Vol. 10, No.1, 2023
P-ISSN: 2355-1798, e-ISSN: 2830-3903

Respon Republik Lithuania terhadap Bayang-Bayang Ancaman Perang Generasi Kelima dari Rusia

Mohammad Anwarrudin[1], Bagus Sigit Sunarko[2], Agus Trihartono[3]
Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Jember
bgs_sigit@yahoo.com

Abstract

War have grown more sopisticated as they have grown older. According to some experts, wars are now entering the fifth generation. In this modern battle, the enemy used the kinetic and non-kinetic methods. This coincide with the phenomenon in the Republic of Lithuania, the country experienced attacks from Russia with the latest fifth type of war method. As for overcoming that, the Lithuanian country has some limitations in both military and non-military matters. Then the purpose of this discussion is to explain how Lithuanian strategy in dealing with the threat of the fifth type of war in its territory. In analyzing phenomena in this territory, the researcher will use several concepts and theories, including those of hackers, cybercrime, cybersecurity, national security, and fifth generational war theory. As for this research method, the writer used quasi-qualitative method. Researcher employ literatur review and descriptive analytics. As for the results of the study, the country has created security framework in its country through policies, institutions and cooperations. Thus, the Republic of Lithuania succeeded in establishing the fifth generation war defense system on its territory.

Keywords: *fifth generation war, Russian threat, security strategy of Lithuania*

1. Pendahuluan

Peperangan telah berkembang pesat bersamaan dengan kemajuan ilmu pengetahuan dan teknologi. Dalam penelitian Donald J. Reed (2008) dan Daniel H. Abbott (2010), saat ini, sistem pertempuran telah masuk ke generasi kelima. Adapun jenis peperangan tersebut, suatu negara menyerang lawanya tanpa disadari oleh negara musuh dengan metode militer dan nonmiliter. Sejalan dengan fenomena ini, banyak negara terancam oleh serangan pihak lain dengan tipe perang generasi terbaru ini, salah satunya yaitu Republik Lithuania. Negara tersebut terancam oleh manuver modern negara Rusia di wilayahnya.

Adapun bentuk ancaman bagi Lithuania ini, Rusia telah mengembangkan jenis peperangan ke tahap lebih maju. Bertepatan dengan terpilihnya Presiden Putin, negara beruang merah ini menjalankan kebijakan bersifat mengkhawatirkan bagi Lithuania. Pada masa awal tersebut, Republik Lithuania kerap mengalami masalah manipulasi informasi yang dilakukan oleh negara tetangga ini dalam beberapa

[1]Program Studi Hubungan Internasional, Universitas Jember
[2]Program Studi Hubungan Internasional, Universitas Jember
[3]Program Studi Hubungan Internasional, Universitas Jember

peristiwa pada tahun 2005, seperti disinformasi pada perayaan 9 Mei dan jatuhnya pesawat tempur Rusia di Lithuania (Jurgeleviciute, 2007; Maliukevicius, 2007). Selain itu, Lithuania juga kerap terancam karena penghentian pasokan minyak dari Rusia ke negaranya. Adapun beberapa kejadian masa awal-awal tersebut, Rusia menjelma sebagai ancaman peperangan modern bagi Lithuania.

Dalam menangani hal ini, sayangnya, Republik Lithuania belum memiliki sistem keamanan yang memadai. Adapun keadaan tersebut, negara Lithuania tidak cukup kuat dalam hal kapasitas dan kapabilitas militer maupun nonmiliter. Pertama dalam hal militeristik, negara ini tidak memiliki kemampuan cukup untuk mencegah ancaman Rusia, baik dalam hal jumlah pasukan, alutsista, maupun bentuk kemampuan pertahanan lainnya (Antczak & Sliwa, 2018; Flanagan dkk., 2018; Kementerian Pertahanan Republik Lithuania, 2012). Selain itu dalam hal nonmiliter, Republik Lithuania juga belum memiliki cara penanganan efektif untuk keamanan siber dan keamanan energi di negaranya. Oleh sebab itu, Republik Lithuania perlu untuk meningkatkan keamannnya untuk menangani ancaman perang generasi terbaru ini.

Bersamaan dengan keterbatasan negara ini, Republik Lithuania sebenarnya telah memberlakukan strategi keamanan untuk menanggulangi ancaman perang generasi kelima. Tindakan awal Lithuania ini, pemerintah berupaya mencegah masalah serangan siber dan penghentian pasokan minyak Rusia. Dalam upaya tersebut, negara mengeluarkan beberapa aturan penanganan serangan komputer yang tercermin dalam KUHP dan perlindungan infrastruktur digital negara sejak awal tahun 2000-an hingga tahun 2006. Sedangkan dalam hal energi, pemerintah berupaya menciptakan kebijakan untuk memenuhi kebutuhan suplai energinya (Seimas, 2002). Maka dari itu, strategi keamanan Republik Lithuania ini seharusnya mampu menghadapi ancaman pertempuran era ini di wilayahnya.

Namun demikian, sistem tersebut belum efektif untuk menangani beberapa masalah yang ada, khususnya pada pertempuran yang bersifat komplek. Ketidakmampuan pertahanan siber negara ini karena Republik Lithuania terus mengalami serangan peretas yang meningkat dari tahun ke tahun (CERT, 2006; CERT, 2007; CERT, 2008). Selain itu pada tahun 2008, institusi-institusi penting di negara ini telah menjadi korban dari tindak kriminal siber secara masif oleh negara Rusia ini. Padahal seharusnya, Lithuania memiliki sarana perlindungan digital yang mampu untuk melindungi negara karena banyak fasilitas yang bersifat penting. Adapun beberapa sebab ketidakberdayaan sistem ini karena pemerintah belum melakukan penanganan pada tindakan penyelewengan komputer dalam beberapa hal, seperti pemberlakuan keamanan siber sektor privat, pembentukan lembaga keamanan siber, dan kerjasama keamanan siber dengan negara lain (Stitilis et al, 2017; Stitilis & Klisauskas, 2015). Oleh karena itu menjadi menarik, walaupun sudah ada regulasi untuk perlindungan sistemnya, Republik Lithuania masih memiliki beberapa celah keamanan siber di negaranya yang belum maksimal pada waktu itu.

Karena beberapa kekurangan yang ada pada pertahanan sistem komputer nasional, Republik Lithuania perlu untuk meningkatkan sistem keamanan di teritorialnya. Pentingnya perbaikan manajemen keamanan informasi ini, karena negara ini memiliki banyak sekali fasilitas yang berkaitan dengan internet maupun energi. Pertama pada fasilitas digital Lithuania, ruang siber di negara tersebut berhubungan dengan pemerintahan, bisnis, dan individu (European Commission, 2017). Selain itu, negara Lithuania memiliki kebutuhan energi yang tidak dapat

terpenuhi dari hasil tambang dalam negeri sehingga harus impor dari Rusia dengan ketergantungan sebesar 90 persen minyak dan 100 persen gas alam. Maka menjadi penting bagi Republik Lithuania suatu sistem keamanan baru karena di negara ini terdapat beberapa hal yang butuh perlindungan, khususnya pada keamanan fasilitas elektronik dan pasokan energi dalam negeri.

