BAB I

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. Beberapa dampak positifnya adalah kemudahan berkomunikasi, kemudahan mencari informasi, dan menghemat waktu serta tenaga dalam melakukan suatu pekerjaan. Dampak negatifnya adalah adanya tindakan penyalahgunaan teknologi, terutama dalam teknologi komunikasi. Era globalisasi dan teknologi informasi membawa pengaruh terhadap munculnya berbagai bentuk kejahatan yang sifatnya baru.

Aktivitas hubungan internasional pun tidak lepas dari keterkaitannya dengan penggunaan teknologi komunikasi dan informasi dalam penggunaannya sebagai alat untuk mencapai kepentingan negara. Pertemuan kepala negara bisa dilakukan melalui *teleconference*, menyampaikan informasi pemerintahan ke masyarakat melalui *website* dan media, kemudahan mengetahui dinamika dunia internasional melalui sosial media maupun siaran berita di televisi, dan lain – lain.

Jaringan tanpa batas dalam dunia teknologi informasi sudah banyak ditemukan beberapa tindakan yang melawan hukum. Umumnya kejahatan yang berhubungan dengan teknologi atau disebut *cybercrime*. Dalam kondisi globalisasi yang hubungan antar negara menjadi semakin tak terasa batasannya, hubungan antar negara sudah jauh lebih dekat dan mudah dari sebelumnya, tentu

saja selalu ada kemungkinan untuk suatu negara mengalami konflik dengan negara lain yang menjadi mitra atau negara sahabatnya. Salah satu contoh kejahatan melalui dunia maya adalah sabotase siber atau *cyber sabotage.*

Istilah *cyber* sering muncul di berbagai media dan banyak menjadi topik bahasan utama di kehidupan sehari – hari. Kata *cyber* di pendekkan dari *cyberspace* menjadi *cyber* (siber*)*. Namun pengertian *cyberspace* itu sendiri, menurut salah satu majalah terkemuka *The Economist* menyebut bahwa *cyberspace* merupakan ranah kelima dari kedaulatan suatu bangsa setelah darat, laut, udara, dan angkasa (http://porosnews.com/2017/10/05/cyber-espionage-spionase-siber-dan-dampaknya-di-era-siber/ di upload tanggal 5 Oktober 2017, diakses tanggal 19 Oktober 2017).

Sebagai ranah yang tergolong baru maka perlu juga dipahami apa sajakah unsur pembentuknya sehingga *cyberspace* menjadi penting bagi kedaulatan suatu bangsa. Pesatnya pertumbuhan dan perkembangan ICT *(Information and Communication Technology)* yang kemudian dipergunakan dalam kehidupan sehari-hari sehingga terbentuklah *cyber society* (masyarakat siber) yaitu pembentuk utama dari *cyberspace*. Karena saat ini masyarakat suatu negara selain berinteraksi secara fisik di dunia nyata mereka juga berinteraksi dalam dunia non fisik yaitu dalam dunia *cyber* atau dalam bahasa Indonesia disebut sebagai dunia maya.

Interaksi di dunia maya dewasa ini sudah menjadi aktivitas yang tidak asing lagi bagi masyarakat dunia, melalui sosial media ataupun interaksi melalui sambungan jarak jauh sudah menjadi sebuah rutinitas. Dunia ada dalam

genggaman tangan, informasi dari beribu kilometer jauhnya bisa di dapat dengan mudah. Akses informasi yang mudah pastinya merupakan sebuah hal yang positif apabila diperoleh dan dipergunakan dengan cara dan tujuan yang baik. Tetapi di tangan orang yang tidak bertanggungjawab, kemudahaan mengakses informasi bisa menjadi sebuah celah dalam melakukan tindakan negatif bahkan kriminal.

