SINERGI LEMBAGA INTELIJEN DALAM MENGHADAPI ANCAMAN SIBER DI INDONESIA

SYNERGY OF INTELLIGENCE INSTITUTIONS IN FACING CYBER THREATS IN INDONESIA

Adhitya Prananda[1], Yusuf[2], Rudy A.G. Gultom[3]

UNIVERSITAS PERTAHANAN

(st.adhitya.prananda@gmail.com,nyusuf.ijabah@yahoo.co.id,

rudygultom@idu.ac.id)

Abstrak – Ancaman yang menjadi tantangan bagi negara-negara pada dunia internasional saat ini adalah serangan yang terjadi pada dunia siber. Perlindungan terhadap ancaman siber telah menjadi isu prioritas di semua negara. Perkembangan dunia yang semakin canggih, harus memaksa teknik dalam ilmu intelijen juga harus berkembang mengikutinya. Pemerintah Indonesia telah mendirikan beberapa lembaga-lembaga pemerintah yang memiliki wewenang dalam masalah siber khususnya intelijen siber. Tujuan dari penelitian ini untuk menganalisis sinergi lembaga-lembaga intelijen dalam menghadapi ancaman siber di Indonesia dan efektivitas dari sinergi lembaga-lembaga intelijen dalam menghadapi ancaman siber di Indonesia. Metodologi penelitian ini menggunakan metode kualitatif dengan pendekatan fenomenologi. Teknik pengumpulan data dilakukan melalui wawancara, studi dokumen dan studi pustaka. Hasil dari penelitian menunjukan bahwa kementerian dan lembaga menjalankan tugas pokok dan fungsinya masing-masing. Sinergi yang dilakukan hanya pada tingkat atas, sinergi juga dilakukan dengan melalui rapat koordinasi dalam penyusunan kebijakan dan pelatihan siber. Efketivitas dari sinergi lembaga-lembaga tersebut masih belum efektif. Peneliti memberikan rekomendasi yaitu Sinergitas perlu ditingkatkan agar kementerian dan lembaga dapat efektif dalam mengantisipasi dan menghadapi ancaman siber. Selain itu perlu adanya mekanisme koordinasi yang mengatur mengenai jalannya kerjasama antar lembaga intelijen siber.

Kata Kunci: Sinergi Lembaga, Ancaman Siber, Intelijen, Siber, Lembaga Intelijen Siber

Abstract *– The threat that is a challenge for countries in the international world today is the attacks that occur in the cyber world. Protection against cyber threats has become a priority issue in all countries. The development of an increasingly sophisticated world must force techniques in the science of intelligence to develop accordingly. The Government of Indonesia has established several government institutions that have authority in cyber matters, especially cyber intelligence. The purpose of this study is to analyze the synergy of intelligence institutions in dealing with cyber threats in Indonesia and the effectiveness of the synergy of intelligence institutions in dealing with cyber*

---

[1] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan Indonesia tahun akademik 2018/2019.

[2] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan Indonesia.

[3] Program Studi Teknologi Penginderaan, Fakultas Teknologi Pertahanan, Universitas Pertahanan Indonesia.

threats in Indonesia. This research methodology uses a qualitative method with a phenomenological approach. Data collection techniques were carried out through interviews, document studies, and literature studies. The results of the study show that ministries and institutions carry out their main duties and functions. Synergy is carried out only at the top level, synergy is also carried out through coordination meetings in the preparation of policies and cyber training. The effectiveness of the synergy of these institutions is still ineffective. Researchers provide recommendations that synergy needs to be improved so that ministries and institutions can be effective in anticipating and dealing with cyber threats. Besides, it is necessary to have a coordinating mechanism governing the course of cooperation between cyber intelligence agencies.

Keywords: *Institutional Synergy, Cyber Threats, Intelligent, Cyber, Intelligent Cyber Agency*

Pendahuluan

Pertahanan negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah sebuah negara dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.[4] Pertahanan negara disusun dalam suatu sistem pertahanan semesta dalam rangka melindungi kepentingan nasional. Pembangunan pertahanan negara diselenggarakan dengan berorientasi pada keterpaduan antara pertahanan militer sebagai komponen utama dan pertahanan nirmiliter sebagai komponen pendukung dan cadangan.

Perkembangan lingkungan strategis yang dinamis memengaruhi penyelenggaraan pertahanan negara yang ditujukan untuk menjaga dan mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dan keselamatan segenap bangsa dan negara.[5] Perkembangan lingkungan strategis menyebabkan pergeseran keamanan internasional. Ancaman berkembang tidak hanya berupa ancaman tradisional namun berkembang menjadi ancaman non tradisional salah satunya ancaman asimetris. Perubahan ancaman yang menjadi kompleks dapat mengganggu pertahanan dan keamanan nasional negara. Untuk dapat menghadapi ancaman asimetris dibutuhkan pertahanan negara yang kuat.

Ancaman yang menjadi tantangan bagi negara-negara pada dunia internasional saat ini adalah serangan yang terjadi pada dunia siber yang

[4] Undang-Undang No. 3 Tahun 2002

[5] Kementerian Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Negara*. Jakarta: Kementerian Pertahanan

merupakan dampak dari perkembangan teknologi informasi dan komunikasi.[6] Perkembangan teknologi dan informasi digunakan dalam berbagai aspek kehidupan, baik dalam aspek sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintah, keamanan, pertahanan, dan aspek lainnya. Perkembangan teknologi memiliki beragam manfaat bagi kesejahteraan hidup manusia salah satunya dapat mempermudah hidup manusia dalam segala hal. Namun, perkembangan teknologi dan informasi juga memiliki sisi negatif yang tidak dapat terhindarkan jika penggunaannya tidak baik.

Kemajuan teknologi menyebabkan meningkatnya serangan siber di dunia pelaku kejahatan semakin mudah dalam melakukan tindakannya seperti penyebaran paham ideologi yang salah, penyebaran paham terrorisme, ujaran kebencian, pornografi, perjudian, penyelundupan, pencurian, dan perang informasi melalui penyebaran hoaks atau informasi palsu. Hal ini merupakan kenyataan yang terjadi dalam kehidupan sehari-hari yang intensitasnya semakin tinggi, karena adanya kemajuan teknologi.

