

Analisa Dukungan *Internet of Things (IoT)* terhadap Peran Intelijen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur

Iswahyudhi Utari Turyadi¹, Firman Johan², Dadang Widyanto³

^{1,2,3} Program Studi Magister Operasi Laut Dikreg Seskoal Angkatan ke-59, Sekolah Staf dan Komando Angkatan Laut, Jakarta

Info Artikel

Riwayat Artikel

Diterima: 02-07-2021

Direvisi: 10-07-2021

Disetujui: 27-07-2021

Kata Kunci

Internet of Things;
pengamanan; maritim;
intelijen;

✉ Corresponding Author

Iswahyudi Utari Turyadi,
Program Studi Magister
Operasi Laut Dikreg Seskoal
Angkatan ke-59, Sekolah
Staf dan Komando Angkatan
Laut,
Tel. +6285261013651
iswahyudi@tni.mil.id

ABSTRAK

Internet of things yaitu dapat digambarkan sebagai kemampuan suatu objek untuk mentransmisikan atau mengirimkan data melalui jaringan tanpa menggunakan bantuan perangkat komputer ataupun manusia. *Internet of Things (IoT)* merupakan wujud perkembangan teknologi internet yang akhir-akhir ini mengalami perkembangan yang sangat pesat di bidang IT (*Information Technology*). Permasalahan keamanan di laut di daerah maritim Indonesia wilayah timur karena kurang efektifnya penggalangan intelijen terhadap pencegahan ancaman tindak pidana di laut, kurangnya ketersediaan teknologi yang mendukung pelaksanaan tugas intelijen. Sehingga sangat tepat kalau kegiatan intelijen pengamanan maritim di Indonesia wilayah timur didukung oleh kemampuan *Internet of Things (IoT)* untuk mewujudkan wilayah yang aman untuk dipergunakan bagi pengguna dan harus bebas dari bentuk-bentuk ancaman atau gangguan terhadap berbagai aktifitas penggunaan dan pemanfaatan sumber daya laut, diantaranya yaitu laut yang bebas dari ancaman kekerasan, termasuk ancaman penggunaan kekuatan bersenjata yang dinilai mempunyai kemampuan untuk mengganggu dan membahayakan kedaulatan negara.

PENDAHULUAN

Dengan adanya kemajuan teknologi yang sangat pesat saat ini, maka sejalan dengan itu sudah saatnya menggunakan potensi dari kemajuan teknologi tersebut ke dalam peran intelijen dan pengamanan maritime wilayah Indonesia. Buku Putih Pertahanan menjelaskan bahwa kemampuan intelijen terdiri atas pengembangan kemampuan SDM yang profesional, serta didukung dengan penggunaan teknologi yang mampu menunjang pelaksanaan tugas-tugas secara terintegrasi dan bersinergi dengan pertahanan nirmiliter. Intelijen memiliki dua tindakan utama yang dilakukan, yaitu mengumpulkan dan menganalisa. Kedua hal tersebut harus dapat dilihat menggunakan sudut pandang yang lebih luas sehingga mampu menghubungkan kegiatan-kegiatan tersebut untuk keperluan bagi pengambil dan membuat keputusan serta penggunaan produk intelijen yang sudah selesai. Hal tersebut dilakukan melalui konsep siklus intelijen, yaitu suatu proses dimana informasi yang diperoleh diolah dan diubah menjadi produk intelijen serta disajikan kepada pembuat kebijakan (stakeholder) [1].

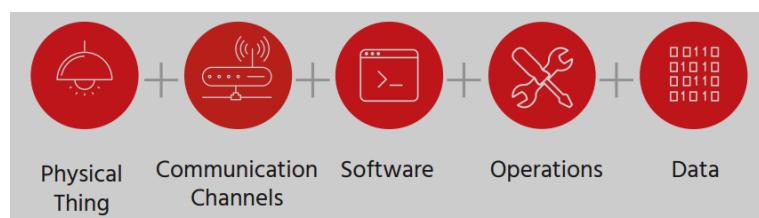
Pada era industri 4.0 yang diantaranya adalah domain *Internet of Things (IoT)* diperkenalkan oleh Kevin Ashton tahun 2002. Perkembangan teknologi intenet mulai diterapkan pada proses-proses produksi di dunia industri pada negara-negara maju, terutama

Amerika Serikat dan negara-negara di Eropa Barat. Keberadaan IoT dimulai membakukan komputer agar dapat memahami dunia nyata dilingkungannya secara mandiri. Pada awal perkembangannya, konsep IoT diaplikasikan kedalam penggunaan komputer diberbagai bidang kebutuhan manusia, yang intinya yaitu penggunaan komputer dimana dan untuk apa saja (*uniquitous computing*). Tapi sejak tahun 2009 dibentuklah Komisi Negara-Negara Eropa yang khusus dibentuk untuk merumuskan kembali definisi IoT, yang lebih lanjut didefinisikan sebagai sebuah tahap evolusi berikutnya dari internet, dengan hal yang paling mendasar yaitu perubahan dari sekedar jaringan dari serangkaian komputer yang saling terhubung menjadi jaringan dari serangkaian obyek atau benda yang saling terhubung (Commision of the European Communities, Internet of Things-an Action Plan for Europe, 2009).

