

Optimalisasi Peran Intelijen dalam Pemanfaatan Sistem Octopus (*Ocean Crime Prevention System*) Sebagai Upaya Deteksi Dini Terhadap Potensi Ancaman di Laut Indonesia

Muhammad Try Yusdi Anjas

Program Studi S1 Agen Intelijen, Sekolah Tinggi Intelijen Negara
Sumur Batu, Babakan Madang, Bogor, Jawa Barat 16810 Telp. (0251) 8271471
Email: mtryanjas@gmail.com

ABSTRAK

Sebagai negara maritim, Indonesia menyimpan potensi maritim yang melimpah. Potensi maritim tersebut belum dikelola secara optimal karena adanya kendala serta terdapat ancaman berupa kejahatan maritim. Ancaman yang terjadi sampai saat ini membuktikan bahwa laut Indonesia tidak aman. Oleh karena itu, peran intelijen penting digunakan dalam upaya deteksi dini dan peringatan dini terhadap keamanan laut di Indonesia dengan cara memanfaatkan penggunaan sistem informasi deteksi ancaman bidang maritim berbasis website yang diberi nama Ocean Crime Prevention System (Octopus). Sistem ini diciptakan untuk menghadapi tantangan keamanan maritim serta dinamika pada era industri 4.0 dengan menggunakan teknologi informasi. Penelitian ini menggunakan metode atau pendekatan kualitatif deskriptif yang akan memberikan gambaran mengenai ancaman-ancaman yang akan dihadapi Indonesia khususnya maritim. Penelitian ini menggunakan teori ketahanan maritim, teori artificial intelligence, teori media baru, ancaman, dan intelijen. Penelitian ini juga menjelaskan peran intelijen dalam mencegah serta menangkal ancaman yang terjadi di laut Indonesia melalui deteksi dini dan peringatan dini dengan memanfaatkan sistem Octopus sebagai upaya dalam peningkatan intensitas dan kualitas keamanan terhadap potensi ancaman di era siber. Hasil penelitian menunjukkan bahwa perlu adanya peningkatan terhadap sistem Octopus sebagai upaya intelijen di bidang maritim dalam mendeteksi potensi ancaman di laut Indonesia yang semakin kompleks. Selain itu, optimalisasi peran intelijen diperlukan dalam meningkatkan upaya deteksi dini dan peringatan dini dengan melakukan perbaikan kualitas sumber daya manusia dan teknologi serta melakukan kerja sama dengan lembaga maritim Indonesia untuk melakukan koordinasi.

Kata Kunci: Maritim, potensi ancaman, sistem Informasi, peran intelijen

ABSTRACT

As a maritime country, Indonesia has abundant maritime potential. This maritime potential has not been managed optimally due to obstacles and threats in the form of maritime crimes. The threat that occurs until now prove that the Indonesian seas are not safe. Therefore, the role of intelligence is important for early detection and early warning of maritime security in Indonesian by utilizing a website based maritime threat detection information system called the Ocean Crime Prevention System (Octopus). This system was created to face maritime security challenges and the dynamics of the industrial era 4.0 by using information technology. This research uses a descriptive qualitative method or approach that will provide an overview of threats that will be faced by Indonesian, especially maritime affairs. This research uses maritime resistance theory, artificial intelligence theory, new media theory, threats, and intelligence. This research also explains the role of intelligence in preventing and warding off threats that occur in Indonesian seas through early detection and early warning by utilizing the Octopus system as an effort to increase intensity and the quality of security against potential threats in the cyber era. The results show that there needs for improvements to the Octopus System as an intelligence effort in the maritime sector in detecting potential threats that increasingly complex in the Indonesian seas. In addition, optimizing the role of intelligence is needed for increasing early detection and early warning efforts by improving the quality of human resources and technology as well as cooperation with the institute of maritime Indonesia to conduct coordination.

Keywords: Maritime, potential threat, information system, the role of intelligence

PENDAHULUAN

Indonesia merupakan negara maritim yang memiliki banyak pulau serta sebagian besar wilayahnya berupa perairan dimana luas laut Indonesia lebih besar dibandingkan dengan luas daratan sehingga Indonesia termasuk kedalam negara yang memiliki wilayah laut terluas di dunia. Kekayaan alam pada laut Indonesia yang melimpah dimanfaatkan oleh pihak asing yang bersifat ilegal dan memiliki kepentingan sendiri sehingga berpotensi terjadinya ancaman bagi stabilitas keamanan dan kedaulatan negara, seperti kejahatan maritim, penggunaan teknologi informasi, serta cuaca. Sebagian besar nelayan Indonesia mengalami kendala dalam menangkap ikan karena masalah cuaca yang tidak dapat diprediksi akibat perubahan iklim yang menimbulkan gelombang besar dan angin kencang sehingga dapat membahayakan keselamatan nelayan. Berdasarkan letak geografisnya, Indonesia yang terletak diantara dua benua, yaitu benua ASIA dan Australia, serta berada diantara dua Samudera, yaitu Samudera Pasifik dan Samudera Hindia, sehingga Indonesia berada pada posisi silang. Dengan demikian, wilayah Indonesia berada pada posisi silang, yang mempunyai arti penting dalam kaitannya dengan iklim dan perekonomian.¹

Akibat dari posisi silang tersebut Indonesia menghadapi berbagai potensi ancaman geopolitik dan geostrategis yang dapat mengganggu keamanan dan kestabilan maritim Indonesia. Dalam konteks geopolitik, ancaman yang dihadapi Indonesia merupakan hubungan politik dan strategi negara dalam mempertahankan wilayah dari negara lain. Sedangkan geostrategis yaitu strategi negara dalam memanfaatkan kondisi lingkungan berdasarkan letak geografisnya.

