KEBIJAKAN PERTAHANAN *CYBER* ESTONIA DALAM MERESPON TINDAKAN *CYBER SABOTAGE* OLEH RUSIA KEPADA ESTONIA

Fathika Anjani Firman

Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Komputer Indonesia
Jalan Dipati Ukur No. 112 Bandung 40132 Indonesia

E-mail: anjanifathika21@gmail.com

ABSTRACT

This research aims to find out how the response provided by the government of Estonia in order to counteract the cyber sabotage actions that had previously befall Estonia by Russia. To answer the problem, researchers conducted an analysis of the actions and policies undertaken by Estonia in making defense and protection in the cyber space.

The research method used in this research is qualitative method. In collecting the data the researchers conducted field studies, literature study, and online searching. While the technique to analyze data using data triangulation.

This study analyzes what are the post-action losses that are economic losses due to the cessation of economic activity and the deterioration of Estonian public facilities, the bilateral relations between Estonia and Russia after the events that were initially blame each other and have improved now, as well as the response of the two countries in addressing it defense policy by Estonia which was then responded to by many countries. The conclusions of this study show that in the field of defense and security, both countries are equally demonstrating their strength, which then triggers an increase in sovereignty safeguard in the new realm of cyberspace. In the present era there have been new threats and cyber-domains requiring special attention in order to safeguard the sovereignty of a country.

Keywords: Estonia, cyber sabotage, cyber defence, Russia.

ABSTRAK

Penelitian ini bertujuan untuk mengetahui bagaimana respon yang diberikan oleh Estonia dalam rangka menangkal tindakan *cyber sabotage* yang sebelumnya telah menimpa Estonia oleh Rusia. Untuk menjawab permasalahan tersebut, peneliti melakukan analisis mengenai tindakan dan kebijakan yang dilakukan oleh Estonia dalam membuat pertahanan di dunia *cyber*.

Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif. Dalam mengumpulkan data-data peneliti melakukan studi lapangan, studi pustaka, dan penelusuran *online*. Sedangkan teknik untuk menganalisis data menggunakan triangulasi data.

Penelitian ini menganalisa apa saja kerugian pasca tindakan tersebut yang berupa kerugian ekonomi akibat berhentinya aktivitas ekonomi dan kerusakan fasilitas publik Estonia, hubungan bilateral Estonia – Rusia pasca kejadian yang pada awalnya masih saling menyalahkan dan telah membaik saat ini, dan juga respon kedua negara dalam menyikapi dibuatnya kebijakan pertahanan oleh Estonia yang kemudian ditanggapi banyak negara. Kesimpulan penelitian ini menunjukan bahwa dalam bidang pertahanan keamanan, kedua negara sama – sama menunjukkan kekuatan yang dimiliki, yang kemudian memicu peningkatan penjagaan kedaulatan di ranah baru yaitu *cyberspace*. Di era sekarang

ini telah bermunculan ancaman – ancaman yang sifatnya baru dan ranah *cyber* memerlukan perhatian khusus dalam rangka menjaga kedaulatan sebuah negara.

Kata Kunci : Estonia, sabotase siber, pertahanan siber, Rusia.

1. Pendahuluan

1.1 Latar Belakang

Di zaman modern sekarang ini globalisasi serta perkembangan teknologi telah dirasakan oleh berbagai khalayak masyarakat akan dampak positif maupun negatif yang menyertainya. Aktivitas hubungan internasional pun tidak lepas dari keterkaitannya dengan penggunaan teknologi komunikasi dan informasi dalam penggunaannya sebagai alat untuk mencapai kepentingan negara. Jaringan tanpa batas dalam dunia teknologi informasi sudah banyak ditemukan beberapa tindakan yang melawan hukum. Umumnya kejahatan yang berhubungan dengan teknologi atau disebut *cybercrime*. Salah satu contoh kejahatan melalui dunia maya adalah sabotase siber atau *cyber sabotage.*

Kini interaksi yang dilakukan antar aktor hubungan internasional tidak hanya pada ruang darat, laut dan udara saja. Interaksi antar aktor juga memadati ruang maya yang menjadi media baru untuk mencapai kepentingan. *Cyberspace* menjadi ruang sekaligus sarana baru dalam mencapai kepentingan yang kemudian dikenal dengan *cyberpower* (https://jipsi.fisip.unikom.ac.id/_s/data/jurnal/olume-06-no-1/8-dewi-triwahyuni-tine-edited.pdf/pdf/8-dewi-triwahyuni-tine-edited.pdf diakses 21 Agustus 2018).

Dalam hubungan antar negara, kegiatan *sabotage* (sabotase) walaupun dilakukan secara diam dan sembunyi – sembunyi tetaplah ada. Mengikuti arah perkembangan teknologi salah satu bentuk *apt (advance persistent threat)* atau serangan melalui jaringan dimana seseorang yang tidak mendapatkan akses legal ke suatu jaringan dan keberadaannya cenderung mengancam adalah *cyber sabotage*. Bentuk baru dari sabotase ini mempengaruhi hubungan antar negara salah satunya di bidang ekonomi dan politik dan keamanan, sekaligus juga membentuk medan perang baru dalam ranah perang dunia modern.

Topik yang dibahas oleh peneliti yaitu tentang tindakan *cyber sabotage* oleh Rusia kepada Estonia dan dampaknya terhadap pembentukan kebijakan pertahanan *cyber* Estonia. Konflik berawal di tahun 2007 yang dipicu oleh pemindahan patung *Bronze Soldier* oleh pemerintah Estonia dari pusat kota Tallin ke pedesaan. Masyarakat Rusia menganggap pemindahan patung tersebut sebagai sebuah aksi diskriminasi terhadap mayoritas dan menganggap Estonia tidak menghargai jasa mereka.

Merespon tindakan tersebut, masyarakat Rusia protes turun ke jalan didepan Kedutaan Estonia pada tanggal 26 dan 27 April 2007. Perisitiwa tersebut dikenal dengan nama *"Bronze Night"* Kemudian serangan *cyber* dimulai pada tanggal 27 April 2007, menyerang website Perdana Menteri Estonia (valitsus.ee/en), website parlemen Estonia, website partai politik, bank (*Hansabank*) dan media *(Post Times)*. Serangan ini melumpuhkan sistem pemerintahan Estonia selama kurang lebih dua pekan **(**https://www.viva.co.id/indepth/sorot/265596-barak-serdadu-cyber-di-estonia di upload 18 November 2011, di akses 27 Februari 2018).

Serangan yang dilancarkan merupakan serangan DDoS *(Distributed Denial of Service)* yaitu dengan cara membanjiri situs – situs yang dituju dengan trafik data yang sangat masif berjumlah 4 juta data per detik, yang otomatis mematikan kinerja situs dan tidak dapat diakses. Pada tanggal 16 Mei 2007 volume serangan mulai menurun, dan kemudian di tanggal 18 Mei 2007 serangan *cyber* berakhir setelah berlangsung 22 hari lamanya. Menteri Luar Negeri Estonia, Urmas Paet mengatakan bahwa Rusia terkait secara langsung dalam *cyber sabotage* tersebut. Namun, pemerintah Rusia membantah terlibat dalam serangan,

Moskow menyatakan tidak bersalah, tetapi tetap bermusuhan dalam prakteknya.