Di dalam penelitian ini akan dianalisa dukungan kemampuan *Internet of Things* (*IoT*) dalam kegiatan tindak pengamanan wilayah laut atau maritime yang bukan hanya terkait dengan penegakan hukum di wilayah laut saja, akan tetapi termasuk wilayah luas yang aman untuk dipergunakan bagi pengguna dan harus bebas dari bentuk-bentuk ancaman atau gangguan terhadap berbagai aktifitas penggunaan dan pemanfaatan sumber daya laut. Permasalahan keamanan di laut di daerah maritim Indonesia wilayah timur karena kurang efektifnya penggalangan intelijen terhadap pencegahan ancaman tindak pidana di laut, kurangnya ketersediaan teknologi yang mendukung pelaksanaan tugas intelijen. Sehingga sangat tepat kalau kegiatan intelijen pengamanan maritim di Indonesia wilayah timur didukung oleh kemampuan *Internet of Things* (*IoT*) untuk mewujudkan wilayah yang aman untuk dipergunakan bagi pengguna dan harus bebas dari bentuk-bentuk ancaman atau gangguan terhadap berbagai aktifitas penggunaan dan pemanfaatan sumber daya laut, diantaranya yaitu laut yang bebas dari ancaman kekerasan, termasuk ancaman penggunaan kekuatan bersenjata yang dinilai mempunyai kemampuan untuk mengganggu dan membahayakan kedaulatan negara.

Teknologi Internet of Things

Internet of things yaitu dapat digambarkan sebagai kemampuan suatu objek untuk mentransmisikan atau mengirimkan data melalui jaringan tanpa menggunakan bantuan perangkat komputer ataupun manusia. Istilah *Internet of Things* (*IoT*) diperkenalkan oleh Kevin Ashton tahun 2002. Perkembangan teknologi intenet mulai diterapkan pada proses-proses produksi di dunia industri pada negara-negara maju, terutama Amerika Serikat dan negara-negara di Eropa Barat. Keberadaan IoT dimulai membakukan komputer agar dapat memahami dunia nyata dilingkungannya secara mandiri. Pada awal perkembangannya, konsep IoT diaplikasikan kedalam penggunaan komputer diberbagai bidang kebutuhan manusia, yang intinya yaitu penggunaan komputer dimana dan untuk apa saja (*uniquitous computing*). Tapi sejak tahun 2009 dibentuklah Komisi Negara-Negara Eropa yang khusus dibentuk untuk merumuskan kembali definisi IoT, yang lebih lanjut didefinisikan sebagai sebuah tahap evolusi berikutnya dari internet, dengan hal yang paling mendasar yaitu perubahan dari sekedar jaringan dari serangkaian komputer yang saling terhubung menjadi jaringan dari serangkaian obyek atau benda yang saling terhubung (Commision of the European Communities, Internet of Things-an Action Plan for Europe, 2009). Adapun bentuk fisik dari IoT tampak seperti gambar 1 [2].



Gambar 1. Bentuk sistem IoT

- Bagian 1 : Benda Fisik. Kemampuan IoT dari benda-benda fisik meliputi sensor, aktuator, pemrosesan, kontrol, dan daya. Adapun spesifikasi fisik tergantung pada biaya, ukuran, kinerja, dan kendala lingkungan.
- Bagian 2 : Saluran Komunikasi. Kombinasi protokol internet dan solusi konektivitas memungkinkan transfer data pada *Thing-to-Thing*, *Thing-to-Server*, atau *Server-to-Server*. Hal tersebut bergantung pada bidang penggunaan desain.
- Bagian 3 : Perangkat Lunak. Perangkat lunak menyediakan kemampuan untuk mengambil, memproses, menyimpan, dan menganalisis data yang berasal dari suatu benda. *Software* juga menyediakan level aplikasi kemampuan manusia untuk memvisualisasikan data dan berinteraksi dengan sistem IoT.
- Bagian 4 : Operasi. Aksesibilitas infrastruktur Cloud dalam menggelar dan maintain IoT.
- Bagian 5 : Data. Data merupakan produk dari sistem IoT. Dengan data merupakan media komunikasi antara point to point dalam sistem IoT.

Persyaratan dasar perangkat untuk dianggap sebagai bagian dari IoT, Novi (2020)

- Secara komputasi mampu men-hosting tumpukan perangkat lunak protokol Internet
- Perangkat keras dan daya yang mampu memanfaatkan transportasi jaringan seperti 802.3
- Bukan perangkat tradisional yang tersambung ke Internet, seperti PC, laptop, ponsel cerdas, server, alat pusat data, mesin produktivitas kantor, atau komputer tablet.

Algoritma pembelajaran mesin memiliki tempatnya di IoT. Kasus tipikal adalah ketika ada sejumlah besar data streaming yang perlu menghasilkan beberapa kesimpulan yang berarti. Sekumpulan kecil sensor mungkin hanya membutuhkan mesin aturan sederhana di edge dalam aplikasi yang sensitif terhadap latensi. Orang lain dapat mengalirkan data ke layanan cloud dan menerapkan aturan di sana untuk sistem dengan permintaan latensi yang kurang agresif. Saat sejumlah besar data, data tidak terstruktur, dan analitik waktu nyata ikut bermain, kita perlu mempertimbangkan penggunaan pembelajaran mesin untuk menyelesaikan beberapa masalah tersulit.

Di bagian ini, tahapan tip dan pengingat dalam menerapkan analisis pembelajaran mesin, dan kasus penggunaan apa yang mungkin memerlukan alat tersebut.

Fase pelatihan:

- Untuk *random forest*, gunakan teknik bagging untuk membuat *ensembles*.
- Saat menggunakan *random forest*, pastikan Anda memaksimalkan jumlah pohon keputusan.
- Awasi *overfitting*. *Overfitting* akan menyebabkan model lapangan tidak akurat. Teknik seperti regularisasi dan bahkan memasukkan noise ke dalam sistem akan memperkuat mode tersebut.
- Penurunan gradien akan menyebabkan kesalahan. RNN secara alami rentan.

