Jurist-Diction
Volume 4 No. 6, November 2021

Tinjauan Yuridis *Cyber Espionage* Berdasarkan Hukum Internasional

Aldo Rahmandana
Aldo.rahmandana-2017@fh.unair.ac.id
Universitas Airlangga

How to cite:
Aldo Rahmandana, 'Tinjauan Yuridis *Cyber Espionage* Berdasarkan Hukum Internasional' (2021) Vol. 4 No. 6 Jurist-Diction.

Histori artikel:
Submit 13 Agustus 2021;
Diterima 15 Oktober 2021;
Diterbitkan 5 November 2021.

DOI:
10.20473/jd.v4i6.31839

p-ISSN: 2721-8392
e-ISSN: 2655-8297

Abstract
Due to the rapid transformation of technology causing a subliminal changes on how states spy upon each other. With the help of technology and cyber infrastructure, states tend to use cyber technology as its main facility to conduct an espionage towards other states. Cyber espionage has come to represent national security and economic threat, due to all the classified information that already been massively stolen by another country. The aim of this research paper is to analyze and clarify pertaining the role of International law specifically towards this kind of act of espionage, and perceive the state responsibility of perpetrator which is states. It can be concluded that cyber espionage does not per se regulated under international law, but its lawfulness depends on the way in which it operation carried out may violate specific international conventions or any other international law principles.
Keywords: *Cyberlaw; Cyber Espionage; International Law.*

Abstrak
Pesatnya perkembangan teknologi dan digitalisasi mengakibatkan terjadinya perubahan metode dan cara dalam pelaksanaan tindakan spionase oleh negara terhadap negara lain guna mengumpulkan fakta dan informasi yang berkaitan dengan perkembangan politik, ekonomi, teknologi, dan lain-lain melalui kapabilitas teknologi siber atau kerap disebut sebagai *cyber espionage*. Tujuan dari penelitian ini adalah untuk menganalisis terkait peranan hukum internasional dalam mengatur tindakan tersebut dalam tataran internasional dan bagaimana pertanggungjawaban dari negara pelaku tindakan *cyber espionage*. Hasil dari penelitian ini menyimpulkan bahwa belum ada konvensi international khusus yang mengatur mengenai *cyber espionage* sehingga tindakan *cyber espionage* itu sendiri merupakan tindakan yang masih belum diatur secara international.
Kata Kunci: Hukum Siber; *Cyber Espionage*; Hukum Internasional.

Pendahuluan

Dengan pesatnya perkembangan teknologi yang terjadi dan proses digitalisasi secara masif yang berkembang di dunia mengakibatkan kerap terjadi berbagai praktik-praktik spionase dalam tingkat yang lebih masif jika diperbandingkan dengan

spionase yang dilakukan secara konvensional. Terdapat berbagai kasus yang terjadi dalam kurun waktu lima belas tahun belakangan ini terkait berbagai negara yang melakukan tindakan *cyber espionage* terhadap negara lain. Sebagai contoh yaitu negara Cina yang kerap meluncurkan berbagai tindakan *cyber espionage* terhadap negara-negara lain dalam kurun waktu satu dekade kebelakang.[1] Pada tahun 2013, ABC News menyebutkan bahwa pemerintah Cina telah mencuri beberapa informasi terkait denah dari markas *Australian Security Intelligence Organisation.*[2]

Menteri luar negeri Australia menduga keras bahwa Cina telah membobol masuk kedalam jaringan sistem dari *Australian Broadcasting Corporation* guna mencuri informasi terkait tata letak kabel dan sistem keamanan dari markas yang terletak di Canberra.[3] Negara yang juga menjadi korban dari spionase Cina adalah Amerika, negara ini menjadi negara yang kerap kali dijadikan sasaran oleh Cina. Dalam jangka waktu dua dekader terakhir terdapat berbagai aktivitas *cyber espionage* yang dilakukan oleh Pemerintah Cina maupun organisasi yang berada dalam arahan pemerintahan Cina. Salah satu yang terkenal adalah APT atau bisa disebut *Advanced Persistent Threat Groups* bernama FireEye dan Temp.Periscope melancarkan *cyber espionage* pada tahun 2013 silam dan mencuri semua data strategi maritim dari Amerika Serikat guna kepentingan ekonomi mereka.[4]

Dapat dilihat bahwa aktivitas *cyber espionage* atau memasuki jaringan siber suatu negara secara tidak sah serta mengambil data dan informasi sesitif milik negara lain telah menimbulkan banyak kerugian bagi negara yang mengalaminya. Kerugian yang diterima dapat dalam bentuk ekonomi melihat beberap arsip rahasia seperti data kekayaan intelektual dan data mengenai peluang restrukturisasi perusahaan-perusahaan dalam negeri dapat diketahui oleh

---

[1] Christopher Bing, "U.S. cybersecurity experts see recent spike in Chinese digital espionage"<www.reuters.com>25 Maret 2020, dikunjungi pada tanggal 27 Maret 2021.

[2] ABC News, " George Brandis briefed by ASIO on Claims China stole classified blueprints of Canberra"<abcnews.go.com> 30 Mei 2013, dikunjungi pada tanggal 2 Juli 2021.

[3] *ibid*.

[4] Fireeye, "Suspected Chinese Cyber Espionage Group (Temp.Periscope) Targeting U.S. Engineering and Maritime Industries <www.fireeye.com> 16 Maret 2018, diakses pada tanggal 3 Juli 2021.

pihak lain, pada akhirnya berdampak pada kondisi perekonomian suatu negara. Dengan adanya praktik tersebut beberapa strategi dan langkah kebijakan suatu negara dapat diketahui oleh negara lain yang kemudian menimbulkan dampak yang sangat signifikan terhadap berjalannya suatu negara.

