Hacker, Fear, and Harm: Data Breaches and National Security

Peretas, Ketakutan, dan Kerugian: Pelanggaran Data dan Keamanan Nasional

Denny Indra Sukmawan
Universitas Pembangunan Nasional "Veteran" Jakarta

David Putra Setyawan
Kementerian Pertahanan

ABSTRACT

This research explains data breaches as national security threat by using cyber security dilemma and cyber harm approaches. For long, Indonesia adopted comprehensive national security system that covers state defense, state security, public security and human security. Cyber security dilemma explains data breaches as threats to state defense and security dimensions, whereas cyber harm explains it as threats to public and human security dimensions. Having employed descriptive qualitative and quantitative methodology, we found that non-state actors have influence to escalate cyber security dilemma in long term. The state's response is by increasing defense and security sector's budget. The threats of data breaches to public and human security took place when government and corporations neglect the responsibilities to protect data and privacy of citizen and consument, as well as non-state actors conduct cyber attacks intentionally.

***Keywords**: cyber security, cyber space, cyber threats, cyber security dilemma, cyber harm, data breaches, bjorka, national security*

Penelitian ini menjelaskan pelanggaran data sebagai ancaman keamanan nasional dengan menggunakan pendekatan dilema keamanan siber dan bahaya siber. Indonesia mengadopsi sistem keamanan nasional yang komprehensif dan melingkupi dimensi pertahanan negara, keamanan negara, keamanan publik dan keamanan insani sejak lama. Dilema keamanan siber menjelaskan pelanggaran data sebagai ancaman ke dimensi pertahanan negara dan keamanan negara, sementara bahaya siber menjelaskan ancaman ke dimensi keamanan publik dan keamanan insani. Menggunakan metodologi penelitian ini deskriptif kualitatif dan kuantitatif, kami menemukan bahwa aktor-aktor non-negara mampu mengeskalasi kondisi dilema keamanan siber dalam waktu lama. Respons negara adalah dengan meningkatkan anggaran bagi instansi-instansi sektor pertahanan dan keamanan siber. Ancaman pelanggaran data terhadap keamanan publik dan keamanan insani justru terjadi ketika pemerintah dan perusahaan lalai atas tanggung jawab untuk melindungi data dan privasi warga negara dan pelanggan mereka, termasuk ketika aktor-aktor non-negara melakukan serangan siber dengan sengaja.

***Kata-kata kunci**: keamanan siber, ruang siber, ancaman siber, dilema keamanan siber, bahaya siber, pelanggaran data, bjorka, keamanan nasional*

Dalam dua dekade terakhir, isu keamanan siber (*cyber security*) makin mendapat perhatian para pengambil kebijakan. Isu tersebut bukan lagi persoalan *low politics* yang berkenaan dengan politik dalam kehidupan sehari-hari, namun juga mencakup persoalan *high politics* tentang keamanan nasional suatu negara, yang berkaitan dengan kelangsungan hidup negara (*state survival*) dan kepentingan strategis (*strategic interest*) negara tersebut (Choucri dan Clark 2019). Hal ini memunculkan konsekuensi bahwa pengertian keamanan siber begitu luas.

Sebagai suatu konsep, keamanan siber dapat dilihat sebagai kondisi terbebas dari ancaman-ancaman di ruang siber (*cyber space*), seperti kriminal siber (*cyber crime*), spionase siber (*cyber espionage*), aktivisme peretasan (*hacktivism*), terorisme siber (*cyber terrorism*) dan perang siber (*cyber war*) (Richards 2014, 5). Konsep ini juga dapat dilihat sebagai kemampuan negara untuk melindungi diri dan institusi-institusi di dalamnya dari ancaman-ancaman siber (*cyber threats*) (Choucri 2012).

Salah satu diskursus menarik dalam keamanan siber sebagai isu "*high politics*" berkaitan dengan potensi terjadinya perang siber di masa depan. Sejumlah pakar, seperti Rid (2012) menegaskan bahwa perang siber tidak akan terjadi karena selama ini, belum ada satu pun serangan siber (*cyber attacks*) yang bisa dipersepsikan sebagai pernyataan perang (*act of war*). Ambil contoh studi kasus Indonesia yang menurut Badan Siber dan Sandi Negara (BSSN) mengalami 495 juta serangan siber pada 2020 (Mashabi 2021). Hampir tidak mungkin negara menyatakan bahwa seluruh serangan tadi sebagai pernyataan perang. Selain itu, menurut Rid (2012), karakteristik serangan siber tidak memiliki kebaruan sama sekali. Tiga bentuk serangan siber, yaitu sabotase, spionase dan subversi (pemberontakan), sebenarnya telah berlangsung sejak lama. Pendapat lain disampaikan Stone (2013), bahwa suatu serangan siber bisa saja dianggap sebagai pernyataan perang. Semua tergantung pada makna yang terkandung di dalam, dan dampak yang muncul dari aspek "kekerasan" dalam suatu serangan siber. Dalam diskursus ini, penulis berada dalam posisi pro, di mana perang siber antar negara sangat mungkin terjadi. Salah satu faktornya adalah kondisi dilema keamanan siber (*cyber security dilemma*) yang dieskalasi oleh aktor non-

negara, meningkatnya dampak serangan siber ke negara, berikut pergeseran makna dan tafsir pemerintah mengenai sejauh mana serangan tersebut mengancam keamanan nasional.

Dalam konteks "*low politics*", salah satu diskursus keamanan siber membahas kegagalan hukum internasional dan hukum nasional di suatu negara dalam merespons serangan siber oleh aktor-aktor non-negara di sektor non-pertahanan dan keamanan seperti ekonomi, sosial (pendidikan dan kesehatan), hukum dan peraturan perundang-undangan (Brown et al. 2018; Youde 2016). Pada dasarnya kegagalan yang dimaksud berkaitan erat dengan tiga persoalan: Pertama, belum ada konsensus dalam hukum internasional mengenai konsep-konsep operasional dalam lingkup keamanan siber. Misalnya, soal definisi dan tipologi ancaman siber dan serangan siber. Sejauh ini penulis belum menemukan satu hukum internasional yang mengatur definisi dan tipologi yang komprehensif. Oleh karena itu, walaupun serangan siber benar-benar terjadi, sampai hari ini belum ada satu pun negara yang bisa menyatakan aktor non-negara yang melakukan serangan siber terbukti melanggar hukum internasional, terkecuali hukum nasional yang berlaku di negara atau kawasannya. Lebih jauh, upaya penegakan hukum pun sulit dilakukan karena berkaitan dengan persoalan selanjutnya. Seperti terjadi dalam banyak kasus pelanggaran data pelanggan (lihat Tabel 1 pada halaman selanjutnya).

Kedua, mengenai atribusi siber (*cyber attribution*). Secara sederhana, konsep atribusi merujuk pada proses politik untuk menentukan siapa aktor yang bertanggung jawab atas suatu serangan siber. Proses atribusi tentu melalui analisis teknis dan strategis. Bilamana pada tingkat teknis, analisis lebih ditujukan untuk mengumpulkan bukti-bukti digital forensik. Maka pada tingkat strategis, analisis berlangsung lebih kompleks lagi karena pertanyaan utama yang harus dijawab adalah "siapa yang harus disalahkan?", dan untuk menjawab pertanyaan ini, pelaku atribusi seringkali harus melakukan analisis geopolitik, sejarah, ekonomi, dan intelijen, untuk membuktikan apakah ada negara lain yang mendukung atau berada dibalik serangan tersebut. Lagi-lagi, hukum internasional dan hukum nasional belum mengatur mengenai standar soal atribusi, khusunya bagi serangan yang

diklaim oleh aktor non-negara. Terakhir, soal dilema hukum. Kondisi ini dapat diilustrasikan ketika aktor non-negara lebih memilih untuk melanggar hukum dengan melakukan serangan siber karena kerugian reputasi dan risiko politik yang dialami mereka terbilang rendah, dibandingkan keuntungan finansial dan reputasi yang diterima (Katagiri 2021). Persoalan terakhir ini bisa dilihat dalam kasus para peretas yang menyerang dan melakukan kejahatan pelanggaran data selama kurun waktu Agustus-September 2020.