Model di lapangan:

- Perbarui model dengan kumpulan data baru saat tersedia. Pertahankan set pelatihan saat ini.
- Model yang berjalan di *edge* dapat diperkuat dengan model yang lebih besar dan lebih komprehensif di *cloud*.
- Eksekusi jaringan neural dapat dioptimalkan di *cloud* dan *edge* dengan kerugian minimum dengan mempertimbangkan teknik seperti pemangkasan *node* dan pengurangan presisi.

Internet of Things (IoT) merupakan wujud perkembangan teknologi internet yang akhir-akhir ini mengalami perkembangan yang sangat pesat di bidang IT (Information Technology). IoT memungkinkan setiap barang (*things*) yang dimiliki dapat terhubung ke internet sehingga dapat dikendalikan dari jarak jauh. Pada tahun 2020 telah mencapai dua puluh miliar perangkat terhubung dalam sistem Internet

Internet of Things (IoT) memerlukan platform yang menghubungkan beberapa sensor dan perangkat data untuk menghasilkan visi lengkap tentang perilaku organisasi, suatu sistem, operasi bisnis atau fenomena. IoT secara langsung terkait dengan aplikasi vertikal yang

merupakan platform untuk menghubungkan berbagai perangkat diskrit (termasuk sensor mesin-ke-mesin) secara holistik.

Ada beberapa unsur pembentuk IoT yang mendasar diantaranya adalah kecerdasan buatan, koneksi, sensor, keterlibatan aktif serta pemakaian perangkat berukuran kecil.

1. Kecerdasan Buatan (*Artificial Intelligence/AI*) – IoT membuat hampir semua mesin yang ada menjadi “Smart”. Ini berarti IoT bisa meningkatkan segala aspek kehidupan kita dengan pengembangan teknologi yang didasarkan pada AI. Jadi, pengembangan teknologi yang ada dilakukan dengan pengumpulan data, algoritma kecerdasan buatan, dan jaringan yang tersedia. Sebagai contoh yaitu mesin yang tergolong sederhana seperti lemari es/kulkas yang memiliki kemampuan untuk mendeteksi jika stok susu sudah hampir habis, bahkan membuat pesanan ke supermarket secara otomatis saat stok mau habis. Penerapan kecerdasan masih memiliki peluang yang sangat luas di bidang-bidang lain.
2. Koneksi – Dalam IoT ada kemungkinan untuk membuat/membuka jaringan baru, dan jaringan khusus IoT. Jadi, jaringan ini tak lagi terikat hanya dengan penyedia utamanya saja. Jaringannya tidak harus berskala besar dan mahal, bisa tersedia pada skala yang jauh lebih kecil dan lebih murah.
3. Sensor – Sensor merupakan pembeda yang membuat IoT unik dibanding mesin canggih lainnya. Sensor ini mampu mendefinisikan instrumen, yang mengubah IoT dari jaringan standar dan cenderung pasif dalam perangkat, hingga menjadi suatu sistem aktif yang sanggup diintegrasikan ke dunia nyata.
4. Keterlibatan Aktif (*Active Engagement*) – *Engagement* yang sering diterapkan pada domain teknologi umumnya bersifat pasif. IoT mengenalkan paradigma yang baru bagi konten aktif, produk, maupun keterlibatan layanan.
5. Perangkat Berukuran Kecil – Perangkat ke depannya akan menjadi semakin kecil, makin murah, dan lebih kuat dari masa ke masa. IoT memanfaatkan perangkat-perangkat kecil yang dibuat khusus ini agar menghasilkan ketepatan, skalabilitas, dan fleksibilitas yang baik.

Aplikasi Internet of Things (IoT) dalam mendukung peran intelijen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur

Secara umum, IoT memberikan banyak peluang untuk dikembangkan yang turut berperan serta dalam berbagai segi mulai dari hal mikro hingga makro di seluruh dunia. Pada saat ini telah dikembangkan teknologi IoT utamanya dalam 3 hal tersebut antara lain:

1. Pengelolaan Bahaya Dan Bencana Alam Secara Lebih Cerdas. Dengan dukungan IoT, setiap individu maupun suatu organisasi bisa mendapatkan akurasi yang lebih baik ketika terjadi potensi bahaya alami. Sebagai contoh, IoT yang terhubung dengan alat deteksi dan alarm di suatu hutan akan dapat memberikan notifikasi dini ketika terjadi potensi kebakaran hutan di suatu kawasan. Dengan pemberitahuan dini, tentu dampak terburuk bisa diminimalisir. Hal ini juga berlaku untuk jenis bahaya dan bencana lain seperti perampukan rumah, tanah longsor, gempa bumi, dan sebagainya.
2. Pengelolaan Perkotaan Secara Lebih Cerdas. Beberapa project IoT diterapkan untuk mempermudah kehidupan masyarakat di berbagai tempat, termasuk masyarakat perkotaan. Dengan sistem IoT yang diterapkan tersebut, pemerintah bisa melakukan otomatisasi manajemen dengan lebih cerdas. Contohnya bisa dilihat pada aplikasi lalu lintas, parkir, sistem pengumpulan sampah, dan sebagainya. Dengan begitu, kehidupan masyarakat perkotaan juga akan menjadi semakin maju.
3. Pengelolaan Penanganan Kesehatan Dan Medis Secara Lebih Cerdas. Pada beberapa contoh yang akan disampaikan pada sub berikutnya akan ada beberapa contoh pengaplikasian IoT di bidang kesehatan. Secara keseluruhan, penambahan fitur IoT ke beberapa perangkat medis bertujuan untuk meminimalisir terjadinya hal-hal yang tidak diinginkan pada pasien. Jadi, bahkan sebelum terjadipun dokter dapat mengetahui potensi gangguan kesehatan pada seorang individu dan melakukan upaya pencegahan.

