LAW AND JUSTICE REVIEW JOURNAL
2021, Vol. 1, No. 1, 12 – 25
http://dx.doi.org/10.11594/ lrjj.01.01.03

Research Article

Cyber Espionage Sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia

Evi Dwi Hastri*

Universitas Wiraraja

Article history:
Submission June 2021
Revised June 2021
Accepted June 2021

**Corresponding author:*
E-mail: gek.eviy@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk menganalisis norma yang memiliki kekaburan (*Vague Norm*) terhadap *Cyber Espionage* terkait kemampuan hukum Indonesia dalam mengakomodir serangan *Cyber Espionage*. Selain itu penelitian ini juga bertujuan untuk menganalisis upaya Indonesia dalam mengatasi serangan *Cyber Espionage* yang dapat mengancam stabilitas pertahanan dan keamanan Negara. Jenis penelitian dalam Metode penelitian hukum yang digunakan adalah yuridis normatif dengan tiga pendekatan masalahyaitu pendekatan Perundang-Undangan (*Statute Approach*), pendekatan konseptual (*Conceptual Approach*), dan pendekatan perbandingan (*Comparative Approach*). Bahan hukum primer dan sekunder yang telah dikumpulkan akan diolah melalui metode deduktif dan dilakukan analisis bahan hukum yaitu dengan interpretasi sistematis dan interpretasi ekstentif. Sehingga berdasarkan hasil pembahasan, maka terdapat norma yang kabur (*Vague Norm*) tentang *Cyber Espionage* yang berpengaruh terhadap hukum Indonesia dalam mengakomodir. Upaya yang dilakukan Indonesia menghadapai *Cyber Espionage* diluar upaya yuridis dimulai dengan upaya preventif *Cyber Security* dan *Cyber Defence*, pengoptimalan peran TNI, BIN, dan POLRI sebagai sumber daya nasional dalam mempertahankan pertahanan Negara.

Keywords: *Cyber Espionage dan Keamanan Negara Indonesia*

Pendahuluan

Negara merupakan sebuah organisasi publik yang terdiri dari beberapa unsur yaitu wilayah, rakyat, pemerintah yang berdaulat, dan pengakuan dari Negara lain, sehingga dari keempat unsur tersebut dapat digukanan untuk menajalankan sistem didalamnya baik sistem pemerintahan dan sistem hukumnya. Dalam suatu Negara terdapat masyarakat sebagai penggerak mobilitas sistem tersebut. Layaknya manusiasebagai makhluk sosial yang tak bisa hidup tanpa melakukan hubungan dengan makhluk sosial lainnya, Negara juga membutuhkan campur tangan dari Negara lain yang merupakan bentuk dari hubungan sosial antar lintas batas. Seperti dalam melakukan kerjasama Internasional dalam beberapa sektor misalnya sektor perdagangan, pendidikan dan politik, selain itu juga melakukan hubungan perjanjian bilateral antar Negara.

How to cite:
Hastri, E. D. (2021). Cyber Espionage sebagai Ancaman terhadap Pertahanan dan Keamanan Negara Indonesia. *Law and Justice Review Journal*. *1*(1), 12 – 25. doi: 10.11594/lrjj.01.01.03

Negara dalam pergaulan Internasional, berkepentingan untuk menjelaskan tentang kekayaan alam dan potensi yang dimiliki kepada Negara dan Bangsa lain demi kemajuan hubungan kerjasama dan pembangunan Internasional. Sensitifitas terhadap perkembangan Internasional semakin tinggi akibat semakin terbukanya sistem Internasional di bidang teknologi dan komunikasi. Di satu sisi hal ini membuka peluang bagi Negara untuk melakukan kerjasama demi mencapai kepentingan mereka dan disi lain hal ini memicu terjadinya persaingan yang tidak sehat. Namun, dalam melakukan kerjasama ini akan timbul persaingan global baik dalam sektor ekonomi mulai dari kualitas dan kuantitas produk yang disajikan, sektor pendidikan dalam mencetak sumber daya manusia yang berpotensi dan mampu berdaya saing, sektor militer dalam kaitannya dengan kekuatan untuk pertahanan dan keamanan negara, hingga pada sektor politik dalam pencapaian strategi. Persaingan global merupakan suatu tahap perkembangan fenomena budaya yang harus dilalui oleh kemajuan peradaban dan kehidupan. Hal yang terpenting adalah bagaimana menentukan sikap dan mempersiapkan diri untuk menghadapi datangnya fenomena tersebut.

Indonesia sebagai suatu Negara yang merupakan sebuah organisasi atau lembaga tertinggi dari kelompok masyarakat yang terdiri dari sekumpulan orang di wilayah tertentu, yang memiliki cita-cita untuk hidup bersama, serta memiliki sistem pemerintahan yang berdaulat maka Indonesia harus mampu mewujudkannya melalui kekuasaan yang dimiliki yaitu kedaulatan sehingga dalam melaksanakan jalannya pemerintahan suatu Negara dapat terlaksana melalui pemerintahan yang berdaulat. Sebab itulah melalui kekuasaan yang dimiliki oleh Indonesia berupa kedualatan, maka untuk menghadapai persaingan global bisa menggunakannya sebagai bentuk proteksi diri dari serangan luar yang dapat mengancam pertahanan dan keamanan Negara.

Persaingan global tersebut dapat memicu Negara – Negara lain untuk bersaing secara tidak sehat dan melalukan berbagai macam upaya untuk memperkuat Negaranya sendiri dengan cara melumpuhkanNegara pesaingnya. Upaya itu salah satunya dilakukan melalui kegiatan Spionase (memata-matai) terhadap Negara yang menjadi target untuk ditaklukkan. Informasi dan data rahasia yang didapat dari kegiatan spionase akan digunakan untuk mengetahui kelemahan-kelemahan Negara tersebut sehingga mereka dapat dengan mudah untuk mengatur dan memperkuat strategi penyerangan. Untuk bisa mendapatkan informasi rahasia dari Negara yang menjadi objek spionase adalah dengan cara memasuki wilayah terlarang dari Negara yang menjadi objek spionase tersebut. Di wilayah terlarang ini mereka yang ditugaskan untuk mengambil data dan informasi rahasia adalah mereka yang biasa disebut sebagai agen mata-mata atau agen spionase dengan cara membawa sebagian atau seluruh informasi yang didapat mengenai kerahasiaan Negara yang didalamnya mencakup kelemahan maupun kekuatan dari Negara yangmenjadi target mata-mata. Namun cara konvensional seperti ini sudah tidak relevan lagi, selain memakan waktu yang cukup lama, data dan informasi rahasia yang ingin didapat juga terbatas, selain itu keberadaan subjek spionase akan lebih mudah diketahui. Sehingga dalam waktu kapanpun, agen spionase atau agen mata-mata dapat melakukan sabotase dan penyadapan (intersepsi) dengan berbagai cara yaitu dengan memanfaatkan kecanggihan teknologi dan percepatan digital, maka beragam kejahatanpun akan muncul dengan variasi masing-masing. Salah satu diantaranya yaitu *Cyber Espionage* atau Spionase melalui dunia maya.

Pemanfaatan *Cyber Space* (dunia maya) dalam melakukan kegiatan Spionase melalui penyadapan (intersepsi) adalah dengan menyerang sistem malware. Penyerangan tersebut dilakukan dengan menyusupmasuk ke dalam sistem malware untuk melakukan pengambilan data dan informasi rahasia Negara yang dijadikan target mata-mata. Dengan beragamnya kegiatan Spionase melalui kemampuan teknologi dan informasi seperti diatas, sehingga dengan sangat mudah penyadapan (intersepsi) dilakukan untuk mengambil informasi rahasia dari Negara yang dijadikan target mata-mata.