Di Indonesia, isu keamanan siber yang paling mendapatkan atensi publik adalah pelanggaran data. Data yang dilanggar (bocor) lalu dijajakan di situs peretasan, seperti BreachedForums dan RaidForums, oleh para peretas (*hackers*) yang menggunakan akun dengan nama-nama seperti lolyta, bjorka, desorden, strovian dan sspX.

Tabel 1

Pelanggaran Data Periode Agustus-September 2022

Tanggal	Aktor yang Mengancam	Objek Pelanggaran Data	Aktor yang Terancam
18/08/22	Lolyta	Data Pelanggan	PT PLN (Persero), Pelanggan PLN
19/08/22	Bjorka	Data Pelanggan	Tokopedia, Pelanggan Tokopedia
20/08/22	Bjorka	Data Pelanggan	PT Telkom Indonesia Tbk, Pelanggan Telkom Indonesia
23/08/22	Desorden	Data Pelanggan, Data Ketenagakerjaan, Data Keuangan Perusahaan	PT Jasa Marga Tbk
26/08/22	WaterAndCoffee	Data Pegawai	Kemenkumham
31/08/22	Bjorka	Data SIM Card	Kementerian Komunikasi dan Informatika, Penyelenggara Pemilu

02/09/22	Desorden	Data Pelanggan, Data Ketenagakerjaan, Data Keuangan Perusahaan	Boga Group
06/09/22	Bjorka	Data Kependudukan	Komisi Pemilihan Umum
08/09/22	Desorden	Data Rekrutmen Pegawai	Honda Mugen Group, Pegawai & Calon Pegawai Honda Mugen
09/09/22	Bjorka	Surat Rahasia, Dokumen	Presiden, Kesekretariatan Presiden, Badan Intelijen Negara
09/09/22	Strovian	Data Pegawai	Badan Intelijen Negara
15/09/22	Desorden	Data Pegawai	PT Elnusa Tbk, Pegawai Elnusa
08-09/22	Bjorka	Informasi Pribadi	Menteri Komunikasi dan Informatika, Menteri BUMN, Menteri Koordinator Bidang Politik, Hukum dan Keamanan, Menteri Koordinator Bidang Kemaritiman dan Investasi, Ketua DPR, Gubernur DKI Jakarta, Ketua PSSI dll

Sumber: diolah peneliti dari berbagai sumber

Hasil penelusuran di situs BreachedForums memperlihatkan: (1) Pada 19 Agustus 2022, bjorka mengunggah 91 juta data pelanggan Tokopedia; (2) Pada 20 Agustus, terdapat 26 juta data pelanggan IndiHome yang diunggah. Termasuk di antaranya NIK, *email*, *handphone*, kata kunci pencarian, domain, platform dan URL; (3) Pada 31 Agustus, bjorka mengunggah lagi 1,3 miliar data registrasi kartu SIM dari Kementerian Komunikasi dan Informasi. Terdiri dari NIK, KK, nama lengkap, tempat dan tanggal lahir, kelamin,

usia, domisil dan TPS; (4) Pada 6 September 2022, bjorka juga mengunggah 105 juta data kependudukan dari Komisi Pemilihan Umum; (5) Pada 9 September 2022, data surat-surat rahasia Presiden Jokowi termasuk dari Badan Intelijen Negara selama 2019-2021 yang diunggah.

Aktivitas bjorka tidak saja terlacak di forum internet, namun juga media sosial Instagram dan Twitter. Khusus di Twitter, bjorka mengunggah informasi pribadi beberapa pejabat publik di Indonesia, seperti Menteri Komunikasi dan Informasi Johnny G Plate, Ketua DPR Puan Maharani, Menteri BUMN Erick Thohir, Gubernur DKI Jakarta Anies Baswedan, Ketua PSSI Mochammad Iriawan, Ketua Umum PKB Muhaimin Iskandar, Menteri Koordinator Bidang Politik, Hukum dan Keamanan Mahfud MD, serta aktivis media sosial seperti Denny Siregar dan Abu Janda (Bjorka 2022).

Pelanggaran data yang menarget Indonesia juga dilakukan oleh akun desorden, lolyta dan strovian. Hasil penelusuran di situs BreachedForums memperlihatkan aktivitas desorden dimulai pada akhir Juni 2022. Hampir dua bulan sejak pertama kali bergabung dengan akun tersebut, desorden telah membuat 27 utas dan 193 *post* dan seluruhnya mengenai Indonesia. Selain itu: (1) Pada 23 Agustus 2022, desorden mengunggah lebih dari 252 *gigabyte* data pelanggan, tenaga kerja, keuangan perusahaan Jasamarga -BUMN Indonesia yang bergerak di pengelolaan jalan toll; (2) Pada 2 September 2022, desorden mengunggah hampir 500 ribu data pelanggan, pekerja, keuangan perusahaan dan anak perusahaan Boga Group; (3) Pada 8 September 2022, desorden juga mengunggah 4 *gigabyte* data rekrutmen, izin mengemudi pelanggan, *resume* dan *curriculum vitae* pekerja Honda Indonesia; (4) Pada 15 September 2022, desorden mengunggah lagi 1,6 *gigabyte* data PT Elnusa, salah satu anak perusahaan Pertamina, BUMN Indonesia yang bergerak di sektor migas. Dalam kurun waktu yang berdekatan, akun lolyta mengklaim memiliki data pelanggan Perusahaan Listrik Negara (PLN), termasuk ID dan nama pelanggan, besar daya, kWh, alamat penggan, tipe dan nomor meteran, serta nama unit UPI. Terakhir, akun strovian mengklaim memiliki data-data agen BIN, baik nama, tempat tanggal lahir, pangkat dan jabatan.

Penelitian ini mengangkat rumusan masalah berupa pertanyaan mengapa pelanggaran data dapat mengancam keamanan nasional? Lantas, bagaimana konsep dilema keamanan siber dan bahaya/kerugian siber dapat menjelaskan ancaman pelanggaran data terhadap keempat dimensi dalam keamanan nasional? Mengingat desain penelitian adalah penelitian deskriptif, peneliti tidak menguji suatu teori atau konsep dan tidak menjelaskan suatu isu atau fenomena seperti yang lazim dilakukan dalam penelitian kuantitatif. Peneliti juga tidak menyelediki suatu isu atau fenomena secara mendalam, seperti yang lazim dilakukan dalam penelitian kualitatif. Peneliti hanya memaparkan data dan informasi yang relevan dengan tema penelitian dan rumusan masalah yang diajukan. Kegunaan teori atau konsep, berikut data dan informasi dalam penelitian ini sebatas untuk memperkuat argumen peneliti dalam menjawab rumusan masalah. Oleh karena itu, desain penelitian menggunakan studi literatur. Dalam studi literatur, peneliti melakukan *review* terhadap materi-materi berupa buku, jurnal, majalah, surat kabar, konten media daring, konten situs dan dokumenter atas kata kunci yang relevan dengan penelitian.

Pelanggaran Data dan Keamanan Nasional: Tinjauan Konseptual

Pelanggaran data (*data breaches*) mencakup segala aktivitas menyebarluaskan data dan/atau informasi yang bersifat rahasia, sensitif dan (patut) dilindungi, kepada pihak-pihak yang tidak berwenang. Dalam kondisi pelanggaran data, terdapat data dan/atau informasi yang dilihat, diakses dan disebarluaskan tanpa seizin pemilik data. Ditinjau dari subjek atau pelakunya, pelanggaran data tidak selalu terjadi karena serangan peretas, seperti dalam kasus bjorka. Ancaman ini juga bisa terjadi karena: (1) Ketidaksengajaan atau kelalaian pihak internal yang memiliki akses terhadap data (*insider*). Seperti dalam kasus Equifax, salah satu dari tiga perusahaan pelaporan kredit nasional di Amerika Serikat, pada September 2017. Di mana insiden kebocoran data (*data leaked*) terjadi karena satu pekerja di divisi teknologi perusahaan tidak mengindahkan peringatan untuk meng-*update* piranti lunak keamanan (Newman 2017); (2) Pihak internal

yang memiliki akses terhadap data (*insider*) memang memiliki intensi jahat untuk menyalahgunakan data. Pada 2013 misalnya, Edward Snowden mengungkap praktik pengawasan massal (*mass surveillance*) yang dilakukan oleh National Security Agency (NSA) di Amerika Serikat dan Government Communication Headquarters (GCHQ) di Inggris. Snowden yang bekerja di kontraktor Booz Allen Hamilton, mengungkap data-data rahasia milik NSA kepada wartawan The Guardian, salah satu media terkemuka di Inggris (Poitras 2014); (3) Kehilangan perangkat seperti laptop, *handphone*, atau *harddisk* eksternal yang di dalamnya terdapat informasi-informasi sensitif, baik karena kelalaian sendiri atau dicuri pihak lain. Salah satu kasus yang muncul di publik terjadi pada 2015, setelah salah satu pegawai NSA mengambil data rahasia dari jaringan dan *database* NSA, lalu menyimpan data tersebut di komputer pribadi miliknya (Lubold dan Harris 2017); dan (4) Tindak kriminal yang dilakukan peretas di luar organisasi, baik serangan siber secara kolektif maupun individual.