Berdasarkan hal tersebut, pemerintah Indonesia melakukan pengajuan kepada Organisasi Maritim Internasional (IMO) tentang penetapan Alur Laut Kepulauan Indonesia (ALKI) di wilayah teritorial perairan Indonesia. Setelah disetujui, pemerintah Indonesia mengeluarkan Undang-Undang Nomor 6 Tentang Perairan Indonesia, sehingga ALKI merupakan alur laut yang dapat dilalui oleh kapal dengan cara normal, langsung dan secepat mungkin di atas perairan kepulauan dan laut teritorial yang berdampingan antara satu bagian laut lepas Zona Ekonomi Eksklusif (ZEE) Indonesia.²

Keterbukaan pada ALKI (Alur Laut Kepulauan Indonesia) ini menimbulkan potensi ancaman karena memungkinkan kapal dari berbagai negara dapat melewati jalur laut Indonesia secara bebas. Hal ini ditunjukkan oleh penggunaan ALKI sebagai sarana untuk melangsungkan pelanggaran teritorial dan tempat pengoperasian sarana prasarana militer berteknologi tinggi.³

Potensi ancaman lainnya yang menjadi atensi sejak lama adalah *illegal fishing*. Faktor-faktor yang menyebabkan terjadinya *illegal fishing* di perairan Indonesia tidak terlepas dari lingkungan strategis global terutama kondisi perikanan di negara lain yang memiliki perbatasan laut, dan sistem pengelolaan perikanan di Indonesia itu sendiri.⁴

Lemahnya pengawasan dan penegakkan hukum terhadap para pelaku *illegal fishing* tidak pernah jera. Proses hukum yang ada selama ini hanya menyentuh kalangan awak kapal semata tanpa berusaha mengungkap otak pelaku yang sesungguhnya, yaitu *corporate* yang membantu kegiatan tersebut.⁵

¹ Nur Lailatul Maghfiroh, "Letak Geografis Indonesia : Pengaruh dan Keuntungannya", diakses dari <https://akupintar.id/info-pintar/-/blogs/letak-geografis-indonesia-pengaruh-dan-keuntungannya-1>.

² Rikard Djegadut, "Alur Laut Kepulauan Indonesia Sebagai Poros Maritim Indonesia", Artikel, diakses dari <https://indonews.id/artikel/311469/Alur-Laut-Kepulauan-Indonesia-Sebagai-Poros-Maritim-Dunia/>

³ Poltak Partogi Nainggolan, "Indonesia dan Ancaman Keamanan di Alur Laut Kepulauan Indonesia (ALKI)", *Kajian*, Vol. 20, No. 3 (September 2015), hal. 195-196.

⁴ Nunung Mahmudah. *ILLEGAL FISHING* Pertanggungjawaban Pidana Korporasi di Wilayah Perairan Indonesia, (Jakarta Timur: Sinar Grafika, 2015), hal. 111.

⁵ *Ibid.*, hal. 2..

Berdasarkan pada kasus tersebut, berbagai macam tantangan yang bersifat kompleks terhadap ketahanan dan stabilitas keamanan nasional menjadi sebuah ancaman terhadap Indonesia, terkhusus potensi ancaman terhadap kejahatan maritim. Salah satu potensi ancaman maritim yang berbahaya adalah penyalahgunaan yang dilakukan oleh negara-negara maju dengan memanfaatkan teknologi, seperti penggunaan alat deteksi bawah laut, senjata rudal selam, pesawat tanpa awak, dan sistem informasi yang dapat mengetahui potensi maritim Indonesia. Dampak negatif yang paling nyata sering terjadi didalam perkembangan teknologi militer atau alat berperang yang sewaktu-waktu berpotensi mengancam kehidupan manusia.⁶

Oleh sebab itu, Badan Intelijen Negara (BIN) sebagai lembaga negara yang berwenang dalam menjaga kedaulatan negara melakukan kerjasama untuk memanfaatkan *surveillance system* berbasis *website* pada sistem Octopus sebagai langkah dalam memperkuat sistem keamanan maritime Indonesia. Sehingga, dapat memberikan informasi dan data untuk mendeteksi adanya ancaman laut di Indonesia

Berdasarkan latar belakang yang disampaikan, maka masalah yang dapat penulis rumuskan adalah sebagai berikut:

- 1) Bagaimana sistem Octopus dapat mendeteksi adanya potensi ancaman di laut Indonesia ?
- 2) Bagaimana optimalisasi peran intelijen dalam pemanfaatan sistem Octopus sebagai upaya deteksi dini terhadap potensi ancaman di laut Indonesia?