Perlindungan terhadap ancaman siber telah menjadi isu prioritas di semua negara. Akibat adanya ancaman siber, seluruh negara di dunia membutuhkan strategi keamanan siber.[7] Hampir seluruh negara di dunia telah memiliki strategi khusus untuk penanganan ancaman siber. Ancaman siber siber sudah sering terjadi di dunia internasional. Salah satu contohnya adalah penyebaran malware di Estonia yang mengakibatkan kerusakan infrastruktur khususnya infrasturktur energi listrik. Akibat dari ancaman tersebut, Estonia mengeluarkan *Tallinn Manual.*

Aktivitas pada ruang siber yang semakin meningkat mengakibatkan resiko juga semakin meningkat. Salah satu kejahatan siber yang sering terjadi adalah perang informasi.[8] Di Indonesia telah terjadi peningkatan pengguna internet di dunia maya. Pada tahun 2016 pengguna internet di Indonesia mencapai

---

[6] Kementrian Pertahanan Republik Indonesia. (2016). *Buku Doktrin Pertahanan Negara*. Jakarta: Kementerian Pertahanan

[7] Yosua Praditya Suratman. (2017). *Penggunaan Strategi Operasi Kontra Intelijen dalam Rangka Menghadapi Ancaman Siber Nasional* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

[8] N. Arfiani & Ojak, R. (2014). *Terorisme, Insurjensi, dan Peperangan Cyber: Kajian Kritis Peperangan Asimetris*. Makassar:Dapur Buku

jumlah sebanyak 132,7 juta atau sekitar 5,15 persen dari total jumlah penduduk Indonesia. Penggunaan media sosial masyarakat Indonesia juga meningkat, pada tahun 2017 tercatat 106 juta atau 40 persen dari total masyarakat Indonesia aktif menggunakan media sosial.[9] *Platform* media sosial tersebut digunakan oleh penggunanya sebagai media untuk menyampaikan informasi. Salah satunya informasi palsu. Penyebaran informasi palsu di media sosial dapat dikatakan sebagai perang informasi pada dunia siber Perang informasi di dunia siber memiliki karakteristik yang berbeda dengan perang informasi pada dimensi lainnya.

Ancaman yang datang dalam dunia siber saat ini, yang semakin lama semakin besar, menjadi pertaruhan akan keamanan dan kedaulatan Negara Indonesia. Karena negara Indonesia merupakan negara yang besar dan mempunyai potensi baik sumber daya alam dan sumber daya manusia, hal ini jelas menjadi sasaran dalam kejahatan siber. Serangan yang terjadi dalam perang siber tidak mungkin akan kita anggap remeh. Menghadapi ancaman siber tersebut diperlukan pertahanan dan perlindungan pada dunia siber dengan adanya Lembaga-lembaga pemerintah yang menangani masalah siber.

Strategi keamanan dunia maya adalah salah satu fokus dalam strategi pertahanan Indonesia. Tujuan strategis dari strategi keamanan siber Indonesia adalah pencapaian ketahanan dunia maya, keamanan layanan publik, penegakan hukum dunia maya, budaya keamanan dunia maya dan keamanan dunia maya dalam ekonomi digital.[10] Strategi keamanan informasi Indonesia diharapkan menjadi salah satu dasar kepercayaan dunia terhadap Indonesia di berbagai forum keamanan siber internasional.

Bidang keamanan siber adalah salah satu bidang pemerintahan yang perlu didorong dan diperkuat sebagai upaya untuk meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional. Untuk mewujudkan upaya keamanan siber, perlu dibentuk suatu badan yang menjamin implementasi kebijakan dan program

---

[9] Vancouver. *New Research Reveals Global Social Media Use Increased by 21 Percent in 2016*. Diakses dari https://hootsuite.com/newsroom/press-releases/digital-in-2017-report

[10] Kementerian Pertahanan Republik Indonesia. (2015). *Strategi Pertahanan Negara*. Jakarta: Kementerian Pertahanan

pemerintah di bidang keamanan siber. Ancaman siber yang sulit dideteksi juga membutuhkan deteksi dini dari aparat intelijen agar ancaman kejahatan siber terutama perang informasi tidak semakin berkembang. Intelijen tidak hanya harus diterapkan dalam dunia nyata, akan tetapi intelijen mau tidak mau harus masuk dalam ranah dunia siber.

Perkembangan dunia yang semakin canggih, harus memaksa teknik dalam ilmu intelijen juga harus berkembang mengikutinya. Intelijen didefinisikan sebagai kemampuan berpikir/analisa manusia. Intilijen juga berarti seni mencari, mengumpulkan dan mengolah informasi strategis yang diperlukan sebuah negara tentang negara "musuh".[11] Intelijen dapat juga didefinisikan pada organisasi yang melakukan seni pencarian, pengumpulan dan pengolahan informasi tersebut di atas.[12] Dengan definisi ini intelijen juga mencakup orang- orang yang berada di dalam organisasi intelijen termasuk sistem operasi dan analisanya.[13]

Dalam dunia siber dapat terjadi interaksi antar masyarakat, dapat terjadinya saling kolaborasi untuk melakukan sebuah aktivitas tertentu, yang mungkin dapat mengancam keamanan individu, kelompok, atau bahkan dapat mengancam kedaulatan suatu negara. Sehingga, teknik-teknik atau penerapan intelijen harus berkembang mengikuti perkembangan dunia yang terjadi. Sehingga kemampuan siber intelijen menjadi hanya sekedar menjadi wacana semata, akan tetapi merupakan kebutuhan yang harus dipenuhi oleh sebuah negara bukan hanya dibutuhkan untuk menanggulangi ancaman tetapi juga tindakan melakukan deteksi dini agar resiko dapat diminimalisir dengan cara yang cepat dan tepat.