Pada bulan Maret 2009, Sergei Markov, seorang wakil dari Deputi Duma dari partai pro Kremlin, *Unified Russia* secara tidak terduga membuka mulut pada sebuah diskusi tentang *warfare*, bahwa asistennya lah yang melaksanakan serangan sabotase *cyber* kepada Estonia. Dia adalah Konstantin Goloskokov, seorang aktivis anggota kelompok pemuda pro-Kremlin, Nashi. Menggunakan metode yang dikenal sebagai serangan *distributed denial of service* (DDoS), Goloskokov mengatakan dia dan sekelompok temannya meretas jaringan internet Estonia, secara efektif melumpuhkan berbagai bagian sistem selama tiga minggu pada bulan April dan Mei 2007.

Beberapa pengamat IT Estonia mengatakan bahwa Goloskokov setidaknya mendapat dukungan diam-diam dari Kremlin. Banyak fakta yang menunjuk bahwa Goloskokov yang berbicara secara bebas tentang insiden itu, tanpa rasa takut akan penuntutan, karena menunjukkan serangan itu didukung oleh kekuatan yang lebih tinggi, ujar Vladimir Pribylovsky, presiden dari *Panorama Information and Research Center* (https://www.computerworld.com/article/2511704/vertical-it/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.amp.html di upload tanggal 9 Desember 2010, di akses tanggal 12 April 2018).

Pengakuan Goloskokov dilakukan selang 14 bulan setelah salah seorang anggota *hacker* sabotase *cyber* ke Estonia ditangkap. Tepatnya pada tanggal 24 Januari 2008, Dmitri Galushkevich, seorang *hacker* beretnis Rusia dinyatakan bersalah karena berpartisipasi dalam serangan. Dia didenda 17.500 kroons (sekitar US$ 1.640) untuk menyerang website Partai Reformasi Estonia.

Implikasi dari serangan sabotase *cyber* tersebut kepada negara Estonia adalah Estonia semankin meningkatkan sistem pertahanan *cyber* nya. Beberapa lembaga pertahanan *cyber* didirikan pasca insiden di tahun 2007. Penyusunan kebijakan pertahanan *cyber* Estonia diwujudkan dengan pendirian lembaga – lembaga diantaranya *Estonia's Cyber Security Strategy, The NATO Cooperative Cyber Defence Center of Excellence,* dan *Cyber Defence League.*

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

"Bagaimana kebijakan pertahanan *cyber* Estonia dalam merespon tindakan *cyber sabotage* oleh Rusia kepada Estonia?"

1.2.2 Rumusan Masalah Minor

1. Apa sajakah kerugian yang dialami oleh Estonia pasca tindakan sabotase *cyber*?
2. Apakah respon yang diberikan oleh Estonia terhadap tindakan *cyber sabotage* oleh Rusia?
3. Bagaimanakah hubungan antara Rusia dan Estonia pasca dibuatnya kebijakan pertahanan *cyber* oleh Estonia?

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Untuk mengetahui apakah tindakan sabotase *cyber* dari Rusia kepada Estonia dapat membawa dampak terhadap penyusunan kebijakan pertahanan *cyber* Estonia.

1.3.2 Tujuan Penelitian

1. Untuk mengetahui kerugian yang dialami Estonia pasca tindakan sabotase *cyber* tersebut.
2. Untuk mengetahui seperti apa respon yang diberikan oleh Estonia terhadap tindakan *cyber sabotage* oleh Rusia.
3. Untuk mengetahui bagaimanakah hubungan antara Rusia dan Estonia pasca dibuatnya kebijakan pertahanan *cyber* oleh Estonia.

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Penelitian ini diharapkan dapat memberi manfaat kepada perguruan tinggi tempat peneliti mengenyam ilmu semasa kuliah, sebagai penerapan dari beberapa kajian ilmu yang telah dipelajari oleh peneliti sejak awal sampai akhir perkuliahan yaitu kajian ilmu tentang Hubungan Internasional di Eropa,

kajian tentang *Cyber Law*, dan kajian tentang Diplomasi dan Negosiasi.

1.4.2 Kegunaan Praktis

Penelitian ini diharapkan dapat membawa manfaat menambah keilmuan bagi peneliti, bagi mahasiswa program studi Hubungan Internasional UNIKOM maupun universitas lainnya, menjadi rujukan atas bahan belajar bagi mahasiswa hubungan internasional, dan menjadi penelitian yang bermanfaat bagi masyarakat dan diharapkan dapat lebih memantapkan penguasaan fungsi keilmuan yang dipelajari oleh peneliti selama menempuh program perkuliahan Ilmu Hubungan Internasional, FISIP Universitas Komputer Indonesia.

Juga diharapkan dapat memberikan sumbangsih bagi pengembangan studi Hubungan Internasional di masa mendatang dan dapat menjadi masukan atau referensi yang berguna untuk almamater Universitas Komputer Indonesia.

2. Tinjauan Pustaka dan Kerangka Pemikiran

2.1 Tinjauan Pustaka

2.1.1 Hubungan Internasional

Hubungan internasional dapat dilihat dari berkurangnya peran sebuah negara sebagai aktor dalam politik global dan ditambah dengan meningkatnya peranan aktor non negara. Batas-batas yang memisahkan antar negara semakin tipis dan tidak relevan. Bagi beberapa aktor non negara bahkan batas-batas wilayah secara geografis sudah tidak dihiraukan (Perwita & Yani, 2005: 4).

2.1.2 Politik Luar Negeri

Politik luar negeri merupakan studi hubungan eksternal dengan aktivitas – aktivitas negara bangsa yang melibatkan cita – cita, strategi, tindakan, metode, panduan dan arahan oleh pemerintah nasional yang saling melakukan interaksi/hubungan internasional dengan aktor – aktor lain (organisasi internasional, LSM, perusahaan, dll) (Jackson dan Sorensen, 2013: 439)

2.1.3 Hubungan Bilateral

Hubungan bilateral merupakan penggambaran hubungan timbal balik antara dua pihak, dan aktor utamanya adalah negara. Hubungan bilateral tercipta dari dua negara yang melakukan interaksi, hubungan bilateral dirasa lebih efektif untuk mencapai kepentingan nasional karena dilakukan secara personal sehingga tidak adanya tingkatan hirarki diantara keduanya (Perwita dan Yani, 2005: 28).

2.1.4 Kepentingan Nasional

Konsep kepentingan nasional mempunyai pengertian dimana negara berperan sebagai aktor utama di dalam formulasi politik yang merdeka dan berdaulat. Selanjutnya didalam mekanisme interaksinya masing-masing negara atau aktor berupaya untuk mengejar kepentingan nasionalnya. Kepentingan inilah yang akhirnya diformulasikan ke dalam konsep "*power*" kepentingan "*interest*" didefinisikan ke dalam terminologi *power* (Sitepu, 2011: 56).