Metode Penelitian

Metode dalam penulisan ini menggunakan metode penelitian yurdis normatif dimana yaitu penelitian yang dilakukan dengan cara meneliti bahas Pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan mengadakan penelusuran terhadap peraturan-peraturan yang terkait isu hukum yang diteliti. Dengan penelitian yang dugunakan adalah pendekatan terhadap beberapa konvensi-konvensi internasional dan pendekatan konsep-konsep hukum Internasional.

Pokok-pokok *Cyber Espionage*

Cyber espionage dapat didefinisikan satu persatu dengan memaknai kata *cyber* dan kemudian e*spionage. Cyber* diartikan sebagai "dunia maya" dan Menurut Prof. Barda Nawawi Arief[5] menyatakan bahwa *cyber* atau siber merupakan suatu istilah untuk menjelaskannya dengan istilah "mayantara". *Cyber* juga dapat diartikan dari bahasa Inggris sebagai suatu istilah "maya, tidak nyata, tidak terlihat, terawang, terawang, tidak ada bentuk". Dengan mengartikan *cyber espionage* dalam penjelasan yang lebih komprehensif, perlu juga di maknai apa itu spionase dan elemen-elemen yang menjadi parameter dalam tindakan spionase.

Espionage atau spionase diartikan oleh Geoffrey B. Demarest[6] sebagai; "*consciously deceitful collection of information, ordered by a government and accomplished by humans unauthorized by the target to do the collection*

[5] Teguh Arifiyadi, "Dunia Siber yang Tidak Maya"< www.hukumonline.com> 25 September 2017,dikunjungi pada 28 November 2020.

[6] Lt. Col. Geoffrey B. Demarest,'Espionage in International law, Denver Journal of International law and Policy' (1991) Denver Journal of International Law and Policy, Denver.[5].

of information".[7] Spionase dalam arti yang lebih spesifik dan terbatas adalah pengumpulan informasi manusia.

Praktik spionase antar negara yang begitu lazim untuk dilakukan dan lazimnya praktik ini didorong oleh perkembangan zaman yang memungkinkan bagi negara untuk melakukan spionase dengan tidak harus berada dalam wilayah yurisdiksi negara lain. Komputer dan Internet telah berkembang dan terus akan berkembang, dengan berkembangnya teknologi tersebut akan mengakibatkan terjadinya kerentanan dalam mencegah *cyber espionage.*

Cyber espionage didefinisikan oleh *Tallin Manual* 2.0 yang merupakan panduan komprehensif untuk pemegang kebijakan dan ahli hukum dalam meninjau hukum internasional terhadap *cyber espionage*, dalam *Rule* 32 nya disebut sebagai tindakan yang dilakukan secara sembunyi-sembunyi atau dengan alasan palsu dengan menggunakan kapabilitas siber untuk mengumpulkan, mencoba untuk mengumpulkan informasi.[8]

Cyber espionage yang dapat disebut sebagai *"cyber-exploitation"* juga didefinisikan oleh Herbert Lin[9] sebagai tindakan dan operasi dalam jangka waktu yang lama untuk memperoleh informasi yang seharusnya dijaga kerahasiaannya dan berada di transit melalui sistem komputer atau jaringan negara musuh. Sebelum memasuki penjelasan bagaimana hukum internasional mengatur *cyber espionage* terhadap negara-negara, ada beberapa terminologi seperti *cyberspace*, *cybercrime* dan *cyberlaw* yang akan membantu untuk memahami bagaimana dan dimana *cyber espionage* dilakukan. Paling pertama adalah *cyberspace*, Definisi terbaru dari *cyberspace* oleh FD Kramer[10] adalah domain global dan dinamis (dapat berubah terus menerus) yang dicirikan oleh penggunaan gabungan elektron dan spektrum

---

[7] Christopher D. Baker,'Tolerance of International Espionage: A Functional Approach', (2003) 19 American University International Law Review.[12].

[8] Michael N. Schmitt, 'Tallin Manual 2.0 International Applicable to Cyberwarfare' (Cambridge University Press 2013).[89].

[9] Herbert S. Lin, "*Offensive Cyber Operations and the Use of Force*' (2009) Vol.4:63 National Research Council (NRC) of the National Academies.[67].

[10] Marco Mayer, 'International Politics in the Digital Age: Power Diffusion or Power Concentration (2013) XXV, International Relations Sections University of Florence.[3].

elektromagnetik, yang bertujuan untuk membuat, menyimpan, memodifikasi, bertukar, berbagi, dan mengekstrak, menggunakan, menghilangkan informasi, dan mengganggu sumber daya fisik.

Pada terminologi yang kedua adalah *cybercrime*, hal tersebut berimplikasi langsung dengan *cyber espionage*. Barda Nawawi[11] merujuk kepada kerangka sistematik dari *Draft Convention* on *cybercrime* dari Dewan Eropa (Draft No. 25, Desember 2000) yang sekarang telah berubah menjadi Budapest Convention mendefinisikannya secara sederhana sebagai "*crime related to technology, computers, and the internet*" atau secara sederhana sebagai kejahatan yang berhubungan dengan teknologi, komputer dan internet.[12]

Menurut Dikdi M. Arief dan Elisatris Gultom, mengklasifikasikan bentuk dari cybercrime menjadi beberapa wujud yaitu;[13]

1. *Unauthorized Acces to Computer System and Service;*
2. *Illegal contents;*
3. *Data forgery;*
4. *Cyber Espionage;*
5. *Cyber Sabotage and Extortion;*
6. *Offense Against Intellectual property;*
7. *Infringement of privacy.*

Cyberlaw merupakan hukum yang digunakan di dunia *cyber* yang umumnya dikorelasikan dengan *internet*.[14] Ruang lingkup yang terkandung dalam cyberlaw adalah segala aspek yang berhubungan dengan subyek hukum yang menggunakan dan memanfaatkan teknologi internet/elektronik yang dimulai pada saat "*online*" da memasuki dunia *cyber* atau maya.