Pemerintah Indonesia telah mendirikan beberapa lembaga-lembaga atau badan-badan pemerintah yang menangani masalah siber khususnya intelijen siber seperti pada tahun 2017 melalui Peraturan Presiden Nomor 53

---

[11] Hendropriyono, AM. (2014). *Filsafat Intelijen*. Jakarta:Salemba Humanik

[12] Toto Gunarto. (2018). *Kerjasama Aparat Intelijen dalam Deteksi Dini dan Cegah Dini Terorisme di Wilayah Bekasi* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

[13] Jusak Nesa Afriando Pardede. (2018). *Peran Komunitas Intelijen Daerah dalam Deteksi Dini Aksi Terorisme di Kota Bandar Lampung* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

tahun 2017, Presiden membentuk Badan Siber dan Sandi Negara yang bertujuan untuk melaksanakan keamanan siber yang memiliki fungsi diantaranya adalah identifikasi, deteksi dan persandian. Akan tetapi, Presiden juga mendirikan Deputi Keamanan Siber Badan Intelijen Negara melalui Peraturan Presiden Nomor 73 tahun 2017 yang memiliki tugas dalam perumusan kebijakan dan pelaksanaan operasi intelijen siber.

Meskipun antar lembaga memiliki peran dan fungsinya masing-masing, namun terdapat potensi tumpang tindih tugas dan fungsi jika dilihat pada Rancangan Undang-Undang Keamanan dan Ketahanan Siber, Badan Intelijen Negara diwajibkan mencatat dan memberitahukan setiap insiden atau serangan siber yang terjadi pada objek pengamanan siber yang menjadi tanggung jawabnya kepada Badan Siber dan Sandi Negara. Akan tetapi, Undang-Undang Nomor 17 tahun 2011 Badan Intelijen Negara hanya melayani Presiden Indonesia. Selain itu, Badan Intelijen Negara merupakan koordinator bidang intelijen, dan Badan Siber dan Sandi Negara merupakan koordinator dalam bidang siber. Sehingga perlu diteliti lebih lanjut keefektivan peran dan fungsi masing-masing lembaga agar tidak terjadi tumpang tindih antar lembaga siber.

Dari latar belakang diatas, peneliti tertarik untuk melakukan penelitian yang membahasa mengenai "Sinergitas Lembaga Intelijen dalam Menghadapi Ancaman Siber di Indonesia"

Adapun permasalahan penelitian dapat dirumuskan dalam dua pertanyaan penelitian sebagai berikut:

1. Bagaimana sinergitas lembaga-lembaga intelijen dalam menghadapi ancaman siber di Indonesia?
2. Bagaimana efektivitas dari sinergitas lembaga-lembaga intelijen dalam menghadapi ancaman siber di Indonesia?

Metode Penelitian

Penelitian mengenai sinergitas lembaga intelijen dalam mengantisipasi ancaman siber di Indonesia menggunakan metode kualitatif. Metode kualitatif merupakan metode-metode untuk mengeksplorasi dan memahami makna yang oleh sejumlah individu atau sekelompok orang dianggap berasal dari

masalah sosial atau kemanusiaan.[14] Penelitian kualitatif sering disebut sebagai penelitian naturalistik, karena penelitiannya selalu dilakukan dalam keadaan yang alamiah, tanpa rekayasa atau diatur sebelumnya.[15] Metode penelitian kualitatif adalah suatu penelitian interpretative yang melibatkan pemahaman mendalam serta keterlibatan secara intensif dengan para partisipan dalam penelitian.[16]

Pendekatan pada peneitian ini adalah pendekatan fenomenologi. Pendekatan fenomenologi merupakan salah satu jenis penelitian yang berusaha untuk memaknai suatu gejala berdasarkan keadaan gelaja itu sendiri.[17] Peneliti harus bertolak pada subyek serta kesadarannya dan berusaha untuk kembali pada kesadaran murni. Penelitian ini dilakukan dalam situasi yang alami. Penelitian fenomoenologi dilakukan untuk memahami dan menafsirkan pemahaman manusia berdasarkan fenomena atau gejala yang tampak.[18] Teknik pengumpulan data dengan wawancara semi terstruktur, studi literatur, dan studi dokumen.

Dalam penelitian ini menggunakan teori dan konsep dalam membahas permasalahan dalam rumusan masalah. Adapun teori yang digunakan adalah teori konsep ilmu pertahanan, teori sinergi, teori efektivitas, teori intelijen, teori ancaman dan konsep siber. Teori yang digunakan sebagai pisau analisis pada penelitian ini adalah teori sinergi dan teori efektivitas.

Hasil dan Pembahasan

Bentuk-Bentuk Ancaman Siber di Indonesia

Ancaman siber di Indonesia sudah menjadi ancaman yang aktual. Serangan siber saat ini tidak hanya dilakukan oleh kelompok tertentu akan tetapi dapat dilakukan juga oleh negara. Serangan siber merupakan salah satu ancaman yang dapat mengancam pertahanan negara, karena serangan siber memiliki dampak yang luas dan penanganannya sangat kompleks. Siber dapat menyerang infrastruktur kritikal nasional sehingga

[14] J. Creswell. (2010). Research Design: Pendekatan Kualitatif, Kuantitatif, dan Mixed. Yogyakarta: PT. Pustaka Pelajar.

[15] Lexy J. Moleong. (1991). *Metodologi Penelitian Kualitatif*. Bandung:Remaja Rosda Karya.

[16] Sugiyono. (2014). Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif Dan R&D. Bandung: Alfabeta

[17] Harsono. (2011). *Etnografi Pendidikan sebagai Desain Penelitian Kualitatif*. Surakarta: Universitas Muhammadiyah Surakarta

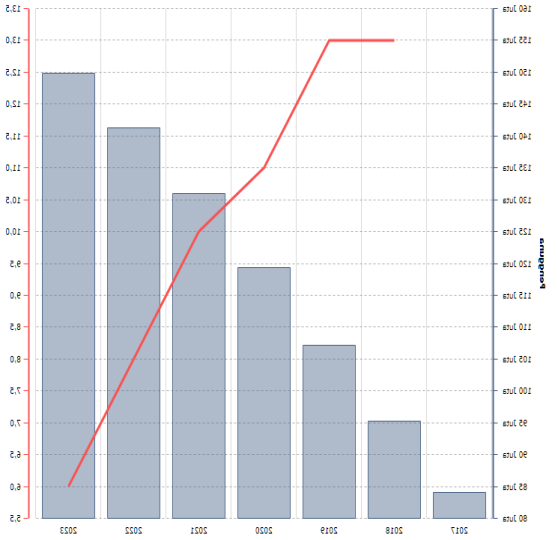
[18] Mahdi, Adnan Mujahidin. (2014) Panduan penelitian praktis untuk menyusun skripsi, tesis dan disertasi. Bandung: Alfabeta

dapat melumpuhkan pertahanan suatu negara.

