BAB I

PENDAHULUAN

1.1 Latar Belakang

Penelitian ini berfokus pada fenomena siber Rusia yang dapat menjadi ancaman bagi keamanan Ukraina. Konflik antara Rusia dan Ukraina yang terjadi sejak tahun 2014 semakin meluas dan mulai masuk dalam ranah penggunaan siber. Pada tahun 2014, Rusia melakukan beberapa serangan siber terhadap Ukraina. Salah satu serangan siber yang dilakukan oleh Rusia adalah percobaan untuk memanipulasi hasil pemilihan Presiden Ukraina. Pada tahun 2015, Rusia kembali melakukan serangan siber terhadap Ukraina yang mengakibatkan padamnya listrik di Ukraina. Puncak serangan siber terjadi pada tahun 2022, sebelum Rusia melakukan invasi terhadap Ukraina. Rusia menyerang kantor berita *Kyiv Post* dan Satelit KA-SAT yang mengacaukan komunikasi di Ukraina (European Parliamentary Research Service 2022).

Seiring perkembangan zaman, maka dimensi keamanan juga berkembang. Jika pada awalnya keamanan sangat identik dengan militer, maka dimensi keamanan juga meliputi keamanan masyarakat, lingkungan, dan ekonomi. Dampak yang dihasilkan oleh penggunaan siber dapat memberi pengaruh terhadap hampir seluruh aspek. Beberapa dampak yang timbul akibat serangan siber adalah padamnya listrik, pencurian data intelijen, dan komunikasi yang terganggu akibat serangan siber.

Perkembangan teknologi terjadi dengan cepat dan kecanggihan dari teknologi itu sendiri juga semakin berkembang. Jika dahulu komunikasi jarak jauh sulit untuk dilakukan, maka sekarang komunikasi lintas negara dapat dengan mudah dilakukan. Beragam manfaat dapat dirasakan dengan perkembangan teknologi yang pesat. Teknologi juga memudahkan individu untuk menjalankan aktivitasnya sehari-hari. Istilah "Dunia dalam genggaman" menjadi istilah yang lazim digunakan untuk mendeskripsikan tingkat kecanggihan teknologi.

Dibalik segala manfaat positif yang dapat dirasakan, maka tentu akan ada hal-hal negatif yang timbul akibat dari perkembangan teknologi. Perkembangan teknologi mengakibatkan pergeseran arena perang antar negara. *Cyberspace* merupakan istilah yang merujuk pada ruang siber yang dijadikan sebagai arena peperangan dalam konteks perang siber (Karisma dan Burhanuddin 2023, 804). Penyerangan siber yang dilakukan oleh sebuah negara dapat dikatakan sebagai operasi siber. Ancaman yang timbul dari ruang siber dapat meliputi pencurian data pribadi, melakukan penhapusan data, kejahatan siber, dan lainnya (Center for Strategic & International Studies 2024).

Dalam upaya menangani ancaman siber yang timbul, beberapa negara telah membentuk satuan tugas yang secara khusus bergerak pada bidang ini. Amerika Serikat memiliki *United States cyber Command*, Australia memiliki *Cyber Security Operational Center*, dan Israel memiliki Unit 8200 yang dinaungi oleh *Israel Difense Force* (Babys 2021, 426). Melihat hal ini, terdapat indikasi bahwa ancaman siber merupakan ancaman yang tidak dapat dipandang sebelah mata. Operasi siber Israel terhadap fasilitas pengembangan nuklir Iran menjadi salah satu

bukti nyata. Israel meluncurkan operasi siber mereka terhadap fasilitas pengembangan nuklir Iran dengan cara merusak sistem jaringan listrik di daerah Natanz yang berakibatkan pada padamnya listrik pada daerah tersebut dan juga mengakibatkan terhentinya aktivitas di daerah tersebut selama beberapa waktu (Martin 2021).

Rusia telah melakukan operasi siber terhadap beberapa negara. Tujuan dilakukannya operasi siber ini adalah untuk mendapatkan data-data yang penting. Data-data tersebut akan digunakan oleh Rusia untuk mencapai kepentingan nasionalnya ataupun untuk menyusun strategi yang dapat membantu Rusia mencapai kepentingan nasionalnya. Salah satu contoh operasi siber yang dilakukan oleh Rusia adalah operasi siber yang ditujukan kepada Jerman. Pada tahun 2017, dilaporkan bahwa Jerman mengalami serangan siber yang besar (Limnell 2018, 69). Setelah mengupayakan pelacakan sumber serangan, maka serangan siber yang dialami oleh Jerman berasal dari Rusia.

Dalam serangan ini, Rusia berhasil masuk dalam sistem Kementerian Luar Negeri Jerman dan Kementerian Pertahanan Jerman dan diketahui juga bahwa Rusia juga menargetkan beberapa negara anggota Uni Eropa (Limnell 2018, 71). Tujuan dilakukannya operasi siber ini adalah untuk mengambil data yang sifatnya rahasia. Dengan berhasilnya Rusia dalam melakukan operasi siber terhadap Jerman, maka hal ini menjadi salah satu alasan untuk melakukan operasi siber terhadap negara lain.

