Jurnal Strategi Pertahanan Darat
Volume 8, Nomor 2 2022 E-ISSN 2830-3075

KESIAPAN OEPRSI *CYBER WARFARE* MARKAS BESAR TNI ANGKATAN DARAT 2018

Cyber Warfare Operating Readiness Indoenesia Army Headquarters 2018

Bambang prasetyo
Prodi Strategi Pertahanan Darat, Fakultas Strategi Pertahanan
Universitas Pertahanan RI
bembyaja1234@gmail.com

Abstract
The rapid development of information and communication technology has implications for the development of cyber life and has opened doors for those intent on achieving criminal aims. Namely, identity theft, cyber blackmail, fraud, data leakage and numbers of cyber crime that in fact they can be so expansive where could harm entire nations.1 Thus, cyber security measures play important role in restraining cyber threats. Indonesian Armed Forces is an military organization whose plays role in constructing sustainable cyber security. It is associated to the effort to protect various national defense entities related to fast response towards threats landscape. This makes the importanc of the readiness of the Indonesian Armed Forces Headquartes Operations in dealing with cyber warfare. This research was conducted to analyze the development of cyber warfare in the Indonesian Armed Forces (2018), the level of readiness of operations of the Indonesian Armed Forces Headquarters in dealing with cyber warfare and the formulation of strategies in improving the readiness operations of the Indonesian Armed Forces Headquarters in dealing with cyber warfare. In order to achieve those objectives, this research was conducted using qualitative methodes with data collection technique of obeservation, related documents review and in-depth interviews. The results of the study found that the development of information and communication technology had the implications on the increasingly massive cyber warfare in Indonesian Armed Forces, specifically the efforts of groups or organizations or countries to collect information, vandalism and sabotage. In addition, the readiness of the Indonesian Armed Forces Headquarters operation in dealing with cyber warfare is divided into two, namely offensive readiness and defensive readiness. Defensive readiness related to how Operations Staff conduct the internet security, ICT security, information security, while offensive readiness is related to digital security such as counter attacks. As for the readiness of the Indonesian Army Headquarters Operations, there are still problems with the limited bbudget, infrastructure and human resources. The strategy to improve readiness is to conduct a comprehensive evaluation of readiness. While the strategy in budgets facet is by setting priority scale according to operating needs. The infrastructure strategy is to procure in stages with measuring software and hardware independence in cyber warfare.

Keywords: Cyber Warfare, Cyber Threats, National Defense, Information Security, Indonesia Armed Force Readiness

[1] Deniele Hadi Irandoost. *Cybersecurity: A National Security Issue?*. (E-International Relations, 2018) Hlm. 1

Abstrak

Pesatnya perkembangan teknologi informasi dan komunikasi telah berimplikasi pada berkembangnya kehidupan cyber dan membuka pintu bagi ancaman strategis baru, misalnya pencurian identitas, pemerasan siber, penipuan, kebocoran data dan beberapa bentuk kejahatan siber lainnya yang begitu ekspansif hingga dapat membahayakan seluruh negara. Dengan begitu langkah-langkah keamanan cyber memainkan peran penting dalam membatasi ancaman dunia maya. TNI AD merupakan organisasi militer yang berperan dalam membangun keamanan siber yang berkelanjutan. Hal ini berkaitan dengan upaya untuk melindungi berbagai entitas pertahanan negara terkait respon cepat terhadap lanskap ancaman. Hal ini menjadikan pentingnya kesiapan Operasi Mabes TNI AD dalam menghadapi peperangan siber. Penelitian ini dilakukan untuk menganalisis perkembangan peperangan siber di lingkungan TNI AD, tingkat kesiapan operasi Markas Besar TNI AD (2018) dalam menghadapi peprangan siber dan formulasi strategi dalam meningkatkan kesiapan operasi Markas Besar TNI AD dalam menghadapi peperangan siber. Guna mencapai tujuan tersebut, maka penelitian ini dilakukan dengan menggunakan metode kualitatif dengan teknik pengumpulan data observasi, penelaahan dokumen terkait dan wawancara secara mendalam. Hasil penlitian ditemukan bahwa Perkembangan teknologi informasi dan komunikasi berdampak pada semakin masifnya peprangan siber di lingkungan TNI AD yaitu berkaitan dengan usaha kelompok/organisasi/negara untuk melakukan pengumpulan informasi, vandalism dan sabotase. Selain itu kesiapan operasi Markas Besar TNI AD dalam menghadapi peprangan siber terbagi menjadi dua, yaitu kesiapan offensive dan kesiapan defensive. Kesiapan defensive berkaitan dengan bagaimana Staf Operasi malakukan internet secruity, ICT security, information security, sedangkan kesiapan offensive berkaitan dengan digital security seperti serangan balik. Adapun kesiapan Operasi Mabes TNI AD masih bermasalah terkait terbatasnya anggaran, infrastukur dan SDM. Adapun strategi meningkatkan kesiapan yaitu dengan melakukan evaluasi secara komprehensif terkait kesiapan. Sedangkan strategi dalam anggaran yaitu dengan penyusun skala prioritas sesuai dengan kebutuhan operasi. Strategi infrastruktur yaitu dengan melakukan pengadaan secara bertahap dengan memperhitungkan kemandirian pada software dan hardware dalam peprangan siber.

Kata kunci : Peperangan Siber, Ancaman Siber, Pertahanan Negara, Keamanan Informasi, Kesiapan TNI AD

1. Pendahuluan

Sejarah telah mendeksripsikan bahwa umat manusia telah berperang dan berusaha untuk memajukan agenda nasional dalam permainan kekuasaan internasional yang terus berubah. Dari pertempuran pedang di masa lalu dan kini serangan pesawat tak berawak, permainan kekuatan ini terus-menerus bergeser dan berkembang dengan memanfaatan teknologi. Pengembangan teknologi tersebut telah melahirkan kendaraan lapis baja, pesawat terbang, kapal dan penggunaan elektronik serta telekomunikasi telah memperluas ruang pertempuran. Seperti halnya inovasi teknologi memicu perlombaan untuk mendominasi semua sektor kehidupan masyarakat termasuk dunia maya (cyber). Thompson dan Nadler menjelaskan bahwa,

"One of the merits of virtual technology is bridging the gaps and long physical distances."2 Idenya bermakna bahwa, salah satu keunggulan teknologi virtual adalah medan ini dapat menjembatani kesenjangan dan jarak fisik yang panjang. Namun Rheingold menjelaskan bahwa, "The internet and cyberspace have influenced just about every realm of our behaviour."3 Dengan kata lain, medan siber telah mempengaruhi hampir setiap aspek perilaku manusia. Sebagaimana doikatakan oleh Barack Obama bahwa "Cyberspace is real and so are the risks that come with it. From now on, our digital infrastructure, the networks and computers we depend on every day, will be treated as they should be, as a strategic national asset"4

Obama memandang bahwa medan siber itu nyata demikian pula resiko yang menyertainya. Dengan begitu pemerintahannya mengelola infrastruktur, jaringan dan komputer yang diandalakannya setiap hari akan diperlakukan sebagaimana mestinya, yaitu sebagai aset nasional yang strategis.