Adanya perkembangan teknologi informasi pada saat ini mengakibatkan Negara Indonesia rentan terhadap serangan siber. Indonesia pernah menjadi target dari serangan-serangan siber baik serangan terhadap institusi pemerintah, swasta maupun individu. Menurut hasil dari Karspersky Lab bahwa Indonesia menempati posisi tertinggi pada serangan siber dalam penipuan online.

Pada era keterbukaan informasi saat ini, masyarakat sangat bergantung pada internet untuk melakukan komunikasi, melakukan jual beli, penyebaran informasi dan masih banyak lagi. Pengguna internet di Indonesia berdasarkan data statistika pada tahun 2019 mencapai 107,2 juta pengguna, diproyeksikan tumbuh sekitar 12,6% dibandingkan pada tahun 2018.[19] Dengan banyaknya pengguna internet di Indonesia, maka Indonesia menjadi negara yang rentan terhadap serangan siber.

Pengguna internet yang besar di Indonesia mendorong Pemerintah untuk lebih memperkuat pertahanan siber dan keamanan informasi. Dibutuhkan sinergitas antar lembaga-lembaga dalam menangani ancaman siber. Bentuk ancaman siber dapat berupa eksploitasi siber dan pengaruh siber. Serangan siber dapat terbagi menjadi empat bentuk yaitu *cyber warfare, cyber espionage, cyber crime*, dan *cyber terrorism.*[20] Keempat serangan tersebut secara nyata dapat mengancam pertahanan negara.



Gambar 1. Proyeksi Pengguna Internet di Indonesia 2017-2023
Sumber: Statista (2019)

Pada tahun 2020 hingga tahun-tahun kedepannya, ancaman serangan siber berada pada level baru, para peretas akan memanfaatkan kecanggihan teknolgi dalam hal ini *artificial intelligent*.

[19] Hamzah Zaelani. (2018). *Rancangan Pedoman Pelaksanaan Nirmiliter dalam Menghadapi Ancaman Siber* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

[20] W. M. Sthepen. (1985). *International Security* Vol-9 No.4 Spring.

Dengan menggunakan *artificial intelligent* maka *virus trojan* dan *malware* dan *ransomware,* akan dapat berkembang pesat. Indonesia pernah mendapat serangan siber jenis *ransomware* yakni sejenis aplikasi perangkat yang dapat merusak sistem komputer dari jarak jauh.[21] Serangan siber *ransomware* berjenis WannaCry menyerang Indonesia pada awal 2017, setidaknya dua rumah sakit di Jakarta yaitu Dharmais dan Harapan Kita. Hal ini menyebabkan data pasien dalam jaringan komputer rumah sakit tidak bisa diakses.

Berdasarkan dari catatan Badan Siber dan Sandi Negara selama kurun waktu 2018, wilayah kedaulatan Indonesia mengalami sekitar 232 juta percobaan serangan siber. Di antaranya sebanyak 122 juta serangan malware dan 16.000 jenis serangan inside dan outside.[22] pada Mei 2019, tercatat jenis serangan siber yang dikategorikan trojan dengan indikasi penyebaran malware mencapai 1,9 juta serangan. Selain itu Kaspersky Lab juga mencatat 50 juta serangan online yang menyerang pengguna internet di Indonesia sepanjang 2018 mengalami peningkatan sebesar 240 persen dibandingkan di tahun 2017.[23]

Kepala Badan Siber dan Sandi Negara menjelaskan terdapat tiga lapisan jaringan infrastruktur kritikal untuk menangani ancaman siber, yang pertama merupakan keamanan siber (*Cyber Security*), bentuknya abstrak, namun sejatinya dapat dijangkau dan dirasakan manfaatnya. Lalu, lapisan kedua senjata siber (*Cyber Weaponry*), bentuknya mungkin abstrak, tidak kasat mata, namun dapat merusak jaringan infrastruktur kritikal. Kemudian, lapisan ketiga adalah pertahanan siber (*Cyber Defense*), bentuknya suatu konsep strategis, harus konkrit, apabila semua jaringan infrastruktur kritikal digelar maka dapat diketahui kebijakan nasional tentang pertahanan siber.[24]

Sinergitas Lembaga Intelijen dalam Menghadapi Ancaman Siber

---

[21] Marissa Elvia. (2018). *Peran Kepolisian dalam Penenaggulangan Tindak Pidana Penyebar Berita Bohong*

[22] Fahmi Yusuf. (2018). *Perang Informasi di Ruang Siber (Studi Kasus Hoax di Media Sosial pada Pilkada DKI Jakarta 2017)* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

[23] CNN Indoneia, *Kaspersky Catat 50 Juta Serangan Siber di Indonesia pada 2018,* diakses dari https://www.cnnindonesia.com/teknologi/20190424193414-185-389389/kaspersky-catat-50-juta-serangan-siber-di-indonesia-pada-2018

[24] Saronto, Y. Wahyu. (2018). *Intelijen Teori Intelijen dan Pembangunan Jaringan*. Yogyakarta: CV Andi Offset

Ancaman siber menjadi ancaman aktual di Indonesia, dibutuhkan sinergitas antar lembaga-lembaga siber terutama sinergitas dalam bidang intelijen siber, karena intelijen merupakan bagian yang sangat menentukan bagi keselamatan negara dari ancaman, tantangan dan hambatan yang datang baik dari dalam maupun dari luar. Intelijen siber dibutuhkan dalam penyediaan bahan-bahan keterangan untuk peringatan awal atau deteksi dini.

Sinergitas yang sudah dilakukan antara lembaga-lembaga intelijen siber adalah hanya sebatas koordinasi dan rapat mengenai ancaman siber yang terjadi di Indonesia. Sinergi juga dilakukan dengan melakukan pelatihan siber bersama. Akan tetapi masih belum terdapat peraturan kerjasama maupun kerjasama lebih lanjut. Setiap instansi melakukan tugas pokok dan fungsinya masing-masing sesuai dengan undang-undang dan peraturan yang berlaku.

