BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Dewasa ini masyarakat telah memasuki masa peralihan dari masyarakat industri ke masyarakat informasi. Masyarakat informasi memulai babak baru dengan adanya internet yang merupakan suatu inovasi yang menyebabkan manusia lebih mudah untuk berinteraksi baik itu komunikasi atau informasi. Pada perkembanganya teknologi komunikasi dan informasi semakin marak tertutama perkembangan dunia siber selaras dengan perkembangann zaman penggunaan internet dalam kehidupan bermasyarakat tidak dapat dibendung dengan akses yang lebih cepat, daya jangkau luas, dan menggunakan biaya terjangkau. Hal itulah yang menciptakan ruang baru untuk saling berinteraksi yang disebut *cyber space* (ruang siber) (Aji & Indrawan, 2019, pp. 4-5).

Interaksi yang terjadi di *cyber space* (ruang siber) yang dilakukan suatu kelompok masyarakat, baik di lingkungan terkecil hingga antarnegara bahkan antarbenua sekalipun dapat terjadi berbagai hal dalam kehidupan bermasyarakat, tetapi harus tetap memperhatikan faktor keamanannya. Untuk itulah terciptanya *cybersecurity* (keamanan dunia maya). *Cybersecurity* merupakan proteksi perlindungan dunia maya dari sumber-sumber bahaya.

Internet yang berada di ruang siber tidak mengenal batas apalagi batasan hukum internasional. Seiring perkembangan ilmu hubungan internasional, ancaman tradisional pun menuju kepada ancaman non-tradisional.

Perbedaan dari ancaman tradisional dan non-tradisional adalah berdasarkan perbedaan dari asumsi dasarnya. Ancaman tradisional memiliki asumsi dasar pertama, fenomena politik dan hubungan internasional adalah tentang negara dan kepentingannya. Kedua, tidak ada kewenangan yang lebih tinggi dari kewenangan negara. Ketiga, kepentingan keamanan didefinisikan secara sepihak oleh negara. Keempat, kestabilan internasional tergantung pada distribusi kekuatan yang seimbang *(balance of power)*. Kelima, negara tidak bisa menggunakan kepentingan keamanannya pada negara lain dan *struggle for power* bersifat permanen. Keenam, hubungan antar negara bersifat *zero sum game* (Perwita & Yani, 2005, pp. 124-125).

Berdasarkan asumsi dasar tradisional yang sudah penulis paparkan bahwa pendekatan tradisional sangat bersifat negara-sentries dan tidak menghendaki terjadinya kerjasama antar negara dalam upaya menciptakan perdamaian mengingat hubungan internasional akan selalu bersifat konfliktual, sehingga masing-masing negara harus memperjuangkan kepentingan nasionalnya.

Sedangkan ancaman non-tradisional memiliki enam asumsi dasar diantaranya (Perwita & Yani, 2005, pp. 126-128), *Pertama*, keamanan seluruh entitas politik dibawah negara *(non-state actor). Kedua,* negara menghadapi tekanan dan

UNIVERSITAS SATYA NEGARA INDONESIA
YAYASAN ABDI KARYA

lingkungan domestik dan lingkungan internsional. *Ketiga,* negara menyerahkan keamanannya kepada entitas internasional. *Keempat,* keamanan bersifat multidimensional dan kompleks tidak hanya bersifat ancaman militer saja. *Kelima,* negara dan kedaulatannya tidak cukup menjelaskan kompleksitas masalah keamanan. Keenam, negara dapat menjadi sumber ancaman keamanan warga negara.

Berdasarkan asumsi dasar dari ancaman non-tradisional yang penulis paparkan bahwa pendekatan non-tradisional melihat ancaman dengan cakupan yang lebih luas dan memasukkan keamanan individu di dalamnya. Menurut pendekatan non-tradisional bahwa ancaman termasuk kepada keamanan ekonomi, lingkungan dan hak asasi manusia.

Serangan siber merupakan termasuk ke dalam ancaman non-tradisional pada abad ke-21 ini. Umumnya serangan siber ini pun mengalami sekuritisasi yaitu isu-isu non-militer bisa menjadi isu yang sangat terkait keamanan, maka dengan demikian dapat dikategorikan dengan status "keamanan nasional" (Indrawan, 2016, pp. 68-70).