Memperkaya apa yang telah tersampaikan sebelumnya, studi perang dalam bentuk serangan siber ini akan bersanding dengan kajian studi-studi terdahulu. Pembahasan peneliti sebelumnya adalah sebagai perbandingan penelitian ini dengan penelitian lain. Berdasarkan fokus hasil riset terdahulu, peninjauan topik serangan siber dan disinformasi di Lithuania ini kebanyakan berkaitan dengan keamanan dunia maya secara umum. Beberapa penulisan ilmiah sudah ada tersebut meliputi aspek regulasi hukum siber, penawaran model keamanan siber, sekuritisasi terhadap ancaman hibrida, dan keadaan keamanan siber (Global Cyber Security Capacity Centre, 2017; Karpaviciute, 2017; Stitilis et al, 2017; Stitilis dan Klisauskas, 2015). Menelaah pengkajian terdahulu yang ada, hasil riset menjelaskan beberapa poin penting, meliputi asal ancaman peretas, bagaimana peretasan terjadi, penanggulangan peretas, dan keadaan sistem defensif. Analisis peneliti sebelumnya masih berfokus pada mekanisme perlindungan siber secara teknis. Sedangkan upaya negara masih kurang tersorot khususnya dalam penanganan ancaman siber dan disinformasi dalam kontek perang generasi kelima. Nantinya dalam penelitian ini, penulis membutuhkan konsep dan teori untuk membantu analisis meliputi konsep peretas, konsep kejahatan siber, konsep keamanan siber, dan teori perang generasi kelima. Hal tersebut melatarbelakangi penelitian ancaman serangan peretas dalam kaitannya dengan perang generasi kelima di Republik Lithuania.

Oleh karena itu, berdasarkan latar belakang tersebut, penulis meneliti: Bagaimana upaya Republik Lithuania dalam merespon ancaman perang generasi kelima dari Rusia?.

Konsep Peretas (*Hacker*)

Peretas merupakan seseorang yang ahli dalam sistem komputer. Adapun dalam pemahaman aktor tersebut, definisi peretas telah mengalami perubahan dari waktu ke waktu. Pada Awalnya, sosok ini terkenal sebagai seorang ilmuan yang ahli dalam hal komputer. Kemudian berkembang ke arah lebih negatif, karena saat ini secara definisi, aktor tersebut lebih berkaitan erat dengan seorang penjahat sistem komputer. Penelitian Chng dkk. (2022) menjelaskan bahwa aktor pengrusakan sistem ini terbagi kedalam beberapa bentuk, meliputi sosok pemula berkemampuan rendah (*novices*), peretas berkemampuan menengah untuk bersenang-senang (*cyberpunks*), orang dalam dari perusahaan (*insiders*), peretas pengungkap kerentanan sistem (*oldguards*), peretas profesional (professionals), penjahat komputer yang terlibat dengan agenda politik (*hacktivists*), hacker milik negara (*nationstate*), seorang pelajar (*students*), penjahat online (*pettythieves*), aktor pendistribusi benda-benda berhak cipta (*digitalpirates*), peretas pelaku sex online (*onlinesexoffenders*), individu-individu yang mengatasi masalah komputer (*crowdsources*), dan pemfasilitas kejahatan (*crimefasilitator*). Negara-negara di dunia mengalami peretasan dengan beberapa jenis serangan seperti ini. Hal tersebut tidak luput bagi Republik Lithuania, beberapa elemen negara ini mengalami serangan peretas dari Rusia dengan tipe peretas negara (*nationstate*). Oleh karena itu, konsep peretas sangat berkaitan dengan fenomena perang modern di Republik Lithuania sehingga perlu untuk digunakan.

Konsep Kejahatan Siber (*Cybercrime*)

Kejahatan siber ialah serangan internet ilegal dengan memanfaatkan komputer. Dalam penggunaan istilah ini, mayoritas administrator menerapkan kata lain yang menggantikannya, meliputi kejahatan komputer (*computercrimes*), komunikasi elektronik (*electroniccommunications*), teknologi informasi (*informationtechnology*), dan kejahatan dengan teknologi tinggi (*high-techcrime*). Terlepas dari kebanyakan pemakaian kata lain, beberapa pemerintah mempergunakan kata kejahatan siber, meliputi Boswana, Bulgaria, Kamboja, Jamaika, Namibia, dan Sinegal. Sedangkan secara pendefinisian, kejahatan siber berhubungan dengan akses ilegal komputer di suatu negara, meliputi tindakan-tindakan penerobosan dengan cara menyerang infrastruktur penting lembaga-lembaga administrator. Dalam dokumen Kantor Perserikatan Bangsa-Bangsa Urusan Narkoba dan Kejahatan (2013), sistem komputer merupakan inti dari tindakan ilegal ini. Terdapat batasan mengenai penjelasan konsep ini yaitu perbuatan pelanggaran komputer tersebut spesifik pada sejumlah tindakan terhadap kerahasiaan, integritas, dan ketersediaan data dalam sistem komputer, tidak pada perbuatan secara pribadi untuk keuntungan finansial. Bertransformasi dari penjelasan-penjelasan terdahulu tersebut, Badan Kepolisian Internasional (2021) menjelaskan bahwa gempuran sistem komputer ini bersifat canggih dengan memanfaatkan teknologi tinggi (*high-techcrimes*), seperti peretasan, serangan perangkat lunak, dan pemerasan menggunakan *DDoS*. Aksi kelompok penjahat komputer tersebut menyasar pada situs-situs otoritas di suatu negara, salah satunya, kegiatan dengan aksi ilegal ini terjadi di Republik Lithuania. Di negara tersebut, tindakan berbahaya peretasan (*hacking*) mengincar lembaga penting milik pemerintah dan swasta.

Konsep Keamanan Siber (*CyberSecurity*)

Keamanan siber adalah suatu sistem perlindungan digital untuk melindungi masyarakat di suatu negara. Konsep keamanan ini pun telah meluas dalam segi pemahaman, mulai dari keamanan komputer teknis hingga kemudian menjelma sebagai bagian dari keamanan negara. Lebih jelasnya, sekuriti sistem informasi ini berkaitan dengan upaya pemerintah dalam menangani masalah komputer. Berdasarkan penelitian Deibert (2002), perlindungan elektronik muncul berwujud pengamanan internet yang dilakukan oleh otorisator di suatu negara. Sejalan dengan pandangan sebelumnya yaitu menurut Helen Nissenbaum (2005), perlindungan sistem ini masuk dalam lingkup keamanan publik atau keamanan nasional untuk mencegah serangan peretas. Berkembang dari pandangan tersebut, Persatuan Telekomunikasi Internasional (2008) menyebutkan bahwa keamanan siber merupakan kumpulan pedoman, kebijakan, konsep keamanan, pengamanan keamanan, manajemen resiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi, yang dapat melindungi lingkungan siber organisasi serta aset pengguna. Konsep perlindungan siber ini tercermin dalam apa yang terjadi di Republik Lithuania. Negara ini mengalami penurunan sehingga tidak dapat melindungi situs-situs yang ada karena ancaman serangan peretas. Meneladan fakta-fakta yang ada tersebut, sistem pertahanan komputer berguna dalam setiap tantangan keamanan masing-masing otoritas negara untuk memastikan keamanan sistem informasi di wilayahnya.

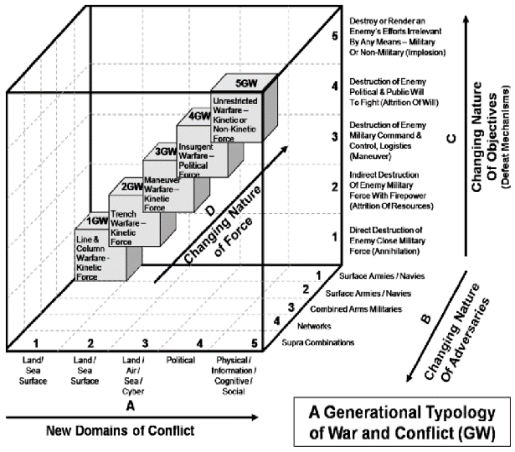
Konsep Keamanan Nasional (*NationalSecurity*)

Keamanan nasional adalah suatu sistem untuk memberikan perlindungan pada negara. Adapun pengertian dari konsep ini, keamanan negara merupakan suatu kondisi ketika suatu bangsa memiliki kemampuan untuk melindungi diri dari ancaman yang bersifat komplek (Lipmann, 1943; Lasswell, 1950; Brown, 1977; Wolvers, 1960; Maier, 1990; Paleri, 2008). Dalam pandangan Sekolah Tinggi Pertanahan Nasional India (1996), keamanan nasional adalah keterpaduan yang tepat dari ketahanan politik, sumber daya manusia, kapasitas ekonomi, kompetensi teknologi, basis industri, ketersediaan sumber daya alam, dan kekuatan militer. Lebih jelasnya, keamanan nasional adalah suatu sistem yang bertujuan untuk menjaga keutuhan fisik dan nonfisik suatu negara dari serangan luar. Pertama dalam keamanan fisik militer, sistem pertahanan ini telah berkembang dari basis darat dan laut pemikiran tradisional, kemudian menuju ranah udara, ruang siber, dan psikologi dalam pandangan terbaru. Sedangkan dalam pertahanan nonmiliter, biasanya negara menerapkan beberapa sistem meliputi keamanan ekonomi, keamanan energi, keamanan lingkungan, keamanan pangan, keamanan batas negara, dan keamanan siber. Lebih tepatnya hal ini berhubungan dengan keadaan di Republik Lithuania karena negara ini terancam oleh beberapa hal yang dilakukan oleh Rusia sehingga membutuhkan suatu sistem perlindungan keamanan nasional.