Sinergitas antar lembaga di koordinikasikan oleh suatu lembaga yang diberikan wewenang sebagai koordinator. Seperti koordinator dalam bidang intelijen dipegang oleh Badan Intelijen Negara sedangkan koordinator dalam bidang siber adalah Badan Siber dan Sandi Negara. Masing-masing kementerian dan lembaga memiliki divisi intelijen dan penyelidikannya maupun divisi siber masing-masing sesuai dengan kebutuhan kementerian dan lembaga tersebut.

Serangan siber merupakan ancaman yang kompleks dan dapat menyerang pertahanan negara karena memiliki dampak yang luas, ancaman siber dapat berdampak pada bidang sosial, ekonomi, keamanan, kesehatan dan infrastruktur kritikal nasional. Maka dari itu, diperlukan kerjasama karena masalah siber menjadi tugas bersama antara kementerian dan lembaga siber yang ada di Indonesia, agar pekembangan siber dunia yang global ini tidak menjadi ancaman bagi ketahanan maupun bagi stabilitas nasional Indonesia. Bagaimana teknik kerjasamanya tergantung kepada tugas pokok dan fungsi masing-masing lembaga intelijen siber tersebut.

Badan Sandi dan Siber Negara melakukan koordinasi dengan kementerian dan lembaga lain melalui penerimaan laporan terkait ancaman siber yang menyerang Indonesia maupun kementerian dan lembaga lain. Kementerian dan lembaga lain melakukan pelaporan kepada BSSN terkait dengan ancaman yang dimiliki.

Bondan Widiawan selaku Direktur Pengendalian Informasi, Investigasi, Forensik Digital menyampaikan bahwa terdapat kerjasama yang tertulis antara Badan Siber dan Sandi Negara dengan Badan Intelijen Negara.

Berkaitan dengan sinergi mengenai intelijen untuk mendeteksi ancaman siber masing-masing kementerian dan lembaga melakukan tugas nya masing-masing sesuai dengan kebutuhan kementerian dan lembaganya. Menurut narasumber, untuk dalam hal intelijen setiap kementerian/lembaga tidak melakukan sinergi dalam hal program kerja dan operasi.

Badan Siber dan Sandi Negara mengatur siber tidak hanya dalam bidang intelijen saja tetapi juga dalam bidang keuangan, bisnis, kritikal infrastruktur, komunitas dan lain-lain. Diperlukan sinergi, hanya dalam hal intelijen belum terdapat sinergi yang mendalam. Mekanisme kerjasama masih dalam pengkajian antar kementerian dan lembaga yang menangani siber. Akan tetapi Badan Siber dan Sandi Negara sangat terbuka bagi semua pihak untuk berbagi informasi terkait serangan dan keamanan siber dengan melalui kolaborasi seperti *working group*, investigasi dan penelitian bersama terkait teknologi, tren, dan permasalahan siber serta melalui *capacity building* dengan melaksanakan *cyber security training*.

Sedangkan Pusat Pertahanan Siber dalam menangani ancaman siber hanya melakukan kerjasama dengan lembaga siber seperti Badan Siber dan Sandi Negara. Pusat Pertahanan Siber tidak menjalin kerjasama dengan badan intelijen seperti Badan Intelijen Negara dan Badan Intelijen Strategis TNI. Kerjasama dengan lembaga-lembaga tersebut hanya dilakukan secara informal antar personil.

Selanjutnya, Sinergitas yang dilakukan oleh Satuan Siber TNI menurut Dande Mitigasi Satkal Satsiber TNI hanya sebatas melalui rapat koordinasi dan pelatihan siber dengan kementerian dan lembaga lain yang berkaitan dengan siber. Satuan Siber TNI tidak menjalin kerjasama dengan lembaga intelijen manapun, termasuk dengan Badan Intelijen Strategis TNI. Satuan Siber TNI hanya fokus pada pertahanan siber dilingkungan TNI dan Satuan Siber TNI hanya memiliki tanggung jawab pelaporan kepada Panglima TNI. Hingga saat ini belum ada perjanjian kerjasama secara tertulis maupun mekanisme yang mengatur koordinasi antara Satuan Siber TNI dengan kementerian/lembaga lain.

Sinegritas hanya dilakukan melalui kerjasama dan komunikasi oleh setingkat pejabat tinggi secara informal yang dilakukan melalui rapat koordinasi.

Kepolisian melakukan kerjasama dengan Badan Siber dan Sandi Negara dan Kementerian Komunikasi dan Informasi. Namun sinergi yang dilakukan oleh Badan Siber dan Sandi Negara, komunikasi tidak begitu intens. Hal ini disebabkan karena kurangnya Badan Siber dan Sandi Negara dalam memberikan informasi kepada Kepolisian. Sinergi dengan Kementerian Komunikasi dan Informasi, komunikasi terjalin dengan baik. Masing-masing instansi saling melakukan monitor.

Cyber Crime Polri tidak melakukan kerjasama dengan Badan Intelijen Negara, Badan Intelijen Strategis TNI, dan Satuan Siber TNI. Kerjasama belum ada karena adanya perbedaan wewenang dan tugas antara Kepolisian dan Tentara Nasional Indonesia. Kepolisian memiliki wewenang dalam penanganan keamanan dan ketertiban masyarakat, sedangkan Tentara Nasional Indonesia memiliki wewenang dalam pertahanan Negara Indoensia. Terkait pertukaran data, pertukaran informasi yang benar dan valid belum pernah ada.

Sinergitas dapat berjalan dengan baik jika dibangun melalui dua acara yaitu komunikasi dan koordinasi. Menurut Stoner sinergi adalah hubungan diantara dua pihak atau lebih dapat menghasilkan tingkatan komunikasi, bila dihadapkan pada elemen kerjasama dan kepercayaan. Tingkatan komunikasi akan menghasilkan tiga tingkatan kerjasama yaitu:[25]

1. *Defensive*, merupakan tingkat kerjasama dan kepercayaan yang rendah dan akan mengakibatkan pola komunikasi menjadi pasif atau defensif.
2. *Respectfull*, merupakan tingkat kerjasama dan kepercayaan yang meningkat, dan muncul pola komunikasi yang bersifat kompromi dan saling menghargai.
3. *Sinergistic*, merupakan tingkatan kerjasama dan kepercayaan yang sangat tinggi, dan menghasilkan pola komunikasi yang bersifat sinergitas. Kerjasama yang terjalin akan menghasilkan keluaran kumulatif yang jauh lebih besar,

[25] Stephen Coven. (2013). *7 Habbits of Highly Effective People.* New York: Simon & Schuster

yang merupakan hasil penjumlahan dari keluaran masing-masing pihak.

