BAB I

P E N D A H U L U A N

1.1 Latar Belakang

Pada zaman modern seperti sekarang ini, perkembangan teknologi merupakan sebuah hal yang tidak dapat dihindari oleh siapapun. Perkembangan teknologi, seperti pada hal umumnya, memiliki dampak positif dan juga negatif. Seluruh dunia merasakan dampak perkembangan teknologi, tidak terkecuali dunia Hubungan Internasional. Aktivitas hubungan internasional tidak terlepas dari penggunaan teknologi komumikasi dan informasi untuk urusan-urusan Negara. Serta, perkembangan teknologi dapat dimanfaatkan oleh tiap Negara untuk kepentingannya masing-masing. Tidak sedikit tindakan-tindakan yang berlawanan dengan hukum yang telah dilakukan. Tindak kejahatan di ruang siber memiliki banyak bentuk, seperti *cyber terrorism, cyber sabotage, hack,* penyadapan, dan bentuk lainnya dan bahkan mungkin akan makin banyak bertambah. Tujuan utama kejahatan siber diantaranya adalah pencurian data, mematikan *website,* dan mengacaukan system informasi dan komunikasi korban. Data yang menjadi incaran kejahatan siber dapat menjadi data pribadi, data kelompok, dan bahkan arsip suatu Negara sekalipun. Salah satu bentuk tindak kejahatan di dunia siber adalah sabotase siber atau *cyber sabotage.* (Wall, 2007)

Salah satu tindakan sabotase siber yang memiliki skala cukup besar adalah konflik sabotase siber Rusia terhadap Estonia. Konflik ini dipicu oleh pemindahan patung "*Bronze Soldier*" yang terletak di pusat kota Tallinn, Estonia, ke pedesaan pada tahun 2007. "*Bronze Soldier*" sendiri merupakan sebuah patung atau tugu peringatan Perang Dunia 2 Uni Soviet, yang dibangun di pemakaman korban perang. Rusia, menganggap pemindahan "*Bronze Soldier*" yang dilakukan oleh Estonia sebagai tindakan diskriminasi terhadap mayoritas. Merespon Estonia, Masyarakat Rusia melakukan protes di Kedutaan Estonia pada tanggal 26 dan 27

April 2007. Peristiwa ini kemudian disebut sebagai "*Bronze Night"*. Kemudian pada tanggal 27 April 2007 penyerangan siber mulai dilakukan oleh Rusia, dengan cara *DDoS* atau *Distributed Denial of Service*. *Distributed Denial of Service* adalah sabotase siber yang membanjiri *website-website* yang dituju dengan *traffic* data yang sangat masif, kurang lebih sekitar 4 juta data per detik. Dengan adanya *traffic* data seperti ini, otomatis *website* yang dituju tidak dapat diakses yang berakibat mematikan kinerja *website* yang terkena serangan. *Website* yang terkena serangan adalah *website* Perdana Menteri Estonia, *website* parlemen Estonia, *website* partai politik, *website* bank, dan media. Intensitas serangan mulai menurun pada tanggal 16 Mei 2007 dan berhenti total pada tanggal 18 Mei 2007. (Firman, 2018)

Bronze Statue yang terletak di Tallinn, Estonia

Menteri Luar Negeri Estonia secara blak-blakan menuding bahwa Rusia merupakan dalang dibalik serangan siber yang melanda Estonia. Moskow, di sisi lain, membantah adanya keterkaitan dengan serangan siber Estonia. Pada Maret

2009 secara tidak terduga, Sergei Markov yang merupakan salah satu wakil Deputi Duma dari partai pro Kremlin, *Unified Russia* menyebut bahwa asistennya yang melancarkan serangan siber terhadap Estonia, pada sebuah diskusi tentang *warfare.* Penyerang tersebut adalah Konstantin Goloskokov.