---

[11] Dikdik M dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi* (Refika Aditama 2005).[8].

[12] Masitoh Indriani, 'Implementasi Peraturan Pemerintah Nomor 82 Tahun 2012 Sebagai Upaya Negara Mencegah Cybercrime Dalam Sistem Transaksi Elektronik' (2014) Vol. 29 No. 3 Yuridika.[333].

[13] Dikdik M. dan Elisatris Gultom, *Cyber Law Op.Cit*.[28].

[14] Asril Sitompul, *Hukum Internet (Pengenalan Mengenai Masalah Hukum di Cyberspace* (Citra Aditya Bakti 2001).[56].

Cyber Espionage dalam Hukum Internasional

Cyber espionage dalam hukum internasional masih menjadi bahasan yang sangat tertinggal dengan belum adanya aturan khusus yang mengatur mengenai *cyber espionage.*[15] Istilah hukum internasional itu sendiri pertama kali dikenalkan oleh Jeremy Bentham[16] yaitu seorang filsuf yang mengemukakan utilitarianisme sekaligus sarjana dari Inggris.

J.L Brierly[17] seorang pakar hukum internasional mendefinisikan Hukum Internasional menjadi kerangka hukum dan prinsip-prinsip yang mengikat negara-negara mengenai keterkaitannya satu sama lain. Seperti observasi yang telah dilakukan oleh John Perkins bahwa hukum internasional berkembang berdasarkan logika gabungan internasional yang tak terhindarkan, dikenakan dengan realita atas kebijakan luar negeri. Akar hukum dan legitmasinya terletak pada dinamika yang dialami oleh negara-negara tersebut.[18]

Statuta Mahkamah Internasional yang tertuang dalam Pasal 38 ayat (1) menetapkan bahwa pengadilan akan mempertimbangkan empat sumber untuk memutuskan suatu kasus. Ini meliputi;[19]

1. Traktat-traktat internasional, umum dan yang spesifik, menetapkan aturan yang secara tegas yang diakui oleh negara peserta dalam traktat tersebut;
2. Kebiasan internasional, termasuk *opinio juris* dan kebiasaan umum. Kaidah kebiasaan ini pada umunya telah melalui sejarah yang sungguh panjang sehingga kemudian diakui oleh masyarakat internasional;
3. Prinsip-prinsip umum Hukum yang diakui oleh bangsa-bangsa beradab;
4. Keputusan-keputusan pengadilan dan ajaran para sarjana yang terkemuka dari berbagai negara sebagai sumber tambahan untuk menetapkan aturan kaidah hukum.

Dengan berbagai sumber hukum yang ada dalam Pasal 38 ayat (1) tersebut, kegiatan *cyber espionage* akan diuji kedalam beberapa sumber Hukum Internasional

---

[15] David Wallace, 'Peeling Back the Onion of Cyber Espionage after Tallin 2.0' (2019) Volume 78 Issue 2 Article 2 Maryland Review.[17].

[16] Gerald Postema, 'Utilitarian International Order: Bentham on International Law and International Order' (2008) University of North Carolina at Chapel Hill", Februari.[1].

[17] J.L. Brierly, *Hukum Bangsa-bangsa: Suatu Pengantar Hukum Internasional* (Bhratara 1963).[56].

[18] *ibid*.

[19] J.G. Starke, *Pengantar Hukum Internasional* (Sinar Grafika 2008).[78].

tersebut. Sehingga akan di tinjau satu persatu mulai dari traktat dan konvensi Internasional yang kemungkinan mengatur mengenai *cyber espionage* sampai dengan peninjauan dari beberapa substansi dari putusan pengadilan internasional yang dapat berimplikasi terhadap *cyber espionage* dan berbagai asas yang kemungkinan bersinggungan.

Pertama, masih belum ada pengaturan khusus yang mengatur dan bersentuhan langsung dengan *cyber espionage,*[20] bahkan masih ada inkonsistensi persepsi pada tahap spionase tradisional itu sendiri atau dapat di kenal sebagai *Human Intelligence.*[21] Mengingat masih ada nya kekosongan hukum pada spionase masa damai dalam hukum internasional, masing-masing negara telah lama mengkriminalisasi tindakan spionase ke dalam hukum domestic mereka masing-masing.[22]

Beberapa konvensi multilateral yang menyebutkan mengenai spionase dalam masa damai secara tidak langsung yaitu Pasal 7(3) *The Antartic Treaty* 1959, dimana pasal tersebut memberikan hak pada pengamat perwakilan dalam melakukan "inspeksi" terhadap stasiun, instalasi, peralatan dan pesawat terbang dari negara-negara yang telah meratifikasi telah patuh terhadap standar konvensi tersebut. Bentuk pengintaian, penyelidikan atau tinjauan sekalipun telah menggambarkan kegiatan spionase. Pada Pasal 19 ayat (2) c UNCLOS (*United Nations Conventions on the Law of the Sea*) menyatakan perbuatan yang bertujuan untuk mengumpulkna informasi yang merugikan bagi pertahanan atau keamanan negara pantai.[23] Pasal tersebut hanya di peruntukan terhadap kapa lasing yang hendak melintasi atau melayarkan kapalnya di perairan territorial suatu negara saja, dan pasal tersebut tidak dapat mengakomodir *cyber espionage* yang dilakukan dari jarak jauh.[24]

Spionase juga kerap disebutkan dalam beberapa pasal dalam *Vienna Convention on Diplomatic Relations*, *Vienna Convention on Consular Relations*

[20] CCDOE, 'Tallin Manual on the International Law Applicable to Cyber Warfare' (2008) CCDOE Daily Review.[45].

[21] Veronika Prochko, 'The International Legal View of Espionage' (2018) E-International Relations.[5].

[22] Tallin 2.0 *Op.Cit*.[218].

[23] Katharina Zilkowki, *Op.Cit*.[228].