Teori Perang Generasi Kelima (*Fifth Gradient of War)*

Peperangan telah mengalami perkembangan seiring dengan majunya ilmu pengetahuan dan teknologi. Menurut William S. Lind (2001), T. X. Hammers (2007), Donald J. Reed (2008), dan Daniel H. Abbott (2010), sistem saling serangan antar bangsa telah berubah sedemikian rupa dari waktu ke waktu. Pertama, sistem pertempuran terjadi secara formal dan teratur oleh kedua belah pihak yang menyebabkan terciptanya budaya militer yang tertib. Generasi selanjutnya yaitu yang kedua, sistem penaklukan musuh mengutamakan pada penggunaan artileri yang memiliki daya tembak lebih canggih dari metode terdahulu. Berbeda dari sebelumnya, teknik mengalahkan lawan periode ketiga mementingkan strategi yang meliputi kecepatan, daya kejut, dan dislokasi mental. Bergeser ke jenis keempat, konflik tidak lagi berfokus pada negara lain sebagai rivalnya, melainkan pada non-negara yang berupa gerakan-gerakan radikalisme, revolusioneris, dan kelompok serupa lainnya. Kemudian berevolusi ke bentuk lain yang bersifat lebih rumit dari sebelumnya, sistem permusuhan antar bangsa telah masuk ke generasi kelima, peperangan menggunakan cara tersembunyi untuk menyerang musuh. Dari beberapa jenis peperangan tersebut, metode perang telah menuju pada hal yang bersifat lebih mutakhir dari sebelumnya.

Dalam perkembangan mekanisme pertempuran terbaru ini, jenis perang fase kelima ini memiliki tipikal tersendiri yang telah bertransformasi dari tipe-tipe perang terdahulu. Hammers (2007) berpendapat bahwa aktor perang generasi ini adalah individu yang menggunakan senjata kimia dengan melakukan aksi terorisme kepada masyarakat. Penelitian dari John Robb (2006), sistem permusuhan kelima ini menggunakan teknik yang mirip dengan metode gerilya untuk menyerang sumber daya, sistem keamanan, dan eksistensi pemerintahan virtual negara lain. Sedangkan pemikiran lebih lanjut menurut Donald J. Reed (2008), perang generasi terbaru ini adalah sebagai berikut:



Gambar 1. Pemetaan perang generasi kelima
(Sumber : Donald J. Reed, 2008)

Dari gambar tersebut, perang generasi kelima telah menuju tahap lebih komprehensif dari perang-perang sebelumnya. Pertama yaitu pada poros A, area konflik telah berubah dari politik kemudian menuju fisik, informasi, kognitif, dan sosial. Pada bagian B, musuh telah mengarah pada mereka yang menggunakan kombinasi yang sedemikian rupa (*supracombination*). Sisi C, tujuan perang adalah untuk menghancurkan upaya-upaya musuh dengan cara militer dan nonmiliter. Terakhir pada kelompok D, aktor berperang menggunakan kekuatan yang berupa kinetik dan non kinetik sehingga menjadikan peperangan tidak terbatas dalam suatu teknik tertentu. Dari hal-hal tersebut, perang generasi terbaru lebih besar kemungkinannya untuk memenangkan pertempuran melawan pihak lain karena kemajuan teknik tempurnya.

Adapun perang generasi kelima dalam penelitian ini yaitu Republik Lithuania mengalami serangan-serangan yang berkaitan dengan perang generasi kelima. Dalam hal tersebut Lithuania menjadi korban negara tetangganya, Rusia kerap melakukan tindakan-tindakan agresif terhadap negara ini. Adapun bentuk manuver negara beruang merah ini adalah berupa serangan siber dan tekanan energi. Oleh karena itu, Lithuania benar-benar terancam oleh tindakan Rusia dengan metode perang modern.

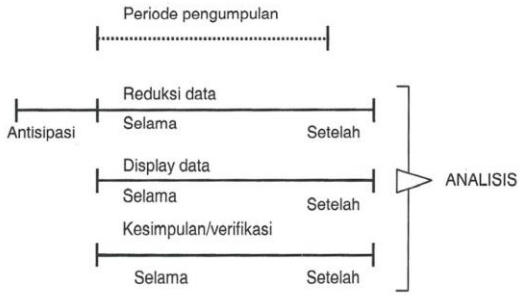
2. Metodologi

Penelitian ini menggunakan metode kuasikualitatif. Menurut Liz Spencer (2003), metode ini merupakan Teknik penelitian yang tujuannya untuk memberikan pemahaman mendalam dengan cara mempelajari suatu keadaan (*material*) dan sejarah. Pendapatdari Klotz (2008), Teknik tersebut berdasar pada data yang mayoritas bersifat non-numerik, seperti dokumentasi kenegaraan, foto, video, dan wawancara. Peneliti akan mengolah data-data ini hingga kemudian menyajikannya dalam bentuk tulisan. Dengan skema penelitian kuasikualitatifini, penulis menganalisis data terkait upaya Republik Lithuania dalam menangani ancaman perang generasi kelima dari Rusia.

Dalam metode pengumpulan data Penelitian ini, penulis menggunakan Teknik studi pustaka. Teknik ini adalah cara untuk mendapat data dari hasil risetpihak lain yang sesuai dengan penelitian. Sedangkan dalam metode ini, data peneliti adalah data sekunder. Jenis data tersebut merupakan data hasil dari orang lain untuk tujuan lain

(Jonston 2014). Data tersebut berasal dari buku, laporan, jurnal, artikel, dan sumber internet resmi.

Sedangkan untuk analisis data, peneliti menggunakan metode deskriptif. Jenis analisis tersebut merupakan suatu teknik yang berfungsi untuk mendeskripsikan atau menggambarkan objek penelitian yang masih berupa data (Sugiyono, 2009). Analisis data kualitatif ini terbagi ke dalam beberapa tahapan. Adapun penjelasanya adalah sebagai berikut:



Gambar 1. Proses analisis data kualitatif

(Sumber: Sugiyono, 2013)

Pada Gambar 1. diatas, dalam penelitian, analisis data memerlukan suatu proses tertentu. Tahapan-tahapan analisis data terdiri dari beberapa hal, meliputi pengumpulan data, reduksi data, penyajian data, dan verifikasi data. Pertama, pengumpulan data ialah suatu proses lanjutan dari pencarian data penelitian untuk memperoleh data sekunder hasil penelitian terdahulu. Kedua, peneliti mereduksi data dengan cara memilih, memfokuskan, dan mencari pola data. Ketiga penyajian data, penulis menyajikan data yang telah diolah dalam bentuk uraian, bagan, tabel, dan bentuk lain sejenisnya. Terakhir verifikasi data, penulis menyimpulkan data dengan cara deduktif yaitu dari yang umum kemudian menuju khusus. Dari proses tersebut, diharapkan peneliti dapat menganalisis data dengan baik sehingga dapat menghasilkan penelitian yang bagus.