---

[2] L. Thomposon & J Nadler. "Negotiatioing via Information Technology: Theory and Application", *Journal of Social Issues,* Vol. 58, No. 1, 2002.
[3] H. Rheingold. *New Smart: How to Thrive Online.* (Cambridge: The Mit Press, 2012)
[4] The New York Times. 29 May 2009. *Text: Obama's Remarks on Cyber-Security.* Diakses di: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html (diakses pada 13/02/2020)

Hal ini dikarekanakan kehidupan siber telah membuka kemungkinan dan ancaman strategis baru yang menyebabkan perebutan untuk mengamankan posisi dominan. Sebaimana dikatakan Ameli:

"Considering the potensials of cyberspace in terms of connectivity, accessibility, dispersality and digitalism, huge changes are perceptible in comparison with physical space. Virtual space therefore is the space of omnipresence, globality and accessibility if one to all and all to one."5 Mempertimbangkan potensi dunia maya dalam hal konektifitas, aksesibilitas, penyebaran dan digitalisme, perubahan besar terlihat dibandingkan dengan ruang fisik. Karena itu, ruang virtual adalah ruang kemahahadiran, globalitas dan aksesibilitas satu ke semua dan semua ke satu. Ancaman keamanan siber merupakan tindakan jahat yang berupaya merusak data, mencuri data atau mengganggu kehidupan digital secara umum. Serangan siber mencakup ancaman seperti virus komputer, pelanggaran data dan serangan Denial of Service (DoS).6

Menurut Salahuddien7, medan siber kini telah menjadi tempat yang potensial untuk menjadi medan pertempuran dan konflik. Seperti upaya dominasi melalui penyebaran informasi hingga kegiatan yang bersifat destruktif seperti web defacing rally sebagai cara propaganda dan intimidasi. Perseteruan tersebut tidak hanya dilakukan oleh amatir namun juga mereka yang punya keterampilan dan kemampuan khusus bahkan banyak kelompok profesional yang menawarkan jasa layaknya tentara bayaran.8

Perkembangan ancaman siber harus diikuti dengan pengembangan keamanan siber. Keamanan siber atau biasa disebut cyber security adalah

---

[5] Saied Reza Ameli. "Dual Spacization of Cultures: Problematization of Cyberspace and Cultural Matters", *Journal of Cyberspace Policy Studies,* Vol. 1, No. 1, Januari 2007.
[6]Hugh Taylor. 22 Januari 2020. *What are Cyber Threats and What To Do about Them.* Diakses di: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/ (diakses pada 13/02/2020)
[7] M. Salahuddien. 2011. *Pertahanan Keamanan Informasi Nasional.* (Indonesia Security Incident Response Team on Internet Infrastructure, 2011)
[8] Muhammad Badri. *Perang Cyber dalam Dinamika Komunikasi Internasional.* (Pekanbaru: Universitas Islam Riau, July 2012) hlm. 101

"The complete universe of tools, practices and rules that protect data assets from malicious actors. It is an upgrading of the traditional concept of information security (InfoSec), which viewed security simply as a corporate issue, rather that a problem affecting consumers and national security (and life itself, on some level)"9

Keamanan siber adalah alat praktik dan aturan yang lengkap yang melindungi aset data dari aktor jahat. Ini merupakan konsep tradisional keamanan informasi yang hanya memandang keamanan sebagai masalah yang memengaruhi konsumen dan keamanan nasional dan kehidupan itu sendiri pada tingkat tertentu. Pertahanan siber menganalisis berbagai ancaman yang mungkin terjadi pada lingkungan tertentu. Ini kemudian membantu dalam merancang dan mengarahkan strategi yang diperlukan untuk melawan serangan siber sehingga dapat meminimalisiar dampak dari serangan.

Di Indonesia, operasionalisasi keamanan siber telah dipraktikkan di kalangan militer selama lebih dari satu dekade. Berbagai macam serangan cyber menempatkan pentingnya organisasi militer yang konsisten membangun cyber security yang berkelanjutan, Hal ini berkaitan dengan upaya untuk melindungi berbagai entitas pertahanan negara terkait respon cepat terhadap lanskap ancaman termasuk juga melakukan analisis teknis untuk mengidentifikasi jalur dan area yang bisa diserang oleh hacker.

Pada sisi ini jelas bahwa urgensi pembentukan kesiapan cyber security oleh organisasi militer berkaitan dengan bagaimana organisasi militer sebisa mungkin dapat mengantisipasi berbagai ancaman siber termasuk didalamnya kegiatan cyber crime yang merugikan. Robinson10 menjelaskan meningkatnya liputan media tentang perang siber berfungsi untuk meningkatkan kesadaran publik bahwa dunia maya telah menjadi arena perang. Dengan begitu, pemerintah sepenuhnya menyadari perlunya mengambil tindakan dalam menanggapi ancaman dari dunia maya. Berbagai lembaga

[9] Hugh Taylor. 18 Desember 2018. *What is Cyber Security.* Diakses di: https://preyproject.com/blog/en/what-is-cyber-security/ (diakses pada 13/02/2020)
[10] Kevin Jones Robinson & Helge Janicke, "Cyber Warfare: Issues and Challenges", *Journal of Computers and Security,* Vol. 8, 2015. hlm. 2

pemerintah dan militer sadar bahwa peperangan siber telah menjadi fenomena ancaman dan penting untuk melakukan tindakan dalam menanggapi ancaman tersebut khususnya dalam rangka menguatkan efektivitas dari pertahanan negara terkait cyber crime.

Contoh cyber crime yang terjadi di Indonesia yaitu pada hari Sabtu 17 April 2004 oleh Dani Firmansyah sebagai konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta berhasil membobol situs resmi milik Komisi Pemilihan Umum (KPU) dan berhasil melakukan perubahan pada seluruh nama partai disitus KPU. Contoh lain dari kasus cyber crime di Indonesia lainnya diketahui ketika National Security Agency (NSA), Edward Snowden memperlihatkan informasi strategis yang bersifat sangat sensitif yaitu data-data penyadapan yang dilakukan intelijen Australia kepada pejabat tinggi Indonesia.

Pada dasarnya aksi dari aktivitas penyadapan tersebut merupakan proses dari cyber crime yang dilakukan dalam rangka menggali berbagai informasi, praktek penyadapan tersebut telah menjadi isu sensitif karena menyinggung privasi dan kedaulatan negara dalam hal intelektual, intelijen dan informasi negara yang tentunya bersifat rahasia. Berdasarkan realitas dari kasus-kasus tersebut jelas bahwa cyber crime merupakan ruang lingkup luas dan kompleks, hal ini telah membangun urgensi bagi organisasi militer di setiap negara untuk lebih responsif/peka terhadap berbagai perkembangan aspek-aspek cyber crime termasuk didalamnya pentingnya organisasi militer untuk menyiapkan cyber defence di organisasi militer.

TNI AD sebagai organisasi militer, dalam menghadapi perkembangan ancaman siber, berperan penting dalam melaksanakan cyber security sebagaimana TNI AD melaksanakan tugas di bidang pertahanan dalam Operasi Militer untuk Perang (OMP) dan Operasi Militer Selain Perang (OMSP). Dalam cyber defence, TNI AD memiliki organisasi khusus seperti Staf Operasi Mabesad yang bertugas menyelenggarakan kegiatan pengendalian/ penyiapan komando, pemeliharaan kesiapan dan kemantapan

operasional termasuk didalamnya adalah kesiapan Staf Operasi Markas Besar TNI AD dalam peperangan siber.

Namun begitu Staf Operasi Mabes TNI AD dalam menghadapi cyber warfare masih belum optimal khususnya jika dihadapkan pada berbagai permasalahan kesipan operasional. Misalnya masih terbatasnya sarana dan prasarana yang dimiliki Staf Operasi Mabes TNI AD apalagi jika dihadapkan pada kebutuhan software dan hardware khusus terkait siber. Terlebih lagi Staf Operasi Mabes TNI AD masih menggunakan satelit yang bergabung dengan kepentingan sipil, baik untuk kepentingan normatif maupun kepentingan khusus dalam cyber warfare.