Konstantin Goloskokov, seorang aktivis anggota kelompok pemuda pro Kremlin, Nashi. Goloskokov menyatakan bahwa dirinya dan kelompoknya meretas jaringan internet Estonia, secara efektif melumpuhkan berbagai bagian sistem selama tiga minggu pada bulan April dan Mei 2007. Sejumlah pengamat IT dari Estonia berpendapat bahwa setidaknya Goloskokov mendapat dukungan secara diam-diam dari Kremlin. Goloskokov yang menyatakan tentang insiden itu secara blak-blakan dan tanpa rasa takut menimbulkan asumsi bahwa penyerangan itu dilakukan oleh kekuatan yang lebih besar. Pengakuan Goloskokov terkait penyerangan terhadap Estonia terjadi selang 14 bulan salah satu seorang hacker penyerangan siber Estonia tertangkap, Dmitri Galuskevich, pada tanggal 24 Januari 2008. (Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, 2011)

Melihat kondisi tersebut, NATO *Cooperative Cyber Defense Centre of Excellence* (NATO CCD COE), yang merupakan sebuah organisasi internasional yang berbasis di Tallinn, Estonia, mengundang kelompok ahli internasional untuk mengindentifikasikan ketentuan beserta aturan internasional yang dapat diterapkan pada ruang siber, khususnya pada bidang *cyber warfare*, yang pada akhirnya diterbitkanlah Tallinn Manual on the International Law Applicable to Cyber Warfare pada tahun 2013, oleh Cambride University Press (Herzog, Journal of Strategic Security, 2011). Tallinn Manual merupakan murni pendapat dari kelompok ahli, tidak bersifat mengikat dan bukan merupakan pernyataan/doktrin dari NATO, negara donatur maupun organisasi manapun.

Tallinn Manual lebih menekankan pada *cyber-to-cyber operations* seperti contohnya operasi siber terhadap infrastruktur kritikal suatu negara, atau serangan siber yang menargetkan kontrol sistem dari Negara yang menjadi target penyerangan. Tallinn Manual tidak ditujukan untuk masalah hukum terkait *kinetic-to-cyber operations*, seperti contohnya serangan udara yang menyerang dengan

cara pengeboman pada sebuah pusat kontrol siber, dikarenakan penyerangan yang dilakukan dengan cara tersebut telah diatur dalam ketentuan mengenai konflik bersenjata. Tallinn Manual pun tidak ditujukan untuk keamanan siber seperti yang pada umumnya dipahami. Spionase siber, pencurian Hak Kekayaan Intelektual, dan aktivitas kriminal dalam cyber space walaupun merupakan suatu ganguan serius bagi negara, namun tidak termasuk dalam lingkup pengaturan dalam Tallin Manual (Kessler, 2013). Menggunakan treaties, case law, dan sumber lainya, Tallinn Manual menghasilkan 95 *black-letters rules* yang dapat dijadikan pedoman negara-negara dalam kondisi *cyber warfare* atau perang siber, termasuk ketentuan operasi siber dalam neutral territory.

Logo *NATO Cooperative Cyber Defense Centre of Excellence*

Melanjutkan Tallinn Manual yang telah diterbitkan sebelumnya pada tahun 2013, *NATO Cooperative Cyber Defense Centre of Excellence* kembali mengundang kelompok ahli yang berhasil membuahkan Tallinn Manual 2.0 *on International Law Applicable to Cyber Operation* atau yang disebut sebagai Tallinn Manual 2.0 yang diterbitkan pada tahun 2017. Tallinn Manual yang diterbitkan pada tahun 2013 kemudian dikenal dengan Tallinn Manual 1.0

Apabila Tallinn Manual 1.0 lebih menekankan dan berfokus pada pembahasan operasi siber terkait *cyber warfare* atau perang siber, maka Tallinn Manual 2.0 membahas mengenai aktivitas siber pada masa damai dengan menekankan pada kejadian siber yang dihadapi negara yang berada di bawah level operasi siber. Dengan menggunakan *treaties* atau perjanjian, *case law* dan sumber lain, Tallinn Manual 2.0 mencetuskan 154 *black-letters rules*.

Dengan adanya Tallinn Manual sebagai pedoman di ruang siber, hal inilah yang akan menjadi perhatian bagi Russia untuk merumuskan kebijakan siber. Merujuk pada latar belakang masalah, penulis tertarik untuk menganalisa bagaimana perumusan kebijakan Russia dalam menghadapi ancaman siber global, bagaimana implikasi Tallinn Manual bagi Rusia dalam perumusan kebijakan siber.