3. Hasil dan Diskusi

Republik Lithuania sedang terancam oleh serangan perang generasi kelima dari Rusia. Dalam menghadapi ancaman pertempuran di wilayahnya ini, Republik Lithuania memiliki beberapa kelemahan untuk mengantisipasi masalah ini. Sehingga negara memerlukan penanganan-penanganan lebih lanjut untuk menanggulangi hal tersebut.

Indikasi Perang Generasi Kelima di Republik Lithuania

Rusia telah melakukan serangan ke Lithuania dengan teknik mutakhir perang terbaru. Negara tersebut melakukan serangan ke Republik Lithuania dengan metode militer dan nonmiliter. Adapun untuk menganalisis permasalahan ini, Donald J. Reed (2010) menjelaskan bahwa perang generasi kelima memiliki beberapa ciri yang dapat diketahui dalam beberapa hal, meliputi area konflik, sifat dari musuh, sifat dari tujuan peperangan, dan sifat dari kekuatan musuh.

Pertama pada area konflik, lingkup ancaman Rusia telah bergeser lebih luas dari sebelumnya. Dalam melebarnya peperangan ini, Lithuania tidak hanya berkonflik dengan negara tersebut dalam hal permusuhan secara politik saja, melainkan pada ranah lain yang bersifat lebih komplek. Adapun kebanyakan, Republik Lithuania bermusuhan dengan Rusia melalui metode nonfisik. Adapun lingkup konflik yang pertama, Rusia kerap menyerang Lithuania melalui serangan informasi dalam bentuk teks, video, gambar, postingan, televisi, radio, dan sebagainya (Andriukaitis, 2018; Kojala dkk., 2020). Masuk ke ranah selanjutnya, Rusia kerap menyerang Republik Lithuania dengan mengandalkan peretas bertipe peretas negara sehingga insiden siber di wilayah ini ini terus meningkat dari tahun ke tahun (CERT, 2008; CERT, 2009; CERT LT, 2010; CERT LT, 2011; CERT LT, 2012). Adapun wilayah konflik yang terakhir, Lithuania kerap berseteru dengan Rusia dalam hal energi karena ketergantungan sumber daya dalam jumlah besar pada negara tersebut, yaitu minyak sebesar 90 persen dan gas beserta listrik sebesar 100 persen (Baran, 2006). Dari beberapa pemaparan di atas, Rusia menyerang Lithuania pada ranah baru sehingga peperangan melebar ke arah nonmiliter.

Sedangkan pada sifat musuh Republik Lithuania, mereka menggunakan kombinasi yang bersifat supra. Dalam hal ini, musuh memanfaatkan beberapa hal meliputi fisik, informasi, kognitif, dan sosial. Secara lebih jelas, seorang musuh tidak hanya berbentuk negara, melainkan datang dalam bentuk bermacam-macam meliputi, non-negara, jaringan, aktor transnasional, individu, dan kelompok (Reed, 2008). Adapun dalam hal ini, Lithuania kerap berseteru dengan media, peretas, perusahaan, dan bentuk lainnya dari Rusia. Pertama dalam kontek ini, seorang musuh adalah adalah seorang peretas (*hackers*) yang disponsori oleh Rusia. Aktor ini menyerang tanpa diketahui identitasnya secara jelas, mengalihkan server identitas, dan melumpuhkan situs negara (Laughlin, 2008; Mullett, 2008; Reuters Staff, 2008; Rhodin, 2008; The Baltic Times, 2008; Adomaitis, 2008; Sytas, 2016; Gotev, 2016; Euronews, 2016). Selain dengan program canggih, Rusia berupaya untuk menyerang pemikiran masyarakat melalui propaganda dengan menggunakan tema sensitif yang menarik perhatian masyarakat meliputi Holokaus, pengungsi, terorisme, dan konfrontasi etnis (Departemen Pertahanan Republik Lithuania, 2017). Terakhir terkait sifat musuh ini, Lithuania bermusuhan dengan Rusia dalam bentuk ekonomi, karena negara tersebut berencana lebih lanjut untuk akuisisi perusahaan minyak, merger perusahaan, dan pembangunan infrastruktur energi (Baran, 2006). Oleh karena itu, Rusia menggunakan cara bersifat tidak langsung yang dapat menyebabkan kerusakan dan kesulitan untuk Republik Lithuania.

Bergeser pada tujuan peperangan, suatu negara akan menghancurkan upaya-upaya musuh dengan cara militer dan nonmiliter. Aktor mencapai tujuannya dengan memanfaatkan beberapa kombinasi dalam level kebijakan, strategi, operasional, dan taktis (Boston & Massicot, 2017). Dalam kasus ini, Rusia mengeluarkan beberapa kebijakan meliputi doktrin militer resmi tahun 2014, strategi keamanan nasional 2015, konsep kebijakan luar negeri 2016, strategi angkatan laut 2017, dan strategi pencegahan nuklir tahun 2020 (Kongres Amerika Serikat, 2020). Dari strategi-strategi tersebut, Rusia membuat kebijakan barunya untuk peningkatan anggaran militer dan pembentukan grup batalyon taktis. Selain itu dalam dua periode terakhir, Rusia melakukan reformasi militer di negaranya yang berdampak cukup besar pada kualitas pasukannya, meliputi pembentukan brigade campuran, penambahan tentara sukarela, memperluas brigade-brigade nya, penggandaan ukuran kesatuan, dan modernisasi alutsista tempur (Boston dkk, 2018). Bersamaan dengan kegiatan tersebut, musuh potensial ini telah mengembangkan kemampuan tempurnya melalui pelatihan, seperti

pada latihan “Snap” tahun 2015, latihan “Zapad” tahun 2017, beserta beberapa latihan tempur lainnya (Boston dkk., 2018). Berdasarkan rencana untuk tahun 2020, Rusia akan mengembangkan tiga divisi senapan mesin, tiga divisi udara, divisi tank, dan empat brigade bersenjata gabungan secara lebih lanjut. Dari hal tersebut, dalam kontek di Lithuania ini, Rusia banyak melakukan inovasi sebagai upaya untuk menghancurkan lawan di kawasan.

Terakhir, pada kekuatan musuh, peperangan tidak terbatas dalam suatu teknik tertentu. Bentuk dari kekuatan perang ini dapat bersifat kinetik (militer) dan non-kinetik (politik, ekonomi, sosial, budaya, media, informasi, teknologi, hukum, dan psikologi). Pada ancaman fisik, Rusia berkapasitas tempur lebih unggul dari Lithuania dalam peperangan darat, laut, dan udara (Boston dkk, 2018: 7-10). Sedangkan dalam ancaman nonfisik, Rusia telah menyerang Lithuania menggunakan propaganda, peretas, dan manipulasi energi (Andriukaitis, 2018; Kojala dkk., 2020; Karpaviciute, 2017; Maliukevicius, 2006; Zemaitis, 2007; NKCS, 2012; Misik &Pracharova, 2016; Baran, 2006). Oleh karena itu, Rusia memiliki kekuatan tempur komplek sehingga pertempuran pun bisa berbentuk beragam yang membahayakan bagi Republik Lithuania.

Resistensi Republik Lithuania dalam Menghadapi Perang Generasi Kelima

Sejak dulu, Republik Lithuania telah memiliki pertahanan tertentu untuk menghadapi ancaman perang generasi kelima dari Rusia ini. Adapun keberadaan kekuatan tempur yang dimaksud, di Lithuania terdapat pertahanan militer dan nonmiliter.