[24] *ibid.*

dan *Convention on Special Mission* pada Pasal 41 VCDR, Pasal 55 VCCR dan Pasal 47(1) dan (2) CSM dari konvensi tersebut.[25] Konvensi tersebut menyebutkan bahwa pejabat diplomatik diwajibkan untuk menghormati hukum dari negara penerima dan dilarang menggunakan fasilitas diplomatik untuk hal-hal yang menyimpangi dari tugasnya sebagai pejabat diplomatik.

Pengaturan mengenai spionase dalam masa perang beberapa kali disebutkan dalam *Convention (IV) Respecting the Laws and Customs of War on Land* yaitu yang terkandung dalam Pasal 29, 30 dan 31. Di dalam traktat tersebut pun tidak disebutkan bahwa tindakan spionase dan pengiriman intelijen ke negara musuh dianggap suatu pelanggaran internasional. Kegiatan spionase antar negara dalam masa damai maupun masa perang merupakan kegiatan yang sudah lazim dan telah diterima oleh masyarakat internasional.[26] Meskipun tindakan tersebut tidak secara jelas dinyatakan sebagai kejahatan perang tetapi secara umum tetap dikriminalisasi oleh negara-negara.

Dengan melihat Bab 5 *Rule* 32 dari *Tallin Manual* 2.0, *cyber espionage* yang merupakan perkembangan dari kegiatan spionase itu sendiri dan salah satu contoh dari *cyber operation* juga masih belum diatur dalam perjanjian internasional yang menyebutkan bahwa tindakan *cyber espionage* merupakan pelanggaran dari Hukum Internasional. Terdapat pengecualian apabila kegiatan tersebut dapat melanggar beberapa norma dan prinsip Hukum Internasional yang ada.[27] kegiatan tersebut dapat saja melanggar berbagai ketentuan dan perjanjian seperti Hukum Diplomatik Konsuler, Hukum Perdagangan Internasional, dan Hukum Kekayaan Intelektual.

Kegiatan *cyber espionage* memang sama sekali belum dituangkan kedalam satu perjanjian internasional tetapi kegiatan tersebut telah diatur dalam berbagai legislasi dari berbagai negara di dunia, seperti di Indonesia yang telah mengaturnya di dalam Pasal 7 Undang-Undang No. 3 Tahun 2002 mengenai Pertahanan Negara dan Pasal 30 Undang-Undang No.11 Tahun 2008 mengenai Informasi Transaksi

[25] Vienna Convention on Diplomatic Relation 1963.

[26] Christopher D. Baker, 'Tolerance of International Espionage: A Functional Approach' (2003) Vol. 19 Issue 5 American University International Law Review.[1092].

[27] *ibid*.[200].

Elektronik, dan berbagai negara seperti Amerika yang sudah memiliki *cyber security bill* pada tahun 2012. Uni Eropa yang merupakan organisasi supranasional, telah memiliki satu instrumen hukum yaitu *Convention on Cybercrime* dimana konvensi tersebut pada pasal 10 mengatur mengenai berbagai kewajiban bagi negara yang tergabung dalam organisasi tersebut untuk mempunyai instrument untuk melarang berbagai tindakan *cybercrime* termasuk *cyber espionage* di dalam negara nya.[28]

Kedua, Implikasi dari kebiasaan Internasional dan *opinio juris* yang menjadi sandaran atau justifikasi bagi legalitas dari *cyber espionage* itu sendiri memang belum ada. Tidak ada *opinio juris* yang dapat mendukung bahwa tindakan *cyber espionage* dibenarkan oleh Hukum Internasional.[29]

Apa yang terkandung dalam Pasal 38 dari Statuta Mahkamah Internasional menjelaskan bahwa kebiasaan internasional menjadi salah satu sumber dari Hukum Internasional. Definisi kebiasaan internasional tersebut memiliki dua elemen penting yang harus terkandung di dalam nya *i.a State Practice* dan *Opinio Juris Necessitatis*.[30] Telah banyak bukti dan kejadian yang mendukung bahwa *cyber espionage* sudah mencukupi elemen pertama yaitu *state practice* tetapi belum ada bukti yang jelas bahwa praktik tersebut dapat di justifikasi sebagaimana di trima sebagai hukum yang berlaku.[31] Sehingga *opinio juris* tidak dapat dijadikan sebagai pembenar bagi aktivitas *cyber espionage* yang dilakukan antar negara.Setelah meninjau dari kedua sumber hukum internasional terhadap *cyber espionage*, selanjutnya adalah implikasi asas-asas dan berbagai putusan yang dapat berkorelasi untuk menjustifikasi *cyber espionage*.

Dengan bermunculannya beberapa pandangan ahli dari berbagai organisasi dibawah naungan NATO yaitu CCDCOE (*Cooperative Cyber Defence Centre*

---

[28] Afitrahim, *Yurisdiksi Berdasarkan Convention on Cybercrime*, TESIS (Universitas Indonesia 2009).[55].

[29] Aaron Shull, Cyber Espionage and International Law (GigaNet 2013).[2].

[30] Tamas Hoffmann, 'Dr. Opinio Juris and Mr. State Practice: The Strange Case of Customary International Humanitarian Law' (Department of International Law).[2].