Maka berdasarkan uraian tersebut peneliti mengangkat judul "**Perumusan Kebijakan Pertahanan Siber Rusia dalam Menghadapi Ancaman Siber Global Pasca Serangan Siber ke Estonia (Estonian Cyber Attack 2007) Melalui Rezim Tallinn Manual"**

1.2 Rumusan Masalah

Serangan siber Estonia tentu saja memrupakan sebuah kejutan bagi dunia Internasional, dimana Estonia diserang pada bidang siber. Hal ini menyebabkan Negara-negara di dunia lebih memperhatikan keamanan sibernya masing-masing. Terutama Rusia, yang disebut-sebut adalah dalang dari serangan siber Estonia.

Dari latar belakang yang telah dijelaskan sebelumnya, maka penulis menarik sebuah rumusan masalah yaitu "Bagaimana Perumusan Kebijakan Pertahanan Siber Rusia dalam Menghadapi Ancaman Siber Global Pasca Serangan Siber ke Estonia (Estonian Cyber Attack 2007) Melalui Rezim Tallinn Manual?"

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini antara lain :

a. Menjelaskan terkait serangan siber Estonia.
b. Menjelaskan pengaruh, dan dampak serangan siber Estonia terhadap Rusia.

c. Menganalisis kebijakan-kebijakan yang akan dirumuskan oleh Rusia pasca serangan Siber Estonia mengacu kepada Tallinn Manual.

1.4 Manfaat Penelitian

Adapun hasil penelitian ini diharapkan dapat menambah wawasan bagi disiplin Ilmu Hubungan Internasional terutama yang memiliki kaitan dengan Dunia Siber. Ada dua manfaat dari penelitian ini sebagai berikut :

a. Secara akademis, penelitian ini dapat bermanfaat untuk memberikan informasi dan data mengenai kebijakan siber yang dirumuskan oleh Rusia untuk menghadapi ancaman siber global.
b. Secara praktis, hasil penelitian ini dapat dimanfaatkan sebagai referensi dan masukan untuk berbagai karya ilmiah yang berkaitan dengan apapun yang menyinggung perumusan kebijakan Rusia pasca serangan siber Estonia dan juga Tallinn Manual.

1.5 Sistematika Penelitian

Untuk memberikan fokus yang lebih jelas dalam penelitian ini, maka tulisan ini akan di bagi menjadi beberapa bagian yang terdiri dari bab dan sub bab. Dengan mengikuti sistematika penulisan, penelitian akan dibagi menjadi ( ) bab untuk memaparkan hasil yang didapat, yaitu:

BAB I PENDAHULUAN

Bab ini akan berisikan pendahuluan dari penulis, yang berisikan sub-bab yakni latar belakang, perumusan masalah, tujuan penelitian dan manfaat penelitian. Selain itu juga perumusam masalah yang akan menjadi inti besar penelitian penulis.

BAB II TINJAUAN LITERATUR

Dalam bab ini, terdapat 5 Sub-bab diantaranya adalah kajian terdahulu, kerangka penelitian, alur pemikiran,asumsi dan hipotesis.

BAB III METODE PENELITIAN

Dalam bab ini, Terdapat 3 Sub-bab seperti Metodelogi penelitian, Metode pengumpulan data, Metode Analisis.

BAB IV ANCAMAN SIBER GLOBAL PASCA SERANGAN SIBER ESTONIA

Bab ini akan menjelaskan ancaman-ancaman yang ada di dunia siber pasca serangan siber Estonia dan dampaknya bagi dunia siber.

BAB V PERUMUSAN KEBIJAKAN SIBER RUSIA MENGACU KEPADA TALLINN MANUAL

Bab ini menjelaskan tentang kebijakan siber yang dirumuskan oleh Russia yang mengacu pada Tallinn Manual setelah Serangan Siber Estonia.

BAB VI PENUTUP

Kesimpulan dan saran.