Serangan siber nasional tahun 2007 yang terjadi di Estonia dapat dikategorikan sebagai sekuritisasi karena mengancam keamanan negara Estonia dengan cara merusak situs dan infrastruktur sehingga mengganggu dan menghambat operasional negara.

Pada tanggal 27 April 2007 Estonia telah mendapat serangan siber yang berlangsung selama sekitar tiga minggu. Serangan yang paling terkenal adalah

penolakan serangan layanan yang mengakibatkan degradasi sementara atau hilangnya layanan pada banyak server komersial dan pemerintah. Sementara sebagian besar serangan menargetkan layanan non-kritis seperti web publik, email, yang lain berkonsentrasi pada pada target yang lebih vital, seperti perbankan *online* (Ottis, 2008).

Serangan ini belangsung antara 27 April hingga 18 Mei 2007. Entitas yang ditargetkan termasuk pemerintah, presiden, parlemen, polisi, bank, penyedia layanan internet, media *online*, serta banyak usaha kecil dan situs pemerintah daerah (Ottis, 2008). Dampak dari serangan siber nasional ini sangat mengancam sebuah negara karena dapat melumpuhkan operasional suatu negara. Serangan siber menjadi semakin umum dan berbahaya. Negara mana pun dengan infrastruktur jaringan yang cukup berkembang rentan terhadap serangan ini.

Siber merupakan kajian baru dalam dunia internsional, sehingga anonimitas relatif dari internet memungkinkan penyangkalan yang hampir sempurna, seperti halnya negara Estonia. Hal ini membuat hampir tidak mungkin untuk membawa para penyerang ke pengadilan, terutama ketika mempertimbangkan kurangnya dasar hukum untuk jenis serangan dan konflik baru ini.

Estonia merupakan negara dengan inovasi teknologi informasi dan komunikasi yang sangat pesat. Bahkan Estonia merupakan negara pertama yang menggunakna *e-government* yang merupakan voting internet pertama untuk

pemilihan lokal dimulai pada tahun 2005. Estonia juga merupakan negara yang memiliki *e-infrastructure* dimana lebih dari 355 lembaga pemerintah telah bergabung bersama di dunia maya. *X-Road* pun sudah ada di Estonia sejak tahun 2001 yang merupakan penggunaan pertukaran data oleh organisasi pemerintah di Estonia untuk saling berhubungan satu sama lain (https://meeting.afrinic.net) (Kim, 2009).

Estonia terkenal sebagai *e-Estonia* karena hampir semua infrastruktur dan operasionalnya menggunakan jaringan internet yang dikenal sebagai *e-infrastructure* dan *e-government*, disamping itu 80% penduduk Estonia yang berusia antara 16-74 tahun adalah pengguna aktif internet (http://www.studyinestonia.ee) (Survival Guide for International Students in Estonia, 2017). Serangan siber nasional pada tahun 2007 sangat merusak dan menghambat operasional negara. Estonia merupakan bagian dari anggota NATO.

Akibat dari serangan siber nasional tahun 2007 di Estonia, akhirnya Estonia memutuskan untuk bekerjasama dengan NATO sebagai upaya untuk memulihkan serta penguatan pertahanan dan keamanan siber Estonia pasca serangan siber nasional pada tahun 2007. NATO beserta anggotanya membangun NATO CCD COE *(Cooperative Cyber Defence Centre of Excellence)* yang berpusat di Tallinn, Estonia. NATO CCD COE merupakan organisasi militer internasional yang berfokus pada interdisipliner penelitian terapan, dan pengembangan, serta konsultasi, pelatihan, dan latihan bidang keamanan maya. Sebagai pusat misi yang bertujuan meningkatkan

kemampuan, kerjasama, dan berbagai informasi antara NATO, sekutu, dan mitra di pertahanan siber.

Jantung NATO CCD COE adalah berbagai kelompok-kelompok ahli internasional dalam keamanan siber. Mereka adalah cendikiawan hukum, kebijakan, dan strategis ahli serta penelitian teknologi dengan latar belakang militer, pemerintah dan industri. NATO CCD COE ini dikelola dan dibiayai oleh negara-negara anggota seperti Austria, Belgia, Republik Ceko, Estonia, Finlandia, Prancis, Jerman, Yunani, Hungaria, Italia, Latvia, Lithuania, Belanda, Polandia, Portugal, Slovakia, Spanyol, Swedia, Turki, Inggris Raya, dan Amerika Serikat, Australia, Bulgaria, Denmark, Jepang, Norwegia, Romania, dan Kroasia (https://ccdcoe.org) (CCDCOE, 2008).

