JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.v5i2

Pengamanan Wilayah Udara: Tanggung Jawab Negara dalam Cyber Espionage di Ruang Angkasa

Muhammad Hendi Hidayat Romadhoni[1], Aulia Nabila Rachman[2], Imam Dwi Cahyo[3]
[1]Universitas Arilangga, Surabaya, Indonesia, hendimuhammadhabsyi@gmail.com
[2]Universitas Airlangga, Surabaya, Indonesia, nabilarachman28@gmail.com
[3]Universitas Airlangga, Surabaya, Indonesia, imam.dc26@gmail.com

Corresponding Author: hendimuhammadhabsyi@gmail.com

Abstract: *The regulation of cyber espionage in the aerospace industry has become a major focus in national and international security. As technology advances, cyberattacks are increasingly complex and can target vital infrastructure, such as aerospace systems. Cyber espionage involves using internet networks to conduct spying activities by infiltrating computer systems of targeted parties. However, there are challenges in enforcing the law, especially when cyber espionage perpetrators operate across national borders. Therefore, state responsibility is important in handling cyber espionage incidents in the aerospace area, including in strengthening international cooperation, strengthening cyber defense systems, and strengthening the relevant legal framework. Recent findings reveal cyber espionage activities by Iran's UNC1549 group targeting Israeli shipping companies and US aerospace and defense firms using unique malware. This research focuses on finding out how cyber espionage is regulated in the aerospace context and the form of state responsibility for cyber espionage acts. The research methods used are the statute approach and the conceptual approach. By analyzing the existing legal framework and relevant concepts, this research aims to provide a comprehensive understanding of how countries can synergize in dealing with the threat of cyber espionage in the aerospace sector.*

Keyword: *Aerospace, Cyber espionage, State Responsibility.*

Abstrak: Regulasi *cyber espionage* dalam ranah *aerospace* telah menjadi fokus utama dalam keamanan nasional dan internasional. Seiring dengan kemajuan teknologi, *cyberattacks* semakin kompleks dan dapat menargetkan infrastruktur vital, seperti sistem *aerospace*. *Cyber espionage* melibatkan penggunaan jaringan internet untuk melakukan kegiatan mata-mata dengan menyusup ke sistem komputer pihak yang ditargetkan. Namun, ada tantangan dalam menegakkan hukum, terutama ketika pelaku *cyber espionage* beroperasi melintasi batas negara. Oleh karena itu, tanggung jawab negara menjadi penting dalam penanganan insiden *cyber espionage* di wilayah *aerospace*, termasuk dalam memperkuat kerja sama internasional, memperkuat sistem pertahanan siber, dan memperkuat kerangka hukum yang relevan. Temuan terbaru mengungkapkan aktivitas *cyber espionage* oleh kelompok UNC1549 Iran yang menargetkan perusahaan pelayaran Israel dan perusahaan kedirgantaraan dan pertahanan AS dengan menggunakan *malware* yang unik. Penelitian ini berfokus untuk mengetahui

bagaimana *cyber espionage* diatur dalam konteks *aerospace* dan bentuk pertanggungjawaban negara atas tindakan *cyber espionage*. Metode penelitian yang digunakan adalah pendekatan perundang-undangan dan pendekatan konseptual. Dengan menganalisis kerangka hukum yang ada dan konsep-konsep yang relevan, penelitian ini bertujuan untuk memberikan pemahaman yang komprehensif mengenai bagaimana negara dapat bersinergi dalam menghadapi ancaman *cyber espionage* di sektor *aerospace*.

Kata Kunci: *Aerospace, Cyber espionage, State Responsibility.*

PENDAHULUAN

Cybercrime mencakup sejumlah besar tindakan, kejahatan, atau perilaku terlarang yang dilakukan oleh individu atau kelompok terhadap komputer, perangkat yang berhubungan dengan komputer, atau jaringan teknologi informasi, serta kejahatan tradisional yang difasilitasi atau dikelola oleh penggunaan internet dan atau teknologi informasi (Donalds & Osei-Bryson, 2019). Ada banyak bentuk *cybercrime*, salah satunya adalah kejahatan yang dilakukan oleh kelompok Iran bernama UNC1549 yang menargetkan perusahaan pelayaran Israel dan perusahaan kedirgantaraan dan pertahanan Amerika Serikat (selanjutnya disebut AS) melalui *malware* yang unik dan termasuk ke dalam kategori *cyber espionage* yang akan dibahas lebih lanjut.