Dengan kata lain, dalam IoT kita bisa menghubungkan bermacam alat dengan koneksi internet, baik itu alat rumah tangga seperti TV kulkas, ac, kompor, lampu, dan entertainment, sampai mesin industri pabrik dan kendaraan bermotor. IoT memungkinkan kita memantau banyak hal dengan cara yang belum pernah bisa dibayangkan sebelumnya, jaman dulu kita tidak bisa membayangkan alat-alat bisa terhubung dengan internet dan bisa dimonitor.

Dalam mendukung mendukung peran intelijen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur, salah satu aplikasinya dengan aneka sensor dan kamera yang terhubung ke internet, server bisa memantau area yang sangat luas dengan sedikit atau bahkan tanpa tenaga kerja. Segala informasi termasuk cuaca, tingkat kelembaban dan suhu di setiap luasan daerah observasi dapat diupdate secara real time dari waktu ke waktu. Dari kumpulan data dan progress data dari waktu ke waktu dapat diprediksi perkembangan di suatu daerah observasi sifat cuaca, medan, dan bahkan meramalkan (estimasi) keadaan mendatang tanpa memakai banyak tenaga kerja, hanya mengawasi dan mengendalikan dari jauh saja sudah bisa, cukup memakai IoT dengan berbagai sensornya dan kamera. Dengan IoT, semua data dari sensor dan kamera ini dikirim lewat internet ke software pengolahan data. Tanpa perlu mendatangi area kita bisa menentukan sifat dan arah perkembangan dari suatu daerah observasi dengan tingkat akurasi yang cukup baik.

Bahkan data informasi intelijen tersebut dapat dibagikan ke layar laptop atau *smartphone* sehingga dapat lebih mudah untuk diakses dan membantu pimpinan dalam mengambil keputusan. Hasil pemantauan cuaca dengan weather station, dapat diamati suhu kelembaban dan juga tekanan udara dan parameter lain daerah tertentu tanpa kita harus datang kesana dari *smartphone* kita .

Dalam pencegahan kegiatan illegal fishing serta illegal logging juga dapat digunakan teknologi IoT tersebut. Dengan memonitor pada luasan daerah observasi tertentu dapat diperoleh data apakah pada daerah tersebut telah terjadi illegal fishing maupun illegal logging. Dengan penggunaan teknologi tersebut akan sangat efektif untuk memonitor suatu luasan daerah tertentu dengan tidak membutuhkan jumlah personel yang banyak serta dukungan operasional yang sangat mahal

Cara kerja IoT yang praktis juga dapat diaplikasikan dengan beberapa inovasi-inovasi yang sangat efektif dalam mengumpulkan data untuk mendukung peran intelijen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur seperti diantaranya adalah menempatkan sensor serta alat monitor pada kapal-kapal nelayan yang merupakan bagian dari kekuatan maritime laut, sehingga dapat menjadi sebuah jaringan data yang besar dan kompleks serta berdaya guna, dalam pengiriman data serta pengumpulan data yang bersifat real time. Misalnya, sensor dan kamera bisa digunakan di kapal-kapal nelayan untuk mengawasi luasan daerah tertentu dan secara real time terhubung dengan server, jadi operator akan segera mengetahui kalau ada tindak kejahatan seperti perompakan atau kejahatan di laut lainnya dan dapat segera diatasi ataupun menjadi barang bukti yang sah. Contoh lain di daerah tersebut, operator dapat memastikan apakah semua pengguna laut sudah melaksanakan seluruh peraturan baik hukum nasional maupun internasional telah terlaksana dengan baik atau belum, karena hal tersebut juga menyangkut dengan keselamatan di laut dan seluruh data tersebut dapat dilihat dengan laptop ataupun oleh *smartphone* saja.

Dengan IoT maka proses *sharing* data serta pengambilan keputusan dapat lebih cepat, dengan sumber daya manusia yang digunakan lebih sedikit, serta dan modal kegiatan operasi menjadi lebih ringan. Perusahaan-perusahaan kelas dunia saat ini telah menggunakan teknologi IoT untuk dapat meningkatkan kinerja perusahaan dan tentunya meningkatkan keuntungan perusahaan. Pengguna dapat menghemat waktu sebab tidak perlu mendatangi daerah yang sangat luas secara bergantian. Pelaksanaan operasional juga tak perlu menggaji banyak tenaga kerja.

METODE

Penelitian ini menggunakan metode literature review, atau gagasan. Adapun lokasi penelitian yang dilaksanakan adalah di Sekolah Staf dan Komando Angkatan Laut, Jakarta, dan Pangkalan Utama TNI Angkatan Laut IX, Sorong. Penelitian ini menggunakan format deskriptif survei yang memungkinkan peneliti untuk melakukan generalisasi suatu variabel tertentu pada populasi tertentu. Dalam pengumpulan sumber data, peneliti melakukan pengumpulan sumber data dalam wujud data primer dan data sekunder.

a. Data Primer

Data Primer ialah jenis dan sumber data penelitian yang di peroleh secara langsung dari sumber pertama (tidak melalui perantara), baik individu maupun kelompok. Jadi data yang di dapatkan secara langsung. Data primer secara khusus di lakukan untuk menjawab pertanyaan penelitian. Penulis mengumpulkan data primer dengan metode angket/kuesioner kepada staf yang bertugas di wilayah kerja Lantamal XIV Sorong.

b. Data Sekunder

Data Sekunder merupakan sumber data suatu penelitian yang di peroleh peneliti secara tidak langsung melalui media perantara (di peroleh atau dicatat oleh pihak lain).