2.1.5 Kebijakan Pertahanan

Dalam Kamus Besar Bahasa Indonesia, kebijakan adalah rangkaian konsep dan asas yang menjadi pedoman dan dasar rencana dalam pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak. Istilah kebijakan biasa diterapkan oleh pemerintahan, organisasi, kelompok sektor swasta, bahkan individu Berdasarkan peraturan perundang-undangan, yaitu Pasal 1, UU No. 34 Tahun 2004 tentang Tentara Nasional Indonesia, yang dimaksudkan dengan pertahanan negara adalah segala usaha untuk menegakkan kedaulatan negara, mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia, dan melindungi keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara, disusun dengan memperhatikan kondisi geografis Indonesia sebagai negara kepulauan. Dapat disimpulkan bahwa kebijakan pertahanan adalah rangkaian konsep dan asas yang menjadi pedoman dan dasar rencana dalam pelaksanaan pembangunan

sistem pertahanan negara yang disesuaikan dengan kondisi dan karakter suatu negara.

2.1.6 Keamanan

2.1.6.1 Offense - Defense Theory

Teori ini berangkat dari konsep *security dilemma* oleh Robert Jervis yang menjelaskan bahwa suatu hubungan aksi dan reaksi antara beberapa negara di mana tindakan suatu negara untuk meningkatkan keamanannya akan berakibat atau dianggap melemahkan keamanan negara lainnya. Asumsi dasar mengenai keseimbangan *offense-defense* adalah apabila *offense* mendominasi maka *security dilemma* akan meningkat, lalu diikuti oleh perlombaan senjata, dan pada akhirnya kemungkinan besar perang akan terjadi (http://global.ir.fisip.ui.ac.id/index.php/global/article/download/45/193 diakses tanggal 1 Juni 2018).

2.1.6.2 Cyber Security

Cyber security adalah kumpulan alat, kebijakan, konsep, perlindungan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, dan jaminan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi/aset pengguna. *Cyber security* merupakan upaya untuk memastikan pencapaian sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan dalam lingkungan *cyber space* (Ardianti, 2014: 98).

2.1.7 Cyber Crime

Kejahatan dunia maya (*cyber crime)* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit/*carding*, *confidence fraud*/penipuan identitas, pornografi anak, dan lain – lain (Wahib dan Labib, 2005:76).

2.1.8 Cyber Sabotage

Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer, atau sistem jaringan komputer yang terhubung dengan internet. Sabotase didefinisikan sebagai tindakan yang disengaja dan berbahaya yang mengakibatkan terganggunya proses dan fungsi normal atau kerusakan atau kerusakan peralatan atau informasi. (https://www.military.com/defensetech/2008/02/06/cyber-sabotage diakses tanggal 10 Desember 2017).

2.2 Kerangka Pemikiran

Rusia dan Estonia memiliki hubungan sejarah yang kurang harmonis sejak dahulu, bahkan sejak Rusia masih bernama Uni Soviet. Permasalahan etnis dan budaya yang terjadi di antara dua negara tersebut, telah berlangsung lama dan ketika tiba di masa sekarang ini dimana ranah kedaulatan sebuah negara bertambah yaitu dunia *cyber,* tak disangka telah terjadi peristiwa sabotase melalui internet di bulan April 2007. Menurut teori hubungan bilateral bahwa hubungan bilateral merupakan keadaan yang menggambarkan hubungan timbal balik antara kedua belah pihak yang terlibat, dan aktor utama dalam pelaksanaan hubungan bilateral itu adalah negara, terpapar dalam kasus ini bahwa tindakan pemindahan patung oleh pihak Estonia telah membuat sebuah reaksi kurang baik dari pihak Rusia sehingga pihak Rusia pun melakukan tindakan protes melalui *cyber sabotage.*

Cyber security merupakan sebuah usaha untuk memastikan tercapainya tujuan dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber space* diterapkan oleh Estonia dalam rangka mengantisipasi serangan *cyber* yang memiliki banyak kemungkinan terus terjadi di kemudian hari.

Dampak dari serangan sabotase *cyber* tersebut kepada negara Estonia dan sebagai bentuk implementasi dari teori *offense – defense* keamanan negara adalah Estonia semakin meningkatkan pertahanan keamanan *cyber* nya dengan membentuk lembaga pertahanan *cyber* diantaranya adalah *Estonia's Cyber Security Strategy, The NATO Cooperative Cyber Defence Center of*

Excellence, dan *Cyber Defence League* dalam rangka bentuk aksi dan reaksi di antara kedua negara di mana tindakan suatu negara untuk meningkatkan keamanannya akan berakibat atau dianggap melemahkan keamanan negara lainnya.

3. Metode Penelitian

3.1 Desain Penelitian

Ditinjau dari jenis datanya, pendekatan penelitian yang digunakan dalam penelitian ini adalah pendekatan kualitatif. Adapun yang dimaksud dengan penelitian kualitatif yaitu penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian secara holistik, dan dengan cara deskripsi dalam bentuk kata-kata dan bahasa, pada suatu konteks khusus yang alamiah dan dengan memanfaatkan berbagai metode ilmiah.

3.2 Teknik Pengumpulan Data

3.2.1 Studi Pustaka

Teknik pengumpulan data merupakan cara yang digunakan peneliti untuk mendapatkan data dalam suatu penelitian. Pada penelitian kali ini peneliti menggunakan teknik pengumpulan data dengan cara studi pustaka melalui buku-buku referensi, laporan-laporan, majalah-majalah, jurnal-jurnal dan media lainnya yang berkaitan dengan objek penelitian.

3.2.2 Studi Lapangan

Studi Lapangan yaitu pengumpulan data yang dilakukan dengan cara mengamati dan turun langsung ke lokasi penelitian. Peneliti melakukan studi lapangan ke Pusat Penelitian Politik LIPI Jakarta dan studi pustaka ke beberapa universitas di Bandung yaitu perpustakaan Universitas Komputer Indonesia, Universitas Parahyangan, Universitas Pasundan dan Universitas Padjajaran.

3.3 Uji Keabsahan Data

Triangulasi adalah cara yang paling umum digunakan dalam penjaminan validitas data dalam penelitian kualitatif. Triangulasi merupakan teknik pemeriksaan keabsahan data dengan memanfaatkan sesuatu yang lain diluar data itu untuk keperluan pengecekan data atau sebagai pembanding terhadap data itu.

3.4 Teknik Analisa Data

Penelitian ini adalah penelitian deskriptif, dengan lebih banyak bersifat uraian dari hasil studi pustaka perpustakaan dan hasil wawancara. Analisis data adalah proses pencarian dan penyusunan data yang sistematis melalui catatan di lapangan, serta dokumentasi yang secara akumulasi menambah pemahaman peneliti terhadap data yang ditemukan.