Kini interaksi yang dilakukan antar aktor hubungan internasional tidak hanya pada ruang darat, laut dan udara saja. Interaksi antar aktor juga memadati ruang maya *(cyberspace)* yang menjadi pilihan lain untuk mencapai kepentingan. Bertambahnya ruang interaksi ini sekaligus memperluas makna *power* dalam hubungan antar negara. Ukuran *power* dalam ruang darat, laut, udara lebih mudah untuk dicari standarisasinya, sebaliknya *cyberspace* mengaburkan standarisasi *power* tersebut. *Cyberspace* menjadi ruang sekaligus sarana baru dalam mencapai kepentingan yang kemudian dikenal dengan *cyberpower* (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 21 Agustus 2018).

Dalam hubungan antar negara, kegiatan *sabotage* (sabotase) walaupun dilakukan secara diam dan sembunyi – sembunyi tetaplah ada dan terus dilakukan. 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 menetap disana dalam suatu jangka tertentu yang keberadaannya cenderung mengancam adalah sabotase yang dilakukan pada ranah siber yaitu *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 dalam merespon tindakan tersebut. Konflik berawal di tahun 2007 yang dipicu oleh pemindahan patung *Bronze Soldier* oleh pemerintah Estonia dari pusat kota Tallin ke pedesaan. Pemerintah Estonia melihat patung tersebut sebagai simbol kebrutalan Uni Soviet ketika dulu menjajah Estonia. Setelah Uni Soviet runtuh, masyarakat Estonia menginginkan patung itu dihancurkan (https://www.viva.co.id/indepth/sorot/265596-barak-serdadu-cyber-di-estonia di upload tanggal 18 November 2011, di akses tanggal 22 Maret 2018).

Masyarakat Rusia menganggap pemindahan patung tersebut sebagai sebuah aksi diskriminasi terhadap mayoritas, masyarakat Rusia sangat membanggakan jasa para Tentara Merah pada Perang Dunia II yang telah mengusir Nazi di wilayah Eropa Timur, dan menganggap Estonia tidak menghargai jasa mereka. Sebelum pemindahan patung tersebut, pemerintah Rusia telah mengingatkan Estonia bahwa pemindahan patung akan berakibat 'malapetaka' bagi mereka (https://amp.dailydot.com/layer8/web-war-cyberattack-russia-estonia/ di upload 20 Mei 2016, di akses 30 Maret 2018).

Merespon tindakan tersebut, masyarakat Rusia protes besar – besaran dan turun ke jalan didepan Kedutaan Estonia yang berada di Moskow pada tanggal 26 dan 27 April 2007. Dalam kerusuhan yang terjadi selama dua malam, satu orang tewas, 153 orang terluka, dan 800 orang diamankan petugas. Pemrotes

meneriakkan “Rusia” dan mengibarkan bendera nasional mereka. Mereka melemparkan bom molotov dengan tujuan agar kerusuhan tersebut bisa menggambarkan protes mereka ke mata dunia internasional. Perisitiwa tersebut dikenal dengan nama *“Bronze Night”* **(**https://inet.detik.com/security/d-883503/hacker-pertama-gugur-di-perang-cyber-rusia-estonia di upload tanggal 24 Januari 2008, diakses tanggal 29 Maret 2018).

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).* Tak urung, serangan ini melumpuhkan sistem pemerintahan Estonia selama dua pekan lamanya **(**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. Estonia merupakan negara yang sistem *online* nya telah terdistribusi seluruhnya. Estonia adalah pionir dari *e-government* dan *internet voting*. Sistem komunikasi lebih banyak menggunakan *Skype* daripada telepon biasa. Sebanyak 98% transaksi bank di Estonia sudah menggunakan sistem *online*. 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 (https://amp.dailydot.com/layer8/web-war-cyberattack-russia-estonia/ di upload 20 Mei 2016, di akses 30 Maret 2018).

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.