Dijelaskan dalam *Rule 32 on Peacetime cyber espionage in the Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* (Schmitt, 2017b), bahwa "*Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so*." Pasal 32 menjelaskan bahwa hukum internasional tidak mengatur spionase siber itu sendiri. Namun, aturan ini menyimpulkan bahwa, tergantung pada pihak-pihak yang terlibat, data yang dikumpulkan, dan kerangka hukum yang berlaku, hukum internasional dapat mengatur tindakan yang mendasarinya. Oleh karena itu, legalitas *cyber espionage* dibahas di bawah aturan hukum internasional lainnya, yaitu prinsip-prinsip kedaulatan teritorial dan non-intervensi, serta hukum diplomatik dan konsuler (Schmitt, 2017a).

Lebih lanjut, NATO juga memberikan definisi terkait *cyber espionage*, sebagai berikut "*any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party*" (Schmitt, 2013). Dari penjelasan tersebut, dapat dikatakan bahwa *cyber espionage* merupakan tindakan melawan hukum yang dilakukan terhadap pihak lain untuk mengumpulkan informasi secara diam-diam. Dalam hal ini, jika tindakan tersebut dilakukan oleh negara, maka tindakan tersebut dapat digolongkan sebagai tindakan yang berbahaya karena dapat berimplikasi menimbulkan konflik dan ancaman terhadap pihak lain yang dirugikan.

Hal ini didasarkan pada pengalaman kasus yang pernah terjadi di AS, laporan intelijen mengatakan bahwa terdapat tindakan *cyber espionage* yang dilakukan oleh Rusia dan China yang dilakukan untuk mencuri data-data rahasia perdagangan dan teknologi AS, terutama data penelitian dan pengembangan teknologi tinggi Amerika dengan tujuan agar data-data rahasia tersebut dapat membantu perekonomian mereka. Teknologi informasi, teknologi militer, *clean energy*, dan teknologi medis merupakan bidang utama ekonomi AS yang menjadi target *economic cyber espionage*. Pemerintah Cina dan Rusia terus menerus membantah peran mereka dalam kegiatan semacam ini. Jumlah uang yang hilang akibat *economic cyber espionage* tidak diperkirakan oleh pemerintah AS. Menurut *US International Trade Commission*, pelanggaran merek dagang, *cyberattacks*, dan *cyber espionage* mungkin telah menyebabkan hilangnya pendapatan hingga $50 miliar. Beberapa kelompok yang terindikasi

melakukan tindakan *cyber espionage* yang ditujukan ke AS adalah *Energetic Bear* (*Dragonfly*) dan *APT28* (*Fancy Bear/Sofacy*), yang berasal dari Rusia, dan *APT1* (*Comment Crew*), yang berafiliasi dengan China. Kelompok-kelompok ini menggunakan *malware* yang sangat disesuaikan dan metode enkripsi canggih untuk mencuri data rahasia, serangan *spear-phishing*, dan *malware* untuk menyusup ke dalam jaringan dan mengambil informasi sensitif.

Serangan *cyber espionage* yang sedang berlangsung menargetkan industri kedirgantaraan, penerbangan, dan pertahanan di Timur Tengah terkait dengan Iran, menurut para peneliti keamanan. Serangan yang dimulai pada Juni 2022 ini terkait dengan organisasi Iran yang dilacak oleh Mandiant di bawah sebutan UNC1549 (Warminsky, 2024). Kelompok ini telah menargetkan perusahaan kedirgantaraan dan pertahanan AS serta perusahaan pelayaran Israel. Kelompok ini berhubungan dengan operasi peretasan lain yang dikenal sebagai *Tortoiseshell*. Informasi menunjukkan adanya afiliasi dengan *Islamic Revolutionary Guard Corps* (selanjutnya disebut IRGC) Iran. Hal tersebut dikarenakan Iran secara terbuka mendukung militan Hamas di Gaza, para peneliti menemukan kemungkinan hubungan dengan IRGC ini signifikan, terutama mengingat ketegangan baru-baru ini dengan Iran terkait konflik Israel-Hamas.