Khusus pada tipe keempat, peretas dapat melakukan serangan siber berupa: (1) *Phishing*, atau serangan yang didesain agar pengguna melakukan kesalahan yang menyebabkan pelanggaran data; (2) *Brute Force Attacks*, yaitu peretas menggunakan sejumlah piranti lunak untuk mencari dan menemukan *password* milik pengguna; dan (3) *Malware*, perangkat lunak untuk memasuki dan merusak sistem operasi, jaringan, dan server; (4) *DDoS*, yaitu serangan yang dilakukan untuk membuat sistem, server, atau sumber daya jaringan menjadi *down*/ tidak dapat diakses dengan cara membanjiri lalu lintas server dengan beban yang berat; (5) *MitM* (*Man in The Middle Attack*), yaitu peretas menyusup pada jaringan komunikasi data antara server dan korban sehingga penyerang memperoleh informasi rahasia seperti *username*/ *password* korban. (6) *Social Engineering*, yaitu peretas berusaha untuk memanipulasi korban sehingga memberikan data atau informasi yang bersifat rahasia. Kasus pelanggaran data yang terjadi di Indonesia selama periode Agustus-September 2022 sendiri bisa masuk dalam keempat tipe pelanggaran data tersebut, apalagi belum ada publikasi resmi dari pemerintah mengenai hasil investigasi kasus-kasus yang telah terjadi.

Selain menggunakan konsep pelanggaran data, peneliti juga

menggunakan konsep keamanan nasional dalam artikel ini. Konsep keamanan nasional pada dasarnya adalah konsep yang selalu diperdebatkan (Wolfers 2011; Ullman 2011; Baldwin 2011). Namun, para pemerhati studi keamanan memiliki konsensus bahwa ruang lingkup keamanan nasional makin "meluas" dan "mendalam" setelah Perang Dingin. Keamanan nasional dikatakan "mendalam" karena konstruksi suatu ancaman minimal dapat dibangun dari dua pertanyaan, siapa atau apa yang mengancam? dan siapa atau apa yang terancam? Sebagai konsekuensinya, isu-isu non-militer seperti pelanggaran data, serta objek referensi –objek yang terancam dan harus dilindungi/diamankan, yaitu masyarakat dan manusia bisa masuk dalam ruang lingkup keamanan nasional. Keamanan nasional juga dikatakan "meluas" karena secara empiris, ancaman-ancaman non-militer pun bisa mengancam keselamatan dan keberlangsungan hidup suatu negara.

Dalam artikel ini, penulis menggunakan konsep keamanan nasional yang dikembangkan oleh pakar-pakar dan institusi di Indonesia. Secara umum, keamanan nasional di Indonesia mengadopsi keamanan komprehensif. Prinsip komprehensif ini terlihat dalam penjelasan Juwono Sudarsono (2007) yang berpendapat bahwa keamanan nasional bertumpu pada empat fungsi pemerintahan negara, yaitu: (1) Pertahanan Negara, untuk menghadapi ancaman dari luar negeri, dalam rangka mempertahankan kedaulatan, keselamatan, kelangsungan hidup dan keutuhan Negara Kesatuan Republik Indonesia; (2) Keamanan Negara, untuk menghadapi ancaman dari dalam negeri; (3) Keamanan Publik, untuk memelihara dan memulihkan keamanan dan ketertiban masyarakat melalui penegakan hukum, perlindungan, dan pelayanan masyarakat; dan (4) Keamanan Insani, untuk menegakkan dan menjamin hak-hak warga negara seperti termaktub dalam UUD 1945.

Penjelasan tersebut diperkuat oleh Arry Bainus (2020) yang menjelaskan bahwa Bangsa Indonesia sejak lama menganut sistem keamanan nasional yang bersifat komprehensif, di dalamnya tidak hanya terkandung dimensi pertahanan negara, keamanan negara dan keamanan publik saja, melainkan sampai dengan keamanan insani. Buktinya bisa dilihat dari frasa yang terkandung dalam

Pembukaan UUD 1945, bahwa tujuan nasional bangsa Indonesia adalah

> "...melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial..."

Karakter keamanan nasional Indonesia yang seperti itu ditegaskan lagi oleh Dewan Ketahanan Nasional (Wantannas) dalam dua publikasinya. Menurut Sekretariat Jenderal Dewan Ketahanan Nasional (2010 & 2022), keamanan nasional Indonesia mencakup keamanan negara, keamanan publik dan keamanan warga wegara. Sekretariat Jenderal Dewan Ketahanan Nasional (2010, 52; 2022) menggunakan istilah keamanan warga negara dibandingkan keamanan individu atau keamanan insani dengan legitimasi bahwa keamanan insani yang termaktub dalam Pembukaan UUD NRI 1945 bersifat kolektif dan sosial, sesuai Sila Kelima Pancasila. Sifat tersebut mendorong pemenuhan hak-hak warga negara yang seimbang dengan kewajiban warga negara untuk berkontribusi menciptakan keamanan publik, keamanan negara dan pertahanan negara. Artinya, ada keseimbangan antara konsep keamanan yang menekankan negara (*state centered security*) dengan warga negara (*human centered security*). Menariknya, Sekretariat Jenderal Dewan Ketahanan Nasional (2022) memisahkan keamanan siber sebagai dimensi tersendiri. Berbeda dengan artikel ini yang menganggap keamanan siber sebagai sesuatu yang melekat dalam keempat dimensi keamanan nasional.

Dilema Keamanan Siber & Bahaya/Kerugian Siber: Tinjauan Konseptual

Sebelum membahas mengenai konsep dilema keamanan siber (*cyber security dilemma*). Penulis perlu menjelaskan terlebih dahulu mengenai konsep dilema keamanan (*security dilemma*), salah satu konsep esensial dalam hubungan internasional, khususnya keamanan tradisional. Kondisi dilema keamanan sendiri merupakan konsekuensi dari sistem internasional yang anarki. Seperti dijelaskan Herz (1950), untuk mewujudkan

keamanan dan meminimalisasi risiko yang berasal dari negara lain, suatu negara pasti berupaya meningkatkan *power*-nya. Oleh karena itu, negara lain pasti akan terancam dengan aktivitas negara tersebut. Peningkatan *power* oleh satu negara akan mengancam negara lain sehingga negara lain di sekitarnya pasti berupaya meningkatkan *power*-nya. Bahkan ditegaskan lagi oleh Herz (1950), bahwa negara yang berupaya menghindari peperangan dan memelihara kedamaian pun tidak lepas dari kondisi ini.

Pada prinsipnya konsep dilema keamanan siber pun tidak jauh berbeda dengan dilema keamanan. Namun, Buchanan (2016) lebih spesifik lagi menjelaskannya sebagai kondisi ketika suatu negara mewujudkan kondisi keamanan di ruang sibernya seringkali harus menerobos (melakukan intrusi) jaringan strategis dan vital dari suatu negara, baik disengaja maupun tidak disengaja. Padahal upaya penerobosan ini pasti mengancam keamanan siber negara lain. Dalam waktu lama, konflik siber akan tereskalasi (Buchanan 2016, 5).