4. Hasil Penelitian dan Pembahasan

4.1 Gambaran Objek Penelitian

4.1.1 Tinjauan Umum Negara Estonia

Estonia adalah negara yang terletak paling utara dari tiga negara di kawasan Baltik, dan memiliki hubungan linguistik dengan Finlandia. Sejak mendapatkan kemerdekaan penuh karena runtuhnya Uni Soviet pada tahun 1991, Estonia telah menjadi salah satu anggota Uni Eropa bagian timur yang paling maju secara ekonomi. Dengan luas wilayah sebesar 45.227 km², Estonia memiliki populasi 1,3 juta penduduk (tahun 2015). Pertumbuhan penduduk Estonia pada tahun 2017 sebesar -0,57% (https://www.indexmundi.com/ estonia/population_growth_rate. html di upload tanggal 20 Januari 2018, diakses tanggal 23 Juli 2018).

Sistem politik Estonia adalah Republik Parlementer. Kepala negara adalah Presiden, kepala pemerintahan adalah Perdana Menteri. Badan legislasi adalah parlemen unikameral Estonia, *Riigikogu*. Parlemen menunjuk Perdana Menteri (dicalonkan oleh Presiden). Estonia sejak 1 Mei 2004 telah menjadi negara anggota Uni Eropa (UE). Kersti Kaljulaid dipilih oleh parlemen sebagai presiden perempuan pertama Estonia pada bulan Oktober 2016. Juri Ratas, perdana menteri Estonia yang partainya populer di kalangan minoritas berbahasa Rusia yang besar di Estonia, mengepalai pemerintahan koalisi yang dilantik pada November 2016 (https://www.bbc.co.uk/news/world-europe-

17220810 di upload tanggal 21 Mei 2018, diakses pada tanggal 18 Juli 2018).

Dalam politik luar negeri, Estonia sangat berkomitmen untuk memajukan hubungan trans atlantik yang baik dan untuk mempromosikan demokrasi dan kebijakan ekonomi pasar bebas secara global. Dengan beberapa tujuan diantaranya memastikan keamanan nasional dan yang tidak terkait dengan keamanan; stabilitas dan prediktabilitas hubungan internasional, memastikan tempat untuk berfungsinya ekonomi Estonia; hubungan ekonomi liberal dan ruang ekonomi liberal, Perlindungan warga negara Estonia di luar negeri dan dalam konteks hubungan luar negeri, dan Ruang nilai yang mempromosikan demokrasi, hak asasi manusia, prinsip-prinsip supremasi hukum, serta kebebasan dan pengembangan ekonomi (https://vm.ee/en/estonias-foreign-policy-objectives di upload 21 Mei 2013, di akses 30 Juli 2018).

Keuntungan ekonomi dari sektor elektronik dan telekomunikasi yang kuat dan hubungan dagang yang kuat dengan Finlandia, Swedia, Jerman, dan Rusia. Peningkatan investasi yang cepat, termasuk pendanaan pembangunan Uni Eropa, dan pemulihan pasar ekspor berkontribusi pada pertumbuhan PDB sebesar 4,2% pada tahun 2017 (https://www.indexmundi.com /estonia/exports_commodities.html di upload tanggal 20 Januari 2018, diakses tanggal 23 Juli 2018).

Masyarakat Estonia pengguna internet sebanyak 1,097,921 jiwa atau 87,2% (2016) dari total populasinya. Persentase penduduk dengan akses internet membantu mengukur seberapa luas penggunaan internet di suatu negara. (https://www.indexmundi.com/estonia/internet_users.html di upload tanggal 20 Januari 2018, diakses tanggal 23 Juli 2018).

Konsep Keamanan Nasional Estonia *(The National Security Concept of Estonia/2010)* menetapkan tujuan, prinsip dan arah kebijakan keamanan negara. Diajukan oleh pemerintah, Konsep Keamanan Nasional tunduk pada persetujuan dari *Riigikogu* (parlemen). Konsep Keamanan Nasional bisa direvisi atau diubah bergantung pada perubahan dalam lingkungan keamanan dan pengembangan langkah-langkah untuk memastikan keamanan Estonia. Konsep Keamanan Nasional merupakan dokumen kerangka kerja, dasar untuk persiapan spesifik dan rencana aksi. Dokumen ini telah menggantikan Konsep Keamanan Nasional Republik Estonia, yang diadopsi oleh *Riigikogu* pada tahun 2004(http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf di upload 12 Mei 2010, di akses 21 Juli 2018).

4.1.1.1 Pertahanan Keamanan *Cyber* Estonia

The Cyber Security Strategy adalah dokumen dasar rencana keamanan *cyber* Estonia dan bagian dari strategi keamanan yang lebih luas di Estonia. Strategi ini menyoroti perkembangan terbaru, menilai tingkat ancaman terhadap keamanan *cyber* Estonia dan menyajikan langkah-langkah untuk mengelola ancaman. Otoritas Sistem Informasi Estonia (*Riigi Infosüsteemi Amet*/RIA) menerima kekuatan dan sumber daya tambahan untuk mengatur perlindungan infrastruktur informasi dan komunikasi negara, dan melakukan pengawasan kepada keamanan sistem informasi. Untuk tujuan pengorganisasian perlindungan infrastruktur, *Department of Critical Information Infrastructure Protection* (CIIP) dibentuk dalam RIA.

Pada tahun 2011, komisi CIIP dibentuk untuk mempromosikan kerjasama publik dengan swasta. Tujuan dari komisi tersebut yang menyatukan keamanan *cyber* dan manajer TI dari lembaga layanan vital, adalah untuk bertukar informasi operasional, mengidentifikasi masalah dan membuat solusi untuk meningkatkan keamanan *cyber* dari infrastruktur penting negara (https://www.mkm.ee/sites/default/files/cyber_security_strategy_20142017_public_version.pdf diakses tanggal 23 Juli 2018).

Pembentukan *Estonian Defence League's Cyber Unit* (EDL CU), yang merupakan hasil kolaborasi antara sektor publik, swasta dan

pihak ketiga, telah berperan dalam menjaga pertahanan nasional. Keahlian relawan EDL CU diterapkan untuk meningkatkan keamanan sistem informasi perusahaan-perusahaan Estonia melalui latihan yang terkoordinasi, pengujian solusi, pelatihan, dan lain – lain. Di bidang *cyber security*, penyedia utama pelatihan dan peningkatan kesadaran adalah *Information Technology Foundation for Education*. Proyek kemitraan negara-swasta diluncurkan pada tahun 2013 untuk meningkatkan keterampilan dan *security awareness* pengguna *smartphone*, pengembang, dan vendor (https://www.mkm.ee /sites/default/files/cyber_security_strategy_201 42017_public_version.pdf diakses tanggal 23 Juli 2018).

4.1.1.2 Tinjauan Umum Negara Rusia

Rusia, salah satu negara terbesar di dunia bangkit kembali setelah satu dekade kekacauan ekonomi dan politik pasca runtuhnya Uni Soviet kemudian berusaha menegaskan kembali negaranya sebagai kekuatan dunia. Memiliki luas wilayah sebesar 7,098,242 km persegi, wilayah darat sebesar 16,377,742 km persegi dan wilayah perairan sebesar 720,500 km persegi (https://www.indexmundi.com/russia/ area.html di upload 20 Januari 2018, di akses 23 Mei 2018).

