

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perserikatan Bangsa-Bangsa (PBB) merupakan organisasi internasional terbesar selama ini dalam sejarah pertumbuhan kerjasama semua bangsa di dunia di dalam berbagai sektor kehidupan internasional.¹ Oleh karena itu, melindungi data, sumber daya, dan reputasi PBB sangatlah penting. Saat organisasi menyimpan, memproses, dan membagikan informasi yang semakin sensitif sifatnya secara elektronik, tindakan pencegahan atas terjadinya pelanggaran terhadap informasi tersebut merupakan hal yang perlu diperhatikan.²

PBB sebagai organisasi internasional terbesar di dunia pada kenyataannya tidak luput dari para pelaku kejahatan siber. Berdasarkan investigasi dari dokumen rahasia internal milik PBB yang didapatkan oleh *The New Humanitarian*, mengungkapkan bahwa organisasi internasional tersebut telah menjadi target

¹ Sumaryo Suryokusumo, *Hukum Organisasi Internasional (Hukum Perserikatan Bangsa-Bangsa) United Nations Law*, Tatanusa, Jakarta, 2015, h.1.

² Office of Information and Communications Technology, “Cybersecurity”, <https://unite.un.org/information-security>, diakses pada 7 Oktober 2020.

serangan siber atau *cyber attack* yang dimulai pada pertengahan Juli 2019.³ Terdapat banyak *server* milik kantor PBB yang berada di Jenewa, Wina, termasuk *server* pada kantor pusat Komisi Tinggi Hak Asasi Manusia PBB (*UN Office of the High Commissioner for Human Rights / OHCHR*) menjadi korban atas serangan siber tersebut, sehingga pelaku berhasil menyusup ke dalam *server* PBB.⁴

Dokumen internal yang berasal dari *UN Office of Information and Communications Technology* (UN OICT) menyatakan bahwa terdapat sebesar 42 *server* berhasil disusupi, dan 25 *server* lainnya dianggap mencurigakan.⁵ Dokumen tersebut menunjukkan bahwa pelaku berhasil lolos dengan data dan informasi sebesar 400 *gigabytes*, termasuk data dan informasi pribadi milik 4.000 anggota staf, serta data dan informasi perusahaan yang berkaitan dengan operasional PBB. Terhadap peristiwa tersebut, PBB memutuskan untuk tidak secara terbuka mengungkapkannya kepada para anggota staf PBB. Para anggota staf hanya diminta untuk mengubah kata sandi yang tersimpan.⁶ *Cyber attack* yang terjadi pada kantor PBB tersebut diketahui disebabkan oleh adanya celah keamanan pada perangkat

³ Ben Parker, “Exclusive: The Cyber attack the UN tried to keep under wraps”, <https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack>, diakses pada 7 Oktober 2020

⁴ Ben Parker, *Ibid.*,

⁵ Jamey Keaten dan Frank Bajak, “Leaked report shows United Nations suffered hack”, <https://apnews.com/article/0d958e15d7f5081dd612f07482f48b73>>, diakses pada 7 Oktober 2020.

⁶ Ben Parker, *Loc.Cit.*,

lunak *Microsoft SharePoint* yang kemudian dimanfaatkan oleh pelaku untuk menyusup ke inti infrastruktur *server* milik kantor PBB, yang mengakibatkan kantor-kantor PBB lainnya menjadi korban dari serangan siber tersebut oleh karena *server* PBB yang saling terhubung satu sama lain. Akan tetapi, tidak diketahui siapa aktor dari penyerangan tersebut, serta *virus* jenis apa yang digunakan oleh pelaku.⁷ Atas terjadinya peristiwa tersebut, dilaporkan bahwa para teknisi kantor PBB di Jenewa telah bekerja selama akhir pekan dalam beberapa bulan untuk mengisolasi pusat data lokal PBB dari internet, menuliskan ulang kata sandi, hingga memastikan bahwa sistem telah bersih dari ancaman-ancaman yang berbahaya.⁸