Pertama dalam hal militeristik, Republik Lithuania memiliki kapasitas militer yang terbilang kecil. Dalam hal ini, negara Lithuania memiliki elemen pertahanan yang tercermin dalam beberapa hal. Pertama dari segi pasukan, Republik Lithuania hanya memiliki jumlah personel militer aktif sebesar 19.850 prajurit pada tahun 2019 (Flanagan dkk., 2019). Kemudian dalam hal anggaran, negara ini telah mengeluarkan biaya militer dari tahun ke tahun hingga mencapai jumlah sebesar USD 1,084 miliar. Selain itu tepatnya sejak tahun 2015, Republik Lithuania telah menggelar kembali wajib militer di wilayah ini karena kekurangan pasukan. Lebih dari itu, Republik Lithuania juga kurang dalam ketahanan masyarakat untuk mendukung militer negara. Sehingga negara ini melakukan peningkatan persatuan senapan untuk mempromosikan pendidikan patriotik dan perlawanan sipil. Juga demikian dalam hal dukungan militer secara global, negara ini terlalu mengandalkan jaminan keamanan dari luar negeri meliputi NATO, Uni Eropa, dan lembaga lainnya (Kementerian Pertahanan Republik Lithuania, 2012; Antczak & Sliwa, 2018). Oleh karena itu, kapasitas dan kapabilitas militer Lithuania belum cukup kuat dalam menghadapi tantangan keamanan dari Rusia.

Kedua dalam hal nonmiliter, Republik Lithuania memiliki beberapa unsur keamanan nonfisik. Elemen tersebut adalah meliputi keamanan siber dan keamanan energi. Adapun penjelasanya adalah sebagai berikut:

Perlindungan Keamanan Siber

Dalam keamanan Siber, Lithuania telah menjelma sebagai negara dengan sistem perlindungan siber yang maju. Berdasarkan penelitian Pusat Keamanan Siber Global Universitas Oxford (2017) dan Persatuan Telekomunikasi Internasional (2018), negara ini memiliki beberapa elemen keamanan siber yang baik dari beberapa hal,

meliputi kebijakan, kelembagaan, teknologi, peningkatan kapasitas, dan budaya. Dari segi regulasi, Republik Lithuania telah mengembangkan regulasi keamanan siber di negaranya yang tercermin dari beberapa kebijakan, meliputi undang-undang kejahatan informasi tahun 2000, strategi keamanan nasional tahun 2002, strategi keamanan militer tahun 2004, keamanan informasi elektronik tahun 2006, dan strategi keamanan siber 2011 (Stitilis dkk., 2016; Parlemen Republik Lithuania, 2002; Kementerian Pertahanan Republik Lithuania, 2004). Selain itu, Republik Lithuania memiliki lembaga-lembaga perlindungan siber di negaranya, meliputi Pusat Keamanan Dunia Maya (National Cyber Security Center) dan Dewan Keamanan Siber (Cyber Security Council). Dalam hal teknologi, Republik Lithuania telah meningkatkan fasilitas keamanan sistem informasinya, meliputi standarisasi internasional, layanan infrastruktur internet andal, perangkat lunaknya berkualitas negara maju, kontrol keamanan siber secara teknis, perlindungan data, dan kerangka pengungkapan kejahatan siber. Selain itu, negara ini memiliki beberapa kultur yang relevan dengan keamanan digital, meliputi prioritas publik untuk keamanan siber, kepercayaan publik pada keamanan siber, pengetahuan publik mumpuni untuk keamanan siber, pelaporan keamanan siber, dan ketertarikan masyarakat pada keamanan siber. Dari beberapa hal di atas, Republik Lithuania telah memiliki sistem yang cukup komplek untuk keamanan internet di wilayahnya.

Kecukupan Kebutuhan Energi

Republik Lithuania memiliki kebutuhan dalam negeri yang besar. Dalam tulisan Baran (2006), pemerintah berupaya memenuhi kecukupan energi yang sejak lama negara ini bergantung pada Rusia. Adapun kekurangan sumber daya alam negara ini adalah pada listrik, gas, dan minyak. Pertama berkaitan dengan koneksi elektrik di negara ini, pemerintah memiliki keterbatasan untuk memenuhi kebutuhan listriknya sehingga mengandalkan jaringan kabel dari negara Federasi Rusia dengan kebutuhan listrik sebesar 100 persen. Serupa dengan masalah sebelumnya, Republik Lithuania juga memiliki kekurangan pasokan gas sebesar 88, 251 juta kubik untuk berbagai kepentingan di teritorial ini sehingga harus impor dari Rusia (Worldometer, 2022). Selain berkaitan dengan kebutuhan gas, Republik Lithuania juga masih harus mendatangkan minyak dari Rusia sebesar 80 persen dari kebutuhannya. Dari itu semua, Republik Lithuania telah memenuhi kebutuhan energinya, tapi sebagian besar harus dengan cara impor dari tetangganya.

Upaya Republik Lithuania dalam Menghadapi Ancaman Perang Generasi Kelima

Dalam menghadapi serangan perang generasi kelima dari Rusia, Republik Lithuania banyak melakukan tindakan pengamanan. Alasanya karena negara terancam oleh eksistensi militer Rusia yang sangat besar dan kuat. Lebih dari itu, Lithuania telah mengalami beberapa insiden dalam bentuk serangan informasi, serangan siber, dan tekanan energi. Untuk menghadapi hal tersebut, Republik Lithuania melakukan beberapa cara untuk merespon melebarnya ancaman perang generasi kelima ini. Dalam penelitian Reed (2008), perluasan ancaman tersebut adalah meliputi ranah peperangan, bentuk musuh, perubahan tujuan perang, dan bentuk peperangan.

Pertama, negara mespon terbentuknya ranah baru peperangan yang diciptakan oleh Rusia. Adapun negara Lithuania ini menjawab tantangan medan baru Rusia dari segi militer dan nonmiliter. Pertama untuk menghadapi meluasnya keberadaan

ancaman militeristik, Republik Lithuania membentuk upaya keamanan militer, yang menegaskan bahwa prinsip-prinsip keamanan Lithuania adalah bersifat total, kolektif, individual, nonkonfronsional, demokratis, aliansi tidak terbagi-bagi, dan pendekatan keamanan komprehensif. Selain dari ancaman militeristik sebelumnya, Republik Lithuania juga berupaya untuk menanggulangi meluasnya ancaman nonfisik dengan cara meningkatkan koordinasi, partisipasi inisiatif internasional, dan kerjasama dalam hal keamanan siber serta energi. Dari beberapa hal tersebut, Republik Lithuania memperkuat keamanannya dengan cara mengembangkan keamanan dalam negeri dan hubungan keamanan luar negerinya.

Kedua, Republik Lithuania menghadapi perubahan bentuk musuh dari Rusia. Dalam hal ini, musuh Lithuania tersebut telah menggunakan kombinasi-kombinasi tertentu untuk mencapai kesuksesan dalam peperangan. Dalam kasus di negara Lithuania, musuh menjelma dalam beberapa bentuk meliputi media, peretas canggih, dan perusahaan minyak Rusia. Lebih jelasnya, Rusia menggunakan metode-metode tertentu untuk menyerang Lithuania menggunakan serangan siber dan tekanan energi. Adapun penjelasanya adalah sebagai berikut:

Musuh dengan Metode Serangan Siber

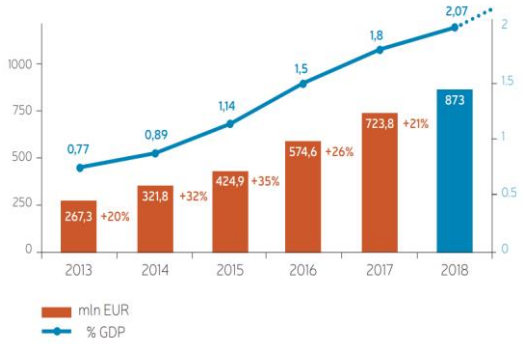
Dalam penanganan masalah ini, Lithuania berfokus pada serangan peretas dan media pro Rusia. Untuk menangani masalah tersebut, negara membentuk kebijakan, kelembagaan, dan kerjasama keamanan siber dengan negara lain. Dari segi kebijakan, negara Lithuania menciptakan regulasi terkait ancaman serangan dunia maya di wilayahnya dengan membentuk strategi keamanan siber dan strategi keamanan nasional. Kemudian dari segi kelembagaan, Republik Lithuania memperkuat keamanannya dengan pembentukan institusi keamanan siber, yaitu Pusat Keamanan Dunia Maya (National Cyber Security Center) dan Dewan Keamanan Siber (Cyber Security Council). Tidak ketinggalan, Republik Lithuania memperkuat kemanan sibernya dengan kerjasama dari dalam negeri dan luar negeri. Kesimpulannya, Republik Lithuania berupaya untuk menciptakan sistem defensif keamanan digital di wilayahnya dengan kebijakan, kelembagaan, dan kerjasama keamanan siber untuk merespon musuh bentuk baru ini.