Vladimir Putin telah menjadi tokoh politik Rusia yang dominan sejak terpilih sebagai presiden pada tahun 2000, menjalani dua masa jabatan dan kemudian empat tahun sebagai perdana menteri, sebelum melanjutkan kembali kepresidenan pada tahun 2012 dan memenangkan pemilihan kembali pada 2018. Kebijakan domestik Putin, terutama di awal kepresidenannya yang pertama, ditujukan untuk menciptakan "kekuatan vertikal" yang ketat. Rusia di bawah kepresidenan Putin menegaskan bahwa ia tidak memiliki niat untuk membangun "edisi kedua" dari sistem politik barat, tetapi lebih pada sistem yang lebih dekat dengan tradisi dan keadaan Rusia sendiri (https://www.csis.org/programs/russia-and-eurasia-program archives/russian-domestic-politics-and-economics di akses 30 Juli 2018).

Pandangan Rusia tentang dunia modern, serta tujuannya tercermin dalam Konsep Kebijakan Luar Negeri yang diadopsi pada tahun 2016. Konsep tersebut mengevaluasi situasi global dan menganalisis proses yang terjadi di dunia dan wilayahnya. Rusia secara konsisten mengadvokasi agenda yang inklusif dan positif yang ditujukan untuk tidak membatasi melainkan memperkuat hubungan antar negara. Rusia siap untuk bergabung dengan semua pihak yang sama-sama mau bekerja sama sejalan dengan prinsip kesetaraan, saling menghormati, saling menguntungkan dan norma hukum internasional, serta pengakuan terhadap peran sentral PBB dalam urusan global. Dewan Keamanan PBB, G-20, BRICS, SCO dan CSTO dengan jelas menunjukkan efisiensi upaya bersama (https://russiaeu.ru/en/russian-foreign-policy di akses 30 Juli 2018).

Rusia telah mengalami perubahan ekonomi yang signifikan sejak runtuhnya Uni Soviet, bergerak dari ekonomi terpusat menuju sistem yang lebih berbasis pasar. Reformasi ekonomi pada 1990-an memprivatisasi sebagian besar industri, dengan pengecualian dalam sektor energi, transportasi, perbankan, dan pertahanan yang terkait. Perlindungan hak milik masih lemah, dan negara terus campur tangan dalam operasi bebas di sektor swasta. Komoditas ekspor unggulan Rusia antara lain produk minyak bumi dan minyak bumi, gas alam, logam, kayu dan produk kayu, bahan kimia, dan berbagai macam manufaktur sipil dan militer (https://www.indexmundi.com/russia/exports_c ommodities.html di upload 20 Januari 2018, di akses 23 Mei 2018).

Masyarakat Rusia pengguna internet sebanyak 108,772,470 jiwa atau 76.4% (2016) dari keseluruhan populasi Rusia. Namun kemajuan internet masyarakat Rusia tidak berbanding lurus dengan manfaat yang didapatkan dari kemudahan internet. Rusia terkenal sebagai negara dengan hacker paling banyak dan memasuki kategori 10 negara dengan jumlah *hacker* terbanyak di dunia**.** (https://techno.okezone.com/read/2017/07/24/2 07/1743067/ngeri-daftar-hacker-paling-

berbahaya-ada-di-negara-ini di upload tanggal 24 Juli 2017 diakses 1 November 2017).

4.1.1.3 Hubungan Estonia Dengan Rusia

Setelah kemerdekaan pada tahun 1991, negara Estonia yang baru berusaha untuk bergerak cepat untuk mengembangkan kemampuan militer dalam rangka mempertahankan kedaulatan nasionalnya yang direklamasi. Personel militer Rusia baru ditarik dari Estonia pada tahun 1994. Hubungan ekonomi Estonia dengan Rusia sederhana dan relatif mudah. Perdagangan bilateral dengan Rusia tetap stabil selama beberapa tahun sekitar 8% dari total ekonomi Estonia, dengan impor didominasi oleh bahan bakar mineral. Investasi langsung ke dalam dari Rusia adalah sekitar 2% dari total ekonomi Estonia, terkonsentrasi dalam tempat transit dan *real estate.*

Kementerian Pertahanan Estonia terus mengawasi aspek hubungan ekonomi yang mungkin berdampak pada energi atau keamanan *cyber*, faktor lain yang menjadi kerentanan Estonia. Estonia akan tetap bergantung pada Rusia untuk sebagian besar minyak dan gasnya selama dekade berikutnya, dan tidak diragukan lagi akan menimbulkan benturan berkala di jalur pada masalah transit dan perdagangan - tetapi hubungan ekonomi Rusia bukanlah hal utama dibanding hubungan Estonia dengan Uni Eropa yang lebih luas (https://www.globalsecurity.org/military/world/europe/et-forrel-ru.html diakses 23 Juli 2018).

Perjanjian kebijakan pemerintah koalisi pada April 2007 menyerukan "prakarsa konkrit dan praktis untuk mengembangkan hubungan antara Estonia dan Rusia".Akibatnya, Estonia terus fokus pada kerjasama lintas batas di bidang infrastruktur transportasi, penegakan hukum, kesehatan, pendidikan, dan budaya. Kesepakatan itu tidak menyebutkan upaya untuk menyelesaikan perjanjian perbatasan antara Estonia dan Rusia.

Dewasa ini, bagian dari komunitas Rusia di Estonia banyak yang masih terisolasi karena banyak etnis Rusia memiliki hubungan yang lebih kuat dengan tanah air bersejarah mereka daripada ke negara tempat tinggal permanen mereka. Melihat fakta bahwa lebih dari tiga ratus ribu orang yang berbahasa Rusia tinggal di Estonia, menyumbang sekitar seperempat dari seluruh penduduk Estonia, tidak mengherankan bahwa keengganan beberapa dari mereka untuk mengintegrasikan diri ke dalam masyarakat Estonia telah menyebabkan sejumlah masalah sosial-ekonomi dan politik.

Pada 11 Februari 2010, Menteri Luar Negeri Estonia Urmas Paet mempresentasikan kesimpulan kebijakan luar negeri Estonia kepada parlemen Estonia. Dalam pidatonya Paet menekankan hubungan positif dengan Rusia, khususnya pada tahun 2010 dalam rangka menandai 90 tahun hubungan diplomatik, dan bahwa Rusia adalah mitra dagang terbesar keempat di luar Uni Eropa. Paet mengatakan Rusia menggunakan hubungan ekonomi untuk tujuan politik, yang meningkatkan risiko dalam perdagangan (http://www.worldaffairsjournal.org/article/russians-estonia-twenty-years-after di upload Agustus 2014, di akses 30 Juli 2018).