Mandiant menemukan bahwa UNC1549 menyebarkan *two backdoor* yang berbeda, *MINIBIKE* dan *MINIBUS*, melalui berbagai strategi penyamaran, terutama dengan memanfaatkan infrastruktur *cloud Microsoft Azure* dan teknik rekayasa sosial. Dengan menggunakan infrastruktur *cloud Azure*, *MINIBIKE,* yang ditemukan antara Juni 2022 dan Oktober 2023, memungkinkan eksekusi perintah, eksfiltrasi file, dan fitur-fitur lainnya. Selain itu, juga ditemukan pada Agustus 2023 hingga Januari 2024, *MINIBUS* adalah *backdoor* unik yang menampilkan kemampuan memata-matai yang lebih baik dan antarmuka eksekusi kode yang dapat disesuaikan. *Malware* ini mencakup tugas-tugas *cyber espionage* yang khas, seperti mengambil informasi login dan memungkinkan aktivitas berbahaya yang lebih jauh. Metode kelompok UNC1549 dalam menanam *malware* sebanding dengan kecelakaan yang terjadi di AS tentang *cyber espionage*.

Cyber espionage di dunia saat ini mengurangi kemungkinan pihak lawan untuk mengetahuinya. Kejahatan semacam itu dapat membahayakan dan mengganggu stabilitas keamanan dan pertahanan nasional. Hal ini didasari fakta bahwa *cyber espionage* merupakan kejahatan transnasional yang menghilangkan batas-batas negara (*borderless*) sehingga berdampak pada kedaulatan negara yang dituju. Berdasarkan permasalahan di atas, terdapat rumusan masalah yang akan dibahas lebih lanjut yaitu mengenai pengaturan *cyber espionage* dalam lingkup hukum internasional khususnya di wilayah ruang angkasa dan terkait bentuk pertanggungjawaban negara terhadap *cyber espionage*.

METODE

Penelitian ini akan menggunakan *statute*, *conceptual*, dan *comparative approaches*. *Statute approach* dan *conceptual approach* akan digunakan dalam pembahasan mengenai metode dan karakteristik *cyber espionage* dan pengaturannya dalam hukum internasional. Selain itu, penelitian ini juga akan membahas tanggung jawab negara terkait tindakan *cyber espionage* yang dilakukan Iran, khususnya di sektor *aerospace*. Terakhir, kasus yang melibatkan UNC1549, kelompok yang berafiliasi dengan Iran, akan dianalisis menggunakan *comparative approach* dengan membandingkannya dengan kasus yang terjadi di Amerika Serikat pada tahun 2013, yang dilakukan oleh kelompok dari Rusia dan Cina.

HASIL DAN PEMBAHASAN

Pengaturan *Cyber Espionage* dalam Hukum Internasional

Pengumpulan informasi merupakan aspek utama dari *cyber espionage*, seperti yang dinyatakan dalam penjelasan Pasal 32 Tallinn Manual dan NATO. Dalam praktiknya, pelaku

cyber espionage menggunakan berbagai macam metode yang sangat bervariasi. Tujuan utamanya adalah untuk mendapatkan informasi penting atau rahasia dari target mereka tanpa adanya izin. Beberapa metode yang dapat digunakan untuk melakukan *cyber espionage* antara lain menggunakan *malware* seperti *viruses* dan *trojans* untuk menyusup ke dalam sistem target, menjalankan serangan *phising* untuk mendapatkan akses ke informasi rahasia dengan cara memanipulasi pengguna, dan lain sebagainya. Selain itu, karakteristik yang dapat diklasifikasikan dalam *cyber-attack*, khususnya dalam *cyber espionage*, adalah sebagai berikut:

a. Akses yang tidak sah,
b. Tanpa kekerasan,
c. Menggunakan peralatan, teknologi, dan memanfaatkan jaringan telematika global (yang meliputi informatika, media, dan telekomunikasi),
d. Dibandingkan dengan kejahatan tradisional, tindakan ini biasanya menyebabkan kerugian yang lebih nyata dan immaterial (waktu, nilai, komoditas, uang, jasa, martabat, dan kerahasiaan informasi(Dewi, 2022).