Perkembangan teknologi informasi di bidang *Cyber* semakin membuka peluang bagi

setiap negara yang berambisi untuk menaklukkan Indonesia maupun Negara - Negara lain dalam melakukan aksi spionase melalui penyadapan. Aksi ini yang dikenal dengan *Cyber Espionage* menjadi semakin marak dan semakin mudah dilakukan karena regulasi yang mengatur tentang perbuatan Spionase melalui penyadapan masih menamppakan kelemahannya dalam mencakup permasalahan ini. Mengingat Spionaseatau aksi mata-mata yang dilakukan melalui cara-cara peperangan sangat jauh berbeda dengan denganaksi mata-mata yang dilakukan tanpa adanya peperangan yaitu melalui penyadapan. Hal inilah yang justru menjadi kelemahan Pemerintah Indonesia dalam mengambil sikap dan menentukan arah kebijakan terhadap kasus *Cyber Espionage*.

Pada dasarnya tindakan penyadapan adalah suatu cara dari kegiatan spionase, karena dalam era modern seperti ini kegiatan spionase yang paling memungkinkan untuk dilakukan dengan sedikit resiko diketahui pihak yang dimata-matai adalah dengan penyadapan. (Atmadja, 2017). Dari sini sudah dapat terlihat betapa berbahayanya kegiatan spionase asing karena merupakan sebuah kejahatan yang dapat merugikan dan mengganggu stabilitas keamanan dan pertahanan Negara. Berikut contoh kasus kegiatan Spionase asing yang dilakukan melalui penyadapan dengan memanfaatkan kecanggihan teknologi informasi dan komunikasi: Dunia internasional baru-baru ini dikejutkan oleh kasus spionase yang dilakukan Amerika Serikat dan Australia terhadap pemerintah Indonesia. Kepala Badan Intelijen Negara (BIN) Marciano Norman mengatakan, bahwa Australia telah melakukan penyadapan percakapan telepon sejumlah pemimpin Indonesia dalam kurun waktu 2007-2009" (Sudiarta, 2015)

Kasus tersebut menjelaskan bahwa kondisi persaingan global saat ini berada dalam tahap yang sangat mengkhawatirkan. Selain karena saat ini sudah berada dalam era digital (*digital age*) dimana kecanggihantekhnologi informasi dan komunkasi dapat disalah gunakan oleh pemakainya dalam hal ini adalah agen spionase, dan ini juga memperlihatkan kelemahan Indonesia sebagai target mata-mata dari segi instrumen hukumnya. Pasalnya, tindakan spionase yang dilakukan melalui penyadapan dengan menggunakan pemanfaat teknologi dan informasi dapat menghilangkan batas-batas wilayah (*borderless*) sehingga akan berdampak pada kedaulatan suatu Negara yang sifatnya akan menjadi kabur ketika informasi dan data rahasia mudah diakses tanpa adanya batas antar ruang dan waktu. Sehingga permasalahan yang timbuldan akan dilakukan telaah lebih lanjut adalah Apakah hukum Indonesia mampu mengakomodir terhadap serangan *Cyber Espionage* serta bagaimana upaya Indonesia dalam mengatasi serangan *Cyber Espionage* yang dapat mengancam stabilitas pertahanan dan keamanan Negara.

Jenis penelilitan hukum yang dipergunakan dalam penelitan ini adalah penelitian hukum normatif (Yuridis Normatif). Sedangkan Pendekatan masalah yang digunakan pada penelitian ini adalah pendekatan Perundang-Undangan (*Statute Approach*), pendekatan konseptual (*Conceptual Apprach*), dan pendekatan perbandingan (*Comparative Approach*). Bahan hukum yang diperoleh diharapkan dapat menunjang penulisan Penelitian ini yang terdiri dari bahan hukum primer dan sekunder. Bahan hukum primer adalah bahan hukum yang terdiri dari peraturan perundang-undangan, dan putusan-putusan hakim yang dijadikan sebagai yurisprudensi. Bahan hukum sekunder adalah bahan hukum berupa publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi misalnya seperti buku literatur, Majalah, Jurnal Hukum, dan Penelitian hukum terkait dengan penelitian yang diambil. Teknik yang dipilih dalam pengumpulan bahan hukum adalah Penelitian Kepustakaan (*Library Research*) dan teknik pengolahan bahan hukum melalui metode deduktif. Analisis pada penelitianini menggunakan teknik analisa bahan hukum deskripstif kualitatif dengan penafsiran yang digunakan adalah penafsiran sistematis dan penafsiran ekstentif.

Hukum Indonesia dalam Mengakomodir Serangan *Cyber Espionage*

Pesatnya perkembangan teknologi informasi menjadikan seluruh sistem kehidupan berubah dan semakin berkembang, yang pada awalnya dilakukan dengan cara-cara konvensional dan kini cukup dengan hanya

menggunakan percepatan digital maka seluruh kegiatan mulai dari berinteraksi sosial, hingga melakukan segala macam bentuk transaksi dengan sangat mudah dapat dilakukan. Fenomena seperti ini telah menjajah seluruh lapisan sistem kehidupan di dunia, karena melalui media ini segala macam bentuk kejahatanpun timbul. Kondisi ini menandakan bahwa sistem hukum nasional maupun internasional juga harus siap. Siap dalam skala global karena cakupannya tidak hanya dibatasi oleh batas teritorial geografis.

Dimasa sekarang ini segala sesuatunya akan selalu berhubungan dengan komputer dan internet, dengan segala konsekuensinya. Begitu juga dunia spionase atau mata-mata. *Cyber Espionage* kini bukan lagi cerita atau film fiksi ilmiah lagi, namun merupakan sebuah fenomena yang amat nyata. Meski tidak ada bukti, namun tidak akan terkejut apabila sudah banyak pemerintah negara-negara didunia yang menggunakan *Cyber Espionage*, dan bisa saja jauh lebih canggih dari sekedar virus trojan GhostNet ini. Dan tentu saja korban *Cyber Espionage* tidak akan mengakui terang-terangan kalau informasi yang dimilikinya bocor ke pihak lain. Salah satu kejahatan inkonvensional tersebut diatas salah satu metode yang digunakanan yaitu Penyadapan atau Intersepsi yang secara umum di Indonesia telah mengaturnya dalam Pasal 31 Undang- Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), pada Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, dan Pada Pasal 31 Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara. Pada prinsipnya penyadapan merupakan suatu kegiatan dengan menembus masuk secara paksa tanpa diketahui oleh objek penyadapan melalui media teknologi informatika. Namun dari ketiga regulasi tersebut memiliki definisi berbeda khususnya terhadap tujuan dilakukan penyadapan atau intersepsi.

Perbedaan tujuan dilakukan penyadapan menunjukkan adanya otoritas tertentu sehingga sangat sulit menyamakan persepsi, dan perbedaan ini memiliki kecenderungan yang justru dapat membahayakan sertadapat menjadi celah hukum. Perlu disinggung bahwa penyadapan dengan tujuan materil dan untuk mempertahankan kebenaran formil secara publik dapat dibenarkan (*Lawful Interception*) sedangkan penyadapan dengan tujuan yang dinilai dapat merugikan pihak-pihak terkait dikatakan sebagai bertentangan dengan hukum (*Unlawful Interception*). Tindakan *Unlawful Interception* merupakan suatu ancaman bagi subjek hukum baik perorangan secara individu kaitannya dengan hak privasi maupun negara sebagai subjek hukum Internasional yang besar kaitannya dengan informasi kerahasiaan negara. Informasi yang berhasil disadap akan sangat riskan terhadap serangan-serangan dari luar (*out of risk*) yang dapat mengancam terhadap pertahanan dan keamanan negara.

