BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan masyarakat, maka teknologi informasi juga turut berkembang. Hal ini disebabkan karena tingginya kebutuhan masyarakat untuk mencari informasi dari berbagai belahan dunia secara cepat. Dengan perkembangan teknologi informasi, semua aspek kehidupan masyarakat menjadi lebih terbuka terhadap dunia baru. Hal ini terkait dengan perkembangan internet, penggunaan *cloud* untuk penyimpanan, kecerdasan buatan, robot, dan teknologi lainnya untuk membantu manusia dalam melakukan aktivitasnya. Isu ini juga berkontribusi pada ranah politik internasional maupun nasional.

Pada ranah politik nasional, birokrasi menjadi salah satu aspek yang terdampak teknologi. Berkat teknologi, publik dapat turut berpartisipasi secara luas, sehingga mengubah proses pembuatan kebijakan dan pengambilan keputusan pemerintah baik secara positif maupun negatif. Pada ranah internasional, teknologi yang kian berkembang signifikan mampu memunculkan berbagai wujud konflik baru. Pada masa lalu, konflik yang terjadi di antara negara di dunia melibatkan banyak persenjataan seperti bom, senjata api, tank, dan sejenisnya. Sementara di era modern ini, konflik bisa muncul melalui media digital, seperti Tindakan kriminal berupa pencurian informasi yang dilakukan oleh negara lain (Schwab, 2016). Hal tersebut merupakan bukti akan adanya ancaman keamanan nasional yang berasal dari dunia siber. Sedangkan metode penyelesaian konflik atau masalah

yang terjadi seharusnya melibatkan kerjasama internasional mengingat dunia siber yang tidak terbatas oleh wilayah geografis.

Menurut Keohane dan Nye, seluruh negara pada dasarnya membutuhkan negara lain untuk menjaga keamanan nasional dan menjamin kelangsungannya. Ketergantungan inilah yang dikenal dengan istilah *complex interdependence* (Keohane & Nye, 2011). Kondisi *complex interdependence* ini sendiri memiliki tiga karakteristik utama, yaitu adanya berbagai jalur komunikasi bagi masyarakat, tidak ada hierarki atau sumber penyebab yang jelas atas asal suatu masalah, serta kekuatan militer yang tidak lagi menjadi preferensi utama negara dalam menyelesaikan konflik. Selain itu, era globalisasi yang mendorong persebaran informasi yang semakin cepat juga mendorong masyarakat dari berbagai belahan dunia untuk turut serta berpartisipasi dalam hubungan internasional sebagai aktor non-negara (Keohane & Nye, 2011). Hal inilah yang kemudian membuat banyak negara di dunia semakin memiliki sifat *complex interdependence* dalam upaya menanggulangi permasalahan global, seperti isu perubahan iklim, perdagangan internasional, hingga isu *cybercrime*.

Annika & Goel (2018) mengemukakan jika pesatnya digitalisasi telah membuat individu, bisnis, dan pemerintah amat bergantung pada dunia digital. Pada waktu yang sama, muncul ancaman dengan inovasi siber yang makin hari makin meluas, sehingga konsekuensinya adalah hilangnya informasi, kerugian finansial, sampai musnahnya nyawa dan harta benda. Para negara di belahan dunia telah mengakui bagaimana peluang *cybercrime* yang ditumpangi militer dan secara aktif dapat mengarah pada adu senjata siber. Hal ini akan menghilangkan

keuntungan sosial dan ekonomi dari ruang siber. *Cybercrime* sendiri memiliki berbagai bentuk seperti domain jahat, *ransom ware, malware, botnet*, *crypto hijacking*, dan kejahatan dunia maya lainnya yang terus berkembang seiring dengan kemajuan teknologi (Sianturi, 2021).

Frost and Sullivan bersama dengan Microsoft melaksanakan penelitian pada tahun 2018 mengenai *cybercrime*. *Cybercrime* menjadi kontributor pada defisit yang dialami Indonesia hingga mencapai angka Rp 478,8 triliun (Kompas.com, 2019). Defisit global akibat serangan siber bisa mencapai Rp 84.000 triliun atau mencapai US$ 6 triliun (Kurniawan, 2020). Defisit atau kerugian tersebut disebabkan oleh berbagai jenis serangan siber, baik berupa virus *ransomware*, ancaman *hacker* yang menargetkan institusi keuangan, hingga berbagai aksi kejahatan dalam bidang *cryptocurrency*.