Tindakan yang dijelaskan diatas terjadi pada kegiatan dalam ruang lingkup *cyberspace*. *Cyberspace* adalah dunia tanpa batas yang tidak mengenal batas negara, serta menghilangkan dimensi ruang, waktu, dan tempat.⁹ *Cyberspace* merupakan platform yang diperlukan untuk menyebarkan inovasi, mendorong pertumbuhan ekonomi, hingga memberdayakan masyarakat. Perkembangan teknologi informasi dan komunikasi dan pesatnya peningkatan akses internet di seluruh dunia dapat memfasilitasi terciptanya masyarakat digital global yang

⁷ Jamey Keaten dan Frank Bajak, *Loc. Cit.*,

⁸ *Ibid.*,

⁹ Muhammad Rizal dan Yanyan M. Yani, “Cybersecurity Policy and Its Implementation in Indonesia”, *Journal of ASEAN Studies*, Vol. 4, No. 1, 2016, h. 62.

berkelanjutan.¹⁰ Akan tetapi, dengan semakin berkembangnya teknologi informasi dan komunikasi serta semakin pesatnya akses internet selain memberikan keuntungan, dilain sisi juga dapat memberikan dampak buruk¹¹ salah satunya yaitu dengan munculnya varian kejahatan baru yang berbasis dengan teknologi, atau yang kemudian dikenal dengan *cybercrime* atau *computer crime*.¹² Keamanan siber atau *cyber security* merupakan kebutuhan yang nyata dan mendesak sebagai akibat dari munculnya berbagai risiko penggunaan teknologi informasi dan komunikasi saat ini. *International Telecommunication Union* (ITU) mendefinisikan “*cyber security*” sebagai kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan siber, termasuk aset organisasi dan pengguna. Aset organisasi dan pengguna mencakup perangkat komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirimkan dan/atau disimpan di lingkungan siber.¹³ Menurut Joseph Nye, *cyber security* dapat dibagi menjadi empat ancaman utama, yaitu *cyber warfare*, *cyber espionage*, *cyber terrorism*, dan

¹⁰ Faustine Felici, “Digitalisation – Opportunities for Development”, *European Cybersecurity Journal*, 2020, h.31.

¹¹ Twenty Purandari, “Pertanggungjawaban Hukum Pelaku Eksploitasi Seksual Pada Anak Melalui Internet”, *Media Iuris*, Vol. 2, No. 2, 2019, h. 234.

¹² Maskun, *Kejahatan Siber (Cybercrime) Suatu Pengantar*, Kencana, Jakarta, 2013, h.47.

¹³ ITU NEWS, “Landmark Decisions from Guadalajara: Cybersecurity”, <https://www.itu.int/net/itunews/issues/2010/09/20.aspx>, diakses pada 5 Mei 2021.

cyber crime.¹⁴ Pada mulanya istilah *cyber security* mengacu pada berbagai masalah yang belum menjadi perhatian utama diantara komunitas peneliti dan pemrograman pengembangan internet pada tahun 1970-an dan 1980-an. Pada tahun 1996, hanya 36 juta orang atau sekitar 1% dari populasi dunia yang menggunakan internet. Akan tetapi, seiring perkembangan zaman, pada awal tahun 2017, sekitar 3,7 miliar orang, atau hampir setengah dari populasi dunia telah menggunakan internet.¹⁵

Ketika jumlah pengguna internet melonjak setelah akhir tahun 1990-an, internet pada akhirnya menjadi elemen penting dalam kegiatan ekonomi, sosial, dan politik. Akan tetapi, seiring dengan meningkatnya saling ketergantungan kegiatan-kegiatan tersebut akan internet, muncul suatu kerentanan dan ketidakamanan yang mengancam para pengguna internet.¹⁶ *Cyber criminals* atau Penjahat siber memanfaatkan *cyberspace* dengan membangun pasar yang memperdagangkan data

¹⁴ Tim Maurer, "Cyber Norm Emergence at the United Nations - An Analysis of the UN's Activities Regarding Cyber-Security", *Discussion Paper No 2011-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs*, Harvard Kennedy School, 2011, h.9

¹⁵ Joseph S. Nye, "How will new cybersecurity norms develop?", <https://www.aspistrategist.org.au/how-will-cybersecurity-norms-develop/>, diakses pada 2 November 2021.