Penggunaan fasilitas *cyber* untuk mendukung seluruh kegiatan mengakses dalam domain yangberbeda disetiap pengguna termasuk kegiatan penyadapan didalamnya merupakan bentuk pelanggaran terhadap ketentuan hukum penggunaan dunia maya (*cyber space*) di berbagai negara termasuk di Indonesia. Dengan munculnya kejahatan di dunia maya (*Cyber Crime*) berbentuk *Cyber Espionage* maka pada tanggal 5 November 2013 Indonesia memberanikan diri untuk turut serta dalam Resolusi Anti Spionase Perserikatan Bangasa-Bangsa yang telah mendapat dukungan lebih dari 193 Negara anggota PBB. Keikutsertaan Indonesia dalam Resolusi tersebut menandakan bahwa Indonesia merasakan dan memandang bahwa tindakan spionase adalah sangat berbahaya bagi kelangsungan stabilitas keamanan Negara.

Kemunculana *Cyber Espionage* merupakan perpaduan antara tiga kejahatan yang dilakukan dalam satu siklus yaitu penyadapan (Intersepsi), Kejahatan Telematika (Teknologi Informatika), dan Spionase (Aksi Mata-Mata). Pada perkembangannya melalui penyadapan kejahatan yang dinamakan *Cyber Espionage* yang mulanya merupakan kejahatan konvensional mata-mata yang bercirikan pertemuan secara fisik yang kini mengalami revolusi kejahatan (*revolution of crime*) dengan menunggangi *cyber space* sebagai transformer. Sistem kerja pada konteks *Cyber Crime* berasal dari tiga komponen utama yang terdiri dari:

1. Komputer
   Sebagai media, komputer berkontribusi besar terhadap keberlangsungan penggunaan

internet karena dengan cara mengoperasikan komputer semua jaringan mulai bekerja sesuai kemauan personalyang secara langsung menggunakan tombol-tombol pada keyboard dan CPU (*Central Processing Unit*) yang memiliki tugas untuk melaksanakan perintah dan mengolah data dari perangkat lunak dan juga sebagai tempat penyimpanan semua data-data penting yang akan secara berkelanjutan di *share* ke beberapa titik melalui situs-situs tertentu yang sudah disiapkan oleh pengolala. Maka dari keleluasaan dari para pengguna komputer muncullah istilah kejahatan komputer (*Computer Crime*) yang timbul dari kegiatan pemanfaatan komputer sebagai media internet.

2. Telematika
   Telematika secara bahasa merupakan singkatan dari Telekomunikasi dan Informatika. Pada konsep dua komponen ini lahir beberapa jenis hukum yang diwujudkan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Pengiriman data melalui *Dial Up System* yang dihubungkan ke jaringan internet baik melalui jalur telepon, sistem komputer, antena khusus nirkabel, *wireless system*, dan semua media telekomunikasi pada penyampaian informasi satu arah dan juga timbal balik dengan menggunakan sistem digitaladalah sangat dimungkinkan. Sehingga lahir Hukum Telematika atau lebih dikenal dengan Hukum Konvergensi.
3. Internet
   Internet berasal dari kata *Interconnection Networking* yang memanfaatkan seluruh jaringan komputer yang tersambung menggunakan *Internet Protocol* (IP) atau *Transmission Control Protocol* (TCP). Dalam jaringan ini disebut sebagai dunia maya atau *Cyber Space* yang memuat berbagai macam *fiture* dan *content* yang tidak dapat dipisahkan satu sama lain dengan teknologi saat ini. Atmosfir ini juga yang menyebabkan bermacam-macam kejahatan dunia maya (*Cyber Crime*) itu timbul karena etika pengguna yang masih minim. Perkembangan ini pula yang mengiringi kemunculan hukum siber atau *Cyber Law*.

Dari ketiga unsur diatas mendeskripsikan bahwa adanya mata rantai yang akan terus berkaitan antara komputer, teknologi informatika, dan internet. Semakin kencangnya pemanfaatan internet membuat stabilitas dan kondusifitas tatanan kehidupan sangat mengkhawatirkan mengingat pengguna internet yang masih minim moral dan etika, dan juga masih belum bijak dalam menggunakan kelebihan ini.

Selain itu terdapat pula aturan dalam konteks Hukum Internasional yaitu dalam Konvensi Den Haag IV 1907. Pasal 29 Konvensi ini menyatakan unsur-unsur spionase yang berbunyi : "Sesesorang hanya dianggap sebagai mata-mata apabila melakukan perbuatan secara sembunyi-sembunyi atau diam-diam dan berpura-pura untuk mendapatkan informasi di daerah operasi dari negara berperang dengan maksud untuk memberitahukannya kepada pihak musuh". Tindakan memata-matai (Spionase) diatur dalam Konvensi Internasional yaitu Konvensi Den Haag yang mengatur tentang tata cara berperang dan alat-alat perang, sedangkan Konvensi Jenewa mengatur tentang perlindungan terhadap korban perang. Pada Pasal 29, 30, dan 31 Konvensi Den Haag IV 1907 tentang Hukum dan Kebiasaan Perang di Darat menyebutkan bahwa seseorang dapat dikatakan sebagai mata-mata apabila perbuatannya dilakukan secara sembunyi-sembunyi atau diam-diam serta berpura-pura dalam rangka mencari informasi rahasia dari negara yang berperang. Sedangkan dalam Pasal 46 Konvensi Jenewa 1949 (Indonesia meratifikasi dalam Undang-Undang Nomor 59 Tahun 1958) Protokol Tambahan 1 menyebutkan aturan tentang perbuatan memata-matai adalah apabila tentara perang dari negara lain tertangkap pada saat melakukan kegiatan spionase atau mata-mata maka tidak akan mendapat status hukum sebagai tawananan perang melainkan dianggap sebagai mata-mata dantidak akan mendapat haknya sebagai tawanan perang sebagaimana Konvensi ini.

Dapat ditarik benang merah bahwasanya spionase pada umumnya secara konvensional dilakukan dalam masa perang, yang dikatakan masa perang menurut prinsip hukum umum adalah bertemunya pasukan bersenjata antar

negara di satu titik untuk merebut dan mempertahankan kedaulatan suatu negara secara paksa dan ada salah satu cara yang dilakukan untuk mencapai tujuan tersebut adalah dengan strategi memata-matai. Legalitas kegiatan spionase dalam masa perang (*espionage in wartime*) diatur dalam Konvensi Jenewa 1949 yang terdiri dari 4 perjanjian dengan 3 Protokol tambahan serta di atur juga dalam Konvensi Den Haag 1907 yang terdiri 13 bagian dan 2 Deklarasi tambahan.

Cyber Warfare dijaman yang telah berkembang pesat ini, tidak hanya dilakukan oleh suatu negara dalam hal ini pasukan militernya saja, tetapi dapat dilakukan oleh individual, organisasi, maupun kelompok-kelompok lainnya yang mengatas namakan nasionalisme suatu bangsa. Dalam hal *Cyber Warfare* ini, kebanyakan yang melakukan serangan-serangan dilakukan oleh sekelompok komunitas yang mereka sebut diri mereka sebagai Anonymous. Dalam klasifikasinya, *Cyber Espionage* dapat dianggap sebagai bentuk dari *Cyber Warfare*. Karena *Cyber Espionage* merupakan jenis kejahatan memata-matai untuk mendapatkan informasi rahasia yang memanfaatkan jaringan internet melalui *malware* dengan berbagai jenis dan tingkat bahaya yang beragam, yang dalam mengkalisifikasikan perbuatan tersebut terhadap perbuatan yang dapat mengancam pertahanan dan keamanan suatu negara yaitu stabilitas NKRI sesuai dengan Pasal 10 Undang-Undang Nomor 3 Tahun 2002 Tentang Pertahanan Negara, dapatdijabarkan sebagai berikut:

1. *Cyber Espionage* mengancam kedaulatan negara
2. *Cyber Espionage* mengancam kutuhan wilayah
3. *Cyber Espionage* mengancam kehormatan dan keselamata bangsa
4. *Cyber Espionage* mengancam perdamaian regional dan internasional