Berdasarkan dengan teori tingkatan komunikasi akan menghasilkan tiga tingkatan kerjasama menurut Stoner, dapat dianalisa bahwa sinergitas yang terjadi antara lembaga-lembaga intelijen siber ini merupakan tingkat kerjasama *defensive* yang memiliki pengertian merupakan tingkat kerjasama dan kepercayaan yang rendah dan akan mengakibatkan pola komunikasi menjadi pasif atau defensif. Akan tetapi tingkat kerjasama yang terjadi juga merupakan tingkat kerjasama *respectfull*, merupakan tingkat kerjasama dan kepercayaan yang meningkat, dan muncul pola komunikasi yang bersifat kompromi dan saling menghargai. Tingkat komunikasi yang terjadi dapat dikategorikan sebagai tingkatan *defensive*, akan tetapi tingkat kerjasamanya dapat dikategorikan sebagai tingakatan *respectfull.*

Tingkat komunikasi yang *defensive* yaitu tingkat kerjasama dan kepercayaan yang rendah dan akan mengakibatkan pola komunikasi menjadi pasif atau defensif. Komunikasi yang terjalin pada sinergi antar lembaga-lembaga intelijen siber dalam hal ini Badan Intelijen Negara, Badan Siber dan Sandi Negara, Satuan Siber TNI, Pusat Pertahanan Siber Kemhan, dan *Cyber Crime* Polri sangatlah pasif dan defensif. Dalam melakukan penyeledikan atau deteksi dini pada ancaman siber, tidak ada komunikasi yang terjalin antar masing-masing lembaga intelijen., pertukaran informasi juga tidak dilakukan. Masing-masing lembaga intelijen siber memiliki kepentingannya sendiri-sendiri.

Tingkat kerjasama antar lembaga-lembaga intelijen siber dapat dikategorikam sebagai tingkat kerjasama *respectfull* yang merupakan tingkat kerjasama dan kepercayaan yang meningkat, dan muncul pola komunikasi yang bersifat kompromi dan saling menghargai. Berdasarkan undang-undang mengenai penunujukan koordinator dalam bidang intelijen dan bidang siber, seperti Badan Intelijen Negara yang ditunjuk sebagai koordinator dalam bidang intelijen dan Badan Siber dan Sandi Negara yang koordinator dalam bidang siber. Dengan adanya badan yang memiliki wewenang sebagai koordinator, masing-masing lembaga saling menghargai tugas dan fungsinya masing-masing dan menghargai lembaga yang sudah ditunjuk menjadi koordinator.

Efektivitas Lembaga Intelijen dalam Menghadapi Ancaman Siber

Sinergitas antara lembaga-lembaga siber yang memiliki divisi intelijen, maupun lembaga-lembaga intelijen yang memiliki divisi siber hanya dilakukan sebatas sinergi dalam kebijakan dan startegi pada tingkat atas. Sinergitas belum dilaksanakan dalam operasi pelaksanaan penyelidikan maupun pertukaran informasi. Kerjasama secara keseluruhan belum terjadi antara kementerian dan lembaga intelijen siber.

Badan Intelijen Negara menyebutkan selama ini tidak ada tumpang tindih yang terjadi antara lembaga-lemaba dalam menghadapi ancaman siber. Pelaksaan tugas masing-masing lembaga sudah sesuai dengan Undang-Undang yang berlaku. Narasumber menjelaskan jika tidak ada tumpang tindih maka pelaksanaan pencarian informasi terkait penanganan siber ini sudah berjalan secara efektif dan tepat.

Badan Siber dan Sandi Negara mengatakan sinergi juga sudah dilakukan secara baik. Kerjasama sudah terjalin diantara kementerian dan lembaga yang menangani intelijen siber. Dari Badan Siber dan Sandi Negara sendiri sudah melakukan perjanjian kerjasama secara resmi maupun tidak resmi dengan lembaga-lembaga lain. Badan Siber dan Sandi Negara selalu melibatkan instansi lain dalam setiap rapat, pelatihan, seminar maupun acara siber lainnya.

Pusat Pertahanan Siber Kementerian Pertahanan, Satuan Siber TNI dan *Cyber Crime* Polri bahwa sinergi yang terjalin belum terlalu efektif jika dilihat pada saat ini. Hal ini dikarenakan sinergitas yang dilakukan hanya sebatas pada tingkat atas yaitu melalui penggabungan atau kerjasama dalam kebijakan dan strategi atau program kerja belum terdapat sinergitas untuk operasi intelijen siber. Selain intelijen bersifat rahasia, kementerian dan lembaga masing-masing memiliki tujuan, maksud dan program nya masing-masing. Ancaman siber saat ini masih dinilai dapat ditangani oleh masing-masing instansi tanpa adanya kerjasama.

Berdasarkan penjelasan dari staff Badan Intelijen Negara, efektivitas dari sinergi lembaga-lembaga intelijen siber ini jika diukur memiliki nilai skala 7-8 dari skala 10. Karena antara lembaga-lembaga intelijen siber seperti Badan Siber dan Sandi Negara sudah terbuka dalam suatu penanganan ancaman siber dan sudah mengajak lembaga lain seperti Badan Intelijen Negara untuk berdiskusi

bersama dan berkomunikasi mengenai ancaman siber tersebut.