Temuan lain juga memperlihatkan persoalan Sumber Daya Manusia (SDM) masih ditemukan ketika jumlah personel dengan spesifikasi kompetensi khusus siber masih belum terpenuhi. Berbagai temuan permasalahan tersebut menunjukan bahwa Staf Operasi Mabes TNI AD pada dasarnya harus melakukan upaya untuk membangun strategi dalam menghadapi cyber warfare, penting bagi Staf Operasi Mabes TNI AD organisasi militer memiliki kesiapan operasional khususnya dalam menghadapi cyber warfare. Maka setiap organisasi militer di setiap negara yang berkaitan dengan cyber warfare, harus siap dalam melakukan operasi-operasi khusus dalam lingkup cyber defence. Dalam pengertiannya, cyber defence merupakan tindakan dan perlindungan infrastruktur penting dan jaminan informasi untuk organisasi, entitas pemerintah, dan jaringan lain11 yang berfokus pada pencegahan, pendeteksian dan pemberian tanggapan tepat waktu terhadap serangan atau ancaman sehingga tidak ada infrastruktur atau informasi yang dirusak. Dengan pertumbuhan volume serta kompleksitas serangan siber, kesiapan pertahanan siber oleh Staf Operasi Mabes TNI AD sangat penting bagi sebagian besar entitas untuk melindungi informasi yang sensitif serta untuk melindungi aset informasi dari organisaisi militer.

[11] Darko Galinec & Boris Guberina, "Cybersecurity and Cyber Defence: National Level Strategic Approach", *Journal of Control, Measurement, Electronics, Computing and Communications,* Vol. 58, No. 3, 2017. Hlm. 274

2. Metode Penelitian

Penelitian ini menggunakan metode kualitatif, melalui pendekatan fenomenologi dengan fokus analisis yaitu strategi kesiapan operasi Tentara Nasional Indonesia Angkatan Darat dalam menghadapi cyber warfare, studi pada Markas Besar Tentara Nasional Indonesia Angkatan Darat Tahun 2018. Dalam analisa data, penelitian ini menggunakan beberapa teori/konsep yang relevan dan mendukung variabel yang diteliti dan hasil penelitian terdahulu yang relevan dengan penelitian. Diantaranya teori strategi, teori kesiapan operasi, konsep cyber warfare, konsep cyber threats, konsep cyber crime, konsep cyber security, dan konsep cyber defense.

Menurut David dalam tulisan Faruq dan Indriana, menjelaskan strategi sebagai:

"Sarana bersama dengan tujuan jangka panjang yang akan hendak dicapai. Strategi bisnis bisa berupa perluasan geografis, diversifikasi, akusisi, pengembangan produk, penetrasi pasar, rasionalisasi karyawan, divestasi, likuidasi dan usaha patungan atau joint venture"12

Menurut Barney dan Hesterly, Strategi dimaknai sebagai: "Sebuah teori tentang bagaimana cara perusahaan meraih keunggulan-keunggulan kompetitif (competitive advantages)"13

Menurut Hitt, strategi adalah sebuah rangkaian yang terpadu dan ter terkoordinasi dari komitmen dan tindakan yang dirancang untuk mengeksplotasi kompetensi utama dan meraih keunggulan kompetitif.14

Meiser berpendapat bahwa strategi berkaitan dengan perpaduan antara tujuan, cara meraih tujuan dan sumber daya yang tersedia dalam meraih tujuan tersebut.

---

[12] Faruq Ammar & Usman, "Penyusunan Strategi dan Strategi Operasi Usaha Kecil dan Menengah pada Perusahaan Konveksi Scissors di Surabaya", *Jurnal Manajemen Teori dan Terapan Tahun 7, No. 3,* 2014. Hlm. 176

[13] Ibid. Faruq Ammar & Usman.

[14] Ibid. Faruq Ammar & Usman.

Strategi direduksi dalam mengalokasikan sumber daya. Pendekatan ini merupakan cara terbaik untuk membuat stabilitas kebijakan.15

Berdasarkan berbagai pengertian strategi tersebut, dapat diketahui bahwa strategi adalah rencana kegiatan yang dirancang untuk mencapai visi. Dalam strategi tersebut, beberapa aspek yang memainkan peran penting dalam tercapainya sebuah tujuan adalah aspek kepemimpinan, jalan untuk mencapai visi, tujuan itu sendiri dan masa depan yang diinginkan serta serangkaian kegiatan untuk mencapai tujuan.

Kaitannya dalam penelitian ini, strategi menjadi bentuk dari aksi nasional untuk mencapai serangkaian tujuan yang berkontribusi pada terciptanya keamanan domain cyberspace atau dunia maya.

Secara umum strategi nasional akan memiliki perbedaan bertujuan seperti untuk menyelaraskan seluruh pemerintahan dan secara koheren fokus serta mengoordinasikan perencanaan untuk menyampaikan peran, tanggung jawab, dan hubungan yang diharapkan antara semua pemangku kepentingan.

Dalam menjelaskan teori kesiapan operasi, berangkat dari pengertian kesiapan. Menurut Yusnawati16, kesiapan adalah suatu kondisi dimana seseorang telah mencapai tahapan tertentu atau dikonotasikan dengan kematangan fisik, psikologi, spiritual dan skill. Sementara Arikunto17 menjelaskan bahwa kesiapan adalah suatu kompetensi yang dimiliki seseorang yang dengannya ia cukup siap untuk berbuat sesuatu. Slameto18 menjelaskan bahwa,

"Kesiapan adalah keseluruhan kondisi yang membuatnya siap untuk memberi respon atau jawaban di dalam cara tertentu terhadap suatu situasi. Penyesuaian kondisi pada suatu saat akan berpengaruh pada kecenderungan untuk memberi respon."

Secara khusus, kesiapan operasi diartikan oleh Permanasari sebagai:

---

[15] Meiser Jeffrey W, "Are Our Strategic Models Flawed? Ends + Ways + Means = (Bad) Strategy", *Journal Parameters,* Vol. 46, No. 4, 2017. Hlm. 82

[16] Yusnawati. *Perencanaan Pengajaran Berdasarkan Pendekatan Sistem.* (Jakarta: Bumi Aksara, 2007). Hlm. 3

[17] Suharasimi Arikunto. *Dasar-Dasar Evaluasi Pendidikan (edisi revisi).* (Jakarta: Bumi Aksara, 2001). Hlm. 54

[18] Slameto. *Belajar dan Faktor yang Mempengaruhinya.* (Jakarta: Rineka Cipta, 2010). Hlm. 3

"Tindakan atau operasi terhadap atau menggunakan suatu komputer atau sistem komputer melalui aliran data, baik dengan cara melakukan infiltrasi atau pengambilan, pengiriman, perusakan, perubahan atau enkripsi data, atau untuk memacu, merubah atau memanipulasi proses pada sistem komputer yang telah terinfiltrasi."19

Dengan begitu, secara umum kesiapan operasi merupakan segala yang berkaitan dengan usaha untuk membentuk suatu situasi sehingga dapat mencapai tujuan-tujuan yang direncanakan atau dikehendaki. Terkait dengan penelitian ini, kesiapan operasi adalah keadaan yang sedang dipersiapkan melalui orang, sistem dan organisasi untuk menghadapi situasi dan melakukan urutan tindakan yang tepat yang bisa didasarkan pada perencanaan dan pelatihan yang menyeluruh.

Tujuan Pembinaan kesiapan operasi TNI AD adalah untuk menyiapkan penyelenggaraan pertahanan darat negara melalui upaya mewujudkan penampilan kekuatan pertahanan negara di darat yang merupakan keterpaduan kekuatan, kemampuan dan gelar kekuatan TNI-AD sebagai komponen utama pertahanan darat negara.

Cyber Warfare merupakan ujuang paling serius dari spektrum tantangan keamanan yang ditimbulkan oleh cyberspace atau dunia maya. Sama hal nya dengan alat perang konvensional, teknologi dunia maya dapat digunakan untuk menyerang mesin negara, lembaga keuangan, energi nasional dan infrastruktur transportasi dan moral masyarakat. Meski, beberapa tindakan yang tampak agresif dan suka berperang, tidak dimaksudkan sebagai tindakan perang. Karena itu, penting untuk membedakan antara perang dan non-perang di dunia maya. Misalnya, tindakan siber kelompok teroris, mata-mata dan penjahat terorganisir bisa berbahaya dan tampak agresif tetapi

[19] Permanasari. "Terorisme Siber, Perang Siber & Hukum Humaniter: Tantangan Bagi Kerangka Hukum Indonesia tentang Pertahanan Siber", *Tri Jurnal,* Vol. 1, 2018. Hlm. 2

mereka tidak dengan sendirinya berevolusi menjadi tindakan perang siber.20 Cornish, dkk juga menjelaskan bahwa,

"Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target."