Cyber espionage menggunakan berbagai metode untuk melakukan *cyber espionage*, termasuk *malware*, *phishing*, *ransomware*, dan pemblokiran layanan. Hal ini menggambarkan bagaimana, selain menjadi masalah teknis, *cyber espionage* memiliki dampak yang jauh lebih luas terhadap ekonomi, infrastruktur teknologi informasi, dan keamanan nasional suatu negara. *Cyber espionage* sulit dideteksi dan lebih sulit untuk menuntut mereka yang terlibat di dalamnya. Mengingat tidak adanya bukti yang cukup untuk menghubungkan serangan dengan pihak tertentu, negara yang dicurigai sebagai pencetus serangan sering kali perlu ikut membantu dalam menyelesaikan masalah ini. Hal ini membuat perlindungan infrastruktur digital dan informasi menjadi semakin penting, oleh karena itu, sangat penting untuk melakukan langkah-langkah keamanan *cyber* yang kuat. *Cyber security* adalah keamanan yang dilakukan di dunia maya karena adanya fakta bahwa terdapat tingkat kejahatan di *cyberspace*, sekumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik unggulan, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* (Nia Wati et al., 2023).

Selain itu, dengan mempertimbangkan metode dan karakteristiknya, *cyber espionage* memiliki keunikan dalam beberapa hal yang signifikan. Mengingat operasi digital dapat dimulai dari dan menargetkan hampir semua tempat di dunia, *cyber espionage* dapat menjangkau hampir semua lokasi. Selain itu, karena "*Internet of Things*" terus tumbuh dan berkembang, menghubungkan setiap aspek masyarakat melalui jaringan data, *cyber espionage* sekarang menjadi ancaman yang signifikan bagi infrastruktur manusia. Dalam konteks tata kelola Internet, istilah "*cyber sovereignty*" sering digunakan untuk menggambarkan niat suatu negara untuk menjalankan dan mempertahankan kontrol atas domain internet di dalam batas-batasnya, termasuk aktivitas politik, ekonomi, budaya, dan teknologi. Laporan *United Nations Group of Governmental Experts on Development* (selanjutnya disebut UN GGE) tahun 2015 menyatakan: "Kedaulatan negara dan norma serta prinsip internasional yang mengalir dari kedaulatan berlaku untuk pelaksanaan kegiatan terkait TIK oleh negara dan yurisdiksi mereka atas infrastruktur TIK di dalam wilayah mereka." (Assembly, 2015).

Oleh karena itu, terlihat jelas bahwa pemasangan *malware* telah melanggar kewajiban negara di bawah hukum internasional untuk memperoleh informasi dalam *cyber espionage*. Tindakan ilegal ini pada dasarnya mengancam perlindungan informasi pribadi, keamanan nasional, *non-intervention*, dan kedaulatan. Pelaku *cyber espionage* membahayakan stabilitas hubungan internasional dan melanggar otonomi negara atau entitas lain dengan memasuki sistem negara atau entitas lain secara diam-diam. Berdasarkan argumentasi yang diberikan, aktivitas tersebut dapat diklasifikasikan sebagai *cyber espionage* jika dikaitkan dengan kasus UNC1549.

Berdasarkan penjelasan di atas, jika dikaitkan dengan kasus UNC1549, tindakan mereka dapat dikategorikan sebagai *cyber espionage*. Tindakan mereka dapat dilihat dari penanaman *malware* untuk mengakses data login terhadap perusahaan pelayaran Israel dan perusahaan kedirgantaraan dan pertahanan Amerika Serikat. Meskipun tidak ada aturan yang tegas mengenai *cyber espionage* dalam hukum internasional, namun tindakan mereka dapat diklasifikasikan sebagai tindakan yang melanggar kedaulatan negara dan perlindungan data pribadi suatu negara. Sehingga mereka dapat dimintai pertanggungjawaban atas tindakan mereka menggunakan hukum nasional negara yang menjadi sasaran.