¹⁶ *Ibid.*,

dan informasi, orang, hingga barang terlarang yang pada dasarnya melanggar hukum nasional maupun internasional.¹⁷

Sebagai subjek hukum internasional, organisasi internasional turut serta bersama negara-negara dalam menangani berbagai masalah di dunia termasuk masalah yang berkaitan dengan siber seperti keamanan siber. PBB, ITU, *European Union* (EU), dan *North Atlantic Treaty Organization* (NATO) adalah contoh beberapa organisasi internasional yang aktif dalam menangani dan mengembangkan kemampuan siber, lebih khusus dengan tujuan melindungi jaringan internet mereka sendiri dari para penjahat siber.¹⁸

Pembentukan UN OICT pada tahun 2009 pada dasarnya ditujukan untuk melakukan pengawasan terhadap program teknologi informasi dan komunikasi, serta memastikan keselarasan strategi atas teknologi informasi dan komunikasi pada seluruh lingkup organisasi PBB.¹⁹ UN OICT ditugaskan untuk menetapkan rezim manajemen risiko teknologi informasi dan kebijakan pendukung bagi

¹⁷ United Nations, “Cyber Risk”, <https://unite.un.org/digitalbluehelmets/cyberrisk>, diakses pada 12 Januari 2021.

¹⁸ Francois Delerue, *Cyber Operations and International Law: Does International Law Matter in Cyberspace*, Cambridge University Press, Cambridge, 2020, h. 37.

¹⁹ Majelis Umum PBB, “*Report of the Board of Auditors on the handling of information and communications technology affairs in the Secretariat*”, Dokumen PBB, A/67/651, 20 Desember 2012 (selanjutnya disingkat Majelis Umum PBB I), h. 3.

organisasi.²⁰ Pada tahun 2013 UN OICT telah mengembangkan *action plan* untuk mengatasi serangan atau gangguan terhadap sistem teknologi dan informasi organisasi yang terdiri atas 10 inisiatif dengan memfokuskan pada 3 (tiga) area, meliputi:²¹

a. Tindakan Pencegahan, yang dilakukan dengan memperkuat kendali teknis atas infrastruktur teknologi informasi dan komunikasi yang dirancang dengan:

- i) Menetapkan kontrol yang lebih ketat atas perangkat komputasi yang digunakan pada jaringan PBB;
- ii) Pencegahan terhadap ancaman-ancaman yang berbahaya dari lalu lintas internet dan email dengan memperkuat tindakan teknis yang melindungi perimeter jaringan PBB;
- iii) Melakukan segmentasi jaringan untuk mengisolasi area di mana virus dimungkinkan dapat menyembunyikan potensi serangan;
- iv) Meningkatkan kesadaran keamanan informasi di antara personel PBB melalui pemberian pelatihan dan sosialisasi.

²⁰ Office of Information and Communications Technology, “Cybersecurity”, <https://unite.un.org/information-security>, diakses pada 1 September 2020.

²¹ Majelis Umum PBB, “*Progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat*”, Dokumen PBB, A/68/552, 25 Oktober 2013 (selanjutnya disingkat Majelis Umum PBB II), h. 2.

- b. Meningkatkan kemampuan deteksi dan respon terhadap suatu insiden. Sekretariat akan memperkenalkan sistem deteksi intrusi tambahan dan memantau jaringannya secara otomatis.
- c. Tata kelola, risiko, dan kepatuhan. Diaturnya terkait keamanan suatu informasi dengan menetapkan prinsip-prinsip dasar keamanan informasi di PBB yang kemudian berlaku sebagai landasan kebijakan dan instrumen tata kelola.