Maknanya, perang cyber dapat menjadi konflik antar negara, dan bisa juga melibatkan aktor non-negara dalam berbagai cara. Dalam perang cyber, sangat sulit untuk mengarahkan kekuatan yang tepat dan proporsional; targetnya bisa militer, industri atau sipil atau bisa juga ruang server yang menampung berbagai klien, dengan hanya satu di antaranya yang menjadi target.

Selanjutnya Hruza dan Cerny21 menjelaskan bahwa Perang cyber telah didefinisikan sebagai tindakan oleh negara-bangsa untuk menembus komputer atau jaringan negara lain dengan tujuan menyebabkan kerusakan atau gangguan. Namun dalam definisi lain, aktor non-negara juga dapat menjadi subjeknya dalam tindakan ini, seperti kelompok teroris, perusahaan, politik atau kelompok ekstremis ideologis, peretas, dan organisasi kriminal transnasional.

Cyber warfare mengacu pada penggunaan teknologi untuk melancarkan serangan terhadap negara, pemerintah dan warga negara, yang menyebabkan kerugian yang sebanding dengan peperangan yang sebenarnya menggunakan persenjataan. Sangat sulit untuk mengetahui siapa yang meluncurkan serangan cyber warfare. Itulah sebabnya entitas pemerintah menetapkannya sebagai kemampuan perang. Dengan begitu, penting bagi organisasi militer dalam hal ini TNI, mengambil langkah offensive dan defensive dalam menghadapi ancaman siber.

---

[20] David Livingstone Cornish, Dave Clemente & Claire Yorke. *On Cyber Warfare.* (London: The Royal Institute of International Affairs, 2010). Hlm. viii

[21]Hruza & Cerny, "Cyber Warfare", *International Conference Knowledge-Based Organization,* Vil. XXIII, No. 1, 2017. Hlm. 155

Ancaman cyber crime dianggap sebagai kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan atau gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan sehingga mengancam kerahasiaan (confidentiality), integritas (integrity), dan ketersedian (availability) sistem dan informasi.22

Ancaman siber dapat terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu dalam aspek kehidupan masyarakat dapat menimbulkan berbagai ancaman fisik, baik nyata ataupun yang tidak nyata dengan menggunakan kode-kode komputer (software) untuk melakukan pencurian informasi (information theft), kerusakan sistem (system destruction), manipulasi informasi (information corruption) atau perangkat keras (hardware) untuk melakukan gangguan terhadap sistem (network instruction) ataupun penyebaran data dan informasi tertentu untuk melakukan kegiatan propaganda.23

Cyber Security atau keamanan siber tidak pernah statis karena infrastruktur informasi terus berkembang. Cyber security tidak hanya berbicara tentang keamanan secara sempit yakni pada perangkat, namu juga berbicara tentang keamanan negara, termasuk di dalamnya keamanan sipil dan militer.

Pada sisi ini jelas bahwa urgensi pembentukan kesiapan cyber security oleh organisasi militer berkaitan dengan bagaimana organisasi militer sebisa mungkin dapat mengantisipasi berbagai ancaman siber termasuk didalamnya kegiatan cyber crime yang merugikan.

Sergei menjelaskan bahwa hubungan sipil militer dapat ditingkatkan melalui mekanisme yang berbeda, dengan memfasilitasi pertukaran informasi antar berbagai pihak dan pemangku kepentingan. Peran dan tanggung jawab yang tepat dari badan intelijen dalam lanskap siber nasional sangat penting di banyak negara. negara harus menyadari bahwa semua pengatuan kelembagaan, seperti keamanan komandan militer

[22] Iwan. *Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber.* (JakartaL Universitas Pertahanan Indonesia, 2012). Hlm.32
[23] Ibid. Iwan. Hlm. 33

untuk pusat siber, serta susunan strategi keamanan siber, hal ini tidak hanya melayani tujuan nasional namun juga memiliki fungsi deklaratori yang kuat jika berhadapa dengan negara atau pihak lain.24

Istilah cyber defense atau pertahanan siber (negara) mengacu pada semua langkah untuk mempertahankan ruang siber dengan militer dan sarana yang tepat untuk mencapai tujuan strategis militer. Pertahanan dunia maya adalah sistem yang terintegrasi, yang terdiri dari implementasi semua tindakan yang berkaitan dengan TIK dan keamanan informasi, kemampuan operasi jaringan komputer serta dukungan kemampuan fisik tentara.25 Dengan perkembangan teknologi informasi saat ini mengambil bagian dari dinamisnya jenis ancaman, maka kesiapan dan strategi operasionalisasi cyber warfare di lingkungan TNI AD berperan penting dalam memajukan agenda nasional terkait cyber security yang mana berpotensi membuka jenis ancaman negara ke tahap yang lebih luas.

3. Pembahasan

3.1 Perkembangan Cyber Warfare di Lingkungan TNI AD

Setiap organisasi militer negara di dunia harus mengembangkan kekuatan dan pengamanan di dunia maya mengingat banyak sekali ancaman yang dilakukan oleh pihak-pihak tertentu di dunia maya. Banyak sekali contoh kasus bagaimana sebuah situs atau website di suatu negara diretas atau disadap oleh pihak-pihak yang tidak bertanggungjawab.

Hal ini mengindikasikan bahwa setiap organisasi militer negara di dunia termasuk Indonesia harus mampu mengembangkan kesiapan dari cyber defence agar dapat menahan serangan dunia maya dari berbagai pihak yang akan melakukan peretasan, penyadapan, dan pengrusakan terhadap berbagai sistem, software, maupun

[24]Caitriona Sergei & Matthijs. *Civil-Military Relations and International Military Cooperation in Cyber Security: common Challenges & State Practices Across Asia and Europe.* (Tallinn: NATO OCS COE Publication, 2015). Hlm. 78-79

[25] Cijic, "Cyberlaw*", Revista Cyberlaw,*No. 1, 2016. Hlm. 11

perangkat lunak lainnya di lingkungan TNI AD. Semua sub kesatuan yang tergabung dalam organisasi TNI AD pada dasarnya harus memiliki komposisi kesiapan pertahanan siber yang dapat mengantisipasi berbagai serangan terhadap fasilitas TNI AD.

Sejak 1998 Indonesia sebenarnya telah melakukan cyber war dengan negara lain, hal itu terkait masalah politik dan sosial yang terjadi, misalnya ketika terjadi kerusuhan rasial, Indonesia berperang di dunia maya dengan para hacker dari China dan Taiwan. Sementara pada 1999 juga muncul kerusuhan di dunia maya antara Indonesia dan Portugal menyangkut kasus Timor Timur. Bahkan ketika terjadi cyber war dengan Portugal, saling serang terjadi hingga masuk sistem dan mampu menghapus semua data. Pada tanggal 6 Agustus 2010, Symantec sebagai produsen Antivirus Norton, mengumumkan bahwa Indonesia berada di urutan kedua setelah Iran di antara 10 negara yang mengalami serangan worm Stuxne.26

Dalam beberapa tahun terakhir terjadi perang siber antara Indonesia dengan Malaysia dimana saling susup antara hacker kedua negara mewarnai perseteruan ini. Aksi ini biasanya terjadi ketika muncul konflik politik ataupun persaingan kedua negara. Meskipun tidak melibatkan pemerintah kedua negara, namun aksi para hacker ini menyerang fasilitas siber milik pemerintah Malaysia maupun Indonesia. Selain itu insiden penyalahgunaan gedung perwakilan diplomatik Australia terhadap penyadapan Kepala Negara Republik Indonesia yang menyebutkan Kedutaan Besar Australia di Jakarta menjadi lokasi penyadapan terhadap pemerintah Indonesia berdasarkan informasi dari Media Internasional Sydney Morning Herald 31 Oktober 2013.