Buchanan (2016, 48;72;92) lebih jauh menjelaskan dilema keamanan siber dalam tiga pernyataan, yaitu: (1) Setiap negara pasti memiliki keinginan untuk meningkatkan kapasitas dan kapabilitas operasi siber (*cyber operations*) mereka, baik defensif maupun ofensif. Salah satu wujud upaya ini adalah merekrut peretas; (2) Suatu negara yang memiliki kapasitas dan kapabilitas teknologi di atas rata-rata pun memiliki alasan defensif untuk menerobos (melakukan intrusi) jaringan milik negara lain. Bagi negara penerobos (*intruders*), upaya tersebut akan meningkatkan pertahanan jaringan mereka karena proses pengumpulan informasi-informasi intelijen yang bisa ditindaklanjuti, proses penggunaan data untuk memproyeksikan ancaman dengan lebih tepat dan akurat juga terjadi; (3) Suatu negara akan menafsirkan upaya penerobosan tersebut sebagai ancaman. Termasuk jika aspek atribusi dalam upaya penerobosan tersebut lemah dan ambigu, negara pasti akan berasumsi yang terburuk. Dalam artikel ini, penulis menambahkan bahwa upaya penerobosan yang mengeskalasi kondisi dilema keamanan siber tidak saja disebabkan oleh aktor negara, namun juga aktor non-negara. Dalam kasus pelanggaran data misalnya, negara pasti akan dituntut untuk meningkatkan kapasitas dan kapabilitas operasi siber mereka.

Salah satunya bisa dilihat dari peningkatan anggaran yang terkait keamanan siber.

Apabila konsep dilema keamanan siber berguna untuk menjelaskan bagaimana pelanggaran data mengancam keamanan nasional pada dimensi pertahanan dan keamanan negara. Maka konsep bahaya/kerugian siber (*cyber harm*) dapat menjelaskan bagaimana pelanggaran data dapat mengancam keamanan nasional, terutama pada dimensi keamanan publik dan keamanan insani.

Penulis terlebih dahulu menjelaskan soal konsep *harm*, yang secara umum bisa dimaknai sebagai konsekuensi buruk atau negatif yang berasal dari aktivitas atau aksi tertentu. *Oxford English Dictionary* misalnya, mendefinisikan *harm* sebagai kejahatan (fisik atau non-fisik) yang dialami dan diderita oleh seseorang, sekelompok orang. Istilah *harm* pun berkenaan dengan "rasa sakit, cedera, kerusakan, ketidakamanan, ketidaknyamanan" yang menyebabkan "kesedihan, kepedihan, kesakitan, kesulitan, penderitaan dan masalah-masalah lain". Menariknya, untuk mengalami kondisi *harm*, seseorang atau sesuatu belum tentu mengalami kekerasan.

Jika diterjemahkan dalam Bahasa Indonesia, penulis memahami *harm* sebagai aktivitas "menyakiti", "merugikan" atau "membahayakan"; aktivitas yang menyebabkan kondisi sakit, rugi dan bahaya. Selain itu, penulis memahami *harm* sebagai kondisi "sakit", "rugi", "bahaya" dan "menderita". Dalam Kamus Besar Bahasa Indonesia (KBBI 2022), kata "menyakiti" didefinisikan sebagai menyebabkan sakit (sedih atau sengsara). Adapun kata "merugikan" adalah mendatangkan sesuatu yang kurang baik (seperti kerusakan dan kesusahan) kepada pihak-pihak tertentu. Sementara "membahayakan" adalah mengancam keselamatan, atau mendatangkan bahaya kepada seseorang atau sesuatu.

Konsep *harm* berbeda dengan konsep *threat* atau "ancaman", konsep *impact* atau "dampak" dan konsep *risk* atau "risiko". Walaupun ketiga konsep ini sering muncul dalam pembahasan studi keamanan. Pada dasarnya, "ancaman" merujuk pada sesuatu, perbuatan dan kondisi yang mengancam. Kata "mengancam" di sini berarti membahayakan, merugikan, menyulitkan,

menyusahkan sampai dengan mencelakakan pihak tertentu. Sementara "dampak" adalah akibat dari aksi yang dilakukan satu pihak kepada pihak lain, yang bisa bersifat positif dan negatif. Sebagai perbandingan, Kamus Besar Bahasa Indonesia (KBBI 2022) mendefinisikan dampak sebagai "pengaruh yang mendatangkan akibat (baik negatif maupun positif)". Terakhir "risiko" adalah "kemungkinan dari suatu ancaman yang dikalikan dengan dampak. Di dalam Kamus Besar Bahasa Indonesia (2022), risiko didefinisikan sebagai "akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan".

Dari tinjauan etimologis ini, penulis melihat istilah ancaman dan bahaya/kerugian memiliki makna lebih luas daripada dampak dan risiko. Baik ancaman dan bahaya/kerugian bisa menjadi "sebab" apabila merujuk pada aktivitas dan kegiatan tertentu yang mengancam, membahayakan, menyakiti, merugikan. Keduanya juga bisa menjadi "akibat" apabila pihak tertentu berada dalam kondisi terancam, bahaya, sakit, dan rugi. Setelah melakukan studi literatur, penulis menganggap makna *harm* lebih mendalam dibandingkan ancaman.

Untuk memahami konsep *harm* sebagai aktivitas, penjelasan Linklater (2011, 41-61) bisa menjadi rujukan. Menurut Linklater, *harm* atau hal-hal yang termasuk upaya menyakiti, dan disakiti oleh pihak lain tergolong luas karena konsep ini merefleksikan ketakutan dan kecemasan satu kelompok atau perorangan. Makna *harm* setidaknya mencakup pengertian: (1) Aktivitas menyakiti dan membahayakan seseorang termasuk membunuh, melakukan kekerasan, memerkosa, menyiksa, memperbudak dan aktivitas-aktivitas semacamnya; (2) Mengingat setiap orang pasti rentan mengalami kesakitan dan penghinaan, maka aktivitas menyakiti dan membahayakan tidak bisa dimaknai dalam konteks fisik saja, namun juga psikologi, sosial, ekonomi bahkan reputasi; (3) Kondisi sakit, rugi dan bahaya yang dialami satu pihak bisa saja terjadi tanpa harus ada intensi untuk menyakiti, membahayakan dan merugikan pihak tersebut; (4) Kelalaian pun bisa masuk dalam kategori menyakiti, membahayakan dan merugikan karena dampak yang muncul terhadap pihak lain; (5) Eksploitasi adalah bentuk khusus dari menyakiti, membahayakan dan merugikan pihak lain, di mana satu pihak bisa memperoleh keuntungan

secara tidak adil dari kerentanan pihak lain; (6) Dengan terlibat saja, satu pihak bisa dikategorikan menyakiti, membahayakan dan merugikan pihak lain, mengingat pihak tersebut terasosiasi dengan institusi dan praktik-praktik yang dilakukan orang lain; (7) Dengan tidak melakukan apa-apa (netral), satu pihak pun bisa dikategorikan menyakiti, membahayakan dan merugikan pihak lain, apalagi ketika pihak lain yang dimaksud di sini mengalami kondisi sakit, bahaya, dan rugi; (8) Konsep bahaya/kerugian publik (*public harm*) mengacu pada dampak kepada institusi sosial-politik yang bertanggung jawab menciptakan dan membangun konsensus mengenai apa itu kondisi sakit, bahaya dan rugi. Dengan kata lain, bahaya/kerugian publik bisa dilihat sebagai dampak kepada institusi negara yang membuat, menjalankan dan melaksanakan regulasi; (9) Konsep bahaya/kerugian struktural (*structural harm*) muncul ketika satu pihak terdampak secara terstruktur dan sistemik atas kekuatan yang memaksa mereka untuk bersama. Konsep ini mengacu pada pandangan kelompok Marxis yang melihat eksploitasi oleh kelompok kapitalis/borjuis sebagai konsekuensi dari struktur sosial, dan bukan karena intensi individual.