Musuh dengan Metode Tekanan Energi

Selain dari serangan peretas, pemerintah Lithuania juga berupaya untuk menangani musuh dengan metode tekanan energi. Adapun dalam hal ini, Republik Lithuania kerap terganggu oleh ancaman politisasi dan pemberhentian minyak negara tetangga tersebut. Kemudian melalui kebijakan keamanan nasional tahun 2012, 2017, dan 2021, Republik Lithuania telah mengurangi ketergantungan energi ini dengan beberapa langkah. Pertama, pemerintah mengintegrasikan keamanan energinya dengan Uni Eropa. Kedua, negara akan meningkatkan infrastruktur energinya melalui renovasi bangunan serta fasilitas. Ketiga, Lithuania juga berupaya untuk mempromosikan penggunaan energi terbarukan. Keempat, Republik Lithuania akan mengembangkan energi nuklir. Terakhir, Lithuania akan memastikan berlangsungnya kegiatan operasi perusahaan energi dengan cara memelihara cadangan minyak dan gas. Dari beberapa hal tersebut, negara Lithuania telah berusaha memastikan kecukupan energi dengan cara menghubungkan jaringan luar negeri.

Ketiga, Republik Lithuania berusaha menghadapi fenomena perubahan tujuan peperangan dari musuh. Dalam kontek ini, Rusia berinisiatif menghancurkan upaya pertahanan Lithuania dengan cara fisik dan nonfisik, meliputi serangan siber dan penyetopan pasokan energi. Dalam merespon hal tersebut, negara ini telah

menciptakan upaya-upaya keamanan meliputi seperti strategi keamanan nasional tahun 2002 dan kebijakan keamanan militer tahun 2004. Kemudian untuk menyempurnakan kebutuhan keamanan, Republik Lithuania membuat penanggulangan terbaru untuk merespon ancaman militer dan nonmiliter. Dari segi militer, Republik Lithuania mempersiapkan negaranya untuk beberapa hal, meliputi pencegahan ancaman, pertahanan diri, pertahanan kolektif, keamanan di luar wilayah, dan keamanan dalam masa damai. Sedangkan dari keamanan nonmiliter, Republik Lithuania melakukan beberapa penanganan, yaitu pembentukan keamanan energi, keamanan siber, keamanan sosial, keamanan identitas, dan kontra intelijen. Dari beberapa hal tersebut, Republik Lithuania memberlakukan kebijakan lebih komprehensif dari sebelumnya.



Gambar 2. Anggaran militer Lithuania dari tahun ke tahun

(Sumber: Kementerian Pertahanan Republik Lithuania, 2017)

Dalam Gambar 2. di atas, Republik Lithuania telah meningkatkan anggaran militernya. Adapun dalam kegiatan ambisius ini, negara secara konsisten menambah jumlah besaran dana militernya. Pada tahun 2018, anggaran militer Lithuania mencapai 2.07 persen dari GDP-nya. Jumlah tersebut bagi Lithuania menjadi yang tertinggi dari tahun-tahun sebelumnya. Dari hal tersebut, negara mengembangkan kekuatan militernya melalui penambahan jumlah biaya militer.

Gambar 3. Proyek modernisasi alutsista di Republik Lithuania

(Sumber: Kementerian Pertahanan Republik Lithuania, 2017)

Dalam Gambar 3. tersebut, Republik Lithuania sedang mengembangkan alutsistanya menjadi lebih canggih dari sebelumnya. Adapun beberapa persenjataan berat tersebut meliputi kendaraan Boxer Vilxas, howitzer PZH2000, dan misil Nasams. Pertama pada kendaraan tempur Boxer Nasams ini, Kementerian Pertahanan memperkuatnya dalam hal mobilitas, perlindungan, dan kekuatan tembakan. Kedua pada howitzer PZH2000, pemerintah mengembangkan senjata ini menjadi lebih efisien pada daya tembaknya. Terakhir yaitu misil Nasams, negara menginovasikannya agar lebih kokoh dan terjamin dalam peperangan. Dari upaya-upaya ini, negara mengembangkan peralatan militernya agar sesuai dengan tantangan keamanan terbaru.

Gambar 4. Peningkatan jumlah personal militer di Republik Lithuania

(Sumber: Kementerian Pertahanan Republik Lithuania, 2017)

Pada Gambar 4., Republik Lithuania telah meningkatkan jumlah personil militernya. Dalam pertambahan tentara ini, negara menambah kapasitas personilnya dari beberapa tahun belakangan. Adapun pada 2009, negara Lithuania memiliki personil sebesar 12.700 orang. Kemudian pada 2018, jumlah ini meningkat menjadi 19.740 orang. Dari peningkatan jumlah tentara tersebut, Lithuania berupaya untuk mengantisipasi pertempuran dengan musuh secara militeristik, khususnya pada jumlah pasukannya.

Terakhir, Republik Lithuania berupaya untuk merespon perubahan bentuk peperangan. Pada perkembangan peperangan ini, Rusia mengancam negara ini secara militer dan nonmiliter. Maka untuk menangani hal ini, Lithuania mencegahnya dengan penanganan secara kinetik dan non-kinetik. Dalam menanggulangi ancaman serangan kinetik, Republik Lithuania merespon hal ini melalui pembentukan upaya keamanan meliputi strategi, kerjasama, dan pelatihan militer. Selain dalam hal bersifat militer tersebut, negara juga berupaya untuk memperkuat keamanan non-kinetiknya melalui strategi keamanan nasional tahun 2012, 2017, dan 2021. Sistem penanggulangan tersebut mendasari beberapa penanganan, meliputi keamanan energi, keamanan siber, dan keamanan identitas. Dalam keamanan energi, negara ini berupaya untuk menghubungkan jaringan minyak dan gasnya dengan Uni Eropa. Selanjutnya dalam keamanan siber, Republik Lithuania telah membangun sistem pertahananya melalui kebijakan, kelembagaan, dan kerjasama. Dari beberapa upaya tersebut, Republik Lithuania berupaya untuk menciptakan sistem defensif yang bisa merespon ancaman secara militer maupun nonmiliter.

TABEL 1.LEMBAGA KEAMANAN SIBER REPUBLIK LITHUANIA

NO	**Lembaga Keamanan Siber**		
	Nama Lembaga	***Tahun***	***Tugas***
1.	Pusat Keamanan Siber	2015	Manajemen
2.	Dewan Keamanan Siber	2015	Perumusan kebijakan

((Sumber: PemerintahRepublik Lithuania, 2015)

Pada Tabel 1. di atas, Republik Lithuania telah mendirikan dua lembaga keamanan untuk urusan dunia maya. Badan perlindungan siber ini adalah Pusat Keamanan Siber dan Dewan Keamanan Siber yang berdiri sejak tahun 2015. Adapun tanggung jawab dari lembaga pertahanan dunia maya tersebut adalah meliputi beberapa hal, seperti manajemen insiden siber, pemantauan pelaksanaan strategi keamanan siber, dan perumusan kebijakan keamanan siber. Dari pendirian keamanan siber ini, Republik Lithuania telah menciptakan badan keamanan siber untuk menanggulangi segala masalah ancaman peretasan di negaranya.