Menteri Luar Negeri Estonia, Urmas Paet menuding Rusia terlibat secara langsung dalam serangan *cyber* tersebut. Namun, pemerintah Rusia membantah terlibat dalam serangan, Moskow menyatakan tidak bersalah, tetapi tetap bermusuhan dalam prakteknya. Pemerintah Estonia mengatakan bahwa serangan terhadap pemerintah dan sektor – sektor swasta negara dengan menggunakan *proxy* yang tidak dikenal cocok dengan pola modus operandi rezim Presiden Vladimir Putin dalam percobaan ‘senjata model baru’. Pernyataan tersebut telah dianalisa melalui kasus – kasus serangan *cyber* sebelumnya yang menimpa negara lain yaitu Georgia dan Ukraina.

Pola yang bermunculan dari kasus – kasus sebelumnya kemudian dianalisa oleh para pakar *cyber* dari Estonia melalui teknik yang digunakan Rusia untuk menghancurkan lawannya. Pertama, pemecahan kepercayaan di masyarakat yang dilakukan dengan menyebarkan ketakutan, kecurigaan dan kebencian. Menyebarnya berita tentang laporan di *Facebook* tentang penganiayaan di wilayah Ukraina, pesan yang dibesar - besarkan beredar di *Instagram* tentang aliran

perpindahan pengungsi yang melarikan diri dari Ukraina, iklan di *billboard* yang tiba – tiba muncul di Kiev dengan slogan pro-Rusia, kemudian diikuti dengan pecahnya demonstrasi. Meningkatnya kecurigaan dan saling tidak percaya telah memecah belah masyarakat Ukraina (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).

Kremlin juga telah menggunakan strategi yang sama terhadap rakyatnya sendiri. Di dalam negeri, buku sejarah, pelajaran sekolah, dan media dimanipulasi, sementara undang – undang disahkan dengan memblokir akses asing ke data *online* populasi Rusia dari perusahaan asing yang merupakan sumber daya penting dalam budaya berbagi informasi global saat ini.

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. Markov menolak untuk membuka identitas asistennya pada saat itu. Sejak itu, asistennya sendiri yang membuka identitasnya. Dia adalah Konstantin Goloskokov, seorang aktivis anggota kelompok pemuda pro-Kremlin, Nashi. Goloskokov mengklarifikasi klaim dari Markov, mengatakan bahwa serangan yang ia lakukan terhadap jaringan internet Estonia adalah benar. Namun aktivis muda Nashi tersebut percaya dia melakukan sesuatu yang tidak ilegal. "Pertama dan terpenting, saya ingin mengklarifikasi bahwa ini bukan serangan, itu bukan peperangan, ini adalah tindakan

pembangkangan sipil.” Goloskokov mendapatkan ide untuk melakukan serangan di kala puncak pertikaian diplomatik Rusia dan Estonia sedang terjadi.

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. Pengakuan Goloskokov telah mendorong spekulasi bahwa aksinya telah menjadi bagian dari strategi serangan *cyber* yang lebih luas yang diperintahkan oleh otoritas Rusia. Goloskokov menggunakan komputernya sendiri bersama tujuh orang temannya.

Sebuah petunjuk penting untuk mengungkap pelaku serangan sabotase tersebut adalah ditemukannya sebuah kabel, yang bereksploitasi dengan perusahaan keamanan *Arbor Networks* dan teridentifikasi tumpang tindih antara *botnet* yang menyerang Estonia dan *botnet* yang sebelumnya digunakan untuk menyerang politisi oposisi Rusia, Garry Kasparov (https://www.rferl.org/amp/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html di upload 30 Maret 2009, di akses 12 Maret 2018).

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).

Yevgeny Volk, direktur kantor *Heritage Foundation* yang berbasis di Washington, mengatakan bahwa meskipun Goloskokov tidak menerima dukungan keuangan dari pihak berwenang, mereka akan memberinya persetujuan diam-diam. Organisasi Nashi adalah bagian dari organisasi pembentukan pemerintah Rusia, dan dikontrol secara ketat oleh struktur pemerintahan. Suasana kebencian yang diciptakan oleh Nashi adalah tanah yang subur untuk tindakan serangan *cyber*. Dari analisa Volk disimpulkan bahwa tindakan semacam itu tidak dapat di organisir dan dilaksanakan oleh seseorang atas inisiatifnya sendiri dan kehendaknya sendiri.