Dalam konflik Rusia-Ukraina, Rusia melakukan operasi siber untuk mendapatkan keuntungan dalam konteks penyusunan strategi. Selain itu, Rusia

juga memanfaatkan operasi siber mereka untuk mengacaukan komunikasi di Ukraina. Sebelum Rusia melakukan invasi terhadap Ukraina, maka operasi siber telah lebih dulu dilakukan (Samad dan Persadha 2022, 140). Operasi siber yang dilakukan oleh Rusia ditargetkan pada jaringan komunikasi yang berakibatkan pada gangguan komunikasi dan masyarakat Ukraina yang sulit mengakses informasi. Perkembangan siber Rusia dimulai dengan kesadaran yang dimiliki oleh beberapa petinggi militer Rusia terkait informasi dapat dijadikan sebuah senjata (Jaitner 2015, 87). Selain itu, Rusia juga menyadari bahwa hubungan antara teknologi, operasi militer, strategi, dan hasil politik merupakan kombinasi yang sangat baik (Wirtz 2015, 30). Berdasarkan kedua pemikiran tersebut, maka Rusia mulai memasukan ruang siber kedalam strategi utama mereka.

Rusia juga menyadari bahwa penggunaan ruang siber merupakan salah satu operasi yang diintegrasikan pada upaya-upaya untuk menjaga situasi politik dan dominasi militer bagi negara mereka. Rusia menggunakan siber mereka untuk kepentingan mencuri informasi intelijen yang pada akhirnya akan membuat Rusia unggul dalam konteks penyusunan strategi (Weedon 2015, 67). Dengan kesadaran ini, maka Rusia mengembangkan siber mereka (seperti *malware* dan *virus*) untuk memaksimalkan operasi siber mereka. Operasi siber dapat dilakukan dengan senyap dan cepat. Bahkan jika sebuah negara memiliki siber yang sangat maju, maka serangan tersebut akan sulit untuk dilacak sehingga negara penyerang akan terhindar dari sanksi internasional, seperti sanksi ekonomi dan sanksi diplomatik.

Peristiwa invasi Rusia ke Ukraina sejak 2014 nyatanya dimulai dengan operasi Siber (Lin 2022, 31). Pada tahun 2014, Ukraina dijadikan sebagai lahan

operasi siber yang dilakukan oleh Rusia. Operasi siber yang dilakukan oleh Rusia pada saat itu adalah percobaan sabotase hasil pemilihan presiden Ukraina (European Parliamentary Research Service 2022, 3). Namun upaya tersebut gagal. Hal ini dikarenakan malware yang digunakan, terdeteksi oleh Ukraina dan berhasil diamankan. Sejak saat itu, operasi siber yang dilakukan oleh Rusia terhadap Ukraina semakin gencar dilakukan. Pada tahun 2015 operasi siber kembali dilakukan oleh Rusia, yang mengakibatkan sekitar 225.000 masyarakat Ukraina mengalami pemadaman listrik selama enam jam (European Parliamentary Research Service 2022, 3)

Secara umum siber memiliki beragam jenis. Mulai dari perangkat lunak hingga perangkat keras. Salah satu alasan mengapa negara-negara mulai mengembangkan siber mereka adalah karena semua negara dapat mengembangkan aspek siber (Blattman 2022). Hal ini yang menjadi salah satu daya tarik dalam penggunaan siber dan pengembangan kemampuan siber. Dalam konteks operasi siber yang dilakukan oleh Rusia terhadap Ukraina, maka dampaknya adalah padamnya listrik di beberapa daerah Ukraina (Balmforth 2023). Dari padamnya listrik, maka tentu masalah ini akan merambat ke bidang yang lain seperti gangguan telekomunikasi dan semua hal yang berkaitan dengan listrik akan terganggu.

Dampak yang dirasakan akibat penggunaan siber sangat luas. Dalam konteks konflik Rusia-Ukraina yang tejadi pada tahun 2022, maka dampak yang dirasakan Ukraina cukup beragam. Sebelum Rusia melakukan invasi militer, maka Rusia menjalankan operasi siber mereka. Dampaknya adalah terganggunya akses internet

di Ukraina. Rusia menyerang Viasat (perusahaan komunikasi), melalui serangan ini maka akses internet terganggu (Foreign, Commonwealth & Development Office 2022). Dengan demikian, pihak Militer Ukraina megalami kesulitan untuk melakukan koordinasi dan pihak Militer Rusia melancarkan invasi mereka dengan posisi yang unggul.