Efektivitas adalah ukuran berhasil tidaknya suatu organisasi mencapai tujuannya. Apabila suatu organisasi berhasil mencapai tujuan maka organisasi tersebut dikatakan telah berjalan dengan efektif. Menurut Ravianto, pengertian efektivitas adalah seberapa baik pekerjaan yang dilakukan, sejauh mana orang menghasilkan keluaran sesuai dengan yang diharapkan. Efektivitas dapat dijelaskan bahwa efektivitas suatu program dapat dilihat dari aspek-aspek. Terdapat beberapa aspek-aspek efektivitas antara lain:

1. Aspek tugas atau fungsi, yaitu lembaga dikatakan efektivitas jika melaksanakan tugas atau fungsinya, begitu juga suatu program pembelajaran akan efektif jika tugas dan fungsinya dapat dilaksanakan dengan baik dan peserta didik belajar dengan baik
2. Aspek rencana atau program, yang dimaksud dengan rencana atau program disini adalah rencana pembelajaran yang terprogram, jika seluruh rencana dapat dilaksanakan maka rencana atau progarm dikatakan efektif
3. Aspek ketentuan dan peraturan, efektivitas suatu program juga dapat dilihat dari berfungsi atau tidaknya aturan yang telah dibuat dalam rangka menjaga berlangsungnya proses kegiatannya. Aspek ini mencakup aturan-aturan baik yang berhubungan dengan guru maupun yang berhubungan dengan peserta didik, jika aturan ini dilaksanakan dengan baik berarti ketentuan atau aturan telah berlaku secara efektif
4. Aspek tujuan atau kondisi ideal, suatu program kegiatan dikatakan efektif dari sudut hasil jika tujuan atau kondisi ideal program tersebut dapat dicapai. Penilaian aspek ini dapat dilihat dari prestasi yang dicapai oleh peserta didik.

Hasil penelitian menunjukkan bahwa sinergitas yang terjadi antara lembaga-lembaga intelijen siber belum efektif. Berdasarkan teori aspek-aspek efektivitas menurut Muasaroh, dari keempat aspek efektivitas, didapatkan hasil bahwa sinergitas yang dilakukan antar lembaga intelijen siber belum cukup efektif karena hanya memenuhi dua aspek yaitu aspek tugas dan fungsi serta aspek program dan rencana.

Sinergitas yang dilakukan hanya sebatas pada penentuan kebijakan dan penentuan tugas masing-masing instansi. Selanjutnya masing-masing lembaga menjalankan tugas dan fungsinya masing-masing lembaga sesuai dengan regulasi yang telah ditetapkan. Menurut aspek tugas dan fungsi yaitu lembaga dikatakan efektivitas jika melaksanakan tugas atau fungsinya. Dalam hal ini masing-masing lembaga sudah melakukan tugas dan fungsinya, tidak terdapat tumpang tindih antara tugas dan fungsi satu sama lain.

Berdasarkan pada aspek rencana atau program, yang dimaksud dengan rencana atau program disini adalah rencana pembelajaran yang terprogram, jika seluruh rencana dapat dilaksanakan maka rencana atau progarm dikatakan efektif. Dalam hal ini, masing-masing lembaga sudah menjalankan program dan rencana yang disusun bersama-sama dengan baik. Selain itu, antar lembaga satu sama lain juga telah bersama-sama melakukan sinergi program pelatihan seibr. Program tersebut juga telah dilaksanakan dengan baik.

Aspek tujuan yang diinginkan dalam sinergitas ini masih belum terjadi. Hal ini dikarenakan masing-masing instansi masih memiliki tujuan dan kepentingannya masing-masing, tujuan bersama yang ingin dicapai hanya untuk mengatasi ancaman siber. Tujuan selebihnya dari masing-masing lembaga berbeda.

Aspek ketentuan dan peraturan mengenai sinergitas juga belum ada. Saat ini hanya terdapat peraturan yang menjelaskan mengenai tugas dan fungsi masing-masing lembaga. Belum terdapat ketentuan dan peraturan mengenai koordinasi atau sinergtitas yang terjadi. Mekanisme koordinasi penanganan ancaman siber juga belum dibuat. Terlebih lagi Indoensia belum memiliki Undang-Undang mengenai Ancaman Siber.

Efektivitas Lembaga Intelijen siber masih sangat belum efektif dalam menangani ancaman siber jika dilihat berdasarkan pada teori aspek-aspek efektivitas. Hal ini dikarenakan masing-masing kementerian dan lembaga masih menjalankan tugas dan fungsinya masing-masing. Belum ada sinergitas antar kedua lembaga intelijen siber yang menyeluruh termasuk sinergitas dalam mencari informasi mengenai ancaman siber. Sinergitas dapat dikatakan berjalan dengan efektif jika terjadi kerjasama dan sinergitas mengenai program kerja dalam penanganan ancaman siber. Jika program kerja tidak dilakukan secara bersama-

sama makan kerjasama tidak dapat diukur dan tidak dapat dikatakan efektif atau tidak.

Optimalisasi kinerja intelijen siber dinilai belum optimal. Kendala bagi optimalisasi kinerja intelijen siber lebih bersumber pada profesionalisme para aparatnya. Profesionalisme pada hakikatnya terkait dengan anggaran. Dengan anggaran yang masih sangat terbatas, intelijen siber praktis tidak optimal dalam mengembangkan sumber daya aparaturnya (sumber daya manusia) dan memodernisasikan peralatannya. Untuk mengembangkan dan memelihara jaringan intelijen, juga memerlukan anggaran yang tidak sedikit. Faktor sumber daya terutama sumber daya manusia, perawatan dan pemeliharaan peralatan, serta jaringam akan sangat mempengaruhi profesionalisme intelijen siber.

Sebuah sinergitas sangat dibutuhkan dalam dunia intelijen siber dalam menhadapi berbagai macam kasus, seperti contohnya yang pasti akan dihadapi oleh setiap bangsa dan negara di dunia adalah kejahatan korupsi, narkotika, dan teroris. Sehingga perlu adanya kerjasama dengan lembaga atau badan lain dalam praktik penanganannya. Sehingga sinergitas antaraparat penegak hukum diperlukan penanggulangan secara preemtif, prefentif, dan represif hingga pada pemberantasannya.

Lembaga-lembaga intelijen siber dalam menjalankan operasi intelijen siber masih dilakukan secara masing-masing. Belum ada sinergitas yang menyeluruh dalam bentuk kerjasama, kolaborasi diantara lembaga-lembaga tersebut. Berdasarkan penjelasan diatas, hal ini diakibatkan karena adanya ego sektoral dari masing-masing lembaga tersebut. Lembaga-lembaga intelijen siber tersebut merasa memiliki kepentingan dan wewenang dalam antisipasi ancaman siber. Selain itu sifat kompetitif juga menghalangi sinergitas antara lembaga intelijen siber yang ada di Indonesia ini.

