusat pemantauan di Bumi. Dan terpenting, satelit ini merupakan hasil kerja keras anak bangsa sehingga kepentingan dibaliknya adalah demi tetap tegak keutuhan dan kedaulatan Negara Kesatuan Republik Indonesia.

KESIMPULAN

Sebagai sebuah kekuatan pertahanan yang dinamika operasional dan fungsinya begitu luas, TNI AL sudah selayaknya memiliki kekuatan besar dibidang komando dan kendali. NCW yang dikembangkan Puskodal TNI AL merupakan sebuah solusi vital atas hal ini. NCW selain sebagai pusat kontrol juga dapat berperan lebih atas setiap olah gerak seluruh jajaran TNI AL. Dihadapkan dengan perang siber yang menjadi bagian penting Perang Generasi ke-5, NCW perlu diperkuat terutama dari segi keamanan. Salah satu hal penting atasnya adalah perkuatan sistem jaringan yang menggunakan satelit produksi dalam negeri, hal yang dilakukan oleh seluruh Angkatan Laut negara-negara besar di dunia karena produksi internal lebih memiliki jaminan keamanan bagi sebuah negara.

[17] Setiawan, I., Irawan, W., (2017). *Lapan libatkan ITS dalam pembuatan satelit baru LAPAN A5*. https://www.antaranews.com/berita/651015/lapan-libatkan-its-dalam-pembuatan-satelit-baru-lapan-a5#:~:text=Heru%20melanjutkan%2C%20teknologi%20yang%20dikembangkan%20untuk%20Satelit,dua%20dimensi%20atau%20tiga%20dimensi%2C%20seperti%20landscape. Diakses 15 Agustus 2024. Pukul 21.30 WIB

DAFTAR PUSTAKA

Abbot, DH., (2010). *The Handbook of 5GW*. Michigan, US : Nimble Books LLC

Alberts DS., Garstka JJ., dan Stein FP., (1999). *Network-Centered Warfare: Alerting and Exploiting Information Advantage*. Londonn, UK : CCRP

Arsilan, R (2023*). KSAL Muhammad Ali Beberkan 5 Strategi untuk Hadapi Perang Hibrida di Era Modern*. Viva.co.id. https://www.viva.co.id/militer/militer-indonesia/1650123-ksal-muhammad-ali-beberkan-5-strategi-untuk-hadapi-perang-hibrida-di-era-modern. Diakses 15 Agustus 2024. Pukul 21.30 WIB

CNN Indonesia (2024). *Indonesia Digempur 6 Juta Ancaman Siber di Awal 2024, Cek Modusnya*. https://www.cnnindonesia.com/teknologi/20240603103200-185-1105033/indonesia-digempur-6-juta-ancaman-siber-di-awal-2024-cek-modusnya. Diakses 15 Agustus 2024. Pukul 12.00 WIB

Cyber Security Agency. (2018). *Cybersecurity Act.* https://www.csa.gov.sg/legislation /cybersecurity-act. Diakses 15 Agustus 2024. Pukul 20.30 WIB

Indodefense (2022). *KSAL Terima Laporan Perkembangan Program Revitalisasi Puskodal. https://indonesiadefense.com/ksal-terima-laporan-perkembangan-program-revitalisasi-puskodal/.* Diakses 15 Agustus 2024. Pukul 12.00 WIB

Kementerian Informasi dan Komunikasi Indonesia (2024). *Ancaman Siber Meningkat, Wamenkominfo Tekankan Pelindungan Data Pribadi*. https://www.kominfo.go.id/content/detail/55668/siaran-pers-no-243hmkominfo032024-tentang-ancaman-siber-meningkat-wamenkominfo-tekankan-pelindungan-data-pribadi/0/siaran_pers. Diakses 15 Agustus 2024. Pukul 12.25 WIB

Kumar, CN., (2020). *Network Centric Warfare and Emerging Communication Technologies.* https://dras.in/network-centric-warfare-and-emerging-communication-technologies/. Diakses 15 Agustus 2024. Pukul 21.00 WIB

Kushner, D. (2013). *The Real Story of Stuxnet,* IEEE Spectrum. Volume **50** Nomor. 3. Hal 48–53

Josh Fruhlinger, J. (2022). *Stuxnet Explained: The First Known Cyberweapon. Https*://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-

cyberweapon.html. Diakses 15 Agustus 2024. Pukul 11.50 wib

Sciarone, MON., (2017). *Cyber Warfare: The New Front. The Cataliyst*. Issue Number 6 (springs). https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware. Diakses 15 Agustus 2024. Pukul 09.53 wib

Schmid, A. (2011). *The Routledge Handbook of Terrorism Research*. Routledge. p.167

Setiawan, I., Irawan, W., (2017). *Lapan libatkan ITS dalam pembuatan satelit baru LAPAN A5*. https://www.antaranews.com/berita/651015/lapan-libatkan-its-dalam-pembuatan-satelit-baru-lapan-a5#:~:text=Heru%20melanjutkan%2C%20teknologi%20yang%20dikembangkan%20untuk%20Satelit,dua%20dimensi%20atau%20tiga%20dimensi%2C%20seperti%20landscape. Diakses 15 Agustus 2024. Pukul 21.30 wib

Stewart E., (2024). Top 10 Biggest Cyber Attacks in History. *Https://em360tech-com.translate.goog/top-10/top-10-most-notorious-cyber-attacks-history?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc* Diakses 15 Agustus 2024. Pukul 11.35 wib

Soewardi, BA., (2013). *Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia.* Majalah Direktorat Jenderal Potensi Pertahanan Kementerian Pertahanan RI, Edisi Maret, hal 31 – 35

United States Navy, Chief of Naval Operations (2009). F*leet Cyber Command/Commander Tenth Fleet Implementation Plan*. (Memorandum).