Kesimpulan dari beberapa hal di atas, Republik Lithuania berusaha untuk menanggapi perubahan bentuk musuh. Adapun kategori musuh di Lithuania berubah dari ancaman militer, kemudian bertambah lebih luas, meliputi peretas, media pro Rusia, dan perusahaan energi. Untuk menanggulangi hal ini, pemerintah Lithuania menciptakan sistem keamanan siber dan keamanan energi. Dalam pelaksanaannya, pemerintah membentuk regulasi, badan penanggulangan, dan kemitraan. Oleh karena itu, negara ini berupaya menangani perubahan bentuk musuh terbaru melalui pembentukan sistem di negaranya dan kemitraan bersama aliansi.

4. Kesimpulan

Republik Lithuania sedang terancam oleh manuver perang generasi kelima dari negara Rusia. Kondisi tersebut karena negara Lithuania rentan oleh serangan Rusia yang menggunakan metode perang generasi terbaru. Sedangkan untuk merespon hal ini, sebelumnya, Republik Lithuania memiliki kapasitas dan kapabilitas yang tidak memadai dalam menghadapi ancaman tersebut. Oleh sebab itu, negara ini perlu mengembangkan keamanannya untuk menanggulangi segala bentuk ancaman modern dari Rusia ini.

Dalam menyikapi hal di atas, Republik Lithuania telah melakukan upaya penanganan pada ancaman perang generasi kelima ini. Adapun bentuk respon tersebut, negara ini melakukan beberapa tindakan untuk menangani berkembangnya ranah, musuh, tujuan, dan bentuk dari peperangan modern ini. Pertama untuk menghadapi ranah baru peperangan, negara ini menanggulangi meluasnya metode serangan perang generasi kelima dari Rusia dengan perluasan prinsip keamanan dan hubungan luar negeri. Kemudian dalam merespon perubahan bentuk musuh, negara ini membentuk penanganan untuk musuh jenis baru ini melalui kebijakan, kelembagaan, dan kerjasama. Sedangkan untuk menghadapi perubahan tujuan peperangan, negara Lithuania ini memperbarui penangananya dengan membentuk strategi lebih baru dari dekade sebelumnya, meliputi strategi militer dan strategi keamanan nasional. Terakhir untuk perubahan bentuk peperangan, negara menciptakan penanggulangan yang bersifat militer dan nonmiliter. Dari beberapa temuan tersebut, secara umum Republik Lithuania telah membentuk sistem defensif keamanan perang generasi kelima di wilayahnya.

Berdasarkan hasil penelitian ini, negara Republik Lithuania telah berhasil menciptakan sistem keamanan perang generasi kelima. Adapun keberhasilan yang dimaksud, Lithuania telah membentuk penanganan militer dan nonmiliter untuk menghalau agresivitas Rusia, meliputi kelembagaan, kebijakan, dan kerjasama. Namun dalam perkembangan saat ini, situasi telah berubah, di antaranya sudah semakin mengarah pada berlangsungnya model perang generasi kelima. Karena ini Lithuania harus terus menguatkan sisi pertahanannya tersebut. Karena ancaman yang muncul akan semakin beragam, baik yang berasal dari fisik dan non-fisik maupun yang bersifat kinetik dan non-kinetik.

Daftar Pustaka

Abbott, D. H. 2010. The Handbook of 5GW. MI, USA: Nimble Books LLC.

Andriukaitis, L. 2019. Russian Disinformation Patterns: NATO is to Blame for Kaliningrad's Militarization. Institutt for Policy Analysis and a Digital Forensic Research Associate. 1: 1-4.

Andriukaitis, L. 2020. Russian Propaganda Efforts in the Baltics and the Wider Region. 1. Vilnius: Vilnius Institute for Policy Analysis.

Antczak, A. Dan Z. Sliwa. 2018. Security Dilemmas of the Baltic Region. Ssp. 3(8): 119-134.

Baltic Times. 2008. Lithuania Cyber Attacks: Round Two. https://www.baltictimes.com/news/articles/20897/ (Diakses pada 14 Desember 2022).

Baran, Z. 2006. Lithuania Energy Security: Challenges and Choices. Hudson Institute.

Boston, S. S. dan D. Massicot. 2017. The Russian Way of Warfare: A Primer. Rand Corporation. 1-14.

Boston, S. S., M. Johnson, N. B. Mustafaga, dan Y. K. Crane. 2018. Assessing the Conventional Force Imbalance in Europe. RAND Corporation. 1-14.

Center For Security Studies. 2002. Lithuania: National Security Strategy. https://css.ethz.ch/en/services/digital-library/publications/publication.html/156885 (Diakses pada 9 April 2020).

CERT-RRT. 2006. CERT-RRT 2006 Metu Insidentu Statistika. Vilnius.

CERT-RRT. 2007. CERT-RRT Apibendrina 2007 Metu Insidentu Statistika. Vilnius.

CERT-RRT. 2008. CERT-RRT Apibendrina 2008 Metu Insidentu Statistika. Vilnius.

CERT-LT. 2009. CERT-LT Apibendrina 2009 Metu Veikla Ir Teikia Prognozes 2010 Metams. Vilnius.

CERT-LT. 2010. CERT-LT Apibendrina 2010 Metu Veikla. Vilnius.

CERT-LT. 2011. CERT-LT Apibendrina 2011 Metu Veikla. Vilnius.

CERT-LT. 2012. CERT-LT Apibendrina 2012 Metu Veikla. Vilnius.

Chng, S., H. Y. Lu, A. Kumar, dan D. Yau. 2022. Hacker Type, Motivations and Strategies: A Comprehensive Framework. Computer in Human Behavior Reports. 5: 1-8.

Departemen Keamanan Negara Republik Lithuania dan Departemen Investigasi Kementerian Pertahanan Nasional Republik Lithuania. 2017. National Security Threat Assessment. 1. Vilnius.

Departemen Minoritas Nasional Lithuania. 2019. Russians in Lithuania. Vilnius.

Departemen Pertahanan Republik Lithuania. 2010. Lithuania Military Doctrine. Information Provision Service of the General Affairs Department of the Ministry of National Defence. Kaunas.

Doktrin Militer Lithuania Tahun 2010 Nomor V-193. Lithuania Military Doctrine. 10 Maret 2010. Vilnius: Kepala Pertahanan Republik Lithuania.

Flanagan, S. J., J. Osburg, A. Binnendijk, M. Kepe, dan A. Radin. 2018. Deterring Russian Aggression in the Baltic States Trought Resilience and Resistance. Rand Cooperation. 1(1): 1-35.

Gotev, G. 2016. Lithuania Parliament under Cyber Attack. https://www.euractiv.com/section/digital/news/lithuanian-parliament-under-cyber-attack/ (Diakses pada 14 Desember 2022).

Global Security. org. Russian Military Personnel. https://www.globalsecurity.org/military/world/russia/personnel.htm (Diakses pada 10 Desember 2022).

Hammers, T. X. 2007. Fourth GenerationWarfare Evolves, Fifth Emerges. Military Review.1: 14-23

International Telecommunication Union. 2019. Lithuania Takes the 4th Position in the Global Cybersecurity Index. https://ltlife-lt.cdn.ampproject.org (Diakses pada 15 Mei 2020).

Interpol. 2020.Cybercrime. https://www.interpol.int/crimes/cybercrime (Diakses pada 17 Februari 2020).

Jonston, M. P. 2014. Secondary Data Analysis: A Method of Which the Time Has Come. Qualitative and Quantitative Methods in Libraries (QQML). 3: 619-626.

Jurgeleviciute, D. 2007. Information Security in Lithuania: The Problem of May 9th and the Crash of the Russian Fighter. Strategic Research Center. 1: 259-278

Karpaviciute, I. 2017. Securitization and Lithuania's National Security Change. De Gruyter. 36 (5): 9-33.

Kementerian Pertahanan Republik Lithuania. 2017. Lithuania Defense System: Facts and Trends. Vilnius: MoND.