Sementara itu, kantor PBB di Jenewa merupakan kantor PBB terbesar lainnya selain kantor pusat di New York, Amerika Serikat.²² Kantor PBB di Jenewa terletak di gedung *Palais des Nations*, yang dibangun untuk Liga Bangsa-Bangsa di Jenewa, Swiss, yang kemudian diperluas pada awal tahun 1950 hingga akhir 1960.²³ Hubungan antara PBB dengan Swiss diatur berdasarkan dengan *Agreement on Privileges and Immunities of the United Nations*²⁴ yang berlaku pada 1 Juli 1946.²⁵ Sebagian besar markas besar PBB yang berada di kota Jenewa, diantaranya meliputi Dewan Hak Asasi Manusia (*Human Rights Council*), Komisaris Tinggi

²²Switzerland, “Headquarters of the UN in Europe”, <https://www.myswitzerland.com/en-id/experiences/headquarters-of-the-un-in-europe/>, diakses pada 3 November 2020.

²³DBpedia, “United Nations Office at Geneva”, [https://dbpedia.org/page/United Nations Office at Geneva](https://dbpedia.org/page/United_Nations_Office_at_Geneva), diakses, pada 3 November 2020.

²⁴ UN Geneva, “Host Country”, <https://www.ungeneva.org/en/host-country>, diakses pada 3 November 2020

²⁵Schweizerische Eidgenossenschaft, “The 44 organizations and secretariats in Switzerland”, <https://www.eda.admin.ch/dam/mission-onu-omc-aele-geneve/en/documents/OI-tabrecap.EN.pdf>, diakses pada 2 Maret 2021.

Hak Asasi Manusia (*High Commissioner to Human Rights*), Komisaris Tinggi untuk Pengungsi (*High Commissioner for Refugees*), Komisi Tinggi untuk Pengungsi (*World Trade Organization*), Organisasi Kesehatan Dunia (*World Health Organization*) dan Organisasi Perdagangan Dunia (*World Trade Organization*).²⁶

Jenewa termasuk kota terpadat kedua di Swiss.²⁷ Swiss bukan negara anggota dari *European Union* (EU) maupun *European Economic Area* (Wilayah Ekonomi Eropa), sehingga Swiss tidak memiliki kewajiban untuk menerapkan atau mematuhi hukum EU. Akan tetapi, hukum Swiss secara umum sangat dipengaruhi oleh hukum EU baik dari substansi hingga interpretasinya. Hal tersebut disebabkan letak Swiss yang berada di tengah Eropa, dan juga adanya kedekatan hubungan ekonomi antara Swiss dengan negara-negara anggota Uni Eropa.²⁸

Seperti di negara Eropa lainnya, *cyber security* menjadi perhatian penting dalam konteks keamanan data di negara Swiss. Perlindungan data dan data privasi merupakan hak konstitusional yang dilindungi oleh Konstitusi Swiss. Pengaturan

²⁶ Michelle Nichols, "U.N. says offices in Geneva, Vienna targeted by 'well-resourced' cyberattack last year", <https://nationalpost.com/pmnn/news-pmnn/politics-news-pmnn/u-n-says-offices-in-geneva-vienna-targeted-by-well-resourced-cyberattack-last-year>, diakses pada 7 Oktober 2020.

²⁷ Wikipedia, "Jenewa", <https://id.wikipedia.org/wiki/Jenewa>, diakses pada 7 Oktober 2020.

²⁸ Jurg Schneider, Monique Sturny, dan Hugh Reeves, *The Privacy, Data Protection and Cybersecurity Law Review*, Law Bussiness Research, 2017, h. 327.

terkait perlindungan data diatur dalam *the Swiss Federal Data Protection Act* (DPA) yang ditetapkan pada 19 Juni 1992 dan peraturan pelaksana yaitu *the Swiss Federal Data Protection Ordinance* (DPO) yang ditetapkan pada 14 Juni 1993.²⁹ Disamping itu, Swiss telah meratifikasi *Convention on Cybercrime of the Council of Europe 2001* pada tahun 2011.³⁰

Pada tahun 2018 terbit *the National Strategy for the Protection of Switzerland against Cyber Risks* yang merupakan dokumen berisi kebijakan utama dengan menetapkan tujuh sasaran strategis dan sepuluh bidang tindakan, disertai dengan rencana implementasi yang merupakan hasil dari diskusi dengan para pemangku kepentingan utama pada lingkup keamanan siber di Swiss.³¹ Rencana implementasi tersebut menetapkan langkah-langkah khusus untuk mengimplementasikan sepuluh bidang tindakan yang ditentukan dalam kebijakan tersebut. Langkah-langkah sebagaimana yang termuat dalam *the National Strategy for the Protection of Switzerland against Cyber Risks* telah disesuaikan dengan *the European Union Network and Information Security (NIS Directive)*³², yaitu pengaturan terkait keamanan siber yang berlaku di Uni Eropa. *NIS Directive*

²⁹ *Ibid.*,

³⁰ Michael Reinle dan Lukas Buhlmann, “Switzerland: Cybersecurity Comparative Guide”, <https://www.mondaq.com/technology/963028/cybersecurity-comparative-guide>, diakses pada 9 Oktober 2020.