Badan Sandi dan Siber Nasional (BSSN) selaku lembaga yang menaungi siber nasional Indonesia saat ini, telah memberikan laporan terkait serangan siber yang terjadi pada tahun 2020. Menurut laporan BSSN, sejak periode 1 Januari sampei 21 April negara ini telah mendapat serangan siber sebanyak 88.414.296. Adapun mayoritas serangan yang terjadi dalam bentuk trojan (56%), kemudian informasi yang dikumpulkan secara illegal mencapai 43%, dan sebanyak 1% lainnya dalam bentuk serangan yang terjadi di aplikasi web. Jumlah serangan makin banyak di akhir tahun 2020, hingga mencapai jumlah sebesar 423.244.053. Angka tersebut diproyeksikan akan terus mengalami peningkatan yang lebih besar lagi di tahun 2021 (Badan Siber dan Sandi Negara, 2020).

Berdasarkan data dari Kaspersky Security Network (KSN) bahwa UMKM dan bank di Indonesia haruslah berantisipasi karena akan menjadi sasaran peretas pada awal tahun 2020. Apalagi UMKM di Indonesia menempati posisi kedua di Asia Tenggara yang mendapatkan serangan siber paling massif (CNN Indonesia, 2020). Tak hanya itu, situs resmi pemerintah Indonesia pun tak luput dari serangan siber. Kemenkominfo menyebutkan jika nama domain internet.go.id yang selama ini menjadi situs web milik Pemerintah Indonesia, dibandingkan dengan domain lainnya telah menjadi sasaran para hacker dunia maya untuk diretas. Peretasan tersebut mencapai 90 persen dari seluruh server milik pemerintah. Keadaan ini begitu menyita perhatian karena peretas bisa saja mencuri data-data penting. Apalagi kebanyakan setiap instansi belum memiliki pengaman server akibat kurangnya sumber daya manusia khususnya di daerah (Tirto, 2017).

Menurut (Nityasari, 2020), mayoritas serangan siber yang dilatarbelakangi politik di Indonesia merupakan perusakan dan peretasan situs web resmi pemerintah. Indonesia juga amat mudah mendapat serangan siber non-politik lainnya seperti *cybercrime* berupa serangan malware, penipuan keuangan, rekayasa sosial yang memanfaatkan email, serta yang marak terjadi yaitu identitas media sosial yang dicuri orang lain. Adapun dari seluruh serangan siber yang terjadi, sebagian besar ditengarai oleh rendahnya kesadaran masyarakat. Fakta-fakta ini menjadi pengingat keras bahwa Indonesia sangat membutuhkan strategi dalam menghadapi *cybercrime* di skala nasional. *Global Cybersecurity Index* (GCI) menjadi usaha guna pemeringkatan komitmen dari 193 negara di dunia kaitanya dengan *cyber security*. Pemeringkatan ini dilandaskan atas lima aspek yang terdiri

dari hukum, teknis dan prosedur, struktur organisasi, peningkatan kapasitas, serta yang terakhir yaitu kerja sama internasional. Menurut penilaian yang dilakukan oleh GCI, Indonesia pada tahun 2020 berada di posisi 77 dari 193 negara (Global Cybersecurity Index, 2020).

Kerja sama internasional sejatinya merupakan hubungan yang dijalin oleh dua negara atau lebih guna mencapai kepentingan atau tujuan bersama (Al Azzam, 2019). Kerja sama internasional sendiri merupakan salah satu aspek penting yang perlu dilakukan guna menanggulangi isu *cybercrime*, sebab *cybercrime* merupakan permasalahan internasional yang dapat melibatkan beberapa negara. Salah satu contohnya adalah ketika seorang *hacker* dari suatu negara yang menyebarkan informasi rahasia milik negara lain, maka kedua negara perlu bekerjasama untuk mengidentifikasi dan menangkap *hacker* tersebut.