Berisi tentang bagaimana cara penelitian ini dilakukan, jenis penelitian, waktu dan tempat penelitian, target/sasaran, subjek penelitian, prosedur, instrumen dan teknik analisis data serta hal-hal lain yang berkait dengan cara penelitiannya. Target/sasaran, subjek penelitian, prosedur, data dan instrumen, dan teknik pengumpulan data, serta teknik analisis data serta hal-hal lain yang berkait dengan cara penelitiannya dapat dituliskan dalam sub-subbab, dengan sub-subheading.

Khususnya untuk penelitian kualitatif, waktu dan tempat penelitian perlu dituliskan secara jelas. Target/subjek penelitian perlu diurai dengan jelas dalam bagian ini. Perlu juga dituliskan teknik memperoleh subjek. Sedangkan untuk penelitian kuantitatif, terdiri dari: variabel penelitian, rancangan penelitian, populasi dan sampel, teknik pengumpulan data dan pengembangan instrumen, dan teknik analisis data serta bagaimana memaknakan data yang diperoleh, kaitannya dengan permasalahan dan tujuan penelitian, perlu dijabarkan dengan jelas.

HASIL DAN PEMBAHASAN

Pasal 1 Undang-Undang Republik Indonesia Nomor 17 Tahun 2011 tentang Intelijen Negara, menjelaskan bahwa intelijen adalah pengetahuan, organisasi, dan kegiatan yang terkait dengan perumusan kebijakan, strategi nasional, dan pengambilan keputusan berdasarkan analisis dari informasi dan fakta yang terkumpul melalui metode kerja untuk pendekstrian dan peringatan dini dalam rangka pencegahan, penangkalan, dan penanggulangan setiap ancaman terhadap keamanan nasional.

Kemudian dalam Pasal 6 Undang-Undang tersebut juga dijelaskan bahwa Intelijen memiliki beberapa fungsi yaitu fungsi penyelidikan, fungsi pengamanan dan fungsi penggalangan. Terdapat dua tindakan utama yang dilakukan intelijen, yakni pengumpulan dan analisa, yang harus dilihat dari sudut pandang yang lebih luas. Sudut pandang tersebut harus menghubungkan kegiatan-kegiatan yang sesuai dengan kebutuhan pembuat keputusan dan penggunaan dari produk intelijen yang sudah selesai. Hal tersebut dilakukan melalui konsep siklus intelijen yakni suatu proses dimana informasi didapatkan, diubah menjadi produk intelijen dan dibuat serta disajikan kepada pembuat kebijakan.

Dalam proses informasi intelijen dikenal Roda Perputaran Intelijen (RPI)/daur intelijen atau *cycle intelligence*. Empat tahapan RPI adalah sebagai berikut Perencanaan dan pengarahan (*planning and direction*), pengumpulan (*collection*), proses pengolahan (*processing*), penggunaan distribusi (*distribution*). Dalam organisasi intelijen ada komunikasi yang dilakukan secara terbuka, yaitu informasi diperoleh secara terbuka melalui saluran komunikasi antar personal, kelompok, maupun saluran media massa seperti koran, radio, dan televisi. Komunikasi secara tertutup atau klandestin mencakup, Pertemuan

personel (*personal meeting*), Perantara hidup (*live drop*), Caraka atau kurir, Sandi, dan Tulisan Rahasia. Terdapat lima sistem dalam pengumpulan informasi intelijen yaitu:

- a. HUMINT (*Human Intelijen*)
- b. IMINT (*Imagery Intelligence*)
- c. MASINT (*Measurement and Signature Intelligence*)
- d. OSINT (*Open Source Intelijigence*)
- e. SIGINT (*Signal Intelijelligence*).

Intelijen bermanfaat dalam pengambilan kebijakan di tingkat strategis. Richard Russell mendefinisikan intelijen strategis sebagai “pengetahuan yang harus dimiliki petinggi sipil dan militer suatu negara untuk menjaga kesejahteraan nasional. Intelijen harus memfasilitasi upaya pencapaian berkesinambungan atas tujuan jangka panjang dengan juga memberikan panduan terhadap pilihan-pilihan taktis yang rasional untuk merespon perkembangan eksternal. Intelijen memiliki fungsi kontribusi terhadap proses, produk dan organisasi yang digunakan oleh pejabat senior untuk membuat dan mengimplementasikan kebijakan nasional dan pertahanan nasional. Intelijen kemudian harus membuat peringatan atas ancaman jangka pendek dan jangka panjang terhadap kepentingan nasional.

Dalam konteks kepentingan nasional, P.H Liotta menyebutkan ada dua tingkatan dalam kepentingan nasional, yaitu kepentingan nasional yang bersifat tetap dan kepentingan nasional yang bersifat aktual. Kepentingan nasional yang bersifat tetap adalah sebuah kepentingan negara merdeka untuk melindungi institusi-institusi negara, rakyat, dan nilai-nilai dasarnya. Sedangkan kepentingan nasional yang aktual adalah segala kepentingan yang tidak secara langsung mempengaruhi kedaualatan sebuah negara.