4.1.1.4 Cyber Sabotage Rusia Terhadap Estonia

Tingkatan komitmen politik dari beberapa kejadian yang telah terjadi di Rusia dan Estonia dilakukan atas penggunaan *soft instrument* dari kekuatan Rusia yang bersifat *coercive* atau memaksa. Sebuah langkah dimana pemerintah Rusia yang menggunakan senjata *non-attributable* yaitu senjata *cyber* sebagai usaha untuk memaksa, menghukum, maupun mengecoh negara lain. (https://www.ceps.eu/files/book/2009/09/1900.pdf. diakses tanggal 13 April 2018).

Serangan yang dilancarkan merupakan serangan DDoS *(Distributed Denial of Service)* yaitu dengan cara membanjiri situs – situs yang dituju dengan trafik data yang sangat masif berjumlah 4 juta data per detik, yang otomatis mematikan kinerja situs dan tidak dapat diakses. Estonia merupakan negara yang sistem *online* nya telah terdistribusi seluruhnya. Estonia adalah pionir dari *e-government* dan *internet voting*. Pada tanggal 9 dan 10 Mei 2007 serangan *cyber* yang mengenai situs

pemerintah dan swasta Estonia bertujuan untuk memutuskan komunikasi Estonia dengan dunia luar. Pada 14 Mei 2007 *Hansabank* dan *SEB Eesti Uhisbank* menjadi sasaran selanjutnya. Pada tanggal 16 Mei 2007 volume serangan mulai menurun, dan kemudian di tanggal 18 Mei 2007 serangan *cyber* berakhir setelah berlangsung 22 hari lamanya (https://amp.theguardian.com/technology/ 2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia di upload 2 Desember 2017, di akses 10 April 2018).

4.1.1.5 Kebijakan Pertahanan *Cyber* Estonia

Estonia telah secara konsisten mengangkat isu-isu *cyber* ke dunia internasional. Tidak hanya menjadi bagian integral dari urusan domestik, tetapi juga dalam hubungan internasional dan ekonomi, sebagai bagian dari gambaran yang lebih besar. Secara signifikan, *cybersecurity* didefinisikan sebagai salah satu bidang kegiatan NATO pada KTT Warsawa. Estonia menganggap *cybersecurity* sebagai aspek integral dari keamanan yang lebih luas yaitu untuk melindungi gaya hidup *digital*. Kebijakan pertahanan *cyber* Estonia tertuang dalam empat poin yaitu pembangunan domestik prosedur dan lembaga terdahulu yang telah didirikan untuk memastikan pembagian kerja yang efisien dalam kerjasama antar lembaga, juga menempatkan penekanan yang lebih besar pada perlindungan infrastruktur vital, tindakan melawan *cybercrime* dan peningkatan kompetensi keamanan informasi.

Yang kedua yaitu kerjasama internasional, tujuan dari kerja sama *cybersecurity* internasional adalah untuk memastikan perlindungan nasional tingkat tinggi terhadap ancaman *cyber*. Yang ketiga adalah kepemimpinan global, selama bertahun-tahun Estonia telah berada di garis depan *cybersecurity* internasional. *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) dan Uni Eropa untuk sistem TI berskala besar dan sejumlah perjanjian internasional telah disetujui di Tallinn. Poin keempat adalah hukum dan norma internasional, Estonia berperan aktif di organisasi internasional seperti PBB dan *Organization for Security and Co-operation* (OSCE) untuk menegaskan penerapan hukum internasional berlaku untuk dunia maya dan menganalisis hal-hal khusus dari penerapannya. Estonia juga berkontribusi terhadap pengembangan konsensus pada norma-norma yang diterima secara universal, dengan penekanan pada penerapan hak asasi manusia di dunia *cyber* (https://vm.ee/en/cyber-security di akses 17 Agustus 2018).

4.2 Analisa Hasil Penelitian dan Pembahasan

4.2.1 Kerugian Estonia Pasca Tindakan Sabotase *Cyber*

Pada tanggal 27 April 2007, Estonia memutuskan untuk memindahkan monumen patung *Bronze Soldier* tentara Soviet dari pusat ibu kota Tallinn. Pada hari itu juga masyarakat Estonia mengetahui bahwa mereka tidak dapat mengakses internet atau membaca *email* mereka. Selama hampir tiga minggu kehidupan internet negara telah terganggu. Seluruh administrasi negara lumpuh, bank-bank juga membekukan operasi mereka. Ini adalah insiden pertama yang menjadi sasaran serangan *cyber*. Baik NATO dan Uni Eropa melihat ini sebagai serangan terhadap salah satu negara anggota mereka, dan NATO bergegas menggencarkan spesialis IT untuk memecahkan dan menganalisis masalah. Tiga ratus ahli IT terbaik Estonia bekerja siang dan malam untuk mempelajari serangan yang belum pernah terjadi sebelumnya.

Meskipun serangan dunia maya tidak meninggalkan lubang-lubang bom di tanah, tetapi kerugian ekonomi itu nyata. Hanya dari satu institusi, *Estonia Hansabank*, melaporkan bahwa kehilangan setidaknya US$ 1 juta karena serangan itu. Serangan DDoS menutup komunikasi via email, menganggu transaksi bisnis dan aktivitas ekonomi.Pemerintah Rusia juga membekukan sementara hubungan

diplomatik dengan Estonia, akses pengiriman bahan baku kedua negara terputus dan mengakibatkan terhambatnya kegiatan ekonomi.

Pada tahun 2007, nominal US$ 1 juta merupakan jumlah yang sangat besar, juga kerugian pribadi dari masyarakat Estonia yang selama dua minggu tersebut terganggu aktivitasnya, terutama aktivitas ekonomi. Fasilitas *m-banking* untuk para pengusaha dan pelaku ekonomi tidak dapat diakses sama sekali. Juga kerusuhan yang terjadi selama dua malam, mengakibatkan satu orang tewas, 153 orang terluka, dan 800 orang diamankan petugas. Kerugian akibat kerusakan fasilitas kota Tallin dan juga penjarahan toko merupakan dampak dari kemarahan masyarakat Estonia akibat serangan *cyber* tersebut (https://abcnews.go.com/International/Technology/story?id=3184122&page=1 di upload 17 Mei 2008, di akses 23 Juli 2018).

4.2.2 Respon Estonia Terhadap Tindakan *Cyber Sabotage* Oleh Rusia

Menurut Jaan Priisalu, peneliti senior dari *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE), serangan tahun 2007 hanyalah sebuah tahap dalam serangkaian perkembangan yang telah dimulai sebelumnya. Para ahli *cyber security* disatukan dan mendiskusikan apa yang seharusnya dilakukan. Instruksi ditulis, garis komunikasi ditata, dan kurikulum *cyber security* disatukan di Universitas Teknologi Tallinn (TUT). Kemudian, pendidikan sistematis di bidang *cyber security* dimulai di Estonia. Kerja sama dengan negara lain sangat penting bagi Estonia. Karena Estonia sangat bergantung pada negara-negara lain secara ekonomi, salah satu cara untuk menyerang Estonia adalah dengan menyerang rantai jalur, atau negara-negara yang bergantung pada Estonia.