Lebih jauh, Linklater (2011, 62-73) membagi tipologi *harm* berdasarkan alasan atau penyebabnya. Mulai dari: (1) yang disengaja sebagai konsekuensi dari perang dan konflik; (2) yang disengaja oleh negara, dengan mereduksi pemenuhan hak asasi manusia dan hak dasar warga negara; (3) yang disengaja oleh aktor non-negara, seperti dilakukan oleh kelompok teroris, pemberontak, peretas dll; (4) yang tidak disengaja dan berdampak pada lingkungan ekologis. Bisa dilakukan baik oleh pemerintah, perusahaan dan perorangan; (5) muncul karena kelalaian negara, perusahaan atau pihak-pihak lainnya yang tidak menjalankan kewajiban mereka untuk memitigasi, mengantisipasi dan menanggulangi risiko yang berpotensi atau dihadapi; (6) muncul karena eksploitasi oleh satu pihak yang lebih berkuasa kepada pihak lain yang lebih lemah; (7) muncul karena keterlibatan satu pihak dalam aktivitas menyakiti, membahayakan dan merugikan pihak lain. Tergantung pada sejauh mana kesadaran pihak pertama mengenai dampak yang muncul dan seberapa besar kekuasaan yang mereka punya untuk mempengaruhi dampak yang muncul tersebut; (8) khusus soal *harm* yang disebabkan

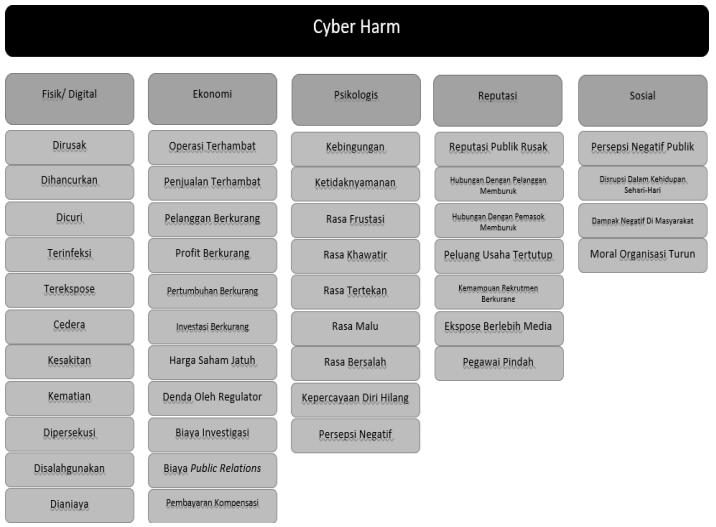
kelalaian, masih menyisakan pertanyaan mengenai kewajiban "negatif" untuk untuk menghindari (munculnya) aktivitas yang menyebabkan harm, dan kewajiban "positif" untuk membantu pihak yang terkena atau berada dalam kondisi *harm*.

Untuk memahami *harm* sebagai kondisi yang disebabkan pelanggaran data. Penulis mengadaptasi taksonomi bahaya/ kerugian siber (*cyber harm*) yang dikembangkan oleh Agrafiotis et al. (2018) di mana bahaya/kerugian siber dapat dijabarkan menjadi lima tipe, yaitu: Fisik/Digital, Ekonomi, Psikologi, Reputasi, dan Sosial. Setiap dimensi memiliki sub-tipe "sakit/bahaya/rugi" masing-masing. Bahaya secara fisik/digital menjelaskan dampak fisik atau digital yang dialami pihak tertentu. Dalam dimensi ekonomi ini berkaitan erat dengan konsekuensi-konsekuensi negatif yang dialami pihak tertentu, utamanya ditinjau dari sisi ekonomi dan finansial. Bahaya secara psikologis terfokus pada kondisi "sakit" pada dimensi psikis dan mental suatu pihak, biasanya paling umum dialami individu/perorangan. Kerugian reputasi berkaitan dengan perubahan persepsi dan pendapat publik atas pihak tertentu, biasanya ke arah negatif. Terakhir, bahaya dalam dimensi sosial berkaitan dengan dampaknya di kehidupan masyarakat sehari-hari.

Ditinjau dari metodologinya, penulis menganggap taksonomi yang ditawarkan Agrafiotis et al. (2018) terbilang komprehensif. Terutama karena alasan: (1) *database* yang digunakan mereka, mencakup lebih dari 5.000 insiden siber di seluruh dunia; (2) pendekatan yang digunakan dalam analisis data adalah campuran. Dengan kata lain, tipologi ini telah melalui proses induksi dan deduksi, terutama atas kata kunci pilihan dalam *database*. Namun, penulis tidak menggunakan semua tipe di dalam taksonomi untuk menjelaskan kasus-kasus pelanggaran data sebagai ancaman keamanan nasional, khususnya yang terjadi dalam kurun waktu Agustus-September 2022.

Diagram 1

Matriks Cyber Harm

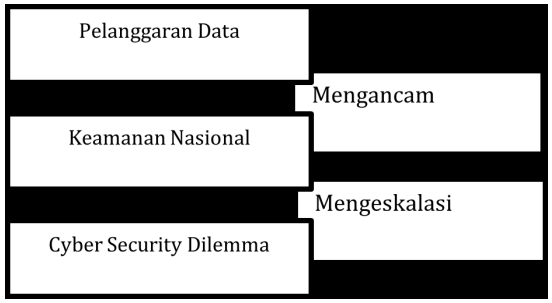


Sumber: diadaptasi dari Agrafiotis et al. (2018) dengan beberapa modifikasi penulis

Pelanggaran Data Mengeskalasi Dilema Keamanan Siber

Gambar 1

Operasionalisasi Konsep I



Sumber: data penulis

Seperti telah dijelaskan sebelumnya, sistem keamanan nasional di Indonesia mengadopsi prinsip keamanan komprehensif yang melingkupi fungsi pertahanan negara, keamanan negara, keamanan publik dan keamanan insani. Pada dasarnya, aktivitas pelanggaran data yang dilakukan dilakukan bjorka, desorden, dan lolyta dalam kurun waktu Agustus-September 2022 bisa mengancam: (1) Dimensi pertahanan negara karena asal ancaman tersebut berasal dari luar negeri dan berdampak langsung kepada kedaulatan negara. Pasalnya, dalam salah satu aksinya, ancaman bjorka ditujukan langsung kepada Presiden Republik Indonesia sebagai simbol kedaulatan negara (BBC News Indonesia, 2022) dan beberapa pejabat publik di Indonesia, seperti Menteri Koordinator Bidang Politik, Hukum dan HAM, Menteri BUMN dan Menteri Komunikasi dan Informatika (Anggrainy 2022). (2) Dimensi keamanan negara karena ancaman pelanggaran data oleh bjorka, desorden, dan lolyta berpotensi menstimulus dan mengeskalasi gangguan terhadap keutuhan negara dan keselamatan bangsa, khususnya yang dilakukan oleh aktor-aktor di dalam negeri yang memiliki intensi untuk medelegitimasi posisi pemerintah dalam menghadapi kasus-kasus pelanggaran data. Berdasarkan pengamatan penulis, tidak lama setelah aktivitas bjorka dan *hacker* lainnya ramai dibicarakan di ruang publik. Di media sosial Twitter, Instagram, Youtube, TikTok, serta di grup-grup Whatsapp dan Telegram muncul akun-akun dan saluran yang menggalang lini massa dengan narasi-narasi yang merusak kredibilitas pemerintah dan mengajak publik untuk tidak lagi percaya kepada pemerintah. Khusus dalam kasus pelanggaran data oleh bjorka, sejumlah pakar, seperti DroneEmprit (2022), berasumsi bahwa bjorka adalah Warga Negara Indonesia dan berjumlah lebih dari satu orang. Kesimpulan tersebut didasarkan analisis linguistik dan konten-konten di Twitter dan Telegram.

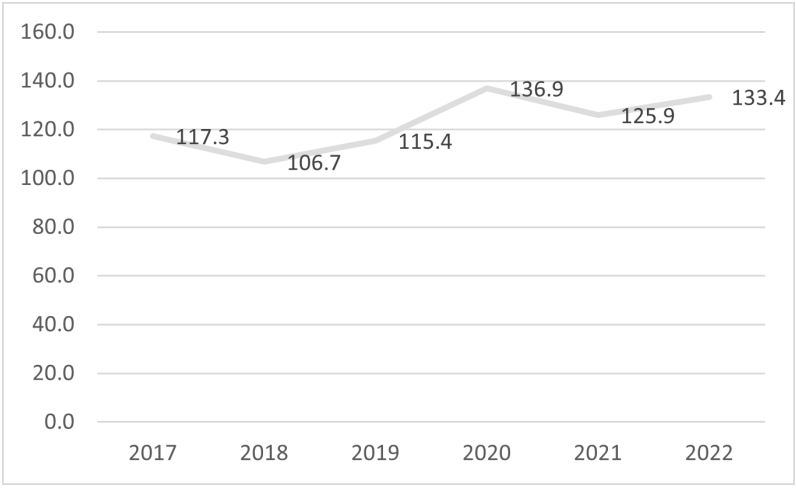
Pelanggaran data yang terjadi dalam kurun waktu Agustus-September 2022 kemarin bisa dikategorikan mengancam keamanan nasional Indonesia, khususnya pada dimensi pertahanan negara dan keamanan negara karena dapat mendorong Indonesia berada dalam kondisi dilema keamanan siber. Sifat ancaman dari kondisi ini konsisten dan berkelanjutan terhadap dimensi pertahanan negara, utamanya karena struktur dari sistem internasional dan ruang siber tergolong anarki. Ketakutan tidak saja tercipta saat

terjadi krisis atau konflik, namun juga di masa "normal", dengan asumsi serangan-serangan serupa, atau lebih besar terjadi.