³¹ Marie Baezner, “Cybersecurity in Switzerland: Challenges and the Way Forward for the Swiss Armed Forces”, *Connections: The Quarterly Journal*, 2020, h.64.

³² *Ibid.*, h.67.

mengatur mengenai pengenalan standar minimum demi mencapai tingkat keamanan jaringan dan sistem informasi yang tinggi dan sama diantara negara anggota, serta kewajiban untuk melapor adanya insiden siber kepada otoritas nasional.³³

Sebelumnya PBB beberapa kali telah menjadi korban dari serangan siber. Pada tahun 2008 diketahui bahwa penjahat siber berhasil memasuki sistem komputer Sekretariat PBB di Jenewa dan bersembunyi di dalamnya selama hampir dua tahun. Serangan tersebut diduga merupakan bagian dari *Operation Shady RAT*.³⁴ Kemudian pada tahun 2016, organisasi penerbangan sipil internasional atau ICAO yang merupakan badan khusus PBB yang berbasis di Montreal juga menjadi korban serangan siber yang paling serius dalam sejarahnya.³⁵ Menyadari pentingnya mitigasi risiko keamanan penggunaan sistem teknologi informasi dan komunikasi oleh organisasi, demi menjaga kerahasiaan dan keamanan data yang disimpan dan dimiliki, oleh karena itu penelitian ini memfokuskan pada hal-hal yang berkaitan dengan strategi maupun kebijakan, serta pengaturan mengenai

³³ European Commision, “The Directive on security of network and information systems (NIS Directive), <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>, diakses pada 9 Oktober 2020.

³⁴ Ahmad Taufiqurrahkman, “PBB Terkena Serangan Cyber Terbesar”, <https://techno.okezone.com/read/2011/08/03/55/487655/pbb-terkena-serangan-cyber-terbesar>, diakses pada 20 Juli 2022.

³⁵ Debra Arbec, “Montreal-based UN aviation agency tried to cover up 2016 cyberattack, documents show”, <https://www.cbc.ca/news/canada/montreal/montreal-based-un-aviation-agency-tried-to-cover-up-2016-cyberattack-documents-show-1.5033733>, diakses pada 20 Juli 2022.

pencegahan dan perlindungan siber termasuk mitigasi risiko keamanan siber oleh PBB, dan negara Swiss sebagai negara tuan rumah (*host country*) kantor PBB.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas, maka penelitian dalam penulisan ini akan berfokus pada perumusan masalah sebagai berikut:

- 1) Bagaimana kebijakan PBB mengatur mengenai mitigasi risiko keamanan sistem teknologi informasi dan komunikasi pada lingkup PBB?
- 2) Bagaimana kesesuaian pengaturan mengenai mitigasi risiko keamanan siber antara Swiss sebagai *host country* dengan PBB?

1.3 Tujuan Penelitian

Berdasarkan uraian latar belakang diatas, maka tujuan dari penelitian ini meliputi:

- 1) Menganalisis kebijakan yang diatur oleh PBB sebagai landasan dan pedoman bagi PBB pada penggunaan sistem teknologi informasi dan komunikasi di lingkup organisasi PBB

- 2) Menganalisis kesesuaian pengaturan mengenai mitigasi risiko keamanan siber antara Swiss sebagai *host country* dengan kebijakan yang diatur oleh PBB.

1.4 Manfaat Penelitian

Penelitian hukum ini diharapkan dapat menjadi referensi dalam hukum internasional, menambah kajian hukum khususnya mengenai mitigasi risiko keamanan sistem teknologi informasi dan komunikasi pada lingkup PBB dan negara Swiss dari segala ancaman kejahatan siber dan memberi manfaat bagi praktisi dan akademisi sebagai referensi.