Perkembangan kepentingan nasional bangsa Indonesia dapat dijadikan sebagai landasan ketika membuat rumusan maupun menetapkan strategi besar (*grand strategy*) dalam bidang keamanan nasional maupun untuk menciptakan sistem pertahanan negara. Dalam konteks mewujudkan ruang pertahanan yang tangguh, pemerintah Indonesia menetapkan pembangunan wilayah perbatasan dan pulau-pulau kecil terluar/terdepan yang merupakan halaman depan Negara Kesatuan Republik Indonesia. Kawasan perbatasan Indonesia berada pada provinsi atau wilayah negara yang memiliki batas dengan sepuluh negara lainnya yang sudah seharusnya memiliki pertahanan yang tangguh.

Sebagai upaya mewujudkan pembangunan kawasan perbatasan yang tangguh perlu dilakukan pengintegrasian peran dan fungsi Kementerian atau Lembaga dan Pemda dengan memaksimalkan peran Badan Nasional Pengelola Perbatasan, serta melalui optimalisasi upaya diplomasi secara bilateral maupun multilateral dengan mengutamakan penyelesaian masalah bidang perbatasan secara damai bersama negara-negara tetangga. Salah satu wilayah pertahanan yang akan dibahas pada penelitian ini adalah wilayah timur Indonesia. wilayah timur Indonesia rawan akan ancaman pelanggaran dan kejahatan karena merupakan wilayah perbatasan Indonesia. Untuk mewujudkan pembangunan kawasan perbatasan di wilayah timur Indonesia, diperlukan operasi terpadu dari segala pihak yang terkait dalam pengamanan wilayah tersebut.

Buku Putih Pertahanan menjelaskan bahwa kemampuan intelijen terdiri atas pengembangan kemampuan SDM yang profesional, serta didukung dengan penggunaan teknologi yang mampu menunjang pelaksanaan tugas-tugas secara terintegrasi dan bersinergi dengan pertahanan nirmiliter. Intelijen memiliki dua tindakan utama yang dilakukan, yaitu mengumpulkan dan menganalisa. Kedua hal tersebut harus dapat dilihat menggunakan sudut pandang yang lebih luas sehingga mampu menghubungkan kegiatan-kegiatan tersebut untuk keperluan bagi pengambil dan membuat keputusan serta penggunaan produk intelijen yang sudah selesai. Hal tersebut dilakukan melalui konsep siklus intelijen, yaitu suatu proses dimana informasi yang diperoleh diolah dan diubah menjadi produk intelijen serta disajikan kepada pembuat kebijakan (*stakeholder*).

Selaras dengan hal tersebut, Armawi menjelaskan bahwa penggalangan terdiri atas serangkaian upaya, pekerjaan, kegiatan dan tindakan yang dilakukan secara terencana dan terarah untuk mempengaruhi sasaran agar menguntungkan kepentingan dan keamanan nasional. Penggalangan dalam konteks intelijen adalah semua usaha, pekerjaan, kegiatan dan tindakan yang dilakukan secara berencana dan terarah oleh sarana-sarana intelijen, khususnya menciptakan dan atau merubah suatu kondisi di daerah tertentu / lawan (baik diluar maupun didalam negeri), dalam jangka waktu tertentu yang menguntungkan, sesuai dengan kehendak atasan berwenang, untuk mendukung kebijakan yang ditempuh dan menghilangkan hambatan-hambatan. Penggalangan adalah upaya, langkah dan kegiatan yang dilakukan dengan tujuan membina, mengarahkan dan mengkondisikan suatu lingkungan dengan segala potensinya agar tercipta kondisi yang kondusif. Oleh karena itu, spektrum kegiatan intelijen dalam pelaksanaan tugas intelijen maritime adalah mendahului, menyertai dan mengakhiri setiap kegiatan operasional intelijen maritim.

Didalam kegiatan tindak pengamanan wilayah laut atau maritim, tidak hanya terkait dengan penegakan hukum di wilayah laut saja, akan tetapi termasuk wilayah luas yang aman untuk dipergunakan bagi pengguna dan harus bebas dari bentuk-bentuk ancaman atau gangguan terhadap berbagai aktifitas penggunaan dan pemanfaatan sumber daya laut, diantaranya yaitu laut yang bebas dari ancaman kekerasan, termasuk ancaman penggunaan kekuatan bersenjata yang dinilai mempunyai kemampuan untuk mengganggu dan membahayakan kedaulatan negara. Laut juga perlu terbebas dari ancaman terhadap navigasi yang ditimbulkan oleh kondisi geografi dan hidrografi, yang membahayakan keselamatan pelayaran. Selain itu laut juga harus terbebas dari pencemaran dan perusakan ekosistem dan yang terakhir adalah laut harus bebas dari ancaman pelanggaran terhadap ketentuan hukum nasional dan internasional yang berlaku seperti illegal logging, illegal fishing dan lain-lain.

Permasalahan keamanan di laut seperti yang telah disampaikan di atas sering terjadi di wilayah timur Indonesia. Permasalahan ini terjadi karena kurang efektifnya penggalangan intelijen terhadap pencegahan ancaman tindak pidana di laut, kurangnya sumber daya manusia untuk pengawasan wilayah tersebut, kurangnya ketersediaan teknologi yang mendukung pelaksanaan tugas intelijen, kurangnya strategi yang tepat dalam menghadapi ancaman tindak pidana di laut, terbatasnya alutsista dalam menghadapi ancaman tindak pidana di laut, kurang efektifnya propaganda yang dilakukan, kurangnya terbentuknya jaring intelijen di wilayah kerja.