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. Dimitri bekerjasama dengan kelompok Galoskokov tetapi melalui serangan yang dilancarkan dari dalam negara Estonia, hal tersebut dilakukan guna membuat pelacakan *hacker* menjadi lebih rumit **(**http://www.iar-gwu.org/node/65 di upload tanggal 12 Maret 2016 diakses pada tanggal 28 Oktober 2017).

Penangkapan Galushkevich yang didukung dengan bukti adanya forum – forum diskusi para anggota *hacker* sabotase ke Estonia dengan bahasa Rusia yang

membahas strategi serta pesan – pesan mengenai mengapa serangan sabotase *cyber* tersebut harus dilakukan (https://amp.dailydot.com/layer8/web-war-cyberattack-russia-estonia/ di upload 20 Mei 2016, di akses 15 April 2018).

Pada tanggal 2 Mei 2007, penyelidikan kriminal atas serangan sabotase *cyber* mulai dilakukan di bawah lembaga investigasi kriminal Estonia, *Estonian Penal Code (*divisi *criminalizing computer sabotage and interference with the working of a computer network)* dengan hukuman tindak pidana berat hukuman penjara hingga tiga tahun (www.mondaq.com/india/x/369712/ Terrorism+Homeland+Security+Defence/Cyber+Wa+r diakses tanggal 1 Juni 2018).

Pada tanggal 10 Mei 2007 Kantor Jaksa Penuntut Umum Estonia mengajukan permintaan resmi berupa bantuan investigasi dari Federasi Rusia Agung *Procurature* di bawah *Mutual Legal Assistance Treaty (MLAT)*. *Russian State Duma Delegation* kemudian datang ke Estonia pada bulan yang sama mengatakan bahwa Rusia akan membantu penyelidikan tersebut dengan setiap cara yang ada. Namun, Pada tanggal 28 Juni 2007, *Russian Supreme Procurature Refused Assistance* menolak bantuan dan mengklaim bahwa proses investigasi yang diusulkan tidak tercakup dalam MLAT yang berlaku (Herzog, 2011: 49).

Respon yang diberikan oleh pemerintah Rusia selama dan pasca tindakan sabotase *cyber* tersebut diantaranya pemerintah Rusia menerapkan sanksi terbatas terhadap Estonia selama periode tersebut dan menangguhkan beberapa kereta yang membawa penumpang dan bahan baku ke Tallin. Pemerintah Rusia juga

membekukan sementara hubungan diplomatik dengan Estonia, yang mana memperparah kondisi ketika serangan sabotase *cyber* terjadi, Kedutaan Estonia di Rusia dirusak oleh sekelompok anak muda Rusia dan mengenai satu orang staf kedutaan Estonia (Medvedev, 2015: 20-21).

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. di akses tanggal 13 April 2018).

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:

1. *Estonia's Cyber Security Strategy*

   Estonia's Cyber Security Strategy adalah sebuah tindakan antisipasi yang signifikan dalam menjaga keamanan *cyber*. Di didirikan pada Mei 2008, strategi pertahanan tersebut disusun oleh dewan multi agensi yang dipimpin oleh Menteri Pertahanan, Jaak Aaviksoo. Strategi keamanan *cyber* ini menjadi pedoman komprehensif bagi pembuatan kebijakan *cyber* negara. Strategi ini menyoroti perkembangan aktivitas

cyber terbaru yang penting, menilai skala ancaman terhadap keamanan *cyber* Estonia dan menyajikan langkah-langkah untuk mengelola dan mengantisipasi ancaman.

Pada tahun 2009, *Cyber Security Council* ditambahkan ke Komite Keamanan Pemerintah Estonia, yang tugas utamanya adalah untuk mendukung kerjasama antar lembaga tingkat strategis dan mengawasi pelaksanaan tujuan *Cyber Security Strategy*. Keamanan *cyber* nasional dipengaruhi oleh para aktor yang beroperasi di dunia maya dengan berbagai keterampilan, target, dan motivasi. Seringkali sulit dibedakan antara aktor dan menentukan hubungan aktor tersebut dengan organisasi nasional atau internasional.