Dari beberapa indikator diatas, menjelaskan bahwa *Cyber Espionage* merupakan ancaman militer yang menempatkan TNI sebagai komponen utama yang memiliki kapabilitas dalam bertindak menurut hal-hal diatas. Tindakan yang dapat dilakukan oleh TNI selaku komponen utama dalam melaksanakan penyelenggaraan pertahanan negara dapat dilihat dalam Pasal 6 ayat (1) Undang-Undang Nomor 34Tahun 2004 tentang Tentara Nasional Indonesia bahwasanya TNI memiliki fungsi dalam menangkal setiap bentuk ancaman militer dan ancaman bersenjata baik dalam maupun luar serta menindak setiap bentuk ancaman tersebut. Namun yang menjadi kerancuan dalam hal ini adalah tidak jelasnya TNI dalam melakukan tindakan apabila serangan *Cyber Warfare* dalam bentuk *Cyber Espionage* tersebut menyerang stabilitas pertahanan dan keamanan NKRI karena hukum Indonesia tentang *Cyber Espionage* tidak secara tegas mengatur, hanya sebagaian yang menjelaskan tentang tindakan memata-matai itupun dilakukan dengan cara konvensional. Sehingga dalam penerapannya hukum Indonesia tentang *Cyber Espionage* terdapat kekaburan norma (*Vague Norm*) dan membutuhkan penafsiran secara ekstentif yaitu melakukan kegiatan pemahaman terhadap ketentuan hukum yang ada dengan tetap mendasarkan diri pada prinsip- prinsip yang ada di dalam ketentuan tersebut. Selain itu penafsiran sistematis juga dibutuhkan untuk mendukung dalam memberikan terang terhadap penafsiran pada Pasal yang dianggap sesuai dengan*Cyber Espionage*.

Aturan tentang kejahatan spionase dalam peraturan perundang-undangan nasional terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Pidana Militer (KUHPM). Unsur-unsur spionase sebagai sebuah kejahatan tertuang dalam Pasal 117 KUHP pada Buku Kedua Bab 1 tentang Kejahatan Terhadap Keamanan Negara adalah sebagai berikut: "Barang siapa tanpawenang, dengan sengaja Memasuki bangunan Angkatan Darat atau Angkatan Laut atau Kapal Perang Melalui jalan yang bukan jalan biasa, Memasuki daerah terlarang, Membuat, mengumpulkan,mempunyai, menyimpan, menyembunyikan, atau mengangkut gambar-potret atau gambar-tangan dan keterangan-keterangan atau petunjuk-petunjuk lain mengenai daerah terlarang".

Sedangkan dalam Pasal 67 KUHPM unsur-unsur kegiatan spionase dijabarkan sebagai berikut : "Barang siapa dengan sengaja untuk

keperluan musuh berusaha mendapatkan informasi demi kepentingan perang di perahu atau pesawat udara dari angkatan perang di dalam garis pos depan di suatu tempat atau pos yang diperkuat atau di duduki didalam bangungan angkatan perang dalam waktu perang dengan sembunyi-sembunyi, dengan pernyataan palsu, dengan penyamaran, menyusup melalui jalan pintas, dan mencatat suatu hal tentang kepentingan militer.

Karakterisasi suatu perbuatan hukum yang dapat menimbulkan akibat hukum tidaklah hanya berpedoman pada konteks yang dapat ditimbulkan melainkan spektrum universal sebagai kaitannya ke arah yang dipengaruhi oleh unsur perbuatan dan kesalahan (*act and mistake*). Unsur-unsur penyadapan atau intersepsi dalam Pasal 31 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) terdiri dari setiap orang (subjek hukum/manusia atau badan hukum/pelaku), dengan sengaja, tanpa hak (*onrechtmatighdaad*), objek (dokumen elektronik), milik orang lain (privasi). Sedangkan ayat (2) pada Pasal yang sama unsur-unsurnya adalah Setiap orang (subjek hukum/manusia atau badan hukum/pelaku), dengan sengaja, tanpa hak (*onrechtmatighdaad*), objek (dokumen elektronik), tidak bersifat publik (rahasia), dalam sistem komputer milik orang lain, menyebabkan dan tidak menyebabkan perubahan, penghilangan, dan/atau penghentian informasi elektronik yang sedang di transmisikan.

Unsur perbuatan penyadapan juga dapat ditemukan pada Undang-Undang tentang Telekomunikasi Nomor 36 Tahun 1999 pada Pasal 40 yaitu Setiap orang (subjek hukum/manusia atau badan hukum/pelaku), melakukan penyadapan informasi, jaringan telekomunikasi dalam bentuk apapun.

Pada kedua Pasal dari Undang-Undang yang berbeda diatas, batasan tentang penyadapan belum terdapat pembahasan tentang *locus delicti* (lokasi atau tempat terjadinya peristiwa) karena bisa saja dilakukan di luar batas teritorial Indonesia dan dengan sangat mudah menghapus jejak digital melalui perangkat yang digunakan dan memanipulasi pengaturan *Share Location*. Tidak jelasnya kedudukan pelaku pada saat melakukan kejahatan maka asas *territorial active* tidak dapat diterapkan.

Pembahasan selanjutnya yang juga belum terdapat dalam Pasal tentang penyadapan atau intersepsi adalah masalah *tempus delicti* (kapan terjadinya peristiwa) karena pelaku dapat dengan mudah membuat waktu dan tanggal terjadinya peristiwa berbeda dengan yang sebenarnya hanya dengan mengubah *setting system* pada perangkat yang digunakan.

Keadaan yurisdiksi suatu negara yang dihubungkan dengan batas-batas georafis menjadi kabur dalam menyikapi kejahatan penyadapan dimana sangat dimungkinkan dilakukan oleh warga negara asing yang berada di luar negeri. Sifat multidimensi transnasional dan *borderless* pada kejahatan ini merambah pada tataran transnasional sehingga penerapan yurisdiksi hukum suatu negara mengalami kekaburan. Kejahatan dunia maya yang bersifat transnasional dan *borderless* memberikan implikasi terhadap Indonesia yang nantinya dapat menyerang Indonesia kapan saja, sehingga hukum di Indonesia mengalamikesulitan memberlakukan yurisdiksi hukumnya. Disamping itu pula dengan asas *personality, territorial,* dan *universal* akan semakin menghambat dalam penegakan hukum karena bukan tidak mungkin kejahatan ini selalu disamakan dengan kejahatan konvensional.

Oleh karena itu penerapan prinsip ubikuitas (*the principle of ubiquity*) dirasa cukup mumpuni dalam menyikapi kejahatan mayantara (*Cyber Crime*) yaitu pada pembahasan ini adalah kasus penyadapan (Intersepsi). Prinsip ini menegaskan bahwa setiap delik yang dilakukan baik didalam maupun diluar batas teritorial negara dapat diselesaikan dengan yurisdiksi pada setiap negara yang bersangkutan. Sehingga, apabila Indoensia menjadi target atau korban dari *Cyber Espionage* maka hukum Indonesia dapat diberlakukan dengan memperhatikan adanya *Locus Delicti* (tempat terjadinya peristiwa).

Namun saat ini yang menjadi problematika selanjutnya adalah apabila hukum di Indonesia dapat diberlakukan pada serangan ini lalu apakah hukum ini memiliki kapabilitas dalam mengakomodir sedangkan konteks kejahatan ini bukan lagi kejahatan konvensional yang bisa saja dapat diterapkan KUHP.

Mengingat banyaknya kendala yuridis seperti pembuktian, legalitas, dan yurisdiksi yang mengakibatkan semakin terlihat kelemahan dan celah hukum di Indonesia maka sudah selayaknya komponen legislatif sebagai pembuat kebijakan bertanggung jawab terhadap dampak dari perkembangan teknologi dan informasi yang mengakibatkan perubahan besar dalam seluruh aspek kehidupan masyarakat.