Pertanggungjawaban Negara terkait Tindakan *Cyber Espionage*

State responsibility dalam hukum internasional mengacu pada prinsip-prinsip yang mengatur kapan dan bagaimana sebuah negara dimintai pertanggungjawaban atas pelanggaran kewajiban internasionalnya. Prinsip-prinsip ini mencakup keadaan-keadaan di mana sebuah negara dianggap telah melakukan tindakan yang melanggar hukum internasional dan konsekuensi-konsekuensi hukum yang menyertainya. *The International Law Commission* (selanjutnya disebut ILC) telah mengkodifikasikan prinsip-prinsip ini dalam *Responsibility of States for Internationally Wrongful Acts* (selanjutnya disebut ARSIWA). Pada umumnya, ketentuan-ketentuan dalam ARSIWA bersifat umum dan terdapat pembahasan mengenai kedudukan instrumen ini di masa depan, dan apakah perlu ada traktat mengenai state responsibility, masih terus berlangsung (Paddeu, 2017). Peraturan tentang *state responsibility* mengatur tiga bidang yang luas. Pertama, hukum ini mencakup pedoman untuk menentukan apakah suatu negara telah melakukan tindakan yang salah secara internasional. Pedoman ini memuat tentang penentuan kesalahan atas tindakan yang dilakukan oleh negara, pelanggaran kewajiban internasional, penentuan kapan sebuah negara bertanggung jawab atas kesalahan negara lain, dan aturan-aturan yang berkaitan dengan pertahanan. Kedua, hukum ini juga mengatur apa yang menjadi tanggung jawab negara karena melanggar kewajiban internasionalnya, yang merupakan hasil dari tindakan yang melanggar hukum internasional. Pengaturan mengenai dampak yang diakibatkan oleh pelanggaran berat terhadap aturan-aturan pencegahan hukum internasional termasuk di dalamnya, seperti halnya kategori umum dari *cessation* dan *reparation* (dalam tiga bentuk yaitu restitusi, ganti rugi, dan kepuasan). Ketiga, mengatur isu-isu yang berkaitan dengan pelaksanaan tanggung jawab Negara, termasuk kewenangan untuk menuntut pertanggungjawaban atas tindakan yang melanggar hukum internasional, serta langkah-langkah penegakan hukum yang spesifik seperti penanggulangan.

Berdasarkan Pasal 2, terdapat dua unsur yang dapat diklasifikasikan sebagai perbuatan melawan hukum internasional dari suatu Negara, yaitu: a) Dapat diatribusikan kepada Negara menurut hukum internasional; dan b) Merupakan pelanggaran terhadap kewajiban internasional Negara. Unsur pertama mengenai atribusi kepada Negara dijelaskan dengan persyaratan bahwa tindakan tersebut dilakukan oleh orang atau entitas yang tindakannya secara hukum dapat dianggap sebagai tindakan Negara menurut hukum internasional. Menurut hukum internasional, negara dapat dimintai pertanggungjawaban atas tindakan entitas yang berbeda. Tindakan yang dilakukan oleh badan-badan resmi negara, termasuk badan legislatif, eksekutif, yudikatif, dan cabang-cabang lainnya, pada dasarnya merupakan tanggung jawab negara. Selain itu, pendelegasian fungsi-fungsi negara tercermin dalam tindakan entitas yang telah diberi wewenang oleh negara untuk melaksanakan aspek-aspek tertentu dari otoritas pemerintahan. Selain itu, jika aktor non-negara bertindak atas nama negara dan melakukannya di bawah arahan, kontrol, atau instruksi negara, negara masih dapat dimintai pertanggungjawaban atas tindakan mereka. Hal ini memperluas cakupan *state responsibility* dengan memasukkan tindakan yang dilakukan oleh orang atau organisasi. Kerangka kerja ini memastikan bahwa negara tidak dapat menghindari tanggung jawab atas tindakan-tindakan yang salah secara internasional dengan mengalihkan tindakan-tindakan tersebut kepada pihak ketiga atau entitas non-negara.

Unsur kedua adalah pelanggaran terhadap kewajiban internasional negara. Apakah tindakan suatu negara melanggar kewajiban internasional pada dasarnya tergantung pada isi dari norma hukum primer tertentu, yang mungkin berasal dari salah satu sumber hukum internasional. Agar suatu pelanggaran dapat terjadi, norma tersebut harus sudah berlaku dan dapat diterapkan pada negara tersebut ketika perilaku tersebut terjadi. Namun, aspek temporal menjadi lebih kompleks ketika pelanggaran yang sedang berlangsung atau beberapa tindakan gabungan merupakan sebuah pelanggaran.