[31] Inaki Navarette, Why Silence Isn't Always Golden: Espionage Exceptions under Customary International Law<leidensecurityandglobalaffairs.nl>10 Oktober 2019, dikunjungi pada tanggal 16 Maret 2021.

of Excellence) yang mengeluarkan Tallin Manual. Panduan tersebut merupakan hasil dari 20 ahli dan praktisi dari seluruh dunia dan ditujukan untuk menjelaskan permasalahan bagaimana hukum internasional diaplikasikan terhadap *cyberspace.* Panduan ini menjelaskan terkait *cyber operation* yang dilakukan oleh negara dan orang perorangan sebagai pelaku.[32]

Pengaturan dan penjelasan (*commentary*) yang terkandung dalam Tallin manual memiliki tujuan merefleksikan *customary international law* atau kebiasaan internasional dan koherensi nya terhadap sumber subsider hukum internasional yaitu "*the teachings of the most highly qualified publicist*". Beberapa pernyataan afirmasi terhadap pengaturan yang ada didalamnya seperti pernyataan pemerintahan AS dapat dijadikan sebagai landasan terbentuknya *opinio juris*.[33]

Ketiga, terdapat tiga asas yang dapat dilanggar oleh tindakan *cyber espionage* yaitu Kedaulatan negara, Non-intervensi dan *non-state actor i.a*;

1. Kedaulatan Negara

   Max Huber dalam *Arbitral Award on the Island of Palmas* mendefinisikan Kedaulatan sebagai;[34] "*..Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the function of a State*.."

   Dalam *United Nations Group of Governmental Experts on Development* (UN GGE) 2013 *report* menyatakan;[35] "*State sovereignty and international norms and principles that flow from sovereignty apply to state conduct of ICT-related activities*".

   Dengan penjelasan dari UN GGE tersebut dapat simpulkan bahwa kedaulatan negara dan norma internasional yang muncul dari asas kedaulatan berlaku terhadap ruang siber. Terdapat dua klasfikasi bagi tindakan *cyber*

[32] Michael N. Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallin Manual Juxtaposed' (2012) Vol.54 Harvard International Law Journal.[3].

[33] *ibid*.

[34] Francois Delerue, Cyber Operations and International Law (Cambridge Studies in International and Comparative Law2008).[204].

[35] Francois Delerue, *ibid*.[207].

espionage untuk ditinjau dari prinsip ini dikarenakan tindakan tersebut dilakukan dengan berbagai metode dan cara pelaksanaan. Pada metode *cyber espionage* yang pertama adalah tindakan spionase yang dilakukan dari luar wilayah kedaulatan negara target atau bisa dikatakan sebagai *remote-cyber espionage*. Ahli seperti Michael N. Schmitt[36] menyatakan bahwa tindakan tersebut yaitu *cyber espionage,* bukan merupakan pelanggaran atas suatu kedaulatan tetapi pelaksanaan dan metode dari tindakan tersebut dapat menjadikan tindakan itu sebagai pelanggaran terhadap kedaulatan suatu negara.[37]

Satu jenis operasi spionase yang memungkinkan dapat berimplikasi terhadap kedaulatan negara lain adalah ketika *cyber espionage* tersebut dilaksanakan dalam wilayah yurisdiksi negara target. Seperti pengiriman agen ke negara lain dan penggunaan fasilitas diplomatik sebagai fasilitas operasi. Keberadaan agen secara fisik dalam wilayah yurisdiksi negara lain dan melakukan operasi spionase tanpa sepengetahuan dan justifikasi yang jelas, menjadikan kedaulatan dari negara yang sedang di target sedang dilanggar oleh negara yang melakukan operasi.[38]

Dalam kasus Corfu meyatakan bahwa tindakan pengumpulan informasi atau data yang dilakukan di negara target merupakan suatu pelanggaran dari kedaulatan negara target.[39] Pendapat Schmitt yaitu ada dua elemen yang dapat membuat *cyber espionage* menjadi tindakan yang melanggar kedaulatan negara lain yaitu ketika negara pelaku atau agen dari negara pelaku masuk kedalam kedaulatan teritorial negara target dan melakukan tindakannya di dalam wilayah tersebut, dan/atau ketika tindakan tersebut mengakibatkan dampak yang nyata terhadap infrastruktur atau fasilitas siber suatu negara.[40]

---

[36] Michael N. Schmitt, 'Respect for Sovereignty in Cyberspace' (2017) 1639, Tex Law Review.[3].

[37] *ibid*.[4].

[38] David Wallace, *Op.Cit*.[27].

[39] International Court of Justice, 'Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)', icj-cij.org, dikunjungi pada tanggal 16 Maret 2021.

[40] Francois Delerue, *Op.Cit*.[217].

Konsep dari *Lotus Case* tersebut juga didukung oleh asas *par in parem non habet imperium* dan konsep yurisdiksi yang merefleksikan prinsip-prinsip dasar dalam kedaulatan negara dimana negara tersebut tidak akan diakui apabila negara tersebut tidak memiliki yurisdiksi.[41] Prinsip hukum *par in parem non habet imperium* memberi penekanan bahwa negara lain tidak dapat mencampuri urusan yurisdiksi negara lainnya, tetapi prinsip ini memberikan celah bagi negara lain untuk mencampuri yurisdiksi negara lain apa bila negara yang bersangkutan memberikan izin.[42]

Kesimpulan dari implikasi asas ini dengan *cyber espionage* adalah tindakan tersebut dapat saja menjadi pelanggaran meskipun tindakan tersebut tidak menimbulkan dampak yang nyata bagi negara target. Penetrasi terhadap kedaulatan teritorial negara target dapat menjadikan tindakan tersebut sebagai pelanggaran, diukur dari seberapa jauh penetrasi negara lain secara fisik ke negara lain.[43]

2. Non-Intervensi

Non-Intervensi adalah suatu prinsip dimana negara tidak diperbolehkan untuk melakukan intervensi hal-hal yang pada pokoknya termasuk dalam urusan atau permasalahan dalam negeri (yurisdiksi domestik). Beberapa urusan yang termasuk dalam yurisdiksi domestik adalah menyangkut terkait penentuan sistem politik, eknomi, sosial, sistem budaya dan sistem kebijakan luar negeri suatu negara.[44]

Yang mendasari prinsip non-intervensi tersebut antara lain adalah pasal 2 paragraf 7 dari Piagam PBB dan beberapa pasal lain seperti pasal 42 dan 51. Prinsip tersebut juga didukung oleh adanya deklarasi tahun 1970 (*United Nations General Assembly Resolution* 2625 XXV), dalam deklarasi tersebut disebutkan bahwa segala bentuk intervensi yang dapat merugikan negara yang