Dengan isu-isu tentang masalah terkait *cybercrime* di dunia, Indonesia dinilai terlambat dalam mengantisipasinya. Indonesia belum memiliki undang-undang yang komprehensif yang mengatur *cyber security* padahal *cyber security* menjadi hal penting untuk menanggulangi *cybercrime*. Selama ini *cyber security* hanya diatur dalam beberapa regulasi yang saat ini dimanfaatkan sebagai landasan pokok untuk isu terkait dunia maya seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan revisi selanjutnya UU ITE Nomor 19 Tahun 2016. Aturan ini meregulasi adanya pelanggaran terhadap perlindungan data, akses ke dalam sistem computer secara tidak sah guna memperoleh data, serta komputer atau sistem elektronik lainnya yang diambil alih atau diawasi secara ilegal. Dan regulasi ini tidak menyinggung aspek esensial *cyber*

security seperti infrastruktur informasi atau kebutuhan modal manusia (Center for Indonesian Policy Studies, 2021). Sehingga, guna mewujudkan pertahanan negara dari *cybercrime* melalui *cyber security* akan sulit dilakukan apabila hanya didasari oleh undang-undang tersebut.

Uraian fenomena di atas menunjukkan betapa lemahnya *cyber security* di Indonesia. Berbagai contoh kasus di atas juga memberikan gambaran bahwa dengan semakin berkembangnya digitalisasi, maka segala bentuk *cybercrime* menjadi permasalahan transnasional. Oleh karena itu, guna menanggulangi permasalahan *cybercrime*, suatu negara harus bekerja sama dengan negara lain. Salah satu strategi yang dapat ditempuh untuk merealisasikan kerja sama tersebut adalah diplomasi. Diplomasi pada dasarnya merupakan instrumen yang dapat digunakan dalam membangun hubungan dengan negara lain. Terdapat berbagai bidang diplomasi, mulai dari diplomasi budaya, diplomasi ekonomi, hingga diplomasi *cyber*. Oleh karena itu, diplomasi *cyber* menjadi solusi penting dalam usaha menganggulangi *cybercrime* sebagai kejahatan lintas negara. Diplomasi *cyber* dapat didefinisikan sebagai praktik kerja sama internasional yang dilakukan sebagai upaya membangun lingkungan siber internasional yang aman dan sehat (Hamonangan & Assegaff, 2020). Diplomasi *cyber* juga merupakan upaya pemerintah untuk melakukan diplomasi kaitannya dengan mempertahankan serta mengamankan segala kepentingan negara di dunia maya terutama untuk fenomena *cybercrime*. Umumnya, agenda yang menjadi fokus dari diplomasi *cyber* berkaitan dengan isu *cybercrime, cyber security, internet freedom, confidence building,* dan *internet governance* (Ar Rahman, 2020). Dengan demikian, penelitian ini akan

mengajukan topik penelitian tentang "**Kerja Sama Internasional Indonesia dalam Menangani *Cyber Crime***". Implikasi dampak kejahatan siber terhadap kondisi sosial masyarakat Indonesia dan keamanan nasional secara umum, menjadi latar belakang yang menarik mengenai topik ini untuk dibahas. Terutama perihal upaya pemerintah dalam menangani kasus kejahatan siber yang tidak terbatas pada wilayah negara tertentu.

1.2 Rumusan Masalah

Potensi kejahatan siber terhadap keamanan nasional Indonesia, serta pergeseran perilaku masyarakat di dalam kehidupan sehari-hari dan kedekatan dengan dunia siber, telah memberikan fenomena yang menarik untuk dikaji lebih jauh. Karenanya di dalam penelitian ini penulis merumuskan Yang menjadi pertanyaan penelitian dalam tulisan ini adalah:

1. Bagaimana *cybercrime* menjadi ancaman baru bagi keamanan nasional Indonesia?
2. Bagaimana upaya kerja sama yang dikembangkan oleh pemerintah Indonesia untuk menangani ancaman siber?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengetahui bentuk-bentuk kejahatan siber yang menjadi ancaman baru bagi stabilitas dan keamanan nasional dalam sudut pandang ilmu Hubungan Internasional. Sehingga pembahasan di dalam penelitian ini akan berkaitan erat terhadap kronologi *cybercrime* dapat terjadi,

pihak-pihak yang terlibat, serta dampak yang ditimbulkan dari hal tersebut yang pada akhirnya bermuara pada ancaman terhadap keamanan nasional.