1.2 Pertanyaan Penelitian

Berdasarkan uraian diatas, maka dapat diperoleh pertanyaan penelitian yaitu "Bagaimana pengaruh kerjasama Estonia-NATO *Cooperative Cyber Defence of Centre Excellence* dalam mendukung pertahanan dan keamanan siber Estonia pasca serangan siber tahun 2007?"

1.3 Batasan Penelitian

Batasan penelitian sangat penting mengingat tingkat pemahaman yang lebih komprehensif terhadap suatu permasalahan dan analisis yang lebih terarah. Adapun batasan dalam penelitian ini yaitu bagaimana kerjasama yang dilakukan oleh Estonia dengan NATO CCD COE *(Cooperative Cyber Defence Centre of Excellence)* dalam upaya untuk mendukung dan meningkatkan pertahanan dan keamanan siber Estonia pasca serangan siber nasional pada tahun 2007.

1.4 Tujuan Penelitian

Tujuan penelitian dalam skripsi ini adalah untuk mengetahui bagaimana kerjasama yang dilakukan antara negara Estonia dengan NATO CCD COE *(Cooperative Cyber Defence Centre of Excellence)* dalam upaya untuk mendukung pertahanan dan keamanan siber Estonia pasca serangan siber nasional tahun 2007.

1.5 Signifikasi Penelitian

Penelitian dalam skripsi ini memiliki beberapa signifikasi. *Pertama,* memperkaya keilmuan hubungan internasional dalam kajian siber yang merupakan kajian yang masih terbilang baru dalam hubungan internasional. *Kedua,* meneliti

bagaimana kerjasama yang dilakukan oleh Estonia dengan NATO CCD CDOE *(Cooperative Cyber Defence Centre of Excellence).*

1.6 Manfaat Penelitian

1.6.1 Manfaat Teoritis

Manfaat teoritis dari penelitian ini yaitu memberikan kontribusi keilmuan bagi hubungan internasional tentang keamanan dan pertahanan siber di negara Estonia.

1.6.2 Manfaat Praktis

Manfaat praktis penelitian ini diharapkan dapat bermanfaat dengan memberikan gambaran bahwa diperlukannya negara-negara yang ikut serta meratifikasi *Tallinn Manual 2.0 on the Internet Law Applicable to Cyber Operations* yang merupakan satu-satunya hukum internasional siber untuk menanggulangi kejadian serangan siber nasional yang terjadi di Estonia pada tahun 2007.

1.7 Sistematika Penulisan

BAB I: Pendahuluan

Bab I berisi latar belakang permasalahan yang akan diteliti, pertanyaan penelitian, batasan penelitian, tujuan penelitian, serta manfaat penelitian, baik secara teoritis maupun praktis.

BAB II: Tinjauan Pustaka

Bab II berisi tinjauan referensi karya ilmiah yang memiliki tema serupa dengan yang penulis teliti, landasan teoritis yang berisi teori keamanan yang penulis ambil untuk menjelaskan permasalahan yang diteliti, landasan konseptual yang merupakan penjelasan dari konsep terorisme dan geostrategi, alur pemikiran yang menjelaskan keterkaitan teori, konsep dan permasalahan yang diteliti.

BAB III: Metode Penelitian

Bab III berisi metodologi deskriptif kualitatif untuk menjawab permasalahan penelitian, teknik pengumpulan data, instrumen penelitian, dan teknik keabsahan data.

BAB IV: Pembahasan

Bab IV berisi analisis dari data penelitian yang menjadi temuan penulis. Hasil ini disajikan susai dengan teori dan konsep yang digunakan. Bab ini akan menjelaskan bagaimana pengaruh dari kerjasama Estonia-NATO *Cooperative Cyber*

Defence Centre of Excellence. Pada bab ini, penulis juga akan menjelaskan gambaran umum serangan siber yang terjadi di Estonia pada tahun 2007.

BAB V: Penutup

Bab V ini berisi penutup yaitu berupa kesimpulan dari pembahasan penelitian beserta saran dari penulis.

UNIVERSITAS SATYA NEGARA INDONESIA
YAYASAN ABDI KARYA