Jumlah aktor negara di dunia maya yang terlibat dalam jaringan dunia maya yang ditargetkan pada komputer yang terhubung ke internet serta jaringan tertutup terus berkembang, dengan tujuan untuk mengumpulkan informasi baik mengenai keamanan nasional maupun kepentingan ekonomi. Jumlah dan keaktifan negara-negara yang mampu melakukan serangan *cyber* pun terus meningkat. Kementerian maupun lembaga yang berhubungan dengan strategi ini adalah Kementerian Urusan Ekonomi dan Komunikasi yang mengarahkan kebijakan keamanan *cyber* dan mengoordinasikan pelaksanaan strategi.

Strategi ini akan dilaksanakan dengan melibatkan semua kementerian dan lembaga pemerintah, terutama Departemen Pertahanan, Otoritas Sistem Informasi, Kementerian Kehakiman, Polisi dan Penjaga

Perbatasan, Kantor Pemerintah, Kementerian Luar Negeri, Kementerian Dalam Negeri dan Kementerian Pendidikan dan Penelitian. LSM, organisasi bisnis, pemerintah, dan lembaga pendidikan akan bekerja sama dalam pelaksanaan dan penilaian strategi yang telah dilaksanakan oleh pemerintah (https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf diakses tanggal 1 Juni 2018).

2. *The NATO Cooperative Cyber Defence Center of Excellence*

The NATO Cooperative Cyber Defence Center of Excellence adalah pusat keahlian pertahanan dunia *cyber* multinasional dan interdisipliner. Organisasi militer internasional yang berpusat di Tallinn berfokus pada teknologi, strategi, operasi dan hukum.

Estonia dan NATO membuat pusat keunggulan *cyber* baru untuk keamanan telekomunikasi yang termasuk dalam kerangka kerja NATO. Negosiasi kerjasama antara Estonia dan negara – negara anggota NATO diresmikan pada tahun 14 Mei 2008, dengan tujuan untuk meningkatkan kerjasama pertahanan *cyber* antara negara – negara anggota NATO. CCDCOE adalah pusat riset internasional yang bertujuan untuk meningkatkan kepedulian dan pengertian dari keamanan informasi secara praktis.

Visi CCDCOE adalah menjadi sumber utama keahlian di bidang pertahanan *cyber* yang kooperatif dengan mengumpulkan, menciptakan, dan menyebarluaskan pengetahuan dalam hal-hal terkait dalam NATO, negara dan mitra NATO. Estonia menjadi mampu untuk mengajak dunia internasional

untuk menyelesaikan permasalahan keamanan *cyber* sejak negaranya pernah mengalami tindakan penyerangan *cyber* (https://ccdcoe.org/ diakses tanggal 13 April 2018).

3. *Cyber Defence League*

Cyber Defence League adalah sebuah persatuan para spesialis teknologi informasi yang secara sukarela bergabung dengan militer Estonia dalam hal keamanan *cyber*. Didirikan pada tahun 2010, para sukarelawan CDL bekerja bersamaan dalam mempertahankan jaringan Estonia. Unit *Cyber* yang berspesialisasi dalam menjaga keamanan dalam infrastruktur kritis nasional, individu dengan keterampilan IT tinggi, termasuk kaum muda yang siap berkontribusi pada keamanan *cyber*, dan spesialis di bidang lain yang berkaitan

dengan keamanan *cyber* (pengacara, ekonom, dll) (http://www.kaitseliit.ee /en/cyber-unit diakses pada tanggal 13 Maret 2018).

Terdapat beberapa penelitian terdahulu yang membahas topik serupa yaitu skripsi yang berjudul Kejahatan Komputer Eksplorasi Kasus *Cyberwarfare* Estonia Tahun 2007 oleh Subektiningsih dari Universitas Islam Indonesia. Persamaan skripsi tersebut dengan milik peneliti adalah sama – sama membahas kronologis awal hingga puncak serangan sabotase *cyber*. Yang membedakannya dengan tulisan peneliti adalah skripsi tersebut hanya membahas kronologis konflik secara umum dan lebih cenderung kepada bidang dan teori ilmu komputer.