TINJAUAN PUSTAKA

Penelitian ini didasarkan pada teori *Sea Power*, *Artificial Intelligence*, teori Koordinasi, konsep Peran Intelijen, dan Konsep Potensi Ancaman.

Teori *Sea Power* atau kekuatan laut pertama kali dicetuskan oleh Sir Alfred Thayer Mahan⁷ yang memiliki beberapa prinsip dalam dasar-dasar pemikirannya mengenai pemberdayaan kekuatan laut dari suatu negara untuk mencapai suatu kekuasaan atas negara lainnya. Di dalam teori *Sea Power* terdapat keamanan maritim. Menurut Christian Bueger, keamanan maritim adalah salah satu kata kunci dalam hubungan Internasional. Aktor utama adalah kebijakan maritim, tata kelola laut dan keamanan internasional. Keamanan maritim mencakup konsep mengenai hubungan internasional, konflik wilayah antar negara, terorisme, pembajakan, peredaran narkoba, perdagangan ilegal, penangkapan ikan ilegal, sampai pengrusakan lingkungan. Walaupun cakupannya luas, keamanan maritim harus spesifik per kasus. Maka dari itu, dalam setiap kasus harus merujuk pada teori-teori turunan yang sesuai. Bueger mencetuskan tiga kerangka utama untuk memahami ketahanan maritim yaitu:⁸

Kerangka pertama dimaksud untuk menganalisis semiotika yang identik dengan konsep ketahanan maritim untuk memetakan makna-makna yang berbeda dan menelusuri keterkaitan di antara makna-makna tersebut. Menurut kerangka ini, ketahanan maritim memiliki empat dimensi, yaitu kekuatan maritim (*seapower*), keamanan maritim (*marine safety*), blue economy, dan ketahanan manusia (*human resilience*). Kemudian, konsep sekuritisasi dapat dijadikan kerangka analisis dalam memahami ketahanan maritim. Dalam hal ini, ancaman terhadap ketahanan maritim dipandang sebagai hasil konstruksi aktor-aktor yang terlibat. Sementara itu, kerangka terakhir adalah memahami ketahanan maritim melalui perspektif komunitas keamanan. Dalam hal ini, analisis beranjak dari beragam tindakan yang dilakukan oleh aktor untuk mengatasi ancaman ketahanan

⁶ Ronan Doare (eds), *Robots on the Battlefield Contemporary Issues and Implications for the Future*, Combat Studies Institute Press, Fort Leavenworth, Kansas, 2014. Hlm. 89-90.

⁷ A.T. Mahan, D.C.L., L.L.D., *The Influence of Sea Power Upon History; 1660-1783*, Little, Brown and Company, Boston, 1890.

⁸ Christian Bueger, "What is maritime security?", *Marine Policy* 53 (2015), hal. 159-160.

maritim secara bersama dalam sebuah komunitas keamanan. Dalam penelitian ini, peneliti mengaitkan teori keamanan maritim pada sistem Octopus yang dimanfaatkan untuk melindungi wilayah maritim Indonesia serta memberikan informasi berupa analisis yang kemudian akan dilaporkan kepada pengambil keputusan untuk segera melakukan tindakan dalam mengatasi potensi ancaman.

Menurut Budiharto & Suhartono, Artificial Intelligence (AI) atau kecerdasan buatan merupakan bidang ilmu komputer yang mencakup cara manusia mengetahui, memahami, memprediksi dan melakukan manipulasi terhadap hal-hal yang lebih besar dan lebih rumit dari yang pernah ada. Dalam teknologi *artificial intelligence* (AI), teknik dasar yang digunakan untuk melakukan penalaran adalah pelacakan (*search*) dan penyocokan pola (*pattern matching*). Dengan diberi informasi awal, program tersebut akan melacak pangkalan pengetahuan untuk mencari pola-pola atau kondisi-kondisi yang spesifik. Ia melacak untuk mencocokkan kriteria yang sesuai agar bisa memecahkan masalah yang diinginkan, sesuai dengan pangkalan pengetahuanyang dimilikinya. Secara harfiah, komputer terus memburu dan mencari pengetahuan yang ada sampai ia menemukan jawaban yang paling cocok.⁹

Koordinasi terkait erat terhadap sebuah manajemen (tata kelola) dalam mewujudkan tujuan baik pada organisasi publik maupun swasta. Sebagaimana dijelaskan oleh Adisasmita bahwa Koordinasi (*coordinating*) adalah tindakan seorang manajer dalam upaya menyelaraskan suatu pekerjaan dari suatu bagian dengan tugas bagian lain, sehingga mencegah timbulnya kesimpangsiuran yang dapat menjadi tidak efektifan.¹⁰ sistem informasi yang ada perlu di integrasikan dengan lembaga kelautan lain agar saling berhubungan dan semua kegiatan mencapai suatu tujuan. Dalam berkoordinasi hal yang harus diperhatikan juga adalah sinkronisasi

dari waktu. Dalam penelitian ini tentu diperlukan sinkronisasi dalam pemanfaatan sistem octopus agar tindakan yang dilakukan tepat sasaran dalam mencegah terjadinya ancaman.