Klotz, A. dan D. Prakash. 2008. Qualitative Methods in International Relations. 1. New York: Palgrave Macmillan.

Kojala, L., J. Kulys, A. Prochorenko. dan A. Rozevic. 2020. Research on the Assessment of the Geopolitical Situation and Perception of Threats. Eastern Europe Studies Centre. 1: 5-44.

Komisi Eropa. 2018. eGovernment in Lithuania. Luxembrug: ISA Editorial Team.

Lind, W. S. dan G. A. Thiele. 2015. 4th Generation Warfare Handbook. 1. Kouvola: Castalia House.

Paleri, P. 2008. National Security Imperatives and Challenges. New Delhi: Tata McGraw-Hill.

Sugiyono. 2013. Metode Penelitian Kuantitatif Kualitatif dan R&D. Bandung: Alfabeta.

Laughlin, D. M. 2008. Lithuania Accuses Russian Hackers of Cyber Assault After Collapse of Over 300 Websites. http://www.irishtimes.com/news/Lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155 (Diakses pada 31 Januari 2020).

Lasswell, H. D. 2017. Power and Society: A Framework for Political Inquiry. New York: Routledge.

Lithuania: Cybersecurity Capacity Review . 2 November 2017. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/Lithuania-cybersecurity-capacity-review-2017 (Diakses pada 14 Mei 2020).

Lithuania National Defense. 2017. National Security Strategy. https://kam.lt (Diakses pada 11 April 2020).

Lipmann, W. 1943. U.S Foreign Policy: Shield of the Republic. Michigan: Little Brown.

Maliukevicius, N. 2007. Russia's Information Policy in Lithuania: the Spread of Soft Power of Information Geopolitics. Baltic Security & Defense Review. 9: 150-170.

Ministry of National Defence Republic of Lithuania. 2015. http://kam.it/en/news_1098/current_issues/cyber_security_council_of_Lithuania_convened_for_first_time.html?c= (Diakses pada 10 Februari 2020).

Misik, M. dan V. Pracharova. 2016. Before 'Independence' Arrived: Interdependence in Energy Relations between Lithuania and Russia. Geopolitics.3: 1-26.

Mullett, A. 2008. Cyber Terrorist Attacks State and Corporate Web Sites. https://www.baltictimes.com/news/articles/20735/ (Diakses pada 14 Mei 2020).

National Audit Office. 2015. Cyber Security Environment In Lithuania. Vilnius: National Audit Office.

National Institute of Justice. 1989. Computer Crime Criminal Justice Resource Manual.Washington DC.

NATO CCDCOE. 2015. National Cyber Security Organisation: Lithuania. Tallinn: CCDCOE.

NCSC. 2012. The Military Strategy of The Republic Lithuania. Vilnius: NCSC.

Nissenbaum, H. 2004. Hackers and the Contested Ontology of Cyberspace. New media and society. 6(2) 195-214.

Nissenbaum, H. 2005. Where computer security meets national security. Ethics and information technology. 7: 61-73.

NKCS. 2020. National Cyber Security Center. https://www.NKCS.lt.t.thn.nkcs.lt/en/reports.html (Diakses pada 9 April 2020).

Pemerintah Republik Lithuania. 2018. Resolution on the Approval of the National Cyber Security Strategy. 818. Vilnius: The Government of the Republic of Lithuania.

Persatuan Telekomunikasi Internasional (ITU). 2018. Global Cybersecurity Index (GCI). Geneva: International Telecommunication Union.

Pusat Keamanan Siber Nasional Kementerian Pertahanan Lithuania. 2017. National Cyber Security Status Report for the Year 2017. Vilnius: MoND.

Pusat Keamanan Siber Universitas Oxford. 2017. Cybersecurity Capacity Review Republik Lithuania. Oxford: Universitas Oxford.

Seimas. 2002. National Security Strategy. Vilnius: Parlemen Republik Lithuania.

Seimas. 2005. e-seimas. https://e-seimas.irs.lt (Diakses pada 22 Maret 2020).

Seimas. 2017. National Security Strategy. Vilnius: The Seimas of the Republic Lithuania.

Spencer, L., J. Ritchie, J. Lewis, dan L. Dillon. 2003. Quality in Qualitative Evaluation: A Framework for Assessing Research Evidence. London: Cabinet Office.

Stitilis, D. dan V. Klisauskas. 2015. Aspect of Cybersecurity: the Case of Legal Regulation in Lithuania. Journal of Security and Sustainability Issues. 5 (1): 45-57.

Stitilis, D., P. Pakutinskas, M. Laurinaitis, dan I. M. Castel. 2017. A Model for the National Cyber Security Strategy. The Lithuanian Case. Journal of Security and Sustainable Issues. 6 (3): 357-372.

Stitilis, Pakutinskas, dan L. Castel. 2017. A Model for the National Cyber Security Strategy. The Lithuanian Case. Journal of Security and Sustainability Issues. 6 (3): 357-372.

Strategi Militer Republik Lithuania Tahun 2004. The Military Strategy of the Republic of Lithuania. Vilnius: The Minister of National Defence of the Republic Lithuania.

Strategi Militer Republik Lithuania Nomor V-1303 Tahun 2012. The Military Strategy of the Republic of Lithuania. V-1305. 22 November 2012. Vilnius: The Minister of National Defence of the Republic Lithuania.

Strategi Militer Republik Lithuania Tahun 2016 Nomor V-252. The Military Strategy of the Republic of Lithuania. 17 Maret 2016. Vilnius: The Minister of National Defence of the Republic Lithuania.

Sytas, A. 2017. Russian Hacking Threatens Lithuania's Banks: Survey. https://www.reuters.com/article/us-lithuania-russia-cyber-idUSKBN18X29T (Diakses pada 14 Desember 2022).

Reed. D. J. 2008. Beyond the War on Terror: Into the Fifth Generation of War and Conflict. Studies in Conflict & Terrorism. 31: 684-722.

Resolusi Parlemen Republik Lithuania Nomor IX-907 Tahun 2002. National Security Strategy. 28 Mei 2002. Vilnius: Seimas Republik Lithuania.

Resolusi Parlemen Republik Lithuania Nomor X-91 Tahun 2005. On the Approval of the National Security Strategy. 20 Januari 2005. Vilnius: Seimas Republik Lithuania.

Resolusi Parlemen Republik Lithuania Nomor XI-2131 Tahun 2012. Amending the Seimas of the Republic of Lithuania Resolution on the Approval of the National Security Strategy. 26 Juni 2012. Vilnius: Seimas Republik Lithuania.

Resolusi Parlemen Republik Lithuania Nomor XII-202 Tahun 2017. National Security Strategy. 17 Januari 2017. Vilnius: Seimas Republik Lithuania.

Resolusi Pemerintah Republik Lithuania Nomor 796 Tahun 2011. On the Approval of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019. 29 Juni 2011. Vilnius: Pemerintah Republik Lithuania.

Resolusi Pemerintah Republik Lithuania Nomor 818 Tahun 2018. National Cyber Security Strategy. 13 Agustus 2018. Vilnius: Pemerintah Republik Lithuania.

Reuters Staff. 2008. Lithuania Tax Office Website Hit by Cyber Attack. https://www.reuters.com/article/lithuania-web-attacks-idUSMAR14153920080721 (Diakses 11 Desember 2022).

Rhodin, S. 2008. Web Sites in Lithuania Attacked. https://www.nytimes.com/2008/06/30/world/europe/30iht-baltic.4.14108611.html (Diakses pada 14 Desember 2022).

Worldometer. 2022. https://www.worldometers.info/gas/lithuania-natural-gas/ (Diakses pada 11 Desember 2022).

Zemaitis, J. 2007. Lithuanian Annual Strategic Review 2006. Strategic Research Center. 2: 1-259.

Vol. 10, No.1, 2023
P-ISSN: 2355-1798, e-ISSN: 2830-3903