Kesimpulan dan Rekomendasi

Setelah melakukan penelitian dan membuat pembahasan terhadap rumusan masalah, maka peneliti dapat menarik kesimpulan umum dari penelitian sinergitas lembaga intelijen dalam menghadapi ancaman siber di Indonesia sebagai berikut:

1. Sinergi Badan Intelijen Negara dilakukan dengan Badan Siber dan Sandi Negara. Badan Intelijen Negara tidak melakukan kerjasama dengan kementerian dan lembaga

lain. Sinergi yang dilakukan dengan Badan Siber dan Sandi Negara melalui rapat koordinasi dan penyusunan peraturan. Badan Siber milik Badan Intelijen Negara melakukan tugas dan fungsinya sesuai dengan undang-undang. Pencarian informasi dilakukan oleh Badan Intelijen Negara hanya untuk instansinya sendiri. Dalam hal intelijen negara, Badan Intelijen Negara berlaku sebagai koordinator.

2. Sinergi Badan Siber dan Sandi Negara melakukan sinergi dengan beberapa lembaga dan instansi seperti BIN, Pushansiber, *cyber crime* polri dan instansi terkait siber lainnya. Sinergi yang dilakukan hanya sebatas koordinasi dan rapat antar kementerian dan lembaga. Badan Siber dan Sandi Negara memiliki wewenang sebagai koordinator dalam bidang siber.
3. Kementerian dan lembaga lain melakukan sinergi hanya sebatas rapat koordinasi dan pelatihan siber. Sinergi dalam pertukaran informasi belum dilakukan.
4. BIN dan BSSN menilai sinergi sudah efektif, namun menurut instansi lain sinergi masih belum efektif.

Berdasarkan kesimpulan diatas, peneliti dapat memberikan rekomendasi kepada peneliti selanjutnya diharapkan adanya penelitian mengenai lembaga-lembaga yang bertugas dalam intelijen siber. Rekomendasi kepada pemerintah Indonesia yaitu antara lain:

a. Setiap – setiap lembaga siber di Indonesia harus mendalami teknik yang ada dalam ilmu Intelijen. Dan begitu pula sebaliknya, bahwa agen intelijen harus mempunyai ilmu siber dikarenakan perang masa depan melalui dunia siber, tidak lagi bersifat konvensional.
b. Sinergitas perlu ditingkatkan agar kementerian dan lembaga dapat efektif dalam mengantisipasi dan menghadapi ancaman siber.
c. Perlu adanya mekanisme koordinasi antara lembaga intelijen siber dalam menangani ancaman siber agar tidak terjadi tumpang tindih.

Daftar Pustaka

Buku

Arfiani, N & Ojak, R. (2014). *Terorisme, Insurjensi, dan Peperangan Cyber: Kajian Kritis Peperangan Asimetris*. Makassar:Dapur Buku

Creswell, J. (2010). *Research Design: Pendekatan Kualitatif, Kuantitatif, dan Mixed.* Yogyakarta: PT. Pustaka Pelajar

Covey, Stephen. (2013). *7 Habits of Highly Effective People.* New York: Simon & Schuster

Harsono. (2011). *Etnografi Pendidikan sebagai Desain Penelitian Kualitatif*. Surakarta: Universitas Muhammadiyah Surakarta

Kementerian Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Negara*. Jakarta: Kementerian Pertahanan

Kementerian Pertahanan Republik Indonesia. (2015). *Strategi Pertahanan Negara*. Jakarta: Kementerian Pertahanan

Kementrian Pertahanan Republik Indonesia. (2016). *Buku Doktrin Pertahanan Negara*. Jakarta: Kementerian Pertahanan

J. Moleong, Lexy. *Metodologi Penelitian Kualitatif*. (1991). Bandung:Remaja Rosda Karya.

Miles, Mattew B dan A. Michael Huberman. (2007). *Analisis Data Kualitatif, Buku Sumber tentang Metode- Metode Baru*. Jakarta: Universitas Indonesia Press.

Mujahidin, Adnan dan Mahdi. (2014). *Panduan penelitian praktis untuk menyusun skripsi, tesis dan disertasi.* Bandung: Alfabeta

Saronto, Y. Wahyu. (2018). *Intelijen Teori Intelijen dan Pembangunan Jaringan*. Yogyakarta: CV Andi Offset

Sugiyono. (2014). Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif Dan R&D. Bandung: Alfabeta

Hendropriyono, AM. (2014). *Filsafat Intelijen*. Jakarta:Salemba Humanika

Jurnal

Elvia, Marissa. 2018. *Peran Kepolisian dalam Penenaggulangan Tindak Pidana Penyebar Berita Bohong*

Gunarto, Toto. 2018. *Kerjasama Aparat Intelijen dalam Deteksi Dini dan Cegah Dini Terorisme di Wilayah Bekasi* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

Pardede, Jusak Nesa Afriando. 2018. *Peran Komunitas Intelijen Daerah dalam Deteksi Dini Aksi Terorisme di Kota Bandar Lampung* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

Sthepen, W. M. (1985). *International Security* Vol-9 No.4 Spring.

Suratman, Yosua Praditya. 2017. *Penggunaan Strategi Operasi Kontra Intelijen dalam Rangka Menghadapi Ancaman Siber Nasional* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

Yusuf, Fahmi. 2018. *Perang Informasi di Ruang Siber (Studi Kasus Hoax di Media Sosial pada Pilkada DKI Jakarta 2017)* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

Zaelani, Hamzah. 2018. *Rancangan Pedoman Pelaksanaan Nirmiliter dalam Menghadapi Ancaman Siber* (Tesis Magister). Peperangan Asimetris, Fakultas Strategi Pertahanan, Unversitas Pertahanan Indonesia.

Undang-Undang

Undang-undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Website

CNN Indonesia. (2017). *Kaspersky Catat 50 Juta Serangan Siber di Indonesia pada 2018*, diakses dari https://www.cnnindonesia.com/teknologi/20190424193414-185-389389/kaspersky-catat-50-juta-serangan-siber-di-indonesia-pada-2018