Aktivitas tersebut dapat dikaitkan dengan negara Iran jika dihubungkan dengan kasus UNC1549. UNC1549 dianggap sebagai kelompok peretas yang berafiliasi dengan Iran. Tindakan mereka, yang melanggar kedaulatan negara dan norma-norma *non-intervention*, merupakan pelanggaran terang-terangan terhadap hukum internasional, termasuk *cyber espionage*. Setiap negara dapat mengatur urusan dalam negerinya sendiri tanpa campur tangan pihak luar. Hal ini dianggap sebagai pelanggaran kedaulatan negara ketika sebuah negara atau organisasi yang didukung negara, seperti UNC1549, terlibat dalam *cyber espionage* terhadap infrastruktur vital atau informasi pribadi negara lain.

Aktivitas semacam itu dapat dianggap sebagai tindakan agresif yang membahayakan integritas politik dan teritorial negara yang menjadi sasaran. Negara juga tidak dapat mencampuri urusan internal negara lain, sesuai dengan prinsip *non-intervention*. Kegiatan yang berkaitan dengan *cyber espionage*, terutama yang memiliki tujuan militer atau politik jelas melanggar aturan ini. Pencurian rahasia perusahaan, perusahaan pertahanan, kedirgantaraan dan penerbangan atau data pemerintah adalah contoh kegiatan yang merusak hubungan internasional, mengacaukan dunia, dan merugikan negara yang menjadi sasaran. Prinsip di balik kedua syarat ini adalah untuk memastikan bahwa negara-negara, khususnya Iran, bertanggung jawab atas tindakan yang benar-benar mencerminkan kegagalan atau ketidakberhasilan mereka dan bahwa tindakan ini melanggar norma dan kesepakatan internasional yang telah ditetapkan.

Pengaturan dan Upaya Penanggulangan *Cyber Espionage* di Wilayah *Aerospace*

Kemampuan negara lain untuk mengeksplorasi dan memanfaatkan ruang angkasa secara bebas dapat terhambat oleh *cyber-attacks* di ruang angkasa, khususnya *cyber espionage*, yang membahayakan operasi ruang angkasa dan benda-benda lain di ruang udara atau di Bumi. Selain itu, hal ini juga menyebabkan kerugian. Namun, hukum internasional dan nasional harus menangani masalah ini secara tepat. Salah satu penjelasannya mungkin adalah kurangnya kejelasan tentang peran negara dalam mempertahankan operasi ruang angkasa dari serangan siber. Pasal VI dan VII dari *the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, menetapkan kewajiban negara untuk kegiatan ruang angkasanya (selanjutnya disebut *Outer Space Treaty*).

Pasal VI *Outer Space Treaty* menyatakan bahwa "Negara-negara Pihak dalam Perjanjian harus memikul tanggung jawab internasional atas kegiatan nasional ....., apakah kegiatan tersebut dilakukan oleh lembaga pemerintah atau lembaga non-pemerintah" (Article VI Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 1966). Hal ini merupakan perbedaan dari pedoman standar hukum internasional untuk menentukan negara yang bertanggung jawab. Klausul terobosan ini meminta pertanggungjawaban langsung dari para Pihak dalam *Outer Space Treaty* untuk setiap pelanggaran terhadap ketentuan-ketentuannya, termasuk yang dilakukan oleh organisasi non-pemerintah, tanpa mempertimbangkan atribusi (Cheng, 1998). Negara memikul tanggung jawab ketika pelanggaran dilakukan, bukan ketika negara tidak mampu menghentikan, menekan, atau mencegah pelanggaran (Cheng, 1998). Oleh karena itu, menentukan sejauh mana aktivitas ruang angkasa nasional suatu negara pihak merupakan tantangan saat ini; suatu negara perlu bersikap terbuka terhadap aktivitas ruang angkasanya.