Respon Estonia pasca peristiwa serangan *cyber* 2007, selain mendirikan pelatihan – pelatihan keahlian *cyber*, memasukkan kurikulum keamanan *cyber* di sekolah dan universitas, pemerintah juga bekerjasama dengan NATO dan Uni Eropa dalam rangka membuat pertahanan lebih besar yang didukung oleh banyak negara. Estonia, dengan pengalaman terlatihnya dalam cara-cara perang *cyber*, telah memimpin dalam mengembangkan strategi pertahanan. Estonia telah mengembangkan rencana aksi nasionalnya sendiri melawan kejahatan dunia maya, dan sekarang NATO telah menunjuk Estonia untuk menjadi tuan rumah *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE), yang terletak di *Estonia's Training and Development Centre of the Defense Forces Communication and Information Systems* (SIVAK). Empat negara Eropa lainnya berkomitmen untuk bergabung: Jerman, Italia, Spanyol dan Latvia. AS juga mengambil bagian dan telah mengirim perwakilan ke Tallinn.

Beberapa lembaga pertahanan *cyber* didirikan pasca insiden di tahun 2007. Penyusunan strategi pertahanan *cyber* Estonia diwujudkan dengan pendirian lembaga – lembaga diantaranya *Estonia's Cyber Security Strategy* di didirikan pada Mei 2008, strategi pertahanan tersebut disusun oleh dewan multi agensi yang dipimpin oleh Menteri Pertahanan, Jaak Aaviksoo. Lalu NATO CCDCOE adalah pusat keahlian pertahanan dunia *cyber* multinasional dan interdisipliner. Organisasi militer internasional yang berpusat di Tallinn berfokus pada teknologi, strategi, operasi dan hukum. Dan yang ketiga *Cyber Defence League*, sebuah persatuan para spesialis teknologi informasi yang secara sukarela bergabung dengan militer Estonia dalam hal keamanan *cyber* (http://www.kaitseliit.ee/en/cyber-unit diakses pada tanggal 13 Maret 2018).

4.2.3 Hubungan Rusia - Estonia Pasca Dibuatnya Kebijakan Pertahanan *Cyber* Oleh Estonia

Selain menolak mengakui segala kesalahan, pemerintah Rusia semakin memperumit upaya untuk melacak para penjahat *cyber* dengan menolak bekerja sama dengan pihak berwenang Estonia untuk menyelidiki kasus tersebut. Karena sejumlah penyerang dalam yurisdiksi Federasi Rusia telah diidentifikasi, Jaksa Penuntut Negara Estonia membuat permintaan

bantuan investigasi resmi, yang ditolak Moskow, dengan menyatakan bahwa masalah prosedural tersebut mencegah kerjasama. Ketika pemerintah tuan rumah gagal bekerja sama dalam penyelidikan serangan *cyber*, seseorang dapat dengan mudah membayangkan bahwa pola *deniability* dan *stonewalling* ini akan mempersulit upaya masa depan untuk melacak dan mengadili para penjahat *cyber* di sejumlah negara.

Hubungan Estonia dan Rusia saat ini telah kembali tenang dan sejuk dalam hubungan antara Estonia dan Rusia. Hubungan Estonia dengan Rusia, serta seluruh hubungan Barat dengan Rusia, akan tiba hanya setelah Rusia meninggalkan pengaturan politik semi-otoriternya saat ini demi demokrasi yang layak dengan segala hal yang biasanya ada seperti persaingan politik, supremasi hukum, media yang belum bebas, dan interpretasi sejarah yang didasarkan pada fakta daripada kebijaksanaan politik atau hubungan sejarah di masa lalu (https://vm.ee/sites/default/files/content-editors/web-static/053/Kadri_Liik.pdf di akses 24 Juli 2018).

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan uraian dan pembahasan diatas, maka dapat ditarik beberapa kesimpulan atas pemaparan dari tiga rumusan masalah yang ada, diantaranya yaitu kerugian terutama di bidang ekonomi adalah nyata. Hanya dari satu institusi, *Estonia Hansabank*, melaporkan bahwa kehilangan setidaknya US$ 1 juta karena serangan itu. Serangan DDoS menutup komunikasi via email, menganggu transaksi bisnis dan aktivitas ekonomi. Masyarakat Estonia sangat bergantung kepada internet, maka itu serangan sabotase *cyber* yang terjadi sangat merugikan bagi masyarakat Estonia. Pemerintah Rusia juga membekukan sementara hubungan diplomatik dengan Estonia, yang mana memperparah kondisi ketika serangan sabotase *cyber* terjadi, akses pengiriman bahan baku kedua negara terputus dan mengakibatkan terhambatnya kegiatan ekonomi.

Respon Estonia pasca peristiwa serangan *cyber* 2007, selain mendirikan pelatihan – pelatihan keahlian *cyber*, memasukkan kurikulum keamanan *cyber* di sekolah dan universitas, pemerintah juga bekerjasama dengan NATO dan Uni Eropa dalam rangka membuat pertahanan lebih besar yang didukung oleh banyak negara. Estonia, dengan pengalaman terlatihnya dalam cara-cara perang *cyber*, telah memimpin dalam mengembangkan strategi pertahanan. Estonia telah mengembangkan rencana aksi nasionalnya sendiri melawan kejahatan dunia maya, dan sekarang NATO telah menunjuk Estonia untuk menjadi tuan rumah *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) dan pendirian lembaga – lembaga lainnya.

Selama tahun – tahun terakhir telah diasumsikan di Estonia bahwa jika penduduk lokal Rusia belajar bahasa Estonia, mereka akan secara otomatis memahami sejarah Estonia, kekhawatiran Estonia tentang Rusia, dan lain - lain. Hal ini tidak terbukti, pada saat yang sama, orang-orang Rusia setempat bukanlah konsumen yang buta dan tidak kritis dari propaganda resmi Kremlin saat ini. Mereka adalah penduduk yang kurang menyadari bahwa ada lebih banyak upaya harus dilakukan untuk menjelaskan kepada penduduk Republik Estonia, dan tindakan serta hubungannya dengan tetangganya yang sangat besar ke Timur.

Hubungan Estonia dan Rusia saat ini telah kembali tenang dan sejuk dalam hubungan antara Estonia dan Rusia. Hubungan Estonia dengan Rusia, serta seluruh hubungan Barat dengan Rusia, akan tiba hanya setelah Rusia meninggalkan pengaturan politik semi-otoriternya saat ini demi demokrasi yang layak dengan segala hal yang biasanya ada seperti persaingan politik, supremasi hukum, media yang belum bebas, dan interpretasi sejarah yang didasarkan pada fakta daripada kebijaksanaan politik atau hubungan sejarah di masa lalu.