1.5 Metode Penelitian

1.5.1 Tipe Penelitian Hukum

Penelitian dalam penulisan skripsi ini dilakukan dengan menggunakan tipe penelitian secara normatif atau sering dikenal dengan penelitian doktrinal (*doctrinal research*). Sebagaimana pendapat dari *The Australian Pearce Committee* yang dikutip oleh Terry Hutchinson, penelitian doktrinal adalah penelitian yang memberikan eksposisi sistematis tentang peraturan yang mengatur kategori hukum tertentu, menganalisis hubungan antara peraturan, menjelaskan area-area yang

bersinggungan, dapat memprediksi perkembangan masa depan.³⁶ Lebih lanjut, Terry Hutchinson mengemukakan bahwa fitur esensial penelitian doktrinal adalah analisis konseptual kritis dari peraturan-peraturan yang relevan dengan masalah yang sedang diselidiki.³⁷ Berkaitan dengan pendapat tersebut, penulisan skripsi ini akan memfokuskan pada analisis ketentuan tentang keamanan siber yang berlaku di lingkup PBB serta diantara PBB dengan negara tuan rumah yaitu Swiss. Diawali dengan menganalisis ketentuan mengenai mitigasi keamanan sistem teknologi informasi dan komunikasi PBB, kemudian dilakukan analisis ketentuan-ketentuan tentang mitigasi keamanan siber di negara Swiss dikaitkan dengan ketentuan yang berlaku di PBB serta perjanjian internasional yang berlaku diantara PBB dan Swiss sebagai negara tuan rumah markas besar PBB.

1.5.2 Pendekatan Masalah

Pendekatan masalah yang digunakan adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Melalui *statute approach*, dalam menghadapi suatu isu hukum, dilakukan penelusuran dengan menelaah semua undang-undang dan regulasi yang relevan.³⁸

³⁶ Terry Hutchinson, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law', *Erasmus Law Review*, No. 3, 2015, h. 131.

³⁷ *Ibid.*,

³⁸ Peter Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi*, Kencana, Jakarta, 2017, h.133.

Statute approach digunakan untuk membahas ketentuan-ketentuan tentang keamanan sistem teknologi informasi dan komunikasi pada lingkup organisasi PBB dan negara Swiss, serta perjanjian internasional diantara keduanya. Selanjutnya, penelitian ini akan menggunakan *conceptual approach*, yaitu pendekatan yang dilakukan dengan mengacu pada pandangan-pandangan yang berasal dari pendapat para ahli maupun doktrin-doktrin dalam ilmu hukum³⁹ mengenai keamanan dalam penggunaan sistem teknologi informasi dan komunikasi. Penggunaan pendekatan konseptual dimaksudkan untuk membangun suatu argumentasi hukum oleh penulis dalam memecahkan isu hukum yang dihadapi.⁴⁰

1.5.3 Sumber Bahan Hukum

Untuk memecahkan isu hukum dan memberikan preskripsi tentang apa yang seyogyanya, diperlukan sumber-sumber penelitian hukum. Sumber-sumber penelitian hukum berasal dari sumber-sumber penelitian yang berupa bahan-bahan hukum.⁴¹ Sumber bahan hukum yang digunakan penulis dalam penulisan skripsi ini terdiri dari beberapa tipe bahan hukum, meliputi:

- a. Bahan hukum primer;

³⁹*Ibid.*, h. 135.

⁴⁰ *Ibid.*, h. 136.

⁴¹ *Ibid.*, h. 181.