Peran Intelijen, menurut Undang Undang Nomor 17 tahun 2011 pasal 4 tentang Intelijen Negara menyebutkan bahwa Intelijen Negara berperan melakukan upaya, pekerjaan, kegiatan, dan tindakan untuk deteksi dini dan peringatan dini dalam rangka pencegahan, penangkalan, dan penanggulangan terhadap setiap hakikat ancaman yang mungkin timbul dan mengancam kepentingan dan keamanan nasional. Berdasarkan pasal tersebut, peran intelijen dalam melakukan upaya, pekerjaan, kegiatan, dan tindakan untuk deteksi dini dan peringatan dini terhadap setiap hakikat ancaman yang termasuk ke dalam sembilan komponen strategis diantaranya ideologi, politik, ekonomi, sosial budaya, pertahanan, keamanan, teknologi, geografi, dan biografi.

Potensi Ancaman, menurut Majdi, kata potensi berasal dari serapan bahasa Inggris, yakni *potencial* yang memiliki dua arti, yaitu kesanggupan dan kekuatan. Dari hal tersebut pada dasarnya potensi dapat diartikan sebagai suatu kemampuan, kesanggupan kekuatan ataupun daya yang mempunyai kemungkinan untuk bisa dikembangkan lagi menjadi bentuk yang lebih besar.¹¹ Berkaitan dengan ancaman, hakikat ancaman menurut UU No. 3 Tahun 2003 tentang Pertahanan Negara adalah setiap usaha dan kegiatan, baik dari dalam maupun luar negeri yang dinilai membahayakan kedaulatan negara, keutuhan wilayah, dan keselamatan negara. Ancaman adalah setiap upaya, pekerjaan, kegiatan, dan tindakan baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat membahayakan keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah Negara Kesatuan Republik Indonesia (NKRI), dan kepentingan nasional di berbagai aspek, baik

⁹ Suparman, *Mengenal Artificial Intelligence*, (Yogyakarta: Andi Offset, 1991). hal. 5.

¹⁰ Adisasmita, Rahardjo. *Manajemen Pemerintahan Daerah*. Yogyakarta: Graha Ilmu, 2011 hal. 166

¹¹ Udo Yamin Efendi Majdi, *Manajemen Diri: Upaya Membangun Karakter (Character Building)* Masisir. Cetakan Kedua, Sinar Grafika, Jakarta, 2007, hal. 11.

ideologi, politik, ekonomi, sosial budaya, maupun pertahanan dan keamanan.¹²

METODOLOGI

Metode yang akan digunakan pada penelitian ini adalah metode penelitian kualitatif. Metode penelitian kualitatif adalah metode penelitian yang berlandaskan pada pendekatan postpositivisme, digunakan untuk meneliti kondisi obyek yang alamiah, dimana peneliti adalah sebagai instrumen kunci, teknik pengumpulan data dilakukan secara triangulasi (gabungan observasi, wawancara, dokumentasi), analisis data bersifat induktif/kualitatif, dan hasil penelitian kualitatif lebih menekankan makna.¹³

Berdasarkan permasalahan dalam penelitian ini, peneliti akan menggunakan metode penelitian kualitatif deskriptif yaitu penelitian yang mengarah pada pendeskripsian secara rinci dan mendalam baik kondisi maupun proses, dan juga hubungan atau saling keterkaitannya mengenai hal-hal pokok yang ditemukan pada sasaran penelitian.

Peneliti memilih pendekatan penelitian kualitatif karena dinilai tepat dalam menjelaskan bagaimana bentuk potensi ancaman yang akan terjadi terhadap maritim Indonesia sehingga akan menghasilkan data deskriptif dalam bentuk tertulis atau kata-kata lisan yang diperoleh dengan metode wawancara, studi literatur dan pemanfaatan dokumen. Hasil dari penelitian berupa output penelitian yang dapat dipertanggungjawabkan secara ilmiah. Proses penelitian kualitatif ini melibatkan upaya-upaya penting, seperti mengajukan pertanyaan-pertanyaan dan prosedur-prosedur, mengumpulkan data yang spesifik dari para partisipan, menganalisis data secara induktif mulai dari tema-tema yang khusus ke tema-tema yang umum, dan menafsirkan makna data. Laporan akhir untuk penelitian ini memiliki

struktur atau kerangka yang fleksibel. Siapa pun yang terlibat dalam bentuk penelitian ini harus menerapkan cara pandang penelitian yang bergaya induktif, berfokus pada makna individual, dan menerjemahkan kompleksitas suatu persoalan.¹⁴

Lofland dan Lofland dalam Moleong menjelaskan bahwa sumber data utama dalam penelitian kualitatif ialah kata-kata, dan tindakan, selebihnya adalah data tambahan seperti dokumen dan lain-lain.¹⁵ Pada penelitian yang menggunakan pendekatan penelitian kualitatif deskriptif ini, peneliti menggunakan dua sumber data, yaitu:

1. Data primer

Menurut Wardiyanta dalam Sugiarto (2017:87), data primer merupakan informasi yang diperoleh dari sumber-sumber primer yaitu informasi dari narasumber. Dalam penelitian ini, data primer yang akan diambil menggunakan metode wawancara. Wawancara dilakukan untuk memperoleh data yang valid dari narasumber yang kemudian dapat dipertanggungjawabkan.

2. Data Sekunder

Menurut Wardiyanta dalam Sugiarto (2017:87), data sekunder merupakan informasi yang diperoleh secara tidak langsung dari narasumber melainkan dari pihak ketiga. Dalam penelitian ini, data sekunder yang akan diambil dengan mengumpulkan literatur, penelitian ilmiah, dokumen dan lain sebagainya. Sumber tersebut akan dilakukan studi kepustakaan yang hasilnya akan menjadi data pelenengkap.

Teknik pengumpulan data merupakan langkah yang paling utama dalam penelitian, karena tujuan utama dari penelitian adalah mendapatkan data. Tanpa mengetahui Teknik pengumpulan data, maka peneliti tidak akan mendapatkan data sesuai yang ditetapkan.¹⁶

Sumber data dalam penelitian ini diklasifikasikan menjadi sumber data primer dan

¹² Undang Undang Nomor 17 tahun 2011 pasal 1 ayat 4

¹³ Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, Alfabeta (Bandung, 2014) hal. 9.

¹⁴ John W. Cresswell, *Research and Design Pendekatan Metode Kualitatif, Kuantitatif, dan*

Campuran, Pustaka Pelajar. (Yogyakarta. 2016), hal. 5.

¹⁵ Lexy J Moleong, *Metode Penelitian Kualitatif*, Remaja Rosdakarya. (Bandung. 2005), hal 4

¹⁶ Sugiyono, *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D*, Alfabeta. (Bandung. 2008), hal 308

sekunder. Data primer dalam penelitian ini dilakukan dengan wawancara oleh:

- 1) Kepala Pusat Penelitian dan Pengembangan Badan Intelijen Negara yaitu Dr. rer. nat. Armi Susandi, M.T.
- 2) Kasubdit Deteksi Potensi Ancaman Direktorat Deteksi Ancaman Deputy 1 Badan Sandi dan Siber Negara yaitu Enggar Ndaru Prasajo, S.ST.
- 3) Kasubdit 5.2 Infrastruktur Jaringan Badan Intelijen Negara yaitu Rion Sahputra
- 4) Peneliti Pascapanen dan Bioteknologi Produk Kelautan Kementerian Kelautan dan Perikanan yaitu Sihono, STP, M.Si.
- 5) Staf Pusat Penelitian dan Pengembangan Badan Intelijen Negara yaitu Fadhil M. Firdhaus

Data sekunder untuk penelitian ini adalah literasi dan kajian pustaka.

HASIL DAN PEMBAHASAN

1. Pemanfaatan Sistem Octopus

Sistem Octopus dibuat untuk menghadapi tantangan di era industri 4.0 serta menjaga kedaulatan dan keamanan maritim Indonesia. Selain itu, sistem Octopus dibutuhkan sebagai pendukung penelitian ilmiah di bidang maritim untuk melakukan proteksi dan preservasi wilayah laut serta untuk mengedepankan kebijakan pembangunan berkelanjutan di bidang maritim. Dalam mendeteksi adanya potensi ancaman, sistem Octopus dimanfaatkan dalam melakukan analisis statistik serta membaca aktivitas ilegal di laut Indonesia. Pemanfaatan sistem Octopus sebagai informasi sangat penting untuk melakukan pemantauan terhadap wilayah perbatasan maritim yang menunjukkan bahwa sistem informasi deteksi potensi ancaman dapat meningkatkan kewaspadaan dalam menghadapi berbagai ancaman maritim.

Pemanfaatan sistem informasi deteksi potensi ancaman maritim berkaitan dengan

sumber daya nasional dalam mewujudkan pertahanan negara. Urgensi dalam pemanfaatan sistem informasi deteksi potensi ancaman berbasis *website* di bidang maritim menjadi semakin berpengaruh karena Indonesia harus menghadapi berbagai perubahan fundamental di sektor keamanan pada era revolusi industri 4.0. Perubahan tersebut ditandai dengan adanya potensi ancaman asimetris yang melibatkan aktor non-negara dan negara-negara yang mengancam perdamaian dunia serta adanya perang siber yang menggunakan teknologi informasi sebagai alat perang untuk melumpuhkan dan mematikan infrastruktur diberbagai bidang.¹⁷

2. Fitur-fitur pada Sistem Octopus

Di dalam sistem Octopus terdapat fitur-fitur yang dapat memudahkan untuk melakukan pemantauan untuk mengetahui segala potensi-potensi ancaman dan perikanan, yaitu:

- a. Fitur Deteksi Ancaman Manusia
- b. Fitur Deteksi Ancaman Alam
- c. Fitur Prediksi Cuaca
- d. Fitur Potensi Perikanan Tangkap