[41] Dinstein, 'Par in parem non habet Imperium' (2016) Vol 1 Israel Law Review.[112].
[42] *ibid*.
[43] *ibid*.[232].
[44] Maziar Jamnejad,'The Principle of Non-Intervention' (2009) Leiden Journal of International Law.[2].

di intervensi merupakan suatu pelanggaran hukum internasional.[45]

Cyber espionage yang merupakan pengumpulan data dan informasi dari negara lain, secara sendirinya bukan merupakan pelanggaran dari asas non-intervensi.[46] Pengumpulan data belaka tidak sendirinya menjadikan tindakan tersebut sebagai tindakan koersif yang bertujuan untuk memberikan pengaruh terhadap kebebasan memilih keputusan suatu negara target. Data yang telah terkumpul mungkin dapat di gunakan untuk secara koersif mempengaruhi negara target, dalam perspektif tersebut bukan berarti aktivitas spionase menjadi sebuah pelanggaran tetapi akan selalu ada langkah-langkah persiapan (*preparatory measures*) atau tindakan gabungan (*composite act*) yang bertujuan untuk melaksanakan operasi secara koersif. Sehingga tindakan tersebut dapat dikatan sebagai pelanggaran asas non-intervensi.[47]

3. *Non-state actor* dan *Due Dilligence*

Demikian pula, *non-state actors* yang melakukan peretasan terhadap negara asing atau jaringan perusahaan asing bukan merupakan sebuah *espionage*, tetapi secara umum telah diatur dalam hukum domestik.[48] Hukum internasional yang mengatur mengenai konsep *due dilligence*, mengharuskan negara untuk memastikan bahwa wilayah kedaulatannya dan objek lain dimana negara tersebut mempunyai kontrol penuh untuk tidak dipergunakan merugikan negara lain.[49]

Apabila *non-state actor* melakukan tindakan *cyber espionage* yang dapat menjadi pelanggaran dari asas-asas tertentu dari hukum internasional, dan tindakan tersebut merupakan instruksi dari pemerintahan negara tersebut maka terdapat asas *state responsibility attributable to the state*.[50]

---

[45] Nurul Wakhidah, 'Prinsip Non-Intervensi ASEAN dalam Upaya Penyelesaian Konflik Rohingnya di Myanmar' (2014) Peace and Conflict Studies FISIPOL UGM.[2].

[46] *ibid*.[258].

[47] *ibid*.

[48] David A. Wallace, *Op.Cit*.[229].

[49] *ibid*.

[50] Joanna Kulesza, 'State Responsibility for cyber-attacks on international peace and security' (2009) Polish Yearbook of International Law, XXIX, [9].

Keterkaitan *Cyber Espionage* dengan *Cybercrime* berdasarkan Hukum Internasional

Dengan sedikitnya aturan dan perjanjian internasional yang mengatur mengenai *cyber espionage*, perlu dikualifikasikan mengenai *cyber espionage* yang sudah pasti masuk kedalam *cybercrime* atau *cybercrime* seperti apa yang telah dikatakan oleh Bassiouni dan tertera dalam Convention on Cybercrime 2001. Konvensi ini adalah perjanjian internasional yang telah diratifikasi oleh berbagai negara di dunia termasuk negara-negara di luar Uni Eropa.

Dalam Pasal 2 dan 3 Dari konvensi ini mengatur mengenai beberapa pengaturan terhadap beberapa substansi dalam *cyber espionage*, tindakan tersebut tidak disebutkan secara lugas tetapi dikualifikasikan sebagai akses ilegal dan intersepsi ilegal. Akses ilegal dalam konvensi ini dijelaskan sebagai mengakses baik secara seluruh atau sebagian sistem komputer baik piranti keras, data yang tersimpan dalam sistem, direktori, trafik dan data konten yang terkait. Memasuki sistem komputer lain yang telah terhubung melalui jaringan telekomunikasi publik atau ke dalam sistem komputer yang berada dalam jaringan yang seperti *local area network* juga termasuk dalam unsur mengakses.[51]

Pasal 3 menjelaskan mengenai *illegal interception* yang dimana melindungi hak pribadi dalam komunikasi data elektronik. Penyadapan tanpa hak, yang dilakukan dengan cara teknis, transmisi data komputer non-publik ke, dari atau dari dalam sistem komputer, termasuk emisi elektromagnetik dari sistem komputer dari sistem komputer yang terkandung data di dalamnya. Penjelasan dalam Pasal 3 tersebut bisa mengakomodir unsur dari *cyber espionage* itu sendiri.[52]

Pertanggungjawaban Negara Pelaku *Cyber Espionage*

Menurut Tugba Bayar terdapat empat elemen substansial yang perlu diperhatikan dalam memahami pertanggungjawaban negara dalam hukum internasional yaitu; *Pertama* adanya *obligation* atau kewajiban negara dalam mematuhi segala substansi

[51] Council of Europe, 'Convention on Cybercrime' (Budapest 2001) 23.XI.
[52] *ibid*.

yang terkandung didalam suatu hukum internasional. Apabila negara sudah masuk dan meratifikasi kedalam suatu perjanjian internasional, negara tersebut diwajibkan untuk melakukan apa yang sudah diperjanjikan atau beberapa sumber hukum internasional lainnya seperti hukum kebiasaan internasional.[53] *Kedua* adalah adanya *wrongful act,* dimana negara tersebut melakukan tindakan yang melanggar kewajibannya atau tidak melaksanakan kewajibannya.