Untuk itu sangatlah penting untuk dapat memahami sistem keamanan laut dengan baik dan kekurangan-kekurangan seperti yang telah disebut di atas khususnya dalam hal penggalangan intelijen, dengan tujuan untuk menciptakan sistem pendekatan yang bersifat komprehensif serta bersifat integral didalam proses penanganannya. Salah satu topik keamanan laut atau maritim yang menjadi perhatian cukup besar pada masa sekarang ini yaitu terkait dengan tindakan kejahatan atau ilegal di wilayah perairan Indonesia. Tindak kejahatan yang dilakukan di wilayah perairan Indonesia justru semakin marak, kegiatan ilegal yang dilakukan telah meningkat baik dalam lingkup intensitas dan kompleksitasnya sehingga sudah sangat mengancam kondisi sosial, ekonomi dan politik negara Indonesia serta diwilayah kawasan yang ada disekitarnya.

Dengan perkembangan kemajuan teknologi yang pesat, dan ditunjang dengan infrastruktur yang semakin lengkap, maka peningkatan kualitas serta kuantitas peran intelijen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur dapat ditunjang dengan perkembangan dan keberadaan teknologi tersebut, khususnya adalah perkembangan *Internet of Things (IoT)*. Dalam mendukung mendukung peran intelijen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur, salah satu aplikasinya dengan aneka sensor dan kamera yang terhubung ke internet, server bisa memantau area yang sangat luas dengan sedikit atau bahkan tanpa tenaga kerja. Segala informasi termasuk cuaca, tingkat kelembaban dan suhu di setiap luasan daerah observasi dapat diupdate secara real time dari waktu ke waktu. Dari kumpulan data dan progress data dari waktu ke waktu dapat diprediksi perkembangan di suatu

daerah observasi sifat cuaca, medan, dan bahkan meramalkan (estimasi) keadaan mendatang tanpa memakai banyak tenaga kerja, hanya mengawasi dan mengendalikan dari jauh saja sudah bisa, cukup memakai IoT dengan berbagai sensornya dan kamera. Dengan IoT, semua data dari sensor dan kamera ini dikirim lewat internet ke software pengolahan data. Tanpa perlu mendatangi area kita bisa menentukan sifat dan arah perkembangan dari suatu daerah observasi dengan tingkat akurasi yang cukup baik.

Bahkan data informasi intelejen tersebut dapat dibagikan ke layar laptop atau *smartphone* sehingga dapat lebih mudah untuk diakses dan membantu pimpinan dalam mengambil keputusan. Hasil pemantauan cuaca dengan weather station, dapat diamati suhu kelembaban dan juga tekanan udara dan parameter lain daerah tertentu tanpa kita harus datang kesana dari *smartphone* kita .

Dalam pencegahan kegiatan illegal fishing serta illegal logging juga dapat digunakan teknologi IoT tersebut. Dengan memonitor pada luasan daerah observasi tertentu dapat diperoleh data apakah pada daerah tersebut telah terjadi illegal fishing maupun illegal logging. Dengan penggunaan teknologi tersebut akan sangat efektif untuk memonitor suatu luasan daerah tertentu dengan tidak membutuhkan jumlah personel yang banyak serta dukungan operasional yang sangat mahal

Cara kerja IoT yang praktis juga dapat diaplikasikan dengan beberapa inovasi-inovasi yang sangat efektif dalam mengumpulkan data untuk mendukung peran intelijen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur seperti diantaranya adalah menempatkan sensor serta alat monitor pada kapal-kapal nelayan yang merupakan bagian dari kekuatan maritime laut, sehingga dapat menjadi sebuah jaringan data yang besar dan kompleks serta berdaya guna, dalam pengiriman data serta pengumpulan data yang bersifat *real time*. Misalnya, sensor dan kamera dapat digunakan di kapal-kapal nelayan untuk mengawasi luasan daerah tertentu dan secara *real time* terhubung dengan server, jadi operator akan segera mengetahui kalau ada tindak kejahatan seperti perompakan atau kejahatan di laut lainnya dan dapat segera diatasi ataupun menjadi barang bukti yang sah. Contoh lain di daerah tersebut, operator dapat memastikan apakah semua pengguna laut sudah melaksanakan seluruh peraturan baik hukum nasional maupun internasional telah terlaksana dengan baik atau belum, karena hal tersebut juga menyangkut dengan keselamatan di laut dan seluruh data tersebut dapat dilihat dengan laptop ataupun oleh *smartphone* saja [3].

Dengan IoT maka proses *sharing* data serta pengambilan keputusan dapat lebih cepat, dengan sumber daya manusia yang digunakan lebih sedikit, serta dan modal kegiatan operasi menjadi lebih ringan. Perusahaan-perusahaan kelas dunia saat ini telah menggunakan teknologi IoT untuk dapat meningkatkan kinerja perusahaan dan tentunya meningkatkan keuntungan perusahaan. Pengguna dapat menghemat waktu sebab tidak perlu mendatangi daerah yang sangat luas secara bergantian. Pelaksanaan operasional juga tak perlu menggaji banyak tenaga kerja.

Namun disamping kemudahan-kemudahan dan efektivitas yang diperoleh dari pengembangan IoT tersebut, dibutuhkan pengamanan data dari proses *sharing* data antar perangkat, khususnya data yang bersifat sensitif maupun strategis, sehingga harus dilengkapi dengan prosedur pengamanan data dari usaha-usaha pencurian dan pembobolan data yang kedepannya akan semakin marak. Data yang dikirimkan atau yang ada di server dapat bocor atau disalahgunakan, akibatnya dapat disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab sehingga dapat mengakibatkan hilangnya *privacy* dari data yang bersifat *sensitive* dan rahasia tersebut. sulit terjaga. Beberapa usaha yang dapat ditempuh yaitu dengan menggunakan data yang terenkripsi baik serta menggunakan prosedur yang ketat dalam membagikan data serta dalam penyimpanannya. Meskipun manfaat dan dampak negatifnya sudah jelas dapat terjadi namun akan masih banyak akibat lain yang nantinya akan belum bisa diantisipasi, sehingga perlu sebuah perencanaan yang tepat dalam pengembangan sistem tersebut.