Temuan menunjukan bahwa perkembangan teknologi telah diikuti dengan semakin menguatnya cyber warfare, sebagaimana hasil penelitian menunjukan bahwa serangan siber lebih kepada perusakan sistem yang tidak langsung dapat menghasilkan profit finansial/pencurian dana, tapi lebih kepada pencurian informasi-inforamsi terkait

[26] Sa'diyah & Vinata. "Rekonstruksi Pembentukan *National Cyber Defense* sebagai Upaya Mempertahankan Kedaulatan Negara.", *Jurnal Perspektif*, Vol. 21, No. 3, 2016. Hlm. 169

strutkur operaisonal pertahanan negara sebagaimana Cyber warfare dilingkungan TNI AD berkaitan dengan beberapa aspek seperti:

Pengumpulan Informasi.

Spionase cyber merupakan bentuk aksi cyber warfare yang ditujukan kepada organisasi TNI AD. Spionase cyber biasanya dilakukan oleh negara lain melalui aktivitas rahasia dan sensitif dalam rangka penyerapan informasi terkai postur pertahanan TNI AD.

Metode yang digunakan dengan cara eksploitasi secara ilegal melalui internet, jaringan, perangkat lunak dan atau komputer negara lain. Hasil wawancara dengan Paban III Siapsat menunjukan bahwa pengumpulan infomasi dalam siber merupakan bagian dari kegiatan intelijen di dunia maya. Mereka yang melakukan pengumpulan informasi biasanya hanya memata-matai dan tidak melakukan operasi fisik. Namun dari hasil memata-matai tersebut dapat juga selanjutnya dilakukan operasi fisik tergantung informasi apa yang mereka dapatkan.

Pengumpulan informasi terhadap organisasi TNI AD penting bagi negara lain dalam rangka mengukur sejauhmana perkembangan pertahanan TNI AD, hal ini berkaitan dengan upaya menggambarkan berbagai titik-titik kelemahan TNI AD yang tentunya dapat dimanfaatkan dalam rangka melemahkan sistem pertahanan maupun mengantisipasi informasi dari kebihakan-kebijakan yang akan diambil yang berkaitan dengan pertahanan negara.

Vandalism.

Vandalism adalah serangan yang dilakukan sering dimaksudkan untuk merusak halaman web atau Deface, atau menggunakan serangan denial of service yaitu merusak sumber daya dari komputer lain.27 Adapun vandalism berkaitan dengan individu/kelompok yang ingin merusak infrastruktur informasi semata-mata untuk kesenangan dan kesenangan mereka sendiri. Hasil wawancara dengan Paban III Siapsat

[27] Michael Evans. "From Kadesh to Kandahar: Military Theory and The Future of War", *Journal Naval War College Review,* Summer 20, 2003. Hlm. 136

menjelaskan bahwa motivasi utama mereka bukan finansial, itu adalah keinginan untuk membuktikan bahwa prestasi dapat dicapai. Begitu masuk mereka meninggalkan bekas mereka sehingga tidak dapat disangkal keberadaan mereka. Jenis serangan ini termasuk dalam kategori serangan DOS atau Denial of Service. Situs yang terkena dampak harus dimatikan dan diperbaiki sebelum dapat kembali ke operasi normal.

Hasil observasi menunjukan bahwa serangan yang dilakukan sering dimaksudkan untuk merusak halaman web (Deface) TNI AD, atau menggunakan serangan denial-of-service yaitu merusak sumberdaya dari komputer lain. Dalam banyak kasus, hal ini dapat dengan mudah dikembalikan oleh Staf Operasi Markas Besar TNI AD. Deface sering dalam bentuk propaganda. Selain penargetan situs dengan propaganda, pesan politik dapat didistribusikan melalui internet via email, instant messges, atau pesan teks masih menjadi bagian dari cyber warfare Staf Operasi Markas Besar TNI AD.

Sabotase.

Sabotase didefinisikan sebagai tindakan yang disengaja dan berbahaya yang mengakibatkan terganggunya proses dan fungsi normal atau penghancuran atau kerusakan peralatan atau informasi.

Sabotase merupakan kegiatan militer yang ditujukan pada TNI AD dengan menggunakan komputer dan satelit untuk mengetahui koordinat lokasi dari peralatan TNI AD yang memiliki resiko tinggi jika mengalami gangguan. Sabotase dapat berupa penyadapan informasi dan gangguan peralatan komunikasi sehingga semua menjadi rentan terhadap gangguan. Sabotase dapat berupa software berbahaya yang tersembunyi dalam hardware komputer yang dimiliki TNI AD.

Temuan dari aktivitas cyber warfare tersebut jelas mengindikasikan bahwa setiap organisasi militer di dunia harus mampu mengembangkan kekuatan pertahanan cyber agar dapat menyerang atau setidaknya mempertahankan inforamsi dari aktivitas cyber warfare seperti peretasan, penyadapan, dan pengrusakan terhadap berbagai sistem,

software, maupun perangkat lunak lainnya. Pada sisi ini jelas bahwa terdapat dampak negarif siber terdapat juga nilai positif untuk membangun pertahanan siber. Dikemukakan oleh Paban III bahwa tidak semua urusan teknologi berkaitan dengan ancaman, ada juga yang berkaitan dengan bagaimana mengatasi ancaman.

TNI AD sebagai lembaga militer menyadari bahwa ancaman keamanan global sekarang ini tidak hanya bersifat fisik semata, melainkan ancaman yang bersifat virtual, digital, dan dunia maya, berupa aksi kejahatan yang menyerang situs, website maupun berbagai instalasi dunia maya lainnya. Inilah yang kemudian melahirkan ancaman baru dalam dunia internasional, berupa ancaman perang cyber warfare di lingkungan TNI AD.

3.2 Tingkat Kesiapan Operasi Markas Besar TNI AD

Kesiapan operasi merupakan hal penting, untuk itu tim cyber masih disempurnakan dalam hal organisasi. Untuk itu TNI AD juga memperkuat pembinaan. Selanjutnya hasil dari wawancara dengan Pabandya Dok menjelaskan bahwa kesiapan bukan hanya sekedar alutsista, tapi bisa saja terkait cyber yang tentunya penting disiapkan khususnya dalam prianti lunak atau doktirin pertempurannya.

Tujuan dari kesiapan operasi Markas Besar TNI AD dalam menghadapi cyber warfare yaitu menyelenggarakan fungsi staf umum TNI Angkatan Darat dibidang pembinaan, pengendalian kekuatan dan kemampuan operasi yang meliputi pembinaan doktrin, pembinaan organisasi, pembinaan latihan dan peningkatan mutu tempur satuan serta penyiapan/penyediaan kekuatan dalam cyber warfare. Pada sisi ini jelas bahwa kesiapan cyber warfare berkaitan dengan bagaimana Staf Operasi memiliki penyiapan/penyediaan kekuatan.

Kesiapan offensive adalah serangan atau sesuatu hal yang bersifat agresif yang digunakan untuk menyerang yang mengakibatkan timbulnya gangguan dan ketidaksenangan. Sedangkan kesiapan defensive adalah suatu hal yang bersifat

melindungi seseorang atau sesuatu terhadap serangan, menjaga keamanan, membentengi diri.

Kesiapan operasi defensif dalam menghadapi cyber warfare berkaitan dengan operasi untuk mengalahkan serangan musuh, mendapatkan waktu, menghemat pasukan, dan mengembangkan kondisi yang menguntungkan untuk operasi ofensif atau stabilitas. Kekuatan yang melekat pada pertahanan operasi Markas Besar TNI AD adalah kemampuan bek untuk menduduki posisi siber sebelum serangan dan menggunakan waktu yang tersedia untuk meningkatkan pertahanan itu.

Temuan menunjukan bahwa Staf Operasi Mabes TNI AD dalam menghadapi cyber warfare tidak hanya menunggu secara pasif untuk diserang. Staf Operasi Mabes TNI AD secara agresif mencari cara untuk menarik dan melemahkan pasukan musuh ketika mereka mempersiapkan penyerangan. Biasanya hal ini ketika diwali dengan inforamis intelijen terkait persiapan musuh untuk menyerang. Hal ini dapat diketahui melalui software yang menjelaskan pada web akan menjadi target serangan. Sebuah manuver Staf Operasi Mabes TNI AD dalam menghadapi cyber warfare untuk menempatkan pasukan musuh pada posisi yang tidak menguntungkan dan menyerang pasukan musuh tersebut di setiap kesempatan. Pada operasionalnya Staf Operasi Mabes TNI AD yang bertahan berusaha untuk mendapatkan kembali inisiatif dari menyerang pasukan musuh dalam sistem siber.

Staf Operasi Mabes TNI AD berusaha untuk mengacaukan serangan siber dengan menggunakan tindakan yang menyinkronkan persiapan pasukan siber musuh. Tindakan gangguan termasuk menipu atau menghancurkan pasukan pengintaian musuh, memecah formasi data, dan menghalangi kemampuan pasukan musuh untuk menyinkronkan serangan gabungan siber. Staf Operasi Mabes TNI AD dalam menghadapi cyber warfare melakukan serangan siber merusak. Staf Operasi Mabes TNI AD melakukan serangan balik untuk menyangkal musuh yang memaksa kemampuan untuk mengeksploitasi. Kekuatan pertahanan Staf Operasi Mabes TNI AD menggunakan peperangan elektronik dan aset ruang siber di samping sistem

mematikan untuk menargetkan komando dan sistem kontrol musuh dan mengganggu pasukan musuh secara mendalam.

Kesiapan Staf Operasi Mabes TNI AD pada dasarnya memiliki kesiapan yang cukup dalam rangka cyber warfare. Kesiapan defensive tercermin ketika berbagai hubungan dari siber dilingkungan TNI AD memiliki pola defensive dalam rangka mengantisipasi berbagai serangan pengumpulan informasi, vandalism dan sabotase kepada fasilitas ataupun indivdu dari pejabat strategis dalam lingkungan TNI AD. Pada lingkungan tersebut kesiapan defensive mencerminkan bagaimana Staf Operasi Mabeas TNI AD dapat menjaga sumber daya informasi yang jamak digunakan dalam cyber warfare. Perlu ditekankan bahwa informasi adalah modal awal bagaimana cyber warfare dapat dilakukan. Cyber warfare tidak dapat terlaksana ketika informasi awal belum didapatkan oleh penyerang dimana hal ini berkaitan dengan prioritas target.

Adapun skema kesiapan defensive dan kesiapan offensive menunjukan bahwa tingkat kesiapan operasi Markas Besar TNI AD dalam menghadapi cyber warfare sudah terbangun walaupun piranti lunak yang tersedia belum sepenuhnya memenuhi operasional. Temuan ini menunjukan bahwa operasional bersifat kebutuhan ancaman yang tentunya berkaitan dengan bagaimana mengankan informasi dan mencari informasi meski hal ini bersifat aksidental. Selanjutnya dalam sisi ini dijelaskan bahwa terdapat serangan yang berkaitan dengan infomasi itu sendiri, yaitu:

Informasi, seperti mencuri informasi dari perangkat penyimpanan misalnya.

Proses berbasis informasi, menyerang proses yang mengumpulkan, menganalisis, dan menyebarluaskan informasi menggunakan media atau bentuk apa pun dan menyerang jaringan.

Sistem informasi dan komunikasi, serangan terhadap infrastruktur, organisasi, personel dan komponen yang mengumpulkan, memproses, menyimpan, mengirimkan, menampilkan, menyebarluaskan, dan bertindak berdasarkan informasi.

Berdasarkan temuan tersebut jelas bahwa kebutuhan inforamsi menjadi bagian dari awal mula cyber warfare. Maksudnya adalah cyber warfare membutuhkan infomasi awal karena hal ini berkaitan dengan infomasi awal yang terususun terhadap targer. Pada sisi ini biasanya mereka baru melakukan cyber crime dan ini menjadi bagian dari Staf Operasi Mabes TNI AD. Ketika hal tersebut di deteksi maka langkah offensive menjadi pilihan dimana disini lah cyber warfare terjadi. Mereka melakukan penyadapan infomasi, vandalism dan sabotase yang tentunya penting untuk disiapkan oleh Mabes TNI AD.

Pada dasarnya kesiapan defensive Staf Operasi Markas Besar TNI AD berkaitan dengan menjaga sumber daya informasi di lingkungan TNI AD yaitu melalui kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk menjaga sumber daya informasi lingkungan siber dan organisasi serta aset di lingkungan TNI AD. Organisasi dan aset tersebut mencakup perangkat komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirim dan atau disimpan di lingkungan maya.

Kesiapan defensive Staf Operasi Markas Besar TNI AD menjaga sumber daya informasi begitu berkaitan dengan informasi-informasi strategis negara khususnya pertahanan yang tentunya membutuhkan langkah-langkah pengamanan.

Adapun penerapan defensive Staf Operasi Markas Besar TNI AD sebagaimana hasil wawancara dengan Paban III Siapsat menjelaskan bahwa menjadi keniscayaan dan merupakan suatu prioritas kewajiban bagi negara dan semua instansi di dalamnya dimana tingkat pentingnya berbanding lurus dengan tingkat ketergantungan pada pemanfaatan di ruang siber tersebut.

Hal ini menyebabkan Kemhan/TNI berkewajiban untuk mengambil langkah-langkah penting terkait dengan pertahanan siber, baik di dalam lingkungannya sendiri maupun dalam rangka mendukung pertahanan siber lintas sektoral. Pertahanan siber

perlu dilaksanakan secara terencana dan terpadu agar penerapannya dapat berjalan secara tepat dan optimal. Pada sisi lain keamanan siber tidak dapat diabstraksikan terlalu jauh dari wilayah aplikasinya dan lingkungan sosial kultural.

Kesiapan defensif adalah proteksi perlindungan dunia maya dari sumber-sumber bahaya cyber warfare. Sedangkan cyber defense adalah segala bentuk usaha untuk mempertahankan keamanan cyber dalam cyber warfare. Kesiapan difensif berbeda dengan security atau keamanan biasa karena ancaman cyber dalam cyber warfare tidak bisa dimasukan begitu saja ke dalam kategori keamanan tradisional. Selain berasal dari dalam negeri, ancaman cyber atau cyber threats juga datang dari luar negeri. Namun, ancaman ini jarang mencapai taraf yang membutuhkan respon agresi militer karena apapun yang akan dilakukan pemerintah dalam menanggapi ancaman cyber ini akan memiliki implikasi domestik dan internasional

Konsep dari kesiapan defensive Staf Operasi Markas Besar TNI AD menjaga sumber daya informasi berkaitan dengan 4 (empat) aspek kemaanan, seperti internet secruity, ICT security, information security, sedangkan kesiapan offensive berkaitan dengan digital security . Pada operasionalnya information security berkaitan bagaimana Staf Operasi Markas Besar TNI AD berperan menjaga aset informasi sebagaimana salah satu fungsi dari operasi yaitu menjaga sumber daya informasi TNI AD dan menjaga keamanan informasi infrastruktur kritis TIK TNI AD agar terlindung dari gangguan dan penyalahgunaan atau pemanfaatan pihak-pihak lain.

Definisi keamanan informasi termasuk juga kerahasiaan, integritas, dan ketersediaan informasi, tetapi dapat mencakup karakteristik tambahan. Penting untuk dicatat bahwa ada perbedaan antara keamanan informasi dan teknologi informasi (atau teknologi informasi dan komunikasi) keamanan.