Namun, kembali hukum Indonesia masih belum memberikan kepastian hukum yang seharusnya diberikan sesuai dengan tujuan hukum itu sendiri, dimana masyarakat yang sedang berkembang maka hukum juga harus mampu merubah dan mengarahkan kegiatan manusia ke arah yang dikehendaki pembangunan dan pembaharuan itu secara cepat sebagai sarana pembangunan masyarakat untuk mencapai ketertiban dan kepastian hukum sehingga norma yang ada dalam masyarakat yang sedang bertansisisi sesuai dengan perkembangan. Hukum dalam arti norma sesuai dengan teori hukum pembangunan Mochtar Kusumaatmadja dalam kasus *Cyber Espionage* masih ambigu dan hukum Indonesia cenderung lemah dalam mengakomodir serangan *Cyber Espionage* yang dapat mengancam stabilitas pertahanan dan keamanan negara karena memiliki kekaburan norma (*Vague Norm*).

Kejahatan terhadap keamanan negara secara eksklusif temaktub dalam KUHP (Kitab Undang- Undang Hukum Pidana) pada Buku Kedua BAB I tentang Kejahatan Terhadap Keamanan Negara. Kejahatan spionase tergolong pada kejahatan yang berpotensi mengancam stabilitas pertahanan dankeamana negara Indonesia. Dalam Pasal tersebut hanya membahas aksi spionase secara langsung yang dilakukan dengan menembus masuk pada daerah pertahanan yang dilarang oleh Pemerintah Indonesia. Masih belum jelas apabila pelakunya bukan pasukan tentara atau pasukan bersenjata suatu negara yang berada dalam masa perang melainkan personal secara pribadi namun atas provokasi Pemerintah negara asing. Mengingat objeknya adalah Negara yang secara komprehensif berkaitan dengan masalah stabilitas pertahanan dan keamanan negara. Karena pada dasarnya persinggungan politik akan turut serta mempengaruhi perbuatan spionase. Selanjutnya kelemahan Pasal ini adalah bentuk memata-matai masih sangat klasik dimana kondisi virtual sudah sering digunakan dalam menjalankan aksi kejahatan sehingga apabila kasus spionase yang dilakukan tanpa bersinggungan secara fisik maka akan dengan sangat mudah lolos dari jeratan Pasal tersebut.

Pemanfaatan instrumen dunia maya memang rentan akan pelanggaran hukum sehingga sangat sulit dilakukan penindakan, mengingat masih lemahnya regulasi di Indonesia serta keterbatasan dalam ruang lingkup regulasi tersebut. Kelemahan ini oleh penulis dapat dijabarkan sebagai berikut:

1. Spionase, tentang pengertian dari istilah tersebut yang masih minim cakupannya hanya terbatas pada kegiatan mata-mata secara konvensional. Sedangkan spionase melalui internet (*Cyber Espionage*) sudah semakin nyata terlihat;
   Pembuktian pada kegiatan spionase masih belum ada pengklasifikasian secara tegas mengingat semakin beragamnya model spionase pada era digital saat ini yaitu *Cyber Espionage*. Misal, (a) pembuktian bahwa pencurian informasi rahasia negara melalalui pemanfaatan internet (penyadapan) tergolong pada aksi spionase; dan (b) pembuktian pelaku kejahatan *Cyber Espionage* merupakan tekananan Pemerintah dari Negara propaganda bukan atas kemauan pribadi. Kegiatan yang dilakukan diluar batas wilayah Indonesia ataupun sebaliknya yang subjeknya berada dalam ruang lingkup Indonesia sedangkan modus operandi serta *locus delicty* diluar batas teritorial Indonesia mempersulit pembuktian kasus spionase melalui penyadapan.
2. Kategori informasi rahasia masih belum jelas. Banyak tipe informasi rahasia yang akan mampu disalah artikan ketika tidak jelas pengklasifikasiannya.
3. Status hukum bagi pelaku masih belum ada kepastian yang jelas, karena pada dasarnya pelaku spionase masih cenderung dianggap berbeda dengan pelaku penyadapan akibatnya celah hukum semakin lebar. Sehingga harus ada ketentuan hukum bagi pelaku spionase melalui penyadapan.

4. Konsekuensi hukum yang rancu, dimaksud adalah akibat hukum dari perbuatan ini masih diibaratkan pedang bermata dua. Unsur-unsur yang termuat masih belum jelas antara pertanggungan jawaban pidana (pemidanaan) atau pertanggung jawaban negara melihat subjek dan objek pada *Cyber Espionage*.
5. Unsur-unsur perbuatan spionase yang masih terbatas pada pertemuan secara fisik. Harus ada klasifikasi secara substansial dan terekonstruktif mana perbuatan *Cyber Crime* diluar *Cyber Espionage* dan mana yang termasuk ke dalam *Cyber Espionage* karena spionase dengan memanfaatkan kecanggihan teknologi informasi dan internet tidak hanya terbatas pada penyadapan banyak istilah lain yang dipakai misal seperti *Unautirezed acces to computer system and service*, *Cyber sabbotage and extortation*, *Hiking,* dan masih banyak lagi.
6. Adanya otoritas tertentu yang diberikan kewenangan oleh Undang-Undang untuk mengakses informasi rahasia kenegaraan (*Lawful Interception*) guna kepentingan penyidikan misal yang hanya diperbolehkan adalah Badan Intelijen Negara. Jadi, pihak-pihak terkait dalam hal penyadapanguna kepentingan penyidikan dan penyelidikan harus tersentral dalam berkoordinasi dengan otoritas tersebut karena memang kewenangan mengakses hanya BIN (Badan Intelijen Negara) guna meminimalisisr penyalahgunaan wewenang oleh setiap pengguna kewenangan.
7. Penegasan hukum terkait legalitasdalam melakukan kegiatan spionase baik dalam masa perang (*espionage in war time*) maupun diluar masa perang (*espionage in peace time*). Karena pada dasarnya spionase dengan pemanfaatan internet (*Cyber Espionage*) justru tak melihat berada dalam masa perang atau dalam masa damai.

Mobilisasi kehidupan yang saat ini sudah berada dalam taraf modernisasi dan era dimensi kedua menunjukkan adanya perkembangan pada nilai-nilai yang hidup dalam masyarakat bukan hanya perubahan yang terjadi secara fisik berupa pembangunan infrastruktur namun juga terjadi pada perubahan secara visual yaitu pada tingkah dan perilaku dalam berinteraksi dan berkomunikasi, serta perubahan pola fikir, emosional yang secara renteng bersinggungan dengan moral masyarakat.

Manusia sebagai mahluk sosial yang sejatinya selalu berhubungan dan berinteraksi mulai dari skala kecil hingga skala global (Internasional) menandakan bahwa telah terjadi dinamika pergaulan hidup. Hal tersebut mendesak agar terwujudnya suatu tatanan hukum yang dapat dijadikan sebagai pedoman dalam bertingkah laku agar kepentingan masing-masing yang terdapat dalam hak dan kewajiban tetap seimbang untuk menjamin kepastian hukum. Hukum yang baik adalah hukum yang tumbuh dan berkembang dalam masyarakat (*the living law*) serta sesuai dengan nilai-nilai kehidupan masyarakat. Setiap masyarakat yang berada dalam tahap membangun selalu diidentikkan dengan adanya perubahan dimana hukum pada konteks ini memiliki fungsi untuk menjamin perubahan tersebut dengan tidak memposisikan dirinya sebagai alat melainkan sebagai sarana pengubah dengan tetap memperhatikan cerminan nilai kehidupan masyarakat yang berada dalam proses perubahan tersebut. Pendapat ini dikenal sebagai teori hukum pembangunan yang dipelopori oleh Mochtar Kusumaatmadja. Mochtar menegaskan bahwa hukum juga harus dapat membantu proses perubahan masyarakat itu. Menurut Mochtar bahwa pandangan yang kolot tentang hukum yang menitikberatkan fungsi pemeliharaan ketertiban dalam arti statis dan menekankan sifat konservatif daripada hukum, menganggap bahwa hukum tidak dapat memainkan suatu peranan yang berarti dalam suatu pembaharuan (Budhijanto, 2014)