Di tengah kondisi ketakutan, negara pasti memiliki intensi meningkatkan kapasitas dan kapabilitas pertahanan siber, baik dari sisi defensif maupun ofensif. Minimal, negara akan meningkatkan alokasi anggaran untuk memperkuat kapasitas dan kapabilitas siber mereka. Di Indonesia, setelah pelanggaran data terjadi selama Agustus-September 2022, pemerintah dan DPR segera mempercepat pengesahan Undang-Undang Perlindungan Data Pribadi. Selain itu, anggaran untuk Badan Siber dan Sandi Negara (BSSN) juga naik dalam Rancangan Anggaran Pembelanjaan Negara (RAPBN). Tahun ini, anggaran BSSN hanya 0,55 triliun rupiah. Tahun depan anggaran tersebut naik menjadi 0,62 triliun rupiah.

Grafik 1

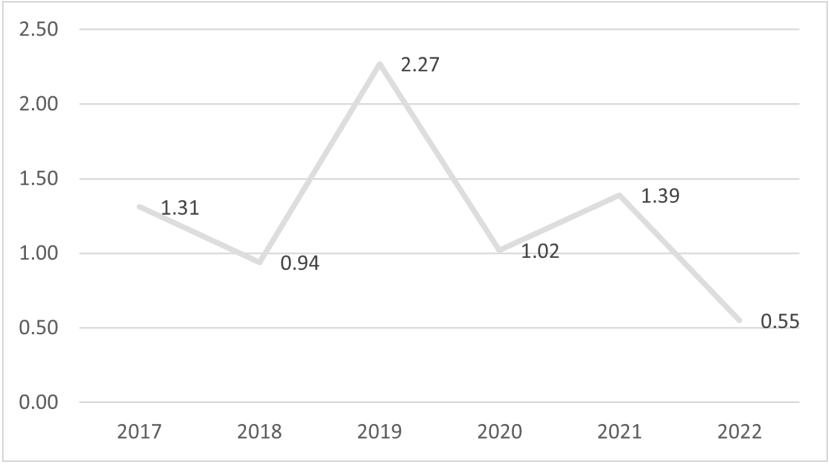
Anggaran Kementerian Pertahanan (triliun rupiah)



Sumber: Kementerian Keuangan (2023)

Grafik 2

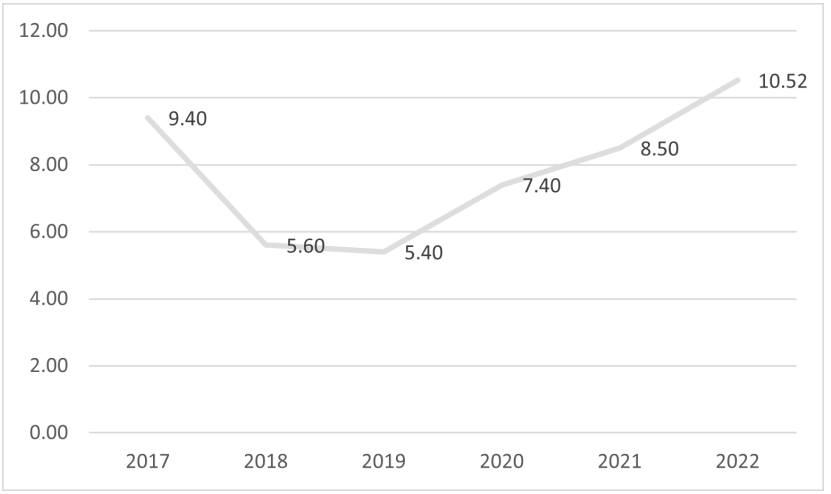
Anggaran Badan Siber dan Sandi Negara (triliun rupiah)



Sumber: Kementerian Keuangan (2023)

Grafik 3

Anggaran Badan Intelijen Negara (triliun rupiah)



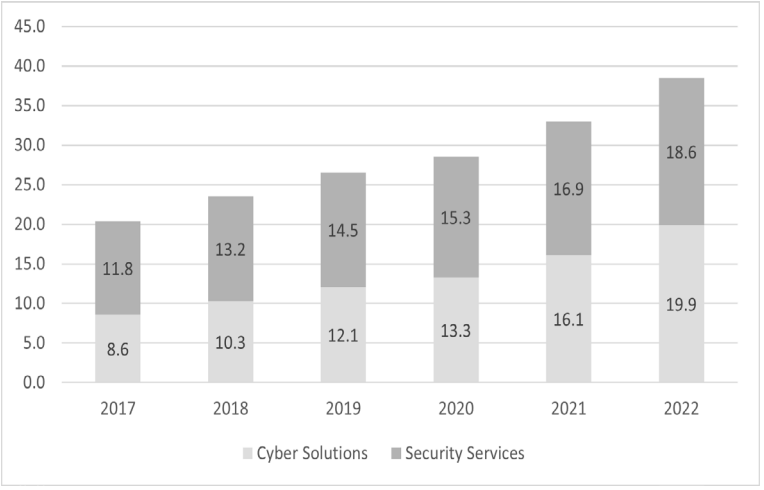
Sumber: Kementerian Keuangan (2023)

Konsekuensi dari kondisi dilema keamanan siber adalah negara-negara berada dalam lingkaran ketakutan. Menariknya, ketakutan ini tidak saja muncul karena kemungkinan-kemungkinan bilamana jaringan keamanan siber negara tersebut diserang negara lain, juga karena secara faktual, negara-negara tesebut diserang oleh aktor-aktor non-negara. Dalam kasus Indonesia, pelanggaran data masif yang terjadi pada Agustus-September 2022 lalu mengeskalasi ketakutan tersebut. Persepsi dan kebutuhan aktual akan pertahanan siber memang bisa meningkatkan kapasitas dan kapabilitas di masa krisis. Namun di masa depan, krisis ini akan tereskalasi.

Selama ini, klaim peningkatan kapabilitas BSSN dan unit-unit siber di institusi pertahanan/keamanan lebih karena alasan defensif. Padahal sistem pertahanan siber memiliki karakter ofensif dan defensif yang natural. Konsekuensi logis dari peningkatan anggaran BSSN adalah rekrutmen SDM yang lebih baik, terutama dari sisi *skill* dan kompetensi. Selain itu, pengadaan alat, teknologi dan jaringan lebih berkualitas dari sebelumnya.

Grafik 4

Valuasi Pasar Keamanan Siber di Asia-Pasifik (miliar dollar)



Sumber: Statista Market Insights (2023)

Bagi suatu negara, keinginan untuk bertahan (defensif) tidak serta merta membuat upaya-upaya penerobosan jaringan (intrusi) negara lain tidak dilakukan. Apalagi, aktivitas tersebut berkaitan dengan pengumpulan intelijen untuk kepentingan pertahanan dan keamanan negara. Kondisi ini bisa terjadi di Indonesia, dengan pertimbangan agar tidak terjadi pelanggaran data yang lebih besar dampaknya oleh aktor non-negara dan semi-negara. Maka BSSN, Divisi Siber di TNI/BIN coba melakukan intrusi ke negara lain.

Sifat dari intrusi yang berorientasi pada pertahanan adalah ambigu. Jika aktivitas-aktivitas intrusi tidak bisa dideteksi negara lain dan target (pengumpulan data) bisa dilakukan. Maka Indonesia bisa mengamankan ruang sibernya dengan efektif. Namun jika sebaliknya, intrusi dideteksi dan direspons negara lain dengan lebih besar, keinginan institusi-institusi pertahanan dan keamanan siber untuk sekadar bertahan bisa saja berubah menjadi menyerang balik. Oleh karena itu, Buchanan (2016) menegaskan bahwa intrusi bisa mengubah konflik dan kompetisi antar negara di masa depan.