Berdasarkan penjelasan di atas, maka topik ini menjadi sebuah topik yang menarik untuk diteliti. Penggunaan siber Rusia menimbulkan dampak yang merugikan bagi Ukraina. Beberapa dampak seperti komunikasi yang terganggu, percobaan sabotase hasil pemilihan Presiden Ukraina, padamnya listrik, hingga memblokir akses terhadap situs Pemerintah Ukraina. Salah satu ancaman yang timbul dari dampak tersebut adalah masyarakat Ukraina sulit untuk mendapatkan informasi mengenai apa yang sedang terjadi. Hal ini menjadi bukti bahwa penggunaan kekuatan siber Rusia menimbulkan ancaman bagi Ukraina.

1.2 Rumusan Masalah

Penggunaan siber oleh Rusia terhadap Ukraina membuat keamanan Ukraina terancam dalam situasi konflik yang masih berlanjut. Ukraina dijadikan lahan operasi siber oleh Rusia. Dampak dari penggunaan siber sangat luas dan tidak kalah dengan dampak dari penggunaan senjata konvensional. Dimulai dari dampak yang dapat mengakibatkan padamnya listrik, percobaan untuk melakukan sabotase pada pemilu negara lain, hingga aksi spionase. Berdasarkan rumusan masalah tersebut, maka pertanyaan penelitian adalah: Bagaimana strategi Ukraina untuk menghadapi ancaman siber dari Rusia dalam konflik Rusia-Ukraina?

1.3 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang ada, maka tujuan penelitian yang ingin dicapai adalah:

1. Menjelaskan strategi Ukraina untuk menghadapi ancaman siber dari Rusia dalam konflik Rusia-Ukraina
2. Menjelaskan dampak strategi Ukraina terhadap keamanan siber Ukraina.

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian, maka diharapkan dalam penelitian ini memiliki manfaat akademis dan praktis sebagai berikut:

1.4.1 Manfaat akademis

Penelitian ini bermanfaat untuk mengembangkan khazanah hubungan internasional yang berkaitan dengan aspek keamanan negara. Khususnya mengenai ancaman senjata non konvensional yakni kekuatan siber yang terjadi pada kasus konflik Rusia-Ukraina. Dengan dilakukannya penelitian ini, maka diharapkan banyak akademisi yang meneliti isu ini agar kajian ancaman siber semakin beragam dan komprehensif untuk memperluas cakupan isu dalam Hubungan Internasional.

1.4.2 Manfaat Praktis

Penelitian ini bermanfaat sebagai rujukan bagi para peneliti selanjutnya yang akan meneliti mengenai operasi siber yang dilakukan oleh sebuah negara. Selain itu, penelitian ini bermanfaat bagi masyarakat untuk menambah wawasan mengenai dunia siber dan dimensi siber dalam konflik Rusia-Ukraina. Serta menjadi rujukan bagi Pemerintah Indonesia untuk dapat melindungi ruang siber Indonesia.

1.5 Sistematika Penulisan

Skripsi ini terdiri atas empat bab, dalam setiap bab terdapat sub-bab yang disesuaikan dengan bahsan penelitian terdiri atas:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah/pertanyaan penelitian, tujuan penelitian, manfaat penelitian dan sistematika penulisan yang menjelaskan tentang mengapa isu ini menarik untuk diteliti mulai dari penjelasan mengenai pengembangan siber. Pada bab ini juga terdapat rumusan masalah yang penulis angkat, dan terdapat tujuan dan manfaat penelitian yang penulis harapkan bisa tercapai.

BAB II KAJIAN PUSTAKA DAN METODE PENELITIAN

Bab ini berisi tinjauan pustaka, kerangka teoritik, kerangka pemikiran, dan hipotesis/argumen utama dan metode penelitian

yang menjelaskan tentang bagaimana isu penggunaan kekuatan siber Rusia terhadap Ukraina diteliti menggunakan teori dan bagaimana teori tersebut dioperasionalisasikan dalam mengkaji isu ini. Metode penelitian yang peneliti gunakan juga akan dijelaskan dalam bab ini.

BAB III ANCAMAN SIBER RUSIA DALAM KONFLIK RUSIA-UKRAINA

Bab ini mencakup gambaran umum mengenai konflik Rusia-Ukraina, perkembangan Siber Rusia, dan penggunaan kekuatan Siber Rusia terhadap Ukraina.

BAB IV STRATEGI UKRAINA UNTUK MENGHADAPI ANCAMAN SIBER DARI RUSIA DALAM KONFLIK RUSIA-UKRAINA

Bab ini mencakup gambaran umum mengenai kekuatan siber Ukraina, strategi Ukraina untuk menghadapi ancaman siber dari Rusia dalam konflik Rusia-Ukraina, kerjasama yang dilakukan oleh Ukraina dengan Amerika Serikat untuk meningkatkan kapasitas keamanan siber Ukraina, dan juga kebijakan Ukraina dalam upaya melakukan peningkatan kapasitas keamanan siber mereka.

BAB V PENUTUP

Bab ini berisi mengenai kesimpulan dari penelitian ini dan juga rekomendasi yang dihasilkan melalui penelitian ini.