Jaminan keamanan terkait informasi-informasi pertahanan dilingkungan TNI AD menjadi tanggungjawab Staf Umum Operasi Angkatan Darat. Pada konteks tersebut operasionalisasi kesiapan Staf Umum Operasi Angkatan Darat sesungguhnya berkaitan dengan keamanan informasi seperti tercantum pada tugas dalam menjaga sumber daya

informasi TNI AD agar terlindung dari gangguan dan penyalahgunaan atau pemanfaatan pihak-pihak lain ataupun terkait menjaga keamanan informasi infrastruktur kritis TIK TNI AD.

Pada kasus keamanan informasi Staf Umum Operasi Angkatan Darat, TIK adalah infrastruktur yang memproses, menyimpan, dan mengkomunikasikan informasi. Dalam hal ini adalah informasi yang dianggap sebagai aset yang memerlukan perlindungan oleh Staf Umum Operasi Angkatan Darat. Teknologi informasi dan komunikasi pada Staf Umum Operasi Angkatan Darat dapat diklasifikasikan sebagai kerentanan yang ditargetkan oleh berbagai ancaman dalam mencoba untuk mengkompromikan aset yaitu informasi.

Selanjutnya dalam tahap kesiapan offensive, kesiapan menyerang tentu berkaitan dengan cara-cara agresif, prajurit tentu harus siap dalam keadaan menyerang ketika dibutuhkan, walaupun hal ini masih pada tahap sederhana, tapi ini akan berkelanjutan untuk dapat menyerang secara agresif dan tepat. Staf Umum Operasi Angkatan Darat melakukan offensive untuk mengalahkan dan menghancurkan pasukan musuh serta mendapatkan kendali atas medan, sumber daya, dan pusat populasi.

Staf Umum Operasi Angkatan Darat juga dapat melakukan offensive untuk menipu atau mengalihkan kekuatan musuh, mengembangkan kecerdasan, atau menahan kekuatan musuh di posisi. Staf Umum Operasi Angkatan Darat menangkap, mempertahankan, dan mengeksploitasi inisiatif ketika melakukan offensive. Operasi spesifik dapat berorientasi pada pasukan musuh atau sasaran medan untuk mencapai posisi yang relatif menguntungkan. Mengambil inisiatif dari pasukan musuh membutuhkan tindakan offensive, bahkan dalam pertahanan.

Staf Umum Operasi Angkatan Darat berkaitan dengan digital security yaitu berkaitan dengan countering risk. Staf Umum Operasi Angkatan Darat menyelenggarakan offensive cyber warfare, menjaga sumber daya informasi TNI AD berkaitan dengan beragai aktivitas, seperti bagaimana Staf Umum Operasi Angkatan Darat berperan dalam pencegahan serangan dimana berkaitan dengan penerapan arsitektur

pengamanan tingkat tinggi yaitu membuat, mengimplementasikan dan mengoperasikan secara efektif arsitektur yang mencakup seluruh tahap siklus pertahanan siber agar mampu mengatasi ancaman terhadap faktor orang, logikal dan teknologi dari penyerang yang memiliki sumber daya yang besar dan akses yang luas dari berbagai aspek antara lain keuangan, teknologi, intelijen dan politik.

Selanjutnya dalam tahap pemantauan pengamanan informasi, Staf Umum Operasi Angkatan Darat melakukan peranan pengawasan baik itu logikal atau fisik serta mendekteksi berbagai proses yang tidak dapat terotoritasi. Pada sisi lain pemantauan juga berkaitan dengan proses analisa dalam rangka membentuk pengamanan informasi yang terjaga. Pada pemantauan pengamanan informasi juga Staf Umum Operasi Angkatan Darat berperan dalam pengalihan serangan sehingga sistem urama dapat terhindar dari serangan siber. Terakhir tahap ini juga berhubungan dengan pemberian peringatan oleh Staf Umum Operasi Angkatan Darat pada berbagai aktivtias serangan yang muncul dalam pertahanan Indonesia.

Hasil penelitian juga menunjukan bahwa pada tahap analisis serangan yang dilakukan, Staf Umum Operasi Angkatan Darat telah melakukan analisa peringatan serangan yaitu memberikan dukungan yang efektif dari arsitektur pengamanan. Staf Umum Operasi Angkatan Darat juga menganalisis piranti lunak yang berbahaya dan melakukan investigasi forensik digital secara efektif sesuai dengan prosedur untuk memastikan integritas hasil dari proses yang dilakukan.

Pada tahap pertahanan dapat diketahui bahwa Staf Umum Operasi Angkatan Darat melakukan isolasi serangan yaitu dengan mengisolasi serangan dengan dukungan implementasi yang efektif dari arsitektur pengamanan tingkat tinggi yang telah ditetapkan, guna mengurangi dampak yang ditimbulkan. Selain itu Staf Umum Operasi Angkatan Darat menemukan backdoor, trojan dan malware lainnya agar tidak menjadi potensi ancaman dikemudian hari. Staf Umum Operasi Angkatan Darat juga memperbaiki sistem dan data yang telah diserang dan melakukan pemulihan sistem dan data ketika terjadi bencana. Adapun Staf Umum Operasi Angkatan Darat juga

melakukan pertimbangan hukum dan diplomatik untuk menentukan langkah-langkah selanjutnya, termasuk melaporkan ke otoritas hukum dan memilih opsi serangan balik atau tidak. Terakhir Staf Umum Operasi Angkatan Darat melakukan koordinasi penanganan serangan dengan organisasi-organisasi terkait.

Tahap serangan balik dapat diketahui bahwa serangan balik merupakan suatu pilihan yang dipertimbangkan secara matang baik dari sisi hukum dan diplomasi. Beberapa contoh serangan balik yang dapat dilakukan oleh tim khusus Staf Umum Operasi Angkatan Darat, antara lain peretasan, penanaman malware, perusakan sistem dan rekayasa kondisi. Tahap Peningkatan Pengamanan Informasi. Peningkatan pengamanan informasi harus selalu dilakukan berdasarkan hasil-hasil pada tahapan-tahapan sebelumnya. Peningkatan pengamanan dapat dilakukan pada salah satu atau keseluruhan dari faktor-faktor arsitektur pengamanan informasi meliputi pengamanan SDM, pengamanan logikal dan pengamanan fisik.

Namun diluar temuan tersebut, kesiapan Staf Operasi Markas Besar TNI AD masih terdapat permasalahan misalnya terdapat dua fungsi Staf Operasi Markas Besar TNI AD yang masih belum optimal khususnya terkait upaya untuk mendorong partisipasi aktif pemanfaatan ruang siber yang aman melalui kerjasama kemitraan nasional dan internasional lintas sektoral dan menyelenggarakan dan mengembangkan pengelolaan kelembagaan Pertahanan Siber yang bertanggung jawab, efektif, efisien dan akuntabel.

Adapun anggaran menjadi kesiapan Staf Operasi Markas Besar TNI AD dalam melaksanakan operasi menghadapi cyber warfare yang tersedia masih mengikuti pada anggaran umum tidak kepada anggaran khusus dalam operasi menghadapi cyber warfare. Selain itu temuan lain menunjukan bahwa masing-masing aktor masih terhambat pada tugas dan fungsi lembaga siber dalam hal menjaga sumber daya informasi. Dimana kerjasama dalam sinergiritas dalam menjaga sumber daya informasi masih belum dilakukan secara komprehensif dan berjalan secara parsial.

4. Simpulan

Atas dasar temuan-temuan empiris dari penelitian ini, dapat disimpulkan, sebagai berikut:

Perkembangan teknologi informasi dan komunikasi berdampak pada semakin masifnya cyber warfare di lingkungan TNI AD. Pelaksanana cyber warfare di lingkungan TNI AD berkaitan dengan usaha kelompok/organisasi/negara untuk melakukan pengumpulan informasi, vandalism dan sabotase. Temuan menunjukan bahwa hal yang paling sering dalam cyber warfare usaha untuk mendapatkan informasi-inforamsi strategis di lingkungan TNI baik bersifat kebijakan ataupun inforamsi bersifat fasilitas strategis TNI AD.Dalam praktiknya kekhasan Tim SAR Tempur dalam Operasi Pembentukan dan Pengoperasian Pangkalan Udara Depan (OP3UD) sangat dibutuhkan dalam membantu terciptanya operasi SAR yang berkelanjutan dengan hadirnya sarana prasarana terbatas semacam itu.