Ketika satu negara mendeteksi upaya penerobosan oleh aktor-aktor lain ke jaringan strategis mereka. Pasti ada dua kemungkinan: (1) entah negara tersebut mempersepsikannya sebagai aktivitas ofensif, atau (2) mempersepsikannya sebagai upaya pertahanan negara lainnya. Menimbang permasalahan atribusi, penentuan persepsi ini kemungkinan besar didasari pada informasi yang tidak lengkap. Buchanan (2016) menggarisbawahi bilamana pengambil keputusan pasti mempertimbangkan skenario terburuk, yaitu negara mereka diserang. Kondisi ini tidak saja menyebabkan konflik siber berpotensi muncul. Sejarah mencatat, beberapa kali aktivitas pelanggaran data oleh aktor non-negara seperti bjorka salah dipersepsikan sebagai aktor *semi-state*. Misalnya dalam kasus Solar Sunrise dan Moonlight Maze. Sejauh ini memang belum ada kasus di mana suatu pelanggaran data tereskalasi menjadi konflik siber antar negara. Namun lagi-lagi, potensi ini terbuka lebar.

Pelanggaran data juga bisa memicu dilema keamanan siber dalam kasus enkripsi. *Oxford English Dictionary* (2022) mendefinisikan enkripsi sebagai proses konversi data atau informasi ke dalam suatu kode, dengan tujuan mencegah akses ilegal. Enkripsi bisa berdampak positif dan negatif bagi keamanan negara. Di satu sisi, negara mengoptimalkan enkripsi untuk mengamankan komunikasi strategis untuk mencegah penerobos (*intruders*) dan pencuri dengar (*eavesdroppers*). Di sisi lain, negara ingin mencari jalan pintas enkripsi ketika mereka berada dalam posisi penerobos dan pencuri dengar. Enkripsi lemah menyebabkan kerentanan informasi dan jaringan. Namun enkripsi kuat kadang-kadang menyebabkan musuh-musuh negara sulit dikejar.

Seperti konsep dasarnya, dilema keamanan siber berkenaan dengan ketakutan, eskalasi dan deeskalasi ketakutan, negara sebagai subjek dalam kondisi ini. Dalam kasus bjorka, penulis melihat ketakutan menyebabkan dilema sedang berlangsung dan tereskalasi. Rasa takut ini kemudian berdampak terhadap proses pengambilan keputusan di ruang siber. Dalam ruang siber yang anarki, negara pasti bersikap skeptis dengan negara lain. Kepentingan mengamankan negara salah satunya diwujudkan dengan membangun kapasitas dan kapabilitas operasi siber, baik ofensif dan defensif. Kondisi ini terjadi sesaat setelah

kasus-kasus pelanggaran data periode Agustus-September 2022 terjadi, pemerintah memutuskan untuk meningkatkan anggaran pertahanan dan keamanan siber sejumlah institusi terkait, salah satunya BSSN.

Pelanggaran Data Mengakibatkan Bahaya/ Kerugian Siber

Gambar 2

Operasionalisasi Konsep II

Sumber: data penulis

Keamanan nasional pun memiliki dimensi yang berorientasi pada lingkungan sosial dan manusia (*social and human centered security*). Bangsa Indonesia menerjemahkannya dalam: (1) dimensi keamanan publik karena ancaman tersebut mengganggu keamanan dan ketertiban masyarakat; dan (2) dimensi keamanan insani karena ancaman tersebut mereduksi hak-hak warga negara.

Secara umum, pendekatan *harm* bisa menjelaskan alasan dan proses ancaman pelanggaran data yang terjadi Agustus-September 2022 lalu mengancam keamanan nasional dalam dua dimensi tersebut. Penjelasan tersebut dapat diuraikan sebagai berikut: (1) Pelanggaran data dilakukan sengaja oleh aktor non-negara kepada institusi negara yang bertanggung jawab menyimpan dan mengelola data; (2) Terjadi kelalaian oleh institusi negara yang belum mengutamakan perlindungan data warga negara, serta dari aktor perusahaan, nasional dan swasta nasional yang belum memprioritaskan perlindungan data pelanggan/

konsumen. Pernyataan ini berlaku untuk seluruh Kementerian/ Lembaga, BUMN dan swasta yang telah dirangkum dalam Tabel 1 sebelumnya; (3) Berlangsung proses eksploitasi dalam kasus pelanggaran data Agustus-September 2022, karena peretas jelas-jelas coba mengambil keuntungan dari kondisi rentan yang dialami institusi negara, perusahaan dan Warga Negara Indonesia. Bukti kuatnya adalah para peretas menjajakan data tersebut di BreachedForums untuk mendapatkan keuntungan finansial; (4) Terjadi bahaya/kerugian siber dialami oleh masing-masing aktor, baik institusi negara/perusahaan yang menyimpan dan mengelola data Warga Negara Indonesia; (5) Sejauh ini, penulis melihat kerugian secara ekonomi dialami oleh institusi negara dan perusahaan. Terutama berkaitan dengan biaya investigasi dan biaya *public relations* untuk menutup atau mengalihkan isu pelanggaran data; (6) Terjadi bahaya/kerugian psikologis berupa ketidak nyamanan, kekhawatiran, dipermalukan, dan persepsi negatif publik yang dialami banyak orang yang dilanggar datanya; (7) Terjadi bahaya/kerugian reputasi berupa rusaknya kepercayaan publik, pengawasan terus menerus oleh media dan warganet dialami oleh sejumlah institusi negara dan perusahaan dalam kurun waktu Agustus-September 2022; (8) Terjadi bahaya/ kerugian sosial yang dialami institusi negara, pejabat publik, perusahaan berupa persepsi negatif publik.

Penulis melihat segala bentuk bahaya/kerugian yang muncul dari kasus pelanggaran data dalam kurun waktu Agustus-September 2022 kemarin berpotensi mengganggu keamanan dan ketertiban sosial di ruang siber. Lalu jelas membahayakan pemenuhan hak privasi warga negara. Pada dasarnya, hak atas privasi memang tidak tertulis secara eksplisit di dalam Undang-Undang Dasar Negara Republik Indonesia 1945 Pasal 28. Namun, secara implisit hak tersebut disebutkan dalam Pasal 28G ayat (1), di mana setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Dalam konteks keamanan insani, kondisi bahaya/kerugian dalam pelanggaran data berkaitan erat dengan hak privasi yang juga

ditegaskan oleh Mahkamah Konstitusi dalam Putusan No. 50/ PUU-VI/2008 tentang Perkara Pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang mana:

> "Tidak seorang pun boleh diganggu urusan pribadinya, keluarganya, rumah tangganya, atau hubungan surat-menyuratnya, dengan sewenang-wenang, juga tidak diperkenankan melakukan pelanggaran atas kehormatannya dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan-gangguan atau pelanggaran seperti ini".

Simpulan

Artikel ini mengulas pelanggaran data sebagai ancaman keamanan nasional dengan komprehensif. Pada dimensi Pertahanan dan Keamanan Negara, penulis dapat menggarisbawahi bahwa aktivitas pelanggaran data yang dilakukan oleh peretas telah mengancam kedaulatan negara, utamanya karena presiden sebagai simbol kedaulatan dijadikan sasaran. Selain itu, aktivitas pelanggaran data dapat menstimulus kondisi dilema keamanan siber karena Indonesia akan merespons intrusi salah satunya dengan meningkatkan anggaran pertahanan dan keamanan siber. Kondisi ini akan direspons oleh negara-negara lain dengan cara yang kurang lebih sama, yaitu meningkatkan kapasitas dan kapabilitas pertahanan siber masing-masing. Penulis juga menemukan bahwa anggaran terkait pertahanan dan keamanan siber di sejumlah institusi relatif mengalami peningkatan dalam beberapa tahun terakhir.

Pada dimensi keamanan publik dan keamanan insani, ancaman berlangsung karena pelanggaran data terbukti menyebabkan bahaya/kerugian siber bagi institusi publik, perusahaan dan banyak individu yang data-data dan informasi pribadinya diakses dan disebarluaskan. Menariknya, ancaman di kedua dimensi ikut mendorong percepatan pengesahan Undang-Undang Perlindungan Data Pribadi baru-baru ini.