3. Analisis Sistem Octopus menggunakan *Artificial Intelligence*

Sistem Octopus dapat mengumpulkan informasi dan data potensi ancaman maritim dengan menggunakan *artificial intelligence* atau kecerdasan buatan yang telah di program oleh manusia pada komputer untuk melakukan pendataan. Dalam melakukan pengumpulan informasi potensi ancaman maritim, sistem Octopus menggunakan *machine learning* seperti pada konsep *artificial intelligence* yaitu kemampuan program komputer untuk memperoleh informasi data yang ada dengan perintah, juga dapat mengolah informasi data yang ada dan yang diperoleh. Pada sistem Octopus,

¹⁷ Hasil wawancara dengan Kepala Pusat Penelitian dan Pengembangan BIN Armi Susandi melalui *Zoom* pukul 21.00-21.20 WIB pada 31 Mei 2021

pengumpulan informasi potensi ancaman maritim dilakukan melalui sumber instrumen pengamatan baik secara langsung maupun pemantauan jarak jauh menggunakan *Automatic Identification System* (AIS) dan *Vessel Monitoring System* (VMS). Dengan adanya keterbatasan data yang tersedia, sistem Octopus menggunakan pengembangan algoritma yang mengirisikan antara daerah potensi ikan dan lokasi kapal berdasarkan AIS.¹⁸

Dalam mengetahui informasi data kondisi laut bersumber dari *Automatic Water Level Recorder* (AWLR) sebagai instrumen pengamatan langsung dan Satelit MODIS AQUA sebagai instrumen pengindraan jarak jauh. Kemudian, informasi data mengenai transportasi laut dan interaksinya diperoleh dari *Automatic Identification System* (AIS), *Intelligent Maritime Transportation System* (IMTS), dan informasi data yang didapatkan dari radar pendeteksi kapal. Selanjutnya, informasi data cuaca diperoleh dari *Automatic Weather Station* (AWS) dan instrumen satelit observasi cuaca. Seluruh data tersebut kemudian akan diproses melalui *High Performance Computing* (komputer berspesifikasi tinggi) dan divisualisasikan melalui laman resmi sistem Octopus yaitu octopuslaut.id.

Keberhasilan dalam pemanfaatan sistem Octopus dalam mendeteksi sejumlah potensi ancaman maritim di Indonesia dibuktikan dengan mengetahui dan mengidentifikasi illegal fishing atau penangkapan ikan secara ilegal di wilayah ZEE Indonesia, terutama di wilayah Laut Natuna Utara serta penangkapan pencurian benih lobster di wilayah selatan Laut Jawa. Selanjutnya, sistem Octopus berhasil mendeteksi ancaman manusia berupa pembajakan kapal dan penyelundupan

manusia di Selat Malaka, penyelundupan narkoba di wilayah selatan Bali, dan ancaman perdagangan gelap hewan dilindungi di Laut Sulu dan Selebes di wilayah utara Sulawesi.

Namun, perlu diketahui bahwa pemanfaatan sistem Octopus masih terdapat kekurangan dan tantangan baik secara teknis maupun operasionalnya, yaitu:

1. Sumber daya manusia yang kurang dan yang dapat mengoperasikan sistem informasi di bidang siber;
2. Kurang tersedianya data terdahulu dan informasi tempat kejadian mengenai kejahatan maritim;
3. Prediksi potensi tangkap perikanan susah diterapkan dikarenakan kurang tersedianya data tangkapan;
4. Sarana serta prasarana yang terbatas dalam pengolahan informasi di berbagai titik di wilayah maritim Indonesia;
5. Adanya ketidakjelasan terkait kesepakatan yang telah dibuat dalam sinergi lintas lembaga.¹⁹

4. Evaluasi Keamanan Maritim Indonesia

Kasus kejahatan maritim di Indonesia meningkat setiap tahunnya, seperti terjadinya penangkapan ikan secara *illegal*. Kegiatan *illegal fishing* yang sering terjadi di Wilayah Pengelolaan Perikanan Negara Republik Indonesia (WPP-NRI) itu oleh kapal-kapal perikanan asing (KIA) yang kebanyakan dari negara tetangga.”²⁰ Dari pernyataan tersebut, kasus yang terjadi di wilayah perairan Indonesia makin meningkat yang bersifat kompleks, pemanfaatan sistem informasi seperti sistem Octopus dapat membantu dalam memetakan dan mendeteksi terjadinya potensi ancaman maritim di Indonesia.

Menurut Marsetio (mantan Kepala Staf Angkatan Laut) sebagai negara maritim,

¹⁸ Hasil wawancara dengan staff Pusat Penelitian dan Pengembangan BIN Fadhil M. Firdaus melalui *Whatsapp* pada 29 Maret 2021

¹⁹ Hasil wawancara dengan Kepala Pusat Penelitian dan Pengembangan BIN Armi Susandi melalui *Zoom* pukul 21.00-21.20 WIB pada 31 Mei 2021

²⁰ Hasil wawancara dengan Peneliti Pascapanen dan Bioteknologi Produk Kelautan KKP Suhono melalui *Whatsapp* pukul 17.00-17.15 pada 29 Mei 2021

wilayah maritim Indonesia setiap harinya dilalui berbagai jenis kapal yang bervariasi mulai dari tanker minyak, kapal yang mengangkut nuklir dan bahan berbahaya lain, armada militer baik kapal dan kapal selam serta kapal angkut lainnya. Indonesia juga dilalui oleh penerbangan baik komersil maupun militer. Hal ini disebabkan perairan Indonesia memiliki 4 choke points dari 9 choke points yang ada di dunia yang berada didalam tiga Alur Laut Kepulauan Indonesia.