Penelitian selanjutnya dari Trisuharto Clinton dari Universitas Diponegoro tahun 2015 yang berjudul Kajian Perang Sibernetika (*Cyber-Warfare*) Sebagai Konflik Bersenjata Internasional Berdasarkan Hukum Humaniter Internasional. Persamaan skripsi tersebut dengan milik peneliti adalah sama – sama membahas tinjauan umum tentang konflik *cyber* beserta karakteristik didalamnya. Yang membedakan dengan tulisan peneliti adalah skripsi tersebut memfokuskan kepada pengaturan hukum humaniter terhadap *cyber warfare*.

Penelitian lainnya berjudul Tindak Pidana *Cyber Espionage* oleh Shelly Nicko dari Universitas Airlangga tahun 2010. Persamaan skripsi tersebut dengan milik peneliti adalah sama – sama membahas tinjauan umum tentang konflik *cyber* beserta karakteristik didalamnya, dan juga dampaknya ke bidang politik negara. Yang membedakan dengan penelitian peneliti adalah skripsi tersebut cenderung membahas kepada pengaturan hukum dan undang – undang tindakan *cyber espionage* serta tinjauannya menurut hukum.

Penelitian lainnya berjudul Kerjasama *Korea International Cooperation Agency (KOICA)* dan Pemerintahan Indonesia Dalam Pengembangan *Cyber Security* oleh Ina Sayang Tanjung dari Universitas Komputer Indonesia tahun 2017. Persamaan dengan penelitian peneliti adalah tujuan dari strategi pengembangan *cyber security* yaitu untuk mencetak sumber daya manusia yang peka terhadap *cyber security*, meningkatkan keamanan terhadap *malware* dan pengawasan pertukaran informasi antara negara dalam mencegah terjadinya *cyber threats.* Yang membedakan dengan penelitian peneliti adalah skripsi tersebut

membahas negara yang berbeda yaitu Korea dan Indonesia, serta bentuk hubungan antara kedua negara tersebut yaitu membentuk sebuah kerjasama.

Dengan latar belakang masalah yang telah terpaparkan diatas, peneliti tertarik untuk menyusun sebuah penelitian yang berjudul **"KEBIJAKAN PERTAHANAN *CYBER* ESTONIA DALAM MERESPON TINDAKAN *CYBER SABOTAGE* OLEH RUSIA KEPADA ESTONIA"**

Kajian hubungan internasional yang terkait dengan topik penelitian ini adalah:

1. Kajian tentang Hubungan Internasional di Eropa karena tindakan *cyber sabotage* terjadi di kawasan Eropa bagian Timur yaitu negara Rusia dan Estonia.
2. Kajian tentang *Cyber Law* dikarenakan tindakan *cyber sabotage* diatur dalam hukum dunia *cyber*.
3. Kajian tentang Diplomasi dan Negosiasi karena penelitian ini membahas hubungan bilateral antara dua negara Rusia dan Estonia, bagaimana konflik sabotase tersebut berada di antara dua negara dan saling mempengaruhi hubungannya.
4. Kajian tentang Dinamika Politik Internasional karena dalam penelitian ini terdapat analisa mengenai penggunaan *power* Rusia dan Estonia secara *offensive* maupun *defensive*.

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?

1.2.3 Pembatasan Masalah

Peneliti menentukan periode 2013 – 2017 dalam penelitian ini. Dikarenakan pasca tindakan serangan sabotase *cyber* yang terjadi pada tahun 2007, pembentukan strategi pertahanan *cyber* Estonia mulai dibentuk dan diimplementasikan pada tahun 2008 dan pembaruan tentang kebijakan pertahanan *cyber* Estonia terus mengalami perkembangan hingga tahun 2017.

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.