Selain itu, untuk mengetahui cara-cara yang dilakukan oleh Pemerintah Indonesia di dalam menangani kejahatan siber. Khususnya cara-cara yang berkaitan erat dengan kerjasama internasional yang melibatkan aktor-aktor dari negara lain, maupun organisasi internasional. Hal tersebut akan berkaitan erat dengan pembahasan mengenai peran pemerintah serta tujuan nasional yang harus direalisasikan oleh Indonesia, khususnya berkaitan dengan keamanan nasional yang terancam oleh *cybercrime.*

1.4 Manfaat Penelitian

Diharapkan penelitian ini mampu berkontribusi bagi akademis maupun praktisi. Manfaat dari penelitian ini terbagi menjadi dua, yaitu manfaat secara teoritis dan manfaat secara praktis

Manfaat teoritis dari penelitian ini adalah memberikan kontribusi terhadap ilmu Hubungan Internasional, khususnya pada kajian terhadap keamanan dunia siber dan ancamannya terhadap keamanan nasional. Peneliti juga berharap bahwa hasil dari penelitian ini mampu memberikan sumber pengetahuan baru terkait cara-cara yang dilakukan oleh pemerintah Indonesia dalam menangani ancaman siber melalui cara-cara diplomasi dan kerjasama internasional.

Adapun Manfaat praktis dari penelitian ini adalah menjadi bahan rujukan bagi peneliti lain yang tertarik untuk melakukan kajian terkait isu keamanan siber dan kerjasama internasional di bidang siber. Serta mampu dijadikan sebagai bahan

rujukan bagi pemerintah yang memerlukan sudut pandang lain terkait ancaman siber dan keamanan nasional dari sudut pandang akademisi.

1.5 Sistematika Penulisan

Bab 1: Bagian bab ini berisi pendahuluan yang meliputi latar belakang penelitian, pemaparan masalah dan urgensi penelitian. Di dalam bab ini juga berisi mengenai rumusan masalah, manfaat penelitian, dan juga tujuan dari penelitian yang berfokus pada masalah ancaman keamanan siber dan kerjasama internasional.

Bab 2: Bagian bab ini merupakan bagian yang memuat kajian terhadap penelitian terdahulu yang serupa dengan judul dari penelitian ini. Tujuannya adalah untuk mengetahui gambaran umum terkait topik yang tengah diteliti, serta dapat pula dijadikan sebagai sumber data yang menguatkan dan melengkapi hasil penelitian yang tengah dilakukan oleh penulis.

Bab 3: Pada bagian bab ini berisi informasi yang lebih rigid perihal metode yang digunakan peneliti di dalam merumuskan penelitian ini. Khususnya akan berkaitan erat dengan metode pengumpulan data yang dipakai, jenis penelitian yang digunakan, sumber data yang akan dipakai, serta latar waktu dan tempat yang akan dipakai oleh penulis di dalam mencari data-data pendukung. Pada bagian bab 3 ini juga penulis akan menjabarkan perihal sistematika penulisan penelitian dari bab 1 sampai bab 5.

Bab 4: Pada bab ini penulis akan memaparkan hasil dari penelitian yang telah dilakukan oleh penulis. Pada bab ini pula penulis akan memberikan pemaparan data dalam bentuk narasi yang akan menjawab rumusan masalah pada

bab 1. Bagian awal dari bab 4 akan dimulai melalui pembahasan perihal bentuk-bentuk ancaman siber di Indonesia dan bagaimana hal tersebut menjadi ancaman baru bagi stabilitas nasional. Kemudian akan dilanjutkan dengan pemaparan cara-cara diplomatis yang dilakukan oleh Indonesia di dalam mengatasi ancaman siber di Indonesia dengan jalan kerjasama internasional.

Bab 5: Pada bagian ini merupakan penutup yang berisi ringkasan serta kesimpulan dari pembahasan-pembahasan masalah penelitian yang dilakukan oleh penulis di bab-bab sebelumnya.