Berkaitan dengan itu, sistem Octopus yang merupakan sistem informasi berbasis website sebagai langkah BIN dalam hal ini intelijen maritim berupaya mengamankan wilayah laut Indonesia. Perlu adanya kerjasama dengan lembaga terkait bidang maritim dalam melakukan kolaborasi dan koordinasi pada pemanfaatan sistem informasi terhadap potensi ancaman di laut Indonesia. Lembaga-lembaga yang dimaksud adalah TNI, Polri, Badan Keamanan Laut (Bakamla), Kementerian Perhubungan, Kementerian Lingkungan Hidup, Kementerian Pertahanan, Kementerian Kelautan dan Perikanan, Kementerian Luar Negeri, Kementerian Dalam Negeri, Kementerian Hukum dan HAM, Bea Cukai, dan Imigrasi yang bertindak dalam urusan Keamanan Laut. Selain itu, dalam peningkatan kapasitas sumber daya manusia dibidang teknologi dan kelautan berkolaborasi dengan Kementerian ESDM, Kemendikbud, Kementerian Tenaga Kerja, Kementerian Sosial, Kementerian Ristek, serta BKPM. Dalam hal peningkatan sistem informasi dibidang maritim berkolaborasi dengan BSSN, Kominfo, dan Lembaga Pengembangan Teknologi Informasi dan Komunikasi.

5. Potensi Ancaman Serangan Siber pada Sistem Octopus

Perlu diketahui bahwa sistem Octopus merupakan sistem informasi berbasis *website*, dimana setiap sistem itu tidak ada aman. Tidak ada sistem yang 100% aman terhadap serangan siber apalagi dengan sekarang muncul dengan teknologi-teknologi seperti APT, resiko yang mungkin terjadi di web ada beberapa macam apakah masih bisa dibobol, tidak ada sistem yang ga bisa dibobol, misalkan dibobolnya dari depan ga bisa didalam itu namanya kontrol terhadap resiko yang mungkin. yang dapat dilakukan dengan memperkuat sistem tersebut dengan memetakan dan mendefinisikan potensi ancaman dan ada kontrol terhadap sistem tersebut bukan aman tapi tahan. Selain itu ada motivasi dibalik serangan siber.²¹

Kalo potensi serangan siber pasti ada dan sejauh ini yang menangani serangan siber di BIN itu di subdit pengamanan sistem dan berkaca pada keamanan sistem itu hanya masalah waktu, sekarang mungkin merasa aman tapi bisa saja kedepannya tidak aman karena sistem yang obsolete. Karena mungkin ada APT, virus yang dimasukkan lewat malware, atau pengguna yang dapat mengakses website yang tidak dikehendaki rentan terkena malware.²²

Motivasi spionase komersial, penyerang dengan motivasi ini merupakan *cybercrime* terorganisir yang canggih atau pihak asing yang ingin mencuri atau merusak informasi rahasia. Aktor dengan motivasi ini sering mencari keuntungan moneter yang signifikan dengan menargetkan sasaran strategis. Motivasi kejahatan siber, dalam hal ini aktor penyerangan siber menargetkan jaringan dan sistem secara langsung untuk dicuri data informasi. Aktor dengan motivasi ini memanfaatkan ransomware dan malware

²¹ Hasil wawancara dengan Kasubdit Deteksi Potensi Ancaman Direktorat Deteksi Ancaman Deputi 1 BSSN Enggar Ndaru Prasajo, S.ST. melalui *Googlemeet* pada pukul 14.00 – 14.15 WIB 10 Mei 2021

²² Hasil wawancara dengan Kasubdit 5.2 Infrastruktur Jaringan Badan Intelijen Negara Rion Sahputra melalui *Zoom* pada pukul 14.30 – 14.40 WIB 28 Mei 2021

yang merusak, dengan demikian aktor serangan dapat mengenkripsi atau memusnahkan data.

KESIMPULAN DAN SARAN

Berdasarkan uraian dalam hasil dan pembahasan maka dapat disimpulkan bahwa:

- 1) Peran intelijen dalam pemanfaatan sistem Octopus melakukan deteksi dini dan cegah dini terhadap segala bentuk hakikat ancaman di laut Indonesia dapat dilakukan dengan cara mengoptimalkan peran BIN yaitu fungsi intelijen dalam memperkuat sumber daya manusia yang memiliki kemampuan di bidang teknologi siber serta melalui koordinasi dan kolaborasi dengan Badan Siber dan Sandi Negara dalam penguatan sistem Octopus serta TNI AL dalam pengamanan wilayah maritim Indonesia. Koordinasi dalam semua lini dengan stakeholder lainnya menjadi unsur penting untuk menyatukan persepsi dan strategi guna mengantisipasi dampak potensi ancaman di laut Indonesia. Selain itu, melakukan kolaborasi dalam pemanfaatan sistem informasi dengan lembaga terkait di bidang maritim terkait keakuratan data sehingga dapat dijadikan bahan pertimbangan dalam pengambilan keputusan.