Tak dapat dipungkiri bahwa kejahatan yang timbul ditengah-tengah masyarakat baik yang sedang dalam tahap berkembang maupun tidak sudah merupakan *fait accompli* dan tanpa sadar memposisikan dirinya selalu sejajar dengan perkembangan masyarakat karena pada hakikatnya tidak ada kejahatan tanpa masyarakat dan tidak ada masyarakat yang tanpa adanya kejahatan mengingat sifat manusia yang selalu ingin memenuhi kepentingan pribadi. Semakin kompleks kegiatan manusia

maka semakin bervariasi jeniskejahatan yang muncul karena kejahatan selain sebagai masalah kemanusiaan (etika dan moral) juga merupakan masalah sosial yang bisa diselesaikan dengan cara-cara sosial yaitu dengan cara mendorong hukum untuk bisa menekan kejahatan sekaligus memberi stimulasi perubahan dalam tatanan masyarakat.

Fenomena kasus *Cyber Espionage* merupakan model kejahatan modern yang saat ini memicu kekhawatiran pemerintah Indonesia dan menuntut agar revisi regulasi serta penemuan hukum baru (*Rechtvinding*) segera dilakukan. Urgensi regulasi memang selayaknya cepat dilakukan sebagai upaya proteksi diri terhadap ancaman tersebut karena pada hakikatnya hukum itu merupakan sarana untuk mencapai kepastian, keadilan, dan kemanfaatan sesuai dengan teori tujuan hukum.

Untuk menyikapi dinamika perkembangan teknologi yang semakin canggih totalitas hukum sangat diperlukan untuk mencapai ketertiban dan memberikan jaminan dalam masyarakat. Tingkat kejahatan yang notabene bergantung pada tingkat perubahan masyarakt itulah yang harus dipandang sebagai adagium bahwasanya hukum sebagai instrumen sosial harus mengikuti perkembangan masyarakat.

Kebijakan hukum yang diwujudkan dalam peraturan perundang-undangan pada kasus *Cyber Espionage* merupakan salah satu upaya untuk mencapai keniscayaan akan tercapainya kedamaian dan terjaminnya rasa khawatir dari suatu ancaman. Kepentingan-kepentingan yang bertentangan dengan konotasi merugikan hak orang lain dalam lalu lintas kehidupan sosial tidak dapat dihindari oleh sebab itulah peran hukum disoroti secara subtansial dan fungsional untuk bisa menjaga dan mempertahankan kondusifitas masyarakat.

Berdasarkan pada beberapa hal diatas maka penerapan Teori Hukum Pembangunan yang digemakan oleh Mochtar Kusumaatmadja yang memiliki kecenderungan dengan konsep *law as a tool of social enginering* yang telah dikemukakan oleh Roscoe Pound yang dikenal sebagai aliran *pragmatical legal realism* bahwasanya hukum merupakan suatu sarana dalam melakukan perubahan sosial dalam kehidupanmasyarakat, sangat pas dan cocok untuk diaplikasikan pada pembaharuan hukum serta pertimbangan- pertimbangan lain dalam usaha untuk merekonstruksi hukum yang harus bersifat dinamis dan sebagai pembawa kedamaian dan keadilan. Jadi sejatinya hukum tidak selalu hanya dipandang sebagai alat untuk mengatur dan mempertahankan nilai tapi juga harus dipandang sebagai sarana pembaharuan dalam masyarakat yang dapat menggiring pada perubahan dan pembangunan nilai yang hidup dalam masyarakat sehingga sisi lain dari hukum semakin terlihat.

Penafsiran hukum dapat dilakukan dengan memperhatikan teori dari Lawrence M. Friedman yang mengemukakan bahwa efektif dan berhasil tidaknya penegakan hukum tergantung tiga unsur sistem hukum, yakni struktur hukum (*struktur of law*), substansi hukum (*substance of the law*) dan budaya hukum (*legal culture*). Struktur hukum menyangkut aparat penegak hukum, substansi hukum meliputi perangkat perundang-undangan dan budaya hukum merupakan hukum yang hidup (*living law*) yang dianut dalam suatu masyarakat.

Sehingga teori sistem hukum Lawrence M. Friedman sangat harmonis jika dikaitkan dengan teori hukum pembangunan Mochtar Kusumaatmadja sebagaimana yang telah di ulas pada pembahasan terdahulu bahwasanya hukum yang baik adalah hukum yang tumbuh dan berkembang dalam masyarakat (*the living law*) serta sesuai dengan nilai-nilai kehidupan masyarakat. Setiap masyarakat yang berada dalam tahap membangun selalu diidentikkan dengan adanya perubahan dimana hukum pada konteks ini memiliki fungsi untuk menjamin perubahan tersebut dengan tidak memposisikan dirinya sebagai alat melainkan sebagai sarana pengubah dengan tetap memperhatikan cerminan nilai kehidupan masyarakat yang berada dalam proses perubahan tersebut.

Teori Hukum Pembangunan Mochtar Kusumaatmadja juga memakai kerangka acuan pada pandangan hidup masyarakat serta bangsa Indonesia yang meliputi struktur, kultur, dan substansi, yang sebagaimana dikatakan oleh Lawrence F. Friedman. Pada dasarnya memberikan dasar fungsi, hukum sebagai sarana pembaharuan masyarakat, dan hukum sebagai suatu sistem yang sangat diperlukan bagi bangsa Indonesia sebagai Negara yang sedang berkembang. Pokok-pokok

pikiran yang melandasi konsep tersebut adalah bahwa ketertiban dan keteraturan dalam usaha pembangunan dan pembaharuan memang diinginkan, bahkan mutlak perlu, dan bahwa hukum dalam arti norma diharapkan dapat mengarahkan kegiatan manusia kearah yang dikehendaki oleh pembangunan dan pembaharuan itu. Oleh karena itu, maka diperlukan sarana berupa peraturan hukum yang berbentuk tidak tertulis itu harus sesuai dengan hukum yang hidup dalam masyarakat. Negara yang diangkat pada penelitian ini untuk dilakukan anlisa terhadap perbandingan hukum yaitu Amerika Serikat yang menjadi target mata-mata oleh negara lain. Selanjutnya, Negara rival dari Negara Adidaya tersebut yang diambil sebagai perbandingan hukum adalah Cina dan Rusia. Amerika Serikatyang juga dikenal sebagai Negeri Paman Sam kini kekuatan militernya melemah. Kelemahan ini juga semakin nampak saat kasus kampanye Amerika Serikat disinyalir ada campur tangan dari Rusia sehingga Rusia dituduh dalam melakukan mata-mata melaui pembobolan e-mail para pemimpin Demokrat Clinton (*Cyber Espionage*). Kasus ini kemudian dilakukan tindakan hukum oleh Amerika Serikat berupa pengusiran Diplomat Rusia dari negara Amerika Serikat dan menjatuhkan sanksi lebih lanjut kepadaRusia sebagai pertanggung jawaban negara. Amerika Serikat dalam menghadapi serangan *Cyber Espionage* yang melanggar prinsip-prinsip kedaulatan wilayah, melaui hukum positif di negaranya adalah dengan cara pertanggung jawaban negara. Namun pada kasus ini, Amerika Serikat memiliki riwayat dalam melakukan serangan *Cyber Espionage* yang sama terhadap Cina dan Rusia sehingga klaim tersebutdapat ditanggalkan.