Penulis juga dapat menyimpulkan bahwa respons negara terhadap ancaman ini, dalam kasus bjorka tergolong reaktif. Seharusnya anggaran BSSN dan unit-unit siber di instansi sektor pertahanan dan keamanan perlu ditingkatkan. Selain itu, respons negara bisa lebih inovatif lagi, misalnya dengan menginisiasi pertahanan siber kolektif di Asia Tenggara.

Pada akhirnya, penulis dapat merekomendasikan sejumlah kebijakan kepada pemerintah dan DPR, seperti: (1) Kementerian Keuangan meningkatkan alokasi anggaran untuk Badan Siber dan Sandi Negara (BSSN) secara bertahap di masa depan sebagai *leading sector* dalam pertahanan dan keamanan siber; (2) Kementerian Luar Negeri mendorong inisiasi Kawasan Bebas Ancaman Siber Konvensional di Asia Tenggara untuk meredam kondisi dilema keamanan siber; (3) DPR mendorong transparansi dan akuntabilitas penggunaan anggaran di Kementerian Pertahanan, Tentara Nasional Indonesia, Kementerian Komunikasi dan Informasi, Badan Intelijen Negara dan Kepolisian Negara Republik Indonesia yang berkaitan dengan pertahanan dan keamanan siber; (4) DPR memperketat pengawasan atas kinerja Kementerian Pertahanan, Tentara Nasional Indonesia, Kementerian Komunikasi dan Informasi, Badan Intelijen Negara dan Kepolisian Negara Republik Indonesia yang berkaitan dengan pertahanan dan keamanan siber.

Tentang Penulis

Denny Indra Sukmawan adalah dosen di Departemen Ilmu Hubungan Internasional, Universitas Pembangunan Nasional "Veteran" Jakarta. Penulis menyelesaikan S1 di Universitas Padjadjaran dan S2 di Universitas Pertahanan. Penulis dapat dihubungi di denny.indras@upnvj.ac.id

David Putra Setyawan adalah analis kebijakan di Pusat Data dan Informasi, Kementerian Pertahanan. Penulis dapat dihubungi di david.setyawan@kemhan.go.id.

Referensi

Buku dan Bab dalam Buku

Baldwin, David, 2011. "The Concept of Security" dalam C.W. Hughes & L.Y. Meng, 2011. *Security Studies: A Reader* (hlm. 24-35). London: Routledge.

Brown, Garrett, et al., 2018. *A Concise Oxford Dictionary of Politics and International Relations* (4th ed.). New York: Oxford University Press.

Buchanan, Ben, 2016. *Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. New York: Oxford University Press.

Choucri, Nazli, 2012. *Cyberpolitics in International Relations*. London: MIT Press.

Choucri, Nazli, dan David D. Clark, 2019. *International Relations in the Cyber Age: The co-evolution dilemma*. London: MIT Press.

Egloff, Florian J., 2022. *Semi-State Actors in Cybersecurity*. New York: Oxford University Press.

Kementerian Keuangan, 2023. *Buku II Nota Keuangan Beserta Rancangan Anggaran dan Pendapatan Belanja Negara*. Jakarta: Kementerian Keuangan

Linklater, Andrew, 2011. *The Problem of Harm in World Politics: Theoretical Investigations*. New York: Cambridge University Press.

Maurer, Tim, 2018. *Cyber Mercenaries: The State, Hackers and Powers*. New York: Cambridge University Press.

Richards, Julian, 2014. *Cyberwar: The Anatomy of Global Security Threat*. New York: Palgrave Macmillan.

Sekretariat Jenderal Dewan Ketahanan Nasional, 2010. *Keamanan Nasional: Sebuah Konsep dan Sistem Keamanan Bagi Bangsa Indonesia*. Jakarta: Dewan Ketahanan Nasional.

Sekretariat Jenderal Dewan Ketahanan Nasional, 2022. *Dewan Keamanan Nasional: Solusi Mengatasi Ancaman Nasional*

Multidimensi. Jakarta: Dewan Ketahanan Nasional.

Singer, P.W., dan Allan Friedman, 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Ullman, Richard, 2011. "Redefining Security" dalam C.W. Hughes & L.Y. Meng, 2011. *Security Studies: A Reader* (pp. 11-17). London: Routledge.

Valeriano, Brandon, dan Ryan Maness, 2018. "International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in Emergent Domains" dalam C. Brown & R. Eckersley, 2018. *The Oxford Handbook of International Political Theory* (hlm. 1-16). New York: Oxford University Press.

Wolfers, Arnold, 2011. "National Security As An Ambigous Symbol" dalam C.W. Hughes & L.Y. Meng, 2011. *Security Studies: A Reader* (hlm. 5-10). London: Routledge.

Jurnal dan Jurnal Daring

Agrafiotis, Ioannis, et al., 2018. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate", *Journal of Cybersecurity*, **4** (1): 1-15.

Herz, John, 1950. "Idealist Internationalism and the Security Dilemma", *World Politics*, **2** (2): 157-180.

Katagiri, Nori, 2021. "Why international law and norms do little in preventing non-state cyber attacks", *Journal of Cybersecurity*, 1-9.

Rid, Thomas, 2012. "Cyber Wall Will Not Take Place", *Journal of Strategic Studies*, **35** (1): 5-32.

Stone, John, 2013. "Cyber War Will Take Place!", *Journal of Strategic Studies*, **36** (1): 101-108.

Youde, Jeremy, 2016. "High Politics, Low Politics, and Global Health", *Journal of Global Security Studies*, **1** (2): 157-170.

Artikel Daring

Anggrainy, Firda Cynthia, 2022. "Menerka Siapa di Balik Topeng Hacker Bjorka", *detikNews*, 12 September, [daring]. dalam https://news.detik.com/berita/d-6286089/menerka-siapa-di-balik-topeng-hacker-bjorka [diakses pada 22 Mei 2023].

BBC News Indonesia, 2022, "Bjorka klaim retas dokumen Presiden Jokowi, pemerintah bentuk satgas dan ungkap motif", *BBC News Indonesia*, 12 September 2022, [daring]. dalam https://www.bbc.com/indonesia/indonesia-62870532 [diakses pada 22 Mei 2023]

Lubold, Gordon, dan Shane Harris, 2017. "Russian Hackers Stole NSA Data on U.S. Cyber Defense", *The Wall Street Journal*, 5 Oktober, [daring]. dalam https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108 [diakses pada 22 Mei 2023].

Luxiana, Kadek Melda, 2022. "Pendiri Drone Emprit: Penjualan Data Indonesia Meningkat Gegara Bjorka", *detikNews*, 14 September, [daring]. dalam https://news.detik.com/berita/d-6292183/pendiri-drone-emprit-penjualan-data-indonesia-meningkat-gegara-bjorka [diakses pada 22 Mei 2023].

Mashabi, Sania, 2021. "BSSN Deteksi 495 Juta Serangan Siber Sepanjang Tahun 2020", *Kompas*, 3 Juni, [daring]. dalam https://nasional.kompas.com/read/2021/06/03/10531031/bssn-deteksi-495-juta-serangan-siber-sepanjang-tahun-2020 [diakses pada 22 Mei 2023].

Newman, Lily H., 2017. "Equifax: CEO Congress Testimony", *Wired*, 3 Oktober, [daring]. dalam https://www.wired.com/story/equifax-ceo-congress-testimony/ [diakses pada 22 Mei 2023].

Statista Market Insights, 2023. "Cybersecurity – Asia", *Statista*, Maret 2023, [daring]. dalam https://www.statista.com/outlook/tmo/cybersecurity/asia [diakses pada 22 Mei 2023]

Film

Poitras, Laura, 2014. Citizenfour. [Film]. New York: Praxis Films, Participant & HBO Documentary Films.

Lain-lain

Bainus, Arry, 2020. "Operasi Militer Selain Perang (OMSP) TNI: Kontra Terorisme dalam Perspektif Keamanan Nasional" dalam Webinar Ikatan Alumni Universitas Pertahanan, 22 September. Jakarta: Ikatan Alumni Universitas Pertahanan.

Choucri, Nazli, 2013. "Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences" dalam World Social Science Forum (WSSF), 13-15 Oktober. Montreal: International Studies Association.

Reardon, Robert, dan Nazli Choucri, 2012. "The Role of Cyberspace in International Relations: A View of Literature" dalam ISA Annual Convention, 1 April. San Diego: International Studies Association.