Pemanfaatan sistem Octopus oleh untuk mendeteksi potensi ancaman di laut Indonesia merupakan langkah dalam hal ini sebagai intelijen maritim untuk melindungi kedaulatan Indonesia. Dengan sistem informasi menggunakan teknologi *Artificial Intelligence* membuat sistem Octopus dapat mendeteksi potensi ancaman di laut Indonesia. Namun, sistem Octopus merupakan sistem berbasis *website* sehingga tidak menutup kemungkinan adanya potensi serangan siber/*cyber attack* yang sewaktu-waktu dapat menyerang. Peran intelijen dalam mengantisipasi serangan dari dalam sebagai sistem informasi adalah memperkuat sistem pengamanan pada *website* yang digunakan dalam memonitoring dengan melakukan kolaborasi terhadap 13 lembaga penanganan urusan kelautan.

Selain itu, penelitian ini telah menghasilkan rumusan terkait pola peningkatan intensitas

kualitas ancaman di era *Artificial Intelligence* khususnya pada sistem informasi BIN dan bagaimana kecerdasan buatan menjadi salah satu alat untuk mendeteksi ancaman. Selanjutnya, agar dapat menghasilkan informasi baru dan solusi alternatif terkait pemanfaatan sistem informasi yang ada di BIN.

Terakhir, Pemerintah Indonesia dalam hal ini Menko Maritim Republik Indonesia agar membentuk satuan atau tim lintas instansi (*stakeholder*) terkait adanya keterbukaan dalam pemanfaatan sistem informasi dalam hal ini lembaga kementerian laut melakukan koordinasi dalam mengamankan wilayah maritim Indonesia. Badan Intelijen Negara melalui Pusat Penelitian dan Pengembangan melakukan peningkatan sistem Octopus sebagai upaya intelijen dalam memanfaatkan *Artificial Intelligence* di bidang maritim. Badan Intelijen Negara melalui Deputy V Intelijen Teknologi melakukan pembaharuan dan pengadaan baru peralatan teknologi dalam penggunaan sistem informasi agar dapat meningkatkan keakuratan informasi data terkait pendeteksian potensi ancaman pada sistem Octopus. Badan Intelijen Negara melalui Deputy VI Intelijen Siber melakukan pengamanan serta pemetaan kerentanan pada sistem jaringan yang dimanfaatkan sebagai langkah deteksi dini terhadap potensi ancaman serangan siber pada sistem Octopus.

DAFTAR PUSTAKA

- Beuger, Christian. (2014), *What is maritime security*. Terjemahan oleh Susandi, A., UK: Palgrave Macmillan.
- Chairul, Anwar. (2017). *Teori-Teori Pendidikan: Klasik Hingga Kontemporer*. Yogyakarta: IRCiSoD
- Cresswell, John W. (2016). *Research and Design Pendekatan Metode Kualitatif, Kuantitatif, dan Campuran*. Yogyakarta: Pustaka Pelajar
- Djegadut, Rikard. 2020. Alur Laut Kepulauan Indonesia Sebagai Poros Maritim Indonesia
<https://indonews.id/artikel/311469/Alur->

Laut-Kepulauan-Indonesia-Sebagai-
Poros-Maritim-Dunia/

- Maghfiroh, Nur L. 2021. Letak Geografis Indonesia: Pengaruh dan Keuntungannya, <https://akupintar.id/info-pintar/-/blogs/letak-geografis-indonesia-pengaruh-dan-keuntungannya-1>
- Mahan, A.T. 198. *The Influence of Sea Power Upon History: 1660-1783*. Boston: Little Brown and Company.
- Mahmudah, Nunung. (2015). *ILLEGAL FISHING Pertanggungjawaban Pidana Korporasi di Wilayah Perairan Indonesia*. Jakarta Timur: Sinar Grafika
- Majdi, Udo Y. E. (2007). *Manajemen Diri: Upaya Membangun Karakter (Character Building)*. Jakarta: Masisir. Cetakan Kedua, Sinar Grafika.
- Moleong, Lexy J. (2005). *Metode Penelitian Kualitatif*. Bandung: Remaja Rosdakarya.
- Nainggolan, Poltak P. 2015. Indonesia dan Ancaman Keamanan di Alur Laut Kepulauan Indonesia (ALKI), *Jurnal Ketahanan Nasional*, 5, Vol. 20, No.3
- Sugiyono. (2008). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta
- Suparman. (1991). *Mengenal Artificial Intelligence*. Yogyakarta: Andi Offset
- Rahardjo, Adisasmita. (2011). *Manajemen Pemerintahan Daerah*. Yogyakarta: Graha Ilmu
- Undang-Undang Republik Indonesia Nomor 17 Tahun 2011 Tentang Intelijen Negara