5.2 Saran

Berdasarkan hasil penelitian yang dilakukan berikut beberapa saran mengenai kebijakan pertahanan *cyber* Estonia dalam merespon tindakan *cyber sabotage* oleh Rusia kepada Estonia yaitu dengan adanya perwujudan dari

tindakan antisipasi Estonia terhadap serangan *cyber* yang kemungkinan bisa terjadi lagi di masa depan berupa pendirian lembaga dan kebijakan di bidang *cyber* , hal tersebut merupakan aksi yang sangat bagus menunjukkan keseriusan dan kesiapan Estonia dalam mengelola ranah kedaulatan di dunia maya. Baiknya jika hubungan bilateral antara Estonia dan Rusia bisa diperbaiki menjadi semakin baik dan mengesampingkan konflik sejarah etnis dan menatap masa depan sebagai negara sahabat.

Power yang ditunjukkan kedua negara sama – sama menggambarkan tindakan pertahanan *offensive* dan *defensive* yang memang diperlukan dalam rangka untuk menjaga kedaulatan dan melindungi kepentingan masing – masing. Jika di masa depan tidak diperlukan lagi tindakan gangguan yang melewati ranah *cyber* dan ketika ingin menyampaikan aspirasi atau protes, perwakilan negara bisa menggunakan jalur diplomasi yang minim konflik. Dalam proses mendapatkan data untuk menyelesaikan penelitian ini, peneliti melakukan observasi ke Pusat Penelitian Politik LIPI di Jakarta Selatan, namun data yang peneliti cari tidak ditemukan dan juga tidak adanya peneliti LIPI yang mengeluarkan sebuah tulisan terkait dengan topik skripsi peneliti. Saran peneliti, sebelum menentukan informan dan lokasi penelitian dengan cara datang langsung ke tempat yang dituju, ada baiknya untuk seorang peneliti agar melakukan penelusuran lebih mendalam terkait informan maupun lokasi penelitian agar sasaran dan tujuan yang hendak dicapai dapat terlaksana tanpa membuang tenaga dan biaya.

DAFTAR PUSTAKA

A. BUKU

Jackson, Robert H. dan Sorensen Georg. 2013. *Pengantar Studi Hubungan Internasional*. Yogyakarta: Pustaka Pelajar.

Perwita, A.A Banyu, dan Yanyan Moch. Yani. 2005. *Pengantar Ilmu Hubungan Internasional*. Bandung : PT Remaja Rosdakarya.

Sitepu, P.Anthonius. 2011. *Studi Hubungan Internasional*. Yogyakarta: Graha Ilmu.

Wahid, Abdul. dan M. Labib. 2005. *Kejahatan Mayantara (Cybercrime)*. Bandung : Refika Aditama.

B. JURNAL DAN KARYA ILMIAH

Alghifari, Fadhil. 2016. *Analisis Teori Offense-Defense Terhadap Reformasi Kebijakan Pertahanan Jepang Dalam Dinamika Keamanan Di Asia Timur.* global.ir.fisip.ui.ac.id/index.php/global/article/download/45/193 diakses tanggal 1 Juni 2018.

Ardianti, Handrini. 2014. *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia.* https://jurnal.dpr.go.id/index.php/politica/article/view/336/270 diakses 12 Agustus 2018.

Medvedev, Sergei. A, 2015, *Offense-Defense Theory Analysis of Russian Cyber Capability.* Monterey, California: Naval Postgraduate School. https://www.ceps.eu/files/book/2009/09/1900.pdf diakses 13 April 2018.

Ministry of Economic Affairs and Communication. 2014. *Cyber Security Strategy*. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf diakses tanggal 1 Juni 2018.

National Security Concept Of Estonia. Melalui http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf di akses 21 Juli 2018.

Triwahyuni, Dewi, dan Tine Agustin Wulandari. "STRATEGI KEAMANAN *CYBER* AMERIKA SERIKAT." *Jurnal Ilmu Politik dan Komunikasi* 6.1 (2017). Melalui https://jipsi.fisip.unikom.ac.id/_s/data/jurnal/volume-06-no-1/8-dewi-triwahyuni-tine-edited.pdf/pdf/8-dewi-triwahyuni-tine-edited.pdf di akses 23 Agustus 2018.

C. RUJUKAN ELEKTRONIK

Barak Serdadu *Cyber* di Estonia. Melalui https://www.viva.co.id/indepth/sorot/265596-barak-serdadu-cyber-di-estonia di akses tanggal 22 Maret 2018.

Cyber Security. Melalui https://vm.ee/en/cyber-security di akses 17 Agustus 2018.

Cyber Sabotage. Melalui https://www.military.com/defensetech/2008/02/06/cyber-sabotage diakses tanggal 10 Desember 2017.

Daftar *Hacker* Paling Berbahaya Ada di Negara Ini!. Melalui https://techno.okezone.com /read/2017/07/24/207/ 1743067/ngeri-daftar-hacker-paling-berbahaya-ada-di-negara-ini diakses 1 November 2017.

Estonia Blamed Russia For Backing 2007 Cyberattacks, Says Leaked Cable https://www.computerworld.com/article/2511704/vertical-it/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.amp.html di akses tanggal 12 April 2018.

Estonia Country Profile. Melalui https://www.bbc.co.uk/news/world-europe-17220810 diakses pada tanggal 18 Juli 2018.

Estonia. Melalui https://www.globalsecurity.org/military/world/europe/et-forrel-ru.html diakses 23 Juli 2018.

Estonia: Ground Zero for World's First Cyber War?. Melalui https://abcnews.go.com/International/Technology/story?id=3184122&page=1 di akses 23 Juli 2018.

Estonian Defence League's Cyber Unit. Melalui http://www.kaitseliit.ee/en/cyber-unit diakses pada tanggal 13 Maret 2018.

Estonia *Economy – Export Commodities*. Melalui https://www.indexmundi.com/estonia/exports_commodities.html diakses tanggal 23 Juli 2018.

Estonia *Internet Users*. Melalui https://www.indexmundi.com/estonia/internet_users.html diakses tanggal 23 Juli 2018.

Estonia *Population*. Melalui https://www.indexmundi.com/estonia/population_growth_rate.html diakses tanggal 23 Juli 2018.

Estonia's Foreign Policy Objectives. Melalui https://vm.ee/en/estonias-foreign-policy-objectives di akses 30 Juli 2018.

Fake News and Botnets: How Russia Weaponised The Web. Melalui https://amp.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia di akses 10 April 2018.

Kadri Liik Director Of The International Centre For Defence Studies. The "Bronze Year" Of Estonia-Russia Relations. Melalui https://vm.ee/sites/default/files/content-editors/web static/053/Kadri_Liik.pdf di akses 24 Juli 2018.

Russia Area. Melalui https://www.indexmundi.com/russia/area.html di akses 23 Juli 2018.

Russia Export Commodities. Melalui https://www.indexmundi.com/russia/exports_commodities.html di akses 23 Juli 2018.

Russian Domestic Politics and Economics. Melalui https://www.csis.org/programs/russia-and-eurasia-program/archives/russian-domestic-politics-and-economics di akses 23 Juli 2018.

Russian Foreign Policy. Melalui https://russiaeu.ru/en/russian-foreign-policy di akses 30 Juli 2018.

The Russians of Estonia: Twenty Years After. Melalui http://www.worldaffairsjournal.org/article/russians-estonia-twenty-years-after di akses 30 Juli 2018.