SIMPULAN DAN SARAN

Dengan perkembangan kemajuan teknologi yang pesat, dan ditunjang dengan infrastruktur yang semakin lengkap, maka peningkatan kualitas serta kuantitas peran intelijen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur dapat ditunjang dengan perkembangan dan keberadaan teknologi tersebut, khususnya adalah perkembangan *Internet of Things (IoT)*.

Segala informasi intelijen di setiap luasan daerah observasi dapat diupdate secara real time dari waktu ke waktu dan selanjutnya dapat diprediksi perkembangan di suatu daerah observasi tanpa memakai banyak tenaga kerja, dan seluruh data tersebut dapat dilihat dengan laptop ataupun oleh *smartphone* saja.

Namun disamping kemudahan-kemudahan dan efektivitas yang diperoleh dari pengembangan IoT tersebut, dibutuhkan pengamanan data dari proses *sharing* data antar perangkat, khususnya data yang bersifat sensitif maupun strategis, sehingga harus dilengkapi dengan prosedur pengamanan data dari usaha-usaha pencurian dan pembobolan data.

DAFTAR PUSTAKA

- [1] Johnson, och K.. Bombs, Bugs, Drugs and Thugs: Intelligence and America's quest for security. New York: New York University Press, 2002
- [2] Greg Dunko, et al, A Reference Guide to the Internet of Things, Bridgera LLC, 500 West Peace Street, Raleigh, NC 27603, 2017
- [3] Anwar, S., Membangun Keamanan Maritim Indonesia Dalam Analisa Kepentingan, Ancaman, dan Kekuatan Laut. Jurnal Pertahanan & Bela Negara, 69-90, 2018
- [4] Ali, I. M., Prakoso, L. Y., & Sianturi, D, Strategi Pertahanan Laut dalam Menghadapi Ancaman Keamanan maritim di Wilayah Laut Indonesia. Strategi Pertahanan Laut, 2021.
- [5] Anwar, S., Membangun Keamanan Maritim Indonesia Dalam Analisa Kepentingan, Ancaman, dan Kekuatan Laut. Jurnal Pertahanan & Bela Negara, 69-90, 2018
- [6] Bainus, A., & Rachman, J. B., Kepentingan Nasional dalam Hubungan Internasional. Intermestic: Journal of International Studies, 109-115, 2018.
- [7] Buzan, People, States, and Fear: The National Security Problem in International Relations, 75-83.
- [8] Furtado, X. International law and the dispute over the spratly Islands: Whither UNCLOS. Contemporary Southeast Asia, 386-404. 1999
- [9] Greg Dunko, et al, A Reference Guide to the Internet of Things, Bridgera LLC, 500 West Peace Street, Raleigh, NC 27603, 2017
- [10] Harefa, H.. Optimalisasi Fungsi Intelijen Kepolisian dalam Penyelidikan Tindak Pidana Narkotika yang Dilakukan Anggota Kepolisian (Studi Sat Intelkam Polres Solok). UNES Law Review, 44-52, 2018
- [11] INFSO D.4, Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, Internet of Things in 2020, Roadmap For The Future, Working Group Rfid Of The Etp Epos, Version 1.1 - 27 May, 2008
- [12] Intelligence, S. The new regulations in intelligence domain state that the intelligence collection disciplines are: ACINT/Acoustic Intelligence, HUMINT/Human Intelligence, IMINT/ Imagery Intelligence, MASINT/Measurement and Signature Intelligence, OSINT/Open Source Intelligence, SIGINT/Signal Intelligence, EW/Electronic Warfare, CYBERINT/Cyber Intelligence and MPE/Materiel and Personnel Exploitation.
- [13] Johnson, och K.. Bombs, Bugs, Drugs and Thugs: Intelligence and America's quest for security. New York: New York University Press, 2002
- [14] Jaya, R. S. F., Widayat, W., & Zulkifli, Z.. Upaya Peningkatan Profesionalisme Insan Intelijen Dalam Rangka Cegah Dini Dan Deteksi Dini Ancaman Di Lingkungan Satuan

Penggalangan Badan Intelijen Strategis Tentara Nasional Indonesia (Bais TNI) Tahun 2016 (Doctoral dissertation, STIE Widya Wiwaha), 2016

- [15] Kementerian Kelautan dan Perikanan Republik Indonesia, Laporan Kementerian Kelautan dan Perikanan Republik Indonesia Tahun 2014, (Jakarta: Sekretaris Jenderal KKP RI, , p. 18-20, 2014
- [16] Kementerian Pertahanan Republik Indonesia., Postur Pertahanan Negara. Jakarta: Kementerian Pertahanan Republik Indonesia, h.23, 2015
- [17] McNicholas, M. Maritime security: an introduction. Butterworth-Heinemann, 2016.
- [18] Siregar, Q. A. Komunikasi dalam Kinerja Intelijen Keamanan. Jurnal Sosioteknologi, 13(1), 72-75, 2014
- [19] Undang-Undang Nomor 3 Tahun 2002 Tentang Pertahanan Negara
- [20] UU Nomor 31 Tahun 2014 Tentang Perubahan Atas UU No 13 Tahun 2006 Mengenai Perlindungan Saksi dan Korban.
- [21] Wahyono, S.K, , Pengertian dan Lingkup Keamanan Nasional, KSKN UI, 19-20, 2003