Upaya Mempertahankan Stabilitas Pertahanan dan Keamanan Negara Indonesia dari Serangan *Cyber Espionage*

Efek dari perang cyber bisa bermacam-macam, salah satu diantaranya adalah pengambilan informasi kerahasiaan negara menggunakan kecanggihan Teknologi Informasi atau yang dikenal dengan *Cyber Espionage* yang dapat mengancam pertahanan dan kemanan suatu Negara.

Tidak bisa dipungkiri bahwa dalam menghadapi tantangan ini, Indonesia dalam upaya-upaya yang harus dilakukan terhadap serangan *Cyber Espionage* sebagai bentuk *Cyber War* juga harus memperhatikan dari sisi preventif bukan hanya menyelesaikan permasalahan dengan jalur hukum namun upaya preventif juga sangat perlu dilakukan. Ketahanan nasional akan keamanan *cyber* sangatlah penting guna mencegah tindak-tindak kriminalitas dan menjaga keamanan industri-industri teknologi, sebagai salah satu contohnya adalah *Cyber Espionage* yang menyerang sistem informasi dan data-data kerahasiaan negara yang nantinya akan membahayakan terhadap stabilitas pertahanan dan keamanan negara.

Keamanan *Cyber* (*Cyber Security*) tidak dapat serta merta merupakan tanggung jawab pemerintah, justru hal ini juga merupakan tanggung jawab bersama karena pada kenyataannya setiap orang adalah *user*. Bukan berarti orang awam yang tidak pernah bersinggungan dengan Teknologi Informasi tidak akanterjerat dalam perangkap para pengguna yang dapat merugikan mereka. Sehingga keadaan semacam ini dimana keamanan *Cyber* lemah yang justru dijadikan sebagai jalur untuk menembus masuk kedalam jaringan sistem komputer lainnya. Serangan di dunia cyber tidak hanya menyasar pada sistem keamanan. Bahkan, sebagian besar malware menargetkan serangannya kepada para pengguna. Selanjutnya, malware tersebut bertugas mencuri password akun seseorang. Kesadaran tentang tanggung jawab berawal dari dalam diri setiap orang bahwasanya dirinya merupakan pengguna yang juga memiliki kemungkinan dapat dijadikan target, jadi harus ada rasa mawas diri dan kepedulian terhadap diri sendiri akan dampak nyata namun seakan tidak berimbas pada dirinya karena anggapan bahwa dirinya bukan merupakan pihak-pihak yang bbersinggungan langsung dengan Teknologi Informasi.

Selain persoalan tentang keamanan *Cyber* (*Cyber Security*), selanjutnya yang juga harus dimaksimalkan dalam melakukan upaya preventif adalah tentang pertahanan *Cyber* (*Cyber Defence*). Pertahanan *Cyber* (*Cyber Defence*) merupakan kebutuhan yang tak dapat terelakkan di era digital seperti saat sekarang ini

karena memang koherensi diantara keduanya sangat erat. Dengan melihat dampak dari *Cyber Warfare* tersebut, maka pembangunan pertahanan cyber adalah sebuah kebutuhan dan keharusan untuk melindungi pertahanan dan keamanan serta keberlangsungan hidup sebuah Negara. Selain melakukan upaya preventif baik dari segi keamanan (*Security*) maupun pertahanan (*Defence*) hal yang juga perlu diketahuia bahwa serangan *Cyber Espionage* adalah dengan memanfaatkan sistem malware. peran *malware* dalam serangan *Cyber Espionage* melalui media internet dapat dengan mudah masuk kedalam system komputer *user* yang tidak memiliki *cyber security* yang mumpuni sehingga melaui perantara tersebut semakin banyak terinfeksi dan menyerang sistem pertahanan *cyber* negara. Oleh karenaitu, sifat mawas diri dan kesadaran akan bahaya *Cyber Espionage* harus ditanamkan pada setiap individu.

Polri dalam kaitannya dengan kehidupan bernegara, merupakan alat negara yang berperan dalam memelihara keamanan dan ketertiban masyarakat, menegakan hukum, serta memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat dalam rangka terpeligharanya keamanan dalam negeri. agar dalam melaksanakan fungsi dan perannya diseluruh wilayah negera Republik Indonesia atau yang dianggap sebagai wilayah negara republik Indonesia tersebut dapat berjalan dengan efektif dan effisien. Undang-Undang No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, menegaskan tugas dan wewenang kepolisian dalam Pasal 13, Pasal 14, Pasal 15, dan Pasal 16 dimana Institusi Kepolisian merupakan salah satu pondasi penegak hukum yang diharapkan dapat memberikan pengayoman dan perlindungan kepada masyarakat terkait serangan *Cyber Espionage*.

Komponen selanjutnya yang posisinya dapat dilakukan pengoptimalan dalam upaya menghadapi serangan *Cyber Espionage* adalah TNI (Tentara Nasional Indonesia) dan BIN (Badan Intelijen Negara). Letak kedudukan Militer dalam kacamata hukum sebagai pemegang peran dalam mempertahankan keamanan negara dari segala ancaman menurut Pasal 3 Undang-Undang Nomor 34 Tahun 2004 Tentang TNI bahwasanya TNI berkedudukan dibawah Presiden dalam hal pengerahan dan penggunaan kekuatan militer sedangkan dalam hal administrasi dan kebijakan strategi pertahanan beradah di bawah koordinasi Departemen pertahanan. Badan Intelijen Negara sebagaimana yang dijelaskan dalam peran, tugas, fungsi, dan ruang lingkup Intelijen Negara pada Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negarasebagaimana dituangkan dalam Pasal 4 "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". Pada pasukan Militer TNI cenderung bertindak dalam melakukan upaya dalam mempertahankan kemanan dan stabilitas negara melalui penjagaan ketat batas- batas geografis dari serangan musuh, sedangkan BIN (Badan Intelijen Negara) titik ordinatnya berada pada upaya pendeteksian dini terhadap ancaman yang dinilai dapat membahayakan stabilitas keamanan negara. Dengan adanya BIN (Badan Intelijen Negara) yang juga merupakan elemen bagi pertahanan dan keamanan negara Indonesia yang sudah tentu sangat berkontribusi dan saling berkoordinasi dengan pasukan Militer untuk mempersatukan kekuatan.Namun pada Pasal 9 UU Nomor 17 Tahun 2011 tentangIntelijen Negara TNI termasuk dalam salah satu penyelenggara Intelijen Negara dalam pertahanan dan atau militer. Dapat diambil kesimpulan bahwa anggota TNI yang terpilih sekaligus sebagai anggota BIN mempunyai hak dan kewajiban sesuai Pasal 17 UU Nomor 17 Tahun 2011 tentangIntelijen Negara yang sama dengan seluruh penyelenggara Intelijen Negara. Maka oleh sebab itu, TNI mempunyai akses yang semakin kuat dalam tugasnya mempertahankan keamanan negara.

Kesiapan militer Indoensia dalam menjaga pertahanan dan keamanan negara masih sangat minim, hal ini sangat jelas terlihat dalam Pasal 7 ayat (2) tentang tugas pokok TNI dalam menegakkan kedaulatan negara, mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia yang hanya dibagi dalam dua aspek yaitu operasi militer untuk perang dan operasi militer selain perang. Pada operasi

militer selain perang ada 14 tugas yang dibebankan dimana tidak ada satupun yang membahas tentang aspek *Cyber*. Aspek ini bersama dengan konvergensi juga menentukan terhadap pengoperasian militer di luar perang. Peralatan perang bukan hanya pada senjata api melainkan berkembang menggunakan teknologi informasi karena dunia virtual yang juga tidak dapat dipisahkan dari setiap lini kehidupan termasuk dalamdunia militer.

Perlu di ingat bahwa negara sebagai subjek hukum internasional yang terbesar tidak dapat serta mertadisamakan dengan subjek hukum internasional lain pada tataran personal atau individu terlebih pada konteks pertanggung jawaban secara hukum. Adanya pertanggung jawaban hukum bagi negara ditentukan oleh sintesa yuridis secara internasional.