Adanya kesalahan oleh negara menjadi hal yang menjadi penting dalam pembasan pertanggungjawaban negara.[54] *Ketiga* adalah ditemukannya kerugian sebagai akibat dari adanya kesalahan yang dilakukan oleh negara lain. Dan *keempat* adalah atribusi dimana keterhubungan antara *act* atau *omission* dengan tindakan negara sebagai subjek hukum internasional. Parameter dalam mengkategorikan tindakan melanggar tersebut sebagai tindakan negara (*act of state*) atau tidak adalah hal yang perlu diperhatikan.

Apabila menganut kepada Pasal 1 dan Pasal 2 pada *Articles on State Responsiility of States Wrongful Acts* 2001, perbuatan suatu negara dapat disalahkan jika tindakan tersebut bisa diatribusikan kepada negara pelaku tersebut (*attribution of conduct to a state*) dan apabila negara tersebut telah melanggar kewajiban internasional atau lalai dalam melaksanakan kewajiban internasionalnya (*breach of an international obligation*).[55] Pada umumnya pertanggung jawaban negara hanya dapat dijatuhkan kepada tindakan negara, organ negara (pemerintah pusat, daerah atau segala individu yang memegang status sebagai organ pemerintahan suatu negara), agen atau (pejabat yang melaksanakan tindakan tersebut atas perintah/ instruksi, pengawasan, anjuran). Orang-orang atau organisasi dalam negara yang tidak secara eksplisit menyatakan untuk bertindak atas negara dan meskipun individu atau organisasi tersebut tidak diklasifikasikan secara hukum nasional oleh negara bersangkutan juga termasuk ke dalam aspek yang dapat diatribusikan.[56]

---

[53] Tugba Bayar, Introduction to State Responsibility (2019) IR 303 International Law, Bilkent Universitesi,[90].

[54] *ibid*.

[55] MaIcoIm D. Evans, *International law, Second Edition* (Oxford University Press 2008).[459].

[56] *ibid*.

Perbuatan ataupun tindakan seorang individu (*non-state actors*) dapat dikatakan sebagai tindakan negara apabila dalam pelaksanaannya entitas atau individu tersebut mendapat arahan, bantuan finansial dan dikontrol penuh oleh negara.[57] Beberapa aspek tersebut berkesinambungan apabila dikaitkan dengan unsur atribusi, kontrol yang dimaksud dalam unsur tersebut masih menjadi perdebatan.

Pasal 8 dalam ARSIWA telah memberikan pandangan mengenai pertanggungjawaban negara terhadap partisipasi pihak lain yaitu individu atau sebuah entitas (*private actors*), menyatakan bahwa tindakan dari seorang individu atau entitas dapat diatribusikan terhadap negara apabila individu atau entitas tersebut memang melaksanakan tindakan tersebut dibawah perintah atau kontrol penuh dari negara.

Pada unsur yang kedua yaitu bentuk pelanggaran suatu konvensi internasional yang dimana *cyber espionage* belum mempunyai koridor yang jelas dalam bentuk konvensi maupun sumber hukum yang lain. Sehingga disimpulkan bahwa negara pelaku *cyber espionage* tidak mempunyai tanggung jawab yang sesuai dengan prosedur dan elemen yang tertera di *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA).

Kesimpulan

Artikel ini menegaskan *bahwa cyber* espionage tergolong sebagai *cybercrime* menurut Pasal 2 dan 3 *Convention on Cybercrime* dan dikategorikan sebagai *Unauthorized Access, illegal access*, dan *Illegal interception*. Konvensi hanya sebuah bentuk upaya harmonisasi legislasi domestik dari negara Uni Eropa saja sehingga tidak berlaku secara global. Tindakan *cyber espionage* antar negara masih belum diatur secara khusus dalam hukum internasional sehingga tidak ada perjanjian khusus yang mengatur dan menyatakan bahwa tindakan tersebut sebagai suatu pelanggaran hukum internasional. Akan tetapi tindakan *cyber espionage* masih dibatasi oleh beberapa koridor yaitu asas dan norma dalam hukum internasional.

[57] *ibid*.

Apabila terdapat aspek dalam pelaksanaan dari kegiatan tersebut yang melanggar beberapa asas hukum internasional maka bisa disebut bahwa kegiatan *cyber espionage* tersebut telah melanggar hukum internasional.

Tidak terpenuhinya dua unsur dalam Pasal 2 dari *Articles on Responsibility of States for Internationally Wrongful Acts* yaitu atribusi dan pelanggaran hukum internasional. Pertama yaitu terdapat tantangan yang baru dalam mengidentifikasi pelaku dari *cyber espionage*, apakah pelaku tersebut sebuah *non-state actor* atau negara. Kemudian, tidak ada perjanjian dan konvensi internasional bilateral maupun multilateral yang menyatakan bahwa *cyber espionage* antar negara merupakan tindakan yang dilarang oleh hukum internasional. Sehingga dua unsur (*attributable*) dan (*breach of an international obligation*) yang tercantum dalam Pasal 2 tidak dapat terpenuhi dalam konteks *cyber espionage*, memberikan negara pelaku tindakan *cyber espionage* ruang untuk tidak bertanggung jawab atas tindakan tersebut.

Daftar Bacaan

Buku

Aaron Shull*, Cyber Espionage and International Law* (GigaNet 2013).

Asril Sitompul, *Hukum Internet; Pengenalan Mengenai Masalah Hukum di Cyberspace* (Citra Aditya Bakti 2001).

Bert-Jaap Koops*, Cybercrime and Jurisdiction* (Information Technology & Series, Chapter 2006).

CCDOE, *Tallin Manual on the International Law Applicable to Cyber Warfare* (CyCon 2013).

Dikdik M, *Cyber Law: Aspek Hukum Teknologi Informasi* (Refika Aditama 2005).

Francois Delerue, *Cyber Operations and International Law* (Cambridge Studies in International and Comparative Law 2020).

J.G. Starke, *Pengantar Hukum Internasional* (Sinar Grafika 2008).