Bahan hukum primer merupakan bahan hukum yang bersifat autoritatif atau mempunyai otoritas.⁴² Bahan hukum primer yang digunakan penulis dalam penulisan ini adalah semua ketentuan yang terkait dengan keamanan sistem teknologi informasi dan komunikasi dan pengaturan yang berkaitan dengan mitigasi risiko keamanan siber pada lingkup PBB termasuk perlindungan data dan data privasi di negara Swiss, antara lain:

- 1) *Agreement on the Privileges and Immunities on the United Nations concluded between Swiss Federal Council and the Secretary-General of the United Nations;*
- 2) *Swiss Federal Act on Data Protection 1992;*
- 3) *Swiss Federal Data Protection Ordinance 1993;*
- 4) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning for a high common level of security of network and information systems across the Union;*
- 5) *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on*

⁴² *Ibid.*,

information and communications technology cybersecurity certification and repealing Regulation (EU) no 526/2013 (Cybersecurity Act).

b. Bahan hukum sekunder.

Bahan hukum sekunder merupakan bahan-bahan yang berupa semua publikasi tentang hukum yang bukan berupa dokumen resmi.⁴³ Adapun bahan hukum sekunder yang akan digunakan penulis dalam penulisan skripsi ini berupa kepustakaan, yaitu meliputi tulisan-tulisan tentang hukum baik dalam bentuk buku, jurnal hukum, hasil penelitian, artikel dari internet, maupun pendapat para ahli⁴⁴ terkait mitigasi risiko keamanan sistem teknologi informasi dan komunikasi sehubungan dengan perlindungan data.

1.5.4 Prosedur Pengumpulan Bahan Hukum

Pengumpulan bahan hukum diperoleh dengan mengidentifikasi peraturan perundang-undangan internasional yang mengatur tentang keamanan siber, perlindungan data pribadi, dan kebijakan organisasi tentang mitigasi keamanan siber. Selanjutnya dilakukan studi pustaka melalui observasi via media elektronik dan digital untuk menemukan buku teks, jurnal, artikel, maupun bahan pustaka

⁴³ *Ibid.*,

⁴⁴ *Ibid.*, h.183.

hukum lainnya untuk kemudian diklasifikasikan secara sistematis yang sesuai dengan pokok masalah dan dilakukan analisis bahan hukum.

1.5.5 Analisis Bahan Hukum

Metode analisis bahan hukum yang digunakan adalah metode analisis deduktif, yaitu dengan menerapkan bahan-bahan hukum pada suatu isu hukum⁴⁵ dengan memberikan kajian terhadap bahan-bahan hukum yang telah dikumpulkan dan diklasifikasikan, untuk kemudian disusun secara sistematis sesuai dengan pokok masalah yang akan dibahas, untuk kemudian didapatkan sebuah kesimpulan yang khusus terkait pokok masalah dalam penulisan ini.⁴⁶

1.6 Sistematika Penulisan

Dalam penelitian ini, sistematika penulisan yang dilakukan adalah sebagai berikut:

Bab I membahas mengenai latar belakang dari permasalahan keamanan siber yang saat ini menjadi permasalahan baru dan urgensi tersendiri oleh karena maraknya *cyberattack* yang terjadi secara global menasar individu, bisnis,

⁴⁵ Philipus M. Hadjon dan Tatiek Sri Djatmiati, *Argumentasi Hukum*, Gajah Mada University Press, Yogyakarta, 2011, h.22.

⁴⁶ Alex Lanur Ofm, *Logika Selayang Pandang*, Kanisius, Yogyakarta, 2017, h. 40.

organisasi, militer, hingga negara. Berdasarkan hal tersebut, Penulis merumuskan rumusan masalah, tujuan, manfaat, dan metode penelitian.

Bab II membahas dan menganalisis tentang ancaman-ancaman kejahatan siber yang dapat mengancam PBB dan bagaimana PBB mengatur kebijakan mengenai penggunaan sistem teknologi informasi dan komunikasi di lingkup organisasi PBB berkaitan dengan pencegahan dan perlindungan dari segala ancaman kejahatan siber.

Bab III membahas dan menganalisis mengenai pengaturan keamanan siber di negara Swiss dan perjanjian internasional antara PBB dan Swiss, serta mengidentifikasi apakah kebijakan PBB dan pengaturan siber di Swiss sebagai negara *host country* telah bersesuaian, sehingga masalah terkait kejahatan siber dapat dicegah dan ditangani secara tepat.

Bab IV membuat kesimpulan dan saran dari keseluruhan penelitian sesuai dengan yang telah diteliti.