Tingkat pengerahan kesiapan operasi Staf Operasi Markas Besar TNI AD dalam menghadapi cyber warfare terbagi menjadi dua, yaitu kesipan offensive dan kesiapan defensive. Kesiapan defensive berkaitan dengan bagaimana Staf Operasi malakukan internet secruity, ICT security dan information security. Sedangkan kesiapan offensive berkaitan dengan digital security seperti serangan balik. Hasil dari penelitian ini juga menemukan bahwa kesiapan masih bermasalah terkait serang balik siber termasuk didalamnya terbatasnya anggaran, infrastukur dan SDM.

Strategi meningkatkan kesiapan operasi Markas Besar TNI AD dalam menghadapi cyber warfare yaitu dengan melakukan evaluasi secara komprehensif terkait kesiapan. Sedangkan strategi dalam anggaran yaitu dengan penyusun skala prioritas sesuai dengan kebutuhan operasi. Strategi infrastruktur yaitu dengan melakukan pengadaan secara bertahap dengan memperhitungkan kemandirian baik dari software dan hardware dalam cyber warfare.

Berdasarkan kesimpulan penelitian, terdapat beberapa rekomendasi yang dapat dikemukakan, yakni: Penelitian lanjutan, penelitian ini dapat dilanjutkan oleh peneliti selanjutnya khususnya terkait aspek-aspek diluar fokus penelitian yaitu penelitian lanjutan terkait penggabungan lembaga siber, formulasi sinergiritas lembaga siber dan ancaman siber di masa depan pada lingkungan TNI AD. Dengan demikian hasil penelitian lanjutan dapat membangun gambaran secara komprehensif terhadap perkembangan siber secara menyeluruh.

Dukungan Komando Atas, dukungan Komando Atas penting untuk dibangun dimana komando Atas berkaitan dengan hal-hal subtansial yang dapat mempengaruhi operasional kesiapan. Dukungan ini dapat difokuskan pada pemenuhan anggaran, infrastruktur dan personel. Dengan demikian, dukungan Komando Atas akan membentuk kesiapan Staf Operasi yang optimal dalam menghadapi cyber warfare.

Program Kemitraan, Staf Operasi Mabes TNI AD agar melakukan program kemitraan dengan lembaga eksternal dalam mendukung berbagai kebutuhan operasionalisasi cyber warfare dilingkungan TNI AD. Kemitraan dapat dibangun sehingga biaya kesiapan dapat ditekan dimana satu sama lain dapat memenuhi kebutuhan sesuai perannya masing-masing.

Rekruitmen Khusus. Staf Operasi Mabes TNI AD agar melaksanakan rekruitmen para Hacker yang memiliki kemampuan untuk dijadikan sebagai personel eksternal personel TNI AD. Hal ini bukan saja lebih efektif, tapi lebih efisien dalam penggunaan sumber daya dibanding harus memulai dari awal yang tentunya belum tentu secara masif dapat meningkatkan kesiapan Staf Operasi.

Penyusunan Regulasi. Markas Besar TNI AD agar melakukan penyusunan regulasi penting dimana memperjelas tupoksi masing-masing dalam rangka cyber warfare khususnya memberikan ruang bagi TNI AD dalam penindakan. Hal ini urgensi untuk dilakukan karena berhubungan dengan pentingnya responsivitas penindakan.

Kemandirian Bank Data, Markas Besar TNI AD agar m membangun sebuah sistem kemandirian bank data dalam pengolahan data khususnya bagi aset bernilai strategis sehingga mampu menciptakan sebuah jaminan keamanan yang maksimal.

Organisasi, Markas Besar TNI AD agar membentuk organisasi Pusat Siber dan Sandi Angkatan Darat dimana organisasi ini berdiri di bawah Kasad. Organisasi ini dapat disusun dengan memperhatikan kedudukan dan fungsi satuan lain termasuk didalamnya Intelijen dan Staf Operasi Angkatan Darat. Dengan demikian, kesiapan dalam menghadapi cyber warfare di lingkungan TNI AD dapat berjalan optimal.

Daftar Pustaka

Buku

Arikunto, Suharasimi. 2001. Dasar-Dasar Evaluasi Pendidikan (edisi revisi). Jakarta: Bumi Aksara.

Badri, Muhammad. 2012. Perang Cyber dalam Dinamika Komunikasi Internasional. Pekanbaru: Universitas Islam Riau.

Cornish, David Livingstone, Clemente, Dave & Yorke, Claire. On Cyber Warfare. 2010. London: The Royal Institute of International Affairs.

Hadi Irandoost, Deniele. 2018 Cybersecurity: A National Security Issue?. E-International Relations.

Iwan. 2012. Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber. Jakarta Universitas Pertahanan Indonesia.

Rheingold, H.. 2012. New Smart: How to Thrive Online. Cambridge: The Mit Press.

Salahuddien, M.. 2011. Pertahanan Keamanan Informasi Nasional. Indonesia Security Incident Response Team on Internet Infrastructure.

Sergei, Caitriona & Matthijs. 2015. Civil-Military Relations and International Military Cooperation in Cyber Security: common Challenges & State Practices Across Asia and Europe. Tallinn: NATO OCS COE Publication.

Slameto. 2010. Belajar dan Faktor yang Mempengaruhinya. Jakarta: Rineka Cipta.

Yusnawati. 2007. Perencanaan Pengajaran Berdasarkan Pendekatan Sistem. Jakarta: Bumi Aksara.

Jurnal

Ameli, Saied Reza. 2007. "Dual Spacization of Cultures: Problematization of Cyberspace and Cultural Matters", Journal of Cyberspace Policy Studies, Vol. 1, No. 1, Januari.

Ammar, Faruq & Usman. 2014. "Penyusunan Strategi dan Strategi Operasi Usaha Kecil dan Menengah pada Perusahaan Konveksi Scissors di Surabaya", Jurnal Manajemen Teori dan Terapan Tahun 7, No. 3.

Cijic. 2016 ."Cyberlaw", Revista Cyberlaw,No. 1.

Galinec, Darko & Guberina, Boris, 2017. "Cybersecurity and Cyber Defence: National Level Strategic Approach", Journal of Control, Measurement, Electronics, Computing and Communications, Vol. 58, No. 3.

Hruza & Cerny. 2017. "Cyber Warfare", International Conference Knowledge-Based Organization, Vil. XXIII, No. 1.

Jeffrey W., Meiser. 2017. "Are Our Strategic Models Flawed? Ends + Ways + Means = (Bad) Strategy", Journal Parameters, Vol. 46, No. 4.

Permanasari. 2018. "Terorisme Siber, Perang Siber & Hukum Humaniter: Tantangan Bagi Kerangka Hukum Indonesia tentang Pertahanan Siber", Tri Jurnal, Vol. 1.

Robinson, Kevin Jones & Janicke, Helge. 2015. "Cyber Warfare: Issues and Challenges", Journal of Computers and Security, Vol. 8.

Sa'diyah & Vinata. 2016. "Rekonstruksi Pembentukan National Cyber Defense sebagai Upaya Mempertahankan Kedaulatan Negara.", Jurnal Perspektif, Vol. 21, No. 3.

Thomposon, L. & Nadler, J. 2002. "Negotiatioing via Information Technology: Theory and Application", Journal of Social Issues, Vol. 58, No. 1.

Website

Hugh Taylor. 18 Desember 2018. What is Cyber Security. Diakses di: https://preyproject.com/blog/en/what-is-cyber-security/ (diakses pada 13/02/2020)

Hugh Taylor. 22 Januari 2020. What are Cyber Threats and What To Do about Them. Diakses di: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/ (diakses pada 13/02/2020)

The New York Times. 29 May 2009. *Text: Obama's Remarks on Cyber-Security.* Diakses di: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html (diakses pada 13/02/2020)