J.L Brierly, *Hukum Bangsa-bangsa: Suatu Pengantar Hukum Internasional*, (Bhratara 1963).

Malcolm D Evans, *International law, Second Edition* (Oxford University Press 1998).

Rushkoff Douglas, *Cyberia: 'Life in the Trenches of Cyberspace* (Clinamen Press Ltd 1994).

Jurnal

Baker D., Christopher,'Tolerance of International Espionage: A Functional Approach'(2003) Vol. 19 Issue 5 American University International Law Review.

Geoffrey B Demarest, Lt. Col, 'Espionage in International law' (1991) Denver Journal of International law and Policy.

Gerald Postema, 'Utilitarian International Order: Bentham on International Law and International Order' (2008) University of North Carolina at Chapel Hill.

Joanna Kulesza, 'State Responsibility for cyber-attacks on international peace and security' (2009) XXIX Polish Yearbook of International Law.

Katharina Ziolkowski, 'Peacetime Regime for State Activities in Cyberspace', International Law (2013) International Relations and Diplomacy, NATO CCD OE Publication.

Marco Mayer, 'International Politics in the Digital Age: Power Diffusion or Power Concentration (2013) XXV International Relations Sections University of Florence.

Masitoh Indriani, 'Implementasi Peraturan Pemerintah Nomor 82 Tahun 2012 Sebagai Upaya Negara Mencegah Cybercrime Dalam Sistem Transaksi Elektronik' (2014) 29 no 3 Yuridika.

Maziar Jamnejad,'The Principle of Non-Intervention' (2009) Leiden Journal of International Law.

Nurul Wakhidah, 'Prinsip Non-Intervensi ASEAN dalam Upaya Penyelesaian Konflik Rohingnya di Myanmar, (2014) Peace and Conflict Studies FISIPOL UGM.

Pratiwi Esty, 'Hukum Siber : Praktik Spionase Dalam Kedaulatan Negara dan Hubungan Diplomasi Berdasarkan Ketentuan Hukum Internasional' (2020) Vol.8 No.3 Jurnal Pendidikan Kewarganegaraan Undiksha.

Russel Buchan, 'Cyber Espionage and International Law' (2019) Hart Publishing, Oxford.

S. Lin, Herbert, "*Offensive Cyber Operations and the Use of Force*", (2010) *National Research Council* (NRC) of the National Academies, Vol.4:63.

Schmitt, Michael N., Tallin Manual 0 International Applicable to Cyberwarfare' (2013) Cambridge University Press.

Stoddart, Kristan, 'UK Cyber Security and Critical National Infrastructure Protection' (2016) 92 5 International Affairs.

Tamas Hoffmann, 'Dr. Opinio Juris and Mr. State Practice: The Strange Case of Customary International Humanitarian Law' (2006) Department of International Law.

Veronika Prochko, 'The International Legal View of Espionage' (2018) E-International Relations.

Wallace, David, 'Peeling Back the Onion of Cyber Espionage after Tallin 2.0', (2019) Maryland Review Volume 78 Issue 2 Article 2.

Laman

ABC News, "George Brandis briefed by ASIO on Claims China stole classified blueprints of Canberra"<ABCnews.com> dikunjungi pada tanggal 2 Juli 2021.

Alexander Abad-Santos, "China is Winning the Cyber War Because They Hacked U.S. Plans for Real War", <theatlantic.com>, dikunjungi pada tanggal 28 Maret 2013.

Christopher Bing, "U.S. cybersecurity experts see recent spike in Chinese digital espionage",<www.reuters.com> , dikunjungi pada tanggal 27 Maret 2021.

Fireeye, "Suspected Chinese Cyber Espionage Group (Temp.Periscope) Targeting U.S. Engineering and Maritime Industries, <www.fireeye.com>, diakses pada tanggal 3 Juli 2021.

Kenneth Rapoza, "U.S. Hacked China Universities, Mobile Phones, Snowden tells China Press", <www.forbes.com> dikunjungi pada 3 Juli 2021.

Navarette Inaki, Why Silence Isn't Always Golden: Espionage Exceptions under Customary International Law, <*leidensecurityandglobalaffairs.nl*>dikunjungi pada tanggal 16 Maret 2021.

Andy Greenberg,' Meet the Mad Scientist Who Wrote the Book on How to Hunt Hackers,' <www.wired.com> dikunjungi pada tanggal 17 Januari 2021.

Arifiyadi Teguh, "Dunia Siber yang Tidak Maya", <www.hukumonline.com> dikunjungi pada 28 November 2020.

DSLA, "Cyber Law: Pengertian dan Tujuan Cyber Law di Indonesia" <*dslawfirm.com*> dikunjungi pada tanggal 25 Desember 2020.

Konvensi Internasional

1907 *Hague Convention IV With Respect to the Laws and Customs of War on Land Articles on State Responsibility of States for Internationally Wrongful Acts* (ARSIWA) 2001.

Council of Europe, *Convention on Cybercrime* (Budapest 2001).

Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States.

Friendly Declaration 1970.

Montevido Convention on the Rights and Duties of States 1933.

Piagam PBB (*UN Charter*).

The Antartic Treaty 1959.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer space.

United Nations Conventions on the Law of the Sea.

Vienna Convention on Diplomatic Relations1961.

Vienna Convetion on Consular Relations 1963.

Putusan

Corfu Channel Case, United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania, Assessment of Compensation, 15 XII 49, *International Court of Justice* (ICJ), 15 Desember 1949.

Military and Paramilitary Activities in and Against Nicaragua, Nicaragua v. United States, Merits, Judgment, (1986) ICJ Rep 14, ICGJ 112.

Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, *International Criminal Tribunal for the Former Yugoslavia* (ICTY), 15 Juli 1999.

S.S. 'Lotus", France v Turkey, *Judgment* No. 9, PCIJ *Series* A no 10, ICGJ 248 (PCIJ 1927).