The International Civil Aviation Organization's (selanjutnya disebut ICAO) telah bekerja dalam bidang *cyber security* penerbangan sejak tahun 2000-an. Inisiatif dan pembicaraan dari ICAO diperluas hingga mencakup seluruh industri transportasi udara seiring dengan meningkatnya ketergantungan sektor ini pada teknologi. Upaya yang dilakukan oleh ICAO dalam hal *cyber security* penerbangan sangat luas dan kompleks. Dalam rangka membantu negara dan pemangku kepentingan lainnya dalam menangani *cyber security* dalam penerbangan sipil dan melaksanakan tanggung jawab mereka di bawah Standar ICAO dan Praktik yang Disarankan terkait *cyber security* penerbangan, ICAO terus menerbitkan materi panduan. Hingga saat ini, materi panduan berikut ini telah diterbitkan oleh ICAO (Aviation Organization, n.d.). *The ICAO Aviation Security Manual (Doc 8973-Restricted),* memandu negara-negara tentang cara mematuhi Standar 4.9.1 dari Lampiran 17-Keamanan Penerbangan. Selain itu, *the Air Traffic Management Security Manual (Doc 9985 – Restricted)* memberikan strategi keamanan menyeluruh untuk lingkungan *Air Traffic Management* dengan memasukkan pedoman untuk keamanan siber dan keamanan fisik. *The guidelines on the Traffic Light Protocol* (selanjutnya disebut TLP*),* yang memungkinkan pertukaran informasi *cyber security*, merupakan sumber daya tambahan untuk hal ini. TLP mengurangi kemungkinan kesalahan manusia yang menyebabkan penyebaran informasi sensitif yang tidak disengaja di luar pihak yang dituju dengan menyediakan cara yang mudah dipahami bagi penyedia informasi untuk menyampaikan batasan-batasan pada kemampuan penerima untuk berbagi informasi sensitif.

Materi dalam *Cybersecurity Policy Guidance* berfokus pada penguatan dan perlindungan infrastruktur penting penerbangan sipil internasional terhadap *cyber-attacks*. Panduan ini menyoroti betapa pentingnya bagi penerbangan sipil dan otoritas eksternal lainnya - seperti militer, *cyber security*, dan badan keamanan nasional - untuk bekerja sama secara multilateral. Laporan ini juga dilengkapi dengan kerangka kerja untuk membantu menciptakan kebijakan *cyber security* nasional untuk penerbangan. Untuk mendukung hal ini lebih lanjut, keberhasilan industri dalam menciptakan lingkungan keselamatan dan keamanan yang kuat dimanfaatkan dalam pedoman budaya *cyber security* dalam penerbangan sipil. Untuk mempermudah pengembangan dan penerapan *cyber security* organisasi yang kuat dalam penerbangan sipil, pedoman ini menggabungkan komponen penting dari sejumlah faktor *cyber security* yang sudah mapan dengan faktor *cybersecurity* yang unik untuk penerbangan.

Hal ini bertujuan untuk mengurangi dampak serangan terhadap *Airport Information Resource Management Systems* (selanjutnya disebut AIRMS), sistem manajemen sumber daya berbasis cloud yang digunakan oleh bandara tertentu untuk keperluan perusahaan. Clark and Hakim (Clark & Hakim, 2016), Martellini (Martellini, 2013), dan Singer and Friedman (Singer & Friedman, 2014) menyarankan untuk menggunakan klasifikasi intelijen bandara, yang dikategorikan sesuai dengan praktik teknologi terbaik untuk masalah keamanan tingkat tinggi, guna mempertahankan infrastruktur dan aset bandara dari *cyber-attacks*. Pada kenyataannya, strategi ini didasarkan pada lingkungan yang kuat dari *cyber security* dan mencakup pembaruan sistem dan anti-virus secara rutin, pelatihan siber untuk karyawan baru, pencadangan data yang sering, dan manajemen kata sandi.

Untuk mencegah terulangnya insiden *cyber espionage* di sektor kedirgantaraan, seperti yang dilakukan oleh kelompok UNC1549, AS dapat mengambil beberapa langkah strategis. Pertama, memperkuat *cyber security* sangat penting. Hal ini dapat dicapai dengan memperbarui semua sistem dan perangkat lunak secara teratur dengan pembaruan keamanan terbaru dan menggunakan enkripsi data yang kuat untuk melindungi informasi sensitif selama pengiriman dan penyimpanan. Selain itu, menerapkan *multi-factor authentication* (selanjutnya disebut MFA) untuk semua akses ke sistem penting sangat penting untuk mengurangi risiko akses yