BAB 1

PENDAHULUAN

1.1. Latar Belakang

Pada abad ke-21 ini, perkembangan teknologi semakin pesat, termasuk pula teknologi di bidang informasi dan komunikasi. Salah satu teknologi informasi dan komunikasi yang sangat dekat dengan manusia saat ini adalah internet/ruang siber (*cyberspace*) (Sutedja K., 2015). Menurut data yang dihimpun oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dalam survei terkait Penetrasi dan Perilaku Pengguna Internet di Indonesia tahun 2017 ((APJII), 2017), dari jumlah penduduk Indonesia yang mencapai 262 juta jiwa, sebanyak lebih dari 50% atau sekitar 143 juta jiwa telah menggunakan internet sepanjang tahun 2017, bukan hanya untuk berkomunikasi namun juga untuk transaksi jual beli, berbisnis dan berkarya. Dari fakta ini, fungsi internet telah meluas bukan hanya sebagai media bertukar informasi, juga untuk menunjang kebutuhan manusia yang lain. Kemudahan yang didapat dari internet tersebut menyebabkan banyak orang memanfaatkannya.

Namun perkembangan teknologi informasi komunikasi di era globalisasi ini, selain mendatangkan keuntungan dan manfaat yang besar, juga dapat menimbulkan ancaman yang besar pula. Hal ini pada sebagian orang memunculkan niat yang tidak baik, mengambil manfaat untuk mendapat keuntungan dan kepuasan pribadi. Niat tidak baik inilah yang tidak jarang menimbulkan kejahatan dalam dunia maya atau yang dikenal dengan istilah kejahatan siber (*cyber crime*).

Kasus kejahatan siber di Indonesia termasuk tinggi. Terbukti berdasarkan laporan Direktorat Reserse Kriminal Khusus Polda Metro Jaya pada tahun 2016, jumlah kasus kejahatan siber di Jakarta tertinggi dibanding jumlah kasus dari direktorat lainnya (direktorat industri perdagangan; direktorat fiskal, moneter, devisa; direktorat sumber daya lingkungan; direktorat korupsi). Dari 1.627 kasus yang terjadi, sebanyak 1.207 kasus adalah kasus kejahatan siber dengan jenis kejahatan yaitu pencemaran nama baik dan provokasi melalui media sosial (Amelia R, 2016). Kasus kejahatan siber yang ditangani Kepolisian Republik Indonesia (Polri) terus meningkat dari tahun ke tahun, yaitu 2.895 kasus (2017), 4.487 kasus (2018), dan hingga Maret 2019 telah ada 935 kasus (Nugroho & Sandy, 2019).

Salah satu ancaman siber yang menjadi tantangan bangsa Indonesia saat ini, seperti yang diungkapkan oleh Jenderal Polisi Drs. Budi Gunawan, SH, MSi, PhD, selaku Kepala Badan Intelijen Negara (BIN) Republik Indonesia, yaitu ancaman *cyber terrorism* (Gunawan, 2017). Arti *cyber terrorism* adalah menggunakan internet sebagai media untuk mendukung, dan melaksanakan aksi terorisme, mulai dari aksi propaganda (termasuk rekrutmen, radikalisasi dan hasutan terhadap terorisme); pembiayaan; latihan; perencanaan (termasuk melalui komunikasi rahasia dan informasi sumber terbuka); eksekusi; dan serangan siber (UNCTITF & UNODC, 2012).

Seiring dengan maraknya kasus kejahatan siber di Indonesia, maka keamanan data pada jaringan internet juga semakin diperhatikan. Hal ini dikarenakan serangan keamanan pada jaringan komputer maupun internet terjadi karena adanya kejahatan dunia maya. Hingga saat ini, terkait keamanan *online*, *Virtual Private Network*

(VPN) dan *The Onion Router* (TOR) adalah alat yang paling ampuh (Veale, 2019). Keduanya serupa tetapi memiliki fungsi yang berbeda. VPN dapat membuat sebuah jaringan bersifat *private* dan aman dengan menggunakan jaringan publik atau internet (Afrianto & Setiawan, 2011). VPN adalah sebuah koneksi virtual yang bersifat *private* karena pada dasarnya jaringan ini tidak ada secara fisik namun hanya berupa jaringan secara virtual, yang tidak semua orang bisa mengaksesnya. VPN menghubungkan pengguna dengan *remote server* dari negara yang dipilih, sehingga akan menyembunyikan alamat IP pengguna, membuat pengguna seperti mengakses internet dari lokasi *remote server*, daripada lokasi sebenarnya (Veale, 2019). VPN digunakan untuk melakukan transmisi paket data, yang terenkripsi sehingga tidak mudah disadap oleh pihak yang tidak berwenang.

Menurut data yang dihimpun oleh "vpnMentor" dalam Statistik Pemakaian VPN dan Privasi Data 2019 berdasarkan sumber "globalwebindex.net", Indonesia menempati posisi kedua, setelah Thailand, sebagai Negara dengan pengguna Internet terbanyak yang mengakses melalui VPN (Hochstadt, 2019). Berdasarkan riset yang dilakukan oleh *Global Web Index* tersebut, alasan terbesar warga Indonesia memakai VPN adalah untuk mengakses situs atau jaringan yang diblokir oleh pemerintah Indonesia (Nistanto, 2016). Dengan melihat fakta ini, tampak bahwa masyarakat Indonesia lebih melihat VPN sebagai alat untuk membantu mereka menembus blokir pemerintah dibanding untuk keamanan data mereka. Hal ini dikarenakan dengan menggunakan VPN, maka akan mengubah lokasi dan alamat IP pengguna pada Negara lain, sehingga alamat IP pengguna menjadi tersembunyi.

Namun VPN hanya memberikan privasi tetapi tidak membuat penggunanya menjadi anonim atau tidak terlacak. Penyedia VPN dapat mengetahui siapa diri pengguna dan dapat melihat aktivitas *online* pengguna. Oleh sebab itu, muncullah teknologi *anonimizer*, yaitu layanan untuk menyembunyikan identitas komputer agar menjadi lebih rahasia (*private)*, dengan membuat identitas menjadi *anonymous*. Salah satu contoh *anonimizer* adalah TOR (Mahardika & Sani, 2013). Dengan menggunakan TOR, maka identitas komputer pengguna akan sulit dilacak termasuk IP (*Internet Protocol*) *address* pengguna, ISP (*Internet Service Provider*) pengguna dan *browser* yang digunakan serta lokasi bahkan penyedia VPN sekalipun tidak dapat melihat IP asli pengguna. Mayoritas pengguna menggunakan TOR untuk mengakses "*deep web*" atau "*dark web*", yaitu situs-situs yang tidak bisa secara bebas diakses oleh karena berisikan hal-hal yang cenderung negatif dan melanggar hukum, seperti situs terlarang peredaran narkoba, jasa pembunuh bayaran, penjualan senjata ilegal, dan lain sebagainya.

Penggunaan VPN atau TOR masing-masing memiliki kelemahan, di mana penyedia layanan VPN masih dapat mengetahui identitas pengguna namun tidak bisa melihat data karena telah dienkripsi, sedangkan TOR tidak memberikan *end- to-end encryption* seperti pada VPN, sehingga masih rentan terhadap serangan dan kebocoran data. Oleh sebab itu, mengkombinasikan VPN dengan TOR akan menjadi solusi terampuh dalam keamanan siber (Veale, 2019). Namun, bisa dibayangkan bagaimana bila pelaku kejahatan siber menggunakan kombinasi ini dalam aksinya seperti untuk melakukan penyebaran *hoax*, transaksi narkoba, penelusuran cara pembuatan bom *high explosive*, bahkan ancaman teror pada

instansi publik, dan lain sebagainya, dengan tujuan agar mereka lebih aman dan tidak terlacak penyidik.

Usaha untuk mendeteksi pengguna VPN atau TOR mungkin saja dapat dilakukan dan pernah dilakukan oleh seseorang maupun pemerintah dalam suatu negara. Seperti misalnya mendeteksi VPN dengan memasang *packet sniffing software*, seperti *Wireshark* (Sari, 2014) atau *tcpdump* (Watson, 2017) pada *router*. Banyaknya masyarakat yang menggunakan VPN untuk membuka situs yang diblokir juga membuat banyak Negara memblokir penggunaan VPN. Namun, seiring berkembangnya teknologi, aplikasi VPN semakin beragam dengan tingkat keamanan yang semakin baik, sehingga proses penyaringan (*filtering*) yang dilakukan pemerintah menjadi tidak berguna. Sedangkan untuk mendeteksi pengguna TOR dapat dengan cara mengetahui relai *router*, analisis protokol, analisis lalu lintas, serangan *man-in-the-middle*, bahkan melalui kesalahan yang dibuat pengguna (seperti kustomisasi peramban TOR). Seperti yang pernah (setidaknya satu kali) dilakukan oleh *Federal Bureau of Investigation* (FBI) untuk mendeteksi pelaku pornografi anak yang menggunakan TOR dengan mengeksploitasi peramban TOR, sehingga dapat menangkap alamat IP pelaku, alamat MAC perangkat dan *hostname Windows* yang digunakan pelaku, namun usaha FBI ini kemudian terdeteksi oleh TOR dan membuat TOR memperbarui sistemnya sehingga setelah itu usaha FBI ini tidak dapat dilakukan lagi (Shavers & Bair, 2016). Metode-metode yang digunakan ini adalah untuk mendeteksi penggunaan VPN atau TOR tersendiri, namun bagaimana metode untuk mendeteksi pengguna VPN dan TOR yang bersamaan, yang memiliki tingkat keamanan yang

lebih tinggi dalam mencegah peretasan oleh pihak ketiga? Terlebih lagi karena VPN dan TOR sangat menjaga kerahasiaan kliennya sehingga selalu memperbarui dan mengembangkan sistem, sehingga usaha pendeteksian pengguna menjadi semakin sulit dan terhambat.

Sejalan dengan penggunaan internet yang semakin menjamur di masyarakat, begitupun penggunaan media sosial, di mana pada era masyarakat milenial ini, hampir seluruh orang di segala usia memiliki akun media sosial untuk berkomunikasi dan eksis di dunia maya. Fenomena ini pula yang menarik perhatian penulis bahwa tidak dipungkiri meningkatkan risiko penyalahgunaan media sosial untuk dijadikan media melakukan kejahatan siber seperti *phishing*, rekayasa sosial, ancaman, *cyber bullying*, kejahatan dan ujaran kebencian, eksploitasi anak, pelecehan seksual, dan penjualan serta distribusi perangkat lunak ilegal (Orebaugh, Kinser, & Allnutt, 2016). Selain itu, media sosial juga digunakan oleh kelompok teroris, komplotan kriminal dan penyelundup siber untuk berkomunikasi dengan jaringannya. Para kriminal siber juga menggunakan media sosial untuk mengirim dan menyebarkan *worm*, virus, *Trojan horse*, dan *malware* lainnya. Oleh sebab itu, metode *profiling* pelaku kejahatan siber melalui media sosial mulai menjadi bagian dari investigasi kriminal.

Di Indonesia terdapat beberapa lembaga yang berwenang dalam *cyber security* di Indonesia, salah satunya yaitu Badan Siber dan Sandi Negara (BSSN). (BSSN, 2019a). Oleh sebab itu, penulis bermaksud ingin meneliti mengenai prosedur yang dilakukan oleh BSSN dalam melakukan pelacakan pelaku kejahatan siber di Indonesia yang menggunakan VPN pada jaringan TOR dengan melakukan

ancaman teror melalui *Facebook, WhatsApp messenger,* dan *e-mail* mengingat semakin meningkatknya angka kejahatan siber di Indonesia dengan kemampuan pelaku yang semakin pintar teknologi dibarengi dengan aplikasi-aplikasi pendukung yang tentunya semakin beragam dan berkembang, upaya ini tentunya demi menjaga keutuhan, kedaulatan dan keamanan Negara Indonesia. Hasil kajian akan digunakan sebagai bahan analisis dan rujukan dalam penelitian selanjutnya yang terkait.

1.2. Rumusan Masalah

Rumusan masalah pada penelitian ini yaitu:

1. Bagaimana prosedur dan strategi dalam pelacakan pelaku kejahatan siber di Indonesia yang menggunakan VPN pada jaringan TOR dengan melakukan ancaman teror melalui *Facebook, WhatsApp messenger,* dan *e-mail* melalui desain implementasi *project profiling*?

1.3. Tujuan Penelitian

1.3.1. Tujuan Umum

Untuk menganalisis prosedur yang dilakukan oleh BSSN dalam hal pelacakan pelaku tindak kejahatan siber di Indonesia yang menggunakan VPN dan TOR untuk melakukan ancaman teror, serta bagaimana strategi yang dilakukan oleh BSSN dalam memantau dan mengendalikan pelaku tindak kejahatan siber di Indonesia yang menggunakan VPN dan TOR.

1.3.2. Tujuan Khusus

1. Untuk mengetahui apakah pelaku tindak kejahatan siber di Indonesia yang menggunakan VPN dan TOR untuk melakukan ancaman teror melalui *Facebook, WhatsApp messenger,* dan *e-mail* dapat dilacak.
2. Untuk mengimplementasikan *project profiling* pada institusi BSSN.

1.4. Manfaat Penelitian

1.4.1. Secara Akademis

Hasil penelitian ini diharapkan dapat menjadi referensi dan penunjang di masa yang akan datang bagi para peneliti di bidang komputer forensik, digital forensik, pertahanan dan bela Negara, teknologi informasi dan komunikasi maupun bidang lain terkait dalam upaya BSSN untuk melakukan pelacakan dan pemantauan kejahatan siber *high class* di Indonesia.

1.4.2. Secara Praktis

Diharapkan hasil penelitian ini dapat dijadikan sebagai bentuk kesiapsiagaan BSSN dalam menjaga kedaulatan Negara dan juga sebagai keunggulan Indonesia di kancah Internasional yang mendukung Revolusi Industri 4.0 dalam hal *cyber security*. Selain itu diharapkan pula dapat untuk penataan kembali kebijakan Negara tentang dunia siber guna menjaga kedaulatan Negara tanpa mengesampingkan hak dan privasi warga Negara Indonesia.