Konsep pertangung jawaban negara muncul berdasarkan dua unsur dan dau unsure tambahan yaitu:

1. Adanya perbuatan maupun kelalaian (*act or omission*);
2. Adanya pelanggaran hak dan kewajiban Internasional; dan
3. Diluar dari dua unsur tersebut terdapat pula unsur kerugian (*loss*) dan kerusakan (*damage*).

Akuntabilitas negara dalam hukum internasional bergantung dari bentuk kegiatan yang dilakukan yaitu kegiatan yang bertentangan dengan kewajiban internasioal negara tersebut, apabila kegiatan itu ada pada batas wilayahnya baik yang bersifat kenegaraan maupun pribadi secara perdata maka sudah pasti negara juga ikut bertanggung jawab oleh karena itu harus ada *check and balances* terhadap seluruh bentukaktivitas yang ada pada lingkup suatu negara.

Kesimpulan

Berdasarkan hasil penelitian dan analisis dalam pembahasan maka dapat disimpulkan bahwa hukum Indonesia dalam menghadapi *Cyber Espionage* sebagai bentuk dari *Cyber Warfare* yang dapat mengancam terhadap stabilitas pertahanan dan keamanan NKRI masih belum mampu mengakomodir karena hukum Indonesia tentang *Cyber Espionage* tidak secara tegas mengatur, hanya sebagaian yang menjelaskan tentang tindakan memata-matai itupun dilakukan dengan cara konvensional. Sehingga dalampenerapannya hukum Indonesia tentang *Cyber Espionage* terdapat kekaburan norma (*Vague Norm*) dan membutuhkan penafsiran secara ekstentif. Selain itu penafsiran sistematis juga dibutuhkan untuk mendukung dalam memberikan terang terhadap penafsiran pada Pasal yang dianggap sesuai dengan*Cyber Espionage*. Upaya Indonesia dalam menghadapi ancaman *Cyber Espionage* yaitu : melakukan upaya preventif dengan *Cyber Defense* dan *Cyber Security*, mengoptimalisasikan alat negara yaitu TNI (Tentara Nasional Indonesia) sebagai penjaga kemanan negara dan BIN (Badan Intelijen Negara) sebagai wadah untuk melakukan deteksi dini terhadap serangan dari luar selain itu juga menempatkan POLRI sebagai sumber hukum nasional sebagai komponen pendukung dalam upaya pertahanan negara. Upaya selanjutnya adalah Penangan terhadap upaya yuridis dalam Hukum positif Indonsia dengan konsep pertanggung jawaban negara.

Daftar Pustaka

Adolf, Huala, (2006). *Hukum Penyelesaian Sengketa Internasional*, Sinar Grafika, Jakarta

Anggriani, Jum, (2012). *Hukum Administrasi Negara*, Graha Ilmu, Yogyakarta

Antaranwes.com, *Kemhan Bangun Pusat "Cyber Defence"*, diterbitkan pada Minggu 21 Juli 2019,diakses dari https://www.antaranews.com/berita/366664/kemhan-bangun-pusat-cyber-defence, pada tanggal 22 Juli 2019 pukul 08.45 WIB

Atmadja, Nugrha Purna (2017), "*Dukungan Indonesia Terhadap Resolusi Anti Spionase Perserikatan Bangsa-Bangsa"*, e-Journal Ilmu Hubungan Internasional, ISSN 2477-2615

Bakrie, Conni Rahakundini (2007). *Pertahanan Negara dan Postur TNI Ideal*, Yayasan Obor Indonesia,Jakarta

Bhakti Ardiwisastra, Yudha, (2012). *Penafsiran dan Konstruksi Hukum*, PT.Alumni, Bandung

Budhijanto, Danrivanto, (2014). *Teori Hukum Konvergensi*, PT. Refika Aditama, Bandung

Budapest Convention (2001). On Cybercrime Kitab Undang-Undang Hukum Pidana (KUHP)

C. R. Terry, Patrick, "*Don't Do as I Do"—The US Response to Russian and Chinese Cyber Espionageand Public International Law*, German Law Journal Vol. 19

Demarest, Lt. Col. Geoffrey B. (1996). *Espionage in International Law*, 24 Denv. J. Int'l L. &Pol'y 321

Effendi, Jonaedi, (2016). *Metode penelitian Hukum Normatif dan Empiris*, Prenamedia Group, Jakarta

Evans, G. dan Grant, B., (1991). *Australia's Foreign Relations in the World of the 1990s*, Melbourne University Press

Hague Convention IV 1907

Henley, *China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence*, ISSN: 1944-0464 (Print); 1944-0472 (Online), Putnam University

Humas Polkam, *Peran Masyarakat dalam Menghadapi Ancaman Terhadap Pertahanan dan Keamanan Negara*, diakses dari https://polkam.go.id/peran-masyarakat-dalam-menhadapi-ancaman-terhadap-pertahanan-dan-keamanan-negara/. Pada Tanggal 30 Desember 2018, Pukul 23.42 WIB

Kitab Undang-Undang Hukum Pidana Militer (KUHPM) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Konvensi Jenewa Tahun 1949 tentang Perlakuan Terhadap Tawanan PerangKonvensi Den Haag IV tahun 1949

Kurdinanto Sarah, *Cyber Warfare (Sudah siapkah Kita Menghadapinya?)*, diakses dari: http://www.lemhannas.go.id/portal/in/daftar-artikel/1556-cyber-warfare.html pada tanggal 20 April 2019, Pukul : 08.05 WIB

Kusumaatmadja, Mochtar (1985). *Pembinaan Hukum Dalam Rangka Pembangunan Nasional*, Bina Cipta,Bandung

Kusumaatmadja dkk, Mochtar, (2003). *Pengantar Hukum Internasional*, PT Alumni, Bandung

Mahmud Marzuki, Peter, (2010). *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta

Maskun, (2013). *Kejahatan Siber Cyber Crime*, Kencana, Jakarta

Reda Manthovani, Peter, *Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia*, PT. Malibu,Jakarta

Sabon, Max Boli, (2017). *Ilmu Negara Bahan Pendidikan untuk Perguruan Tinggi*, Penerbit Universitas Atma Jaya, Jakarta

Shoelhi, Mohammad, (2001). *Diplomasi Praktik Komunikasi Internasional*, Simbiosa Rekatama Media, Bandung

Starke, J.G, (2010), *Pengantar Hukum Internasional*, Edisi Ke-10, Sinar Grafika, Jakarta

Sudiarta, I Ketut, (2015). "*Pelanggaran Kedaulatan Negara Terkait Tindakan Spionase dalam Hubungan Diplomasi Internasional*", Bagian Hukum Internasional Fakultas Hukum Universitas Udayana.

Suhariyanto, Budi, (2013). *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan danCelah Hukumnya*, PT. Raja Grafindo Persada, Jakarta

Supriyadi, Dedi, (2013). *Hukum Internasional (Dari Konsepsi Sampai Aplikasi)*, Pustaka Setia, Bandung

Susanto, Anthon F, (2005). *Semiotika Hukum (Dari Dekonstruksi Menuju Progresifitas Makna)*, PT. Refika Aditama, Bandung

Undang-Undang Dasar 1945

Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik IndonesiaUndang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara

Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional IndonesiaUndang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara

Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Pusat Bahasa Departemen Pendidikan Nasional, (2007). *Kamus Besar Bahasa Indonesia,* Balai Pustaka, Jakarta

Wahid, Abdul dan Labib, Mohammad, (2005) *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung

Wangen, Gaute, *The Role of Malware in Reported Cyber Espionage: A Review of the Impact andMechanism*, Norwegian Information Security Laboratory, Center for Cyber and Information Security, Gjøvik University College, Teknologivn. 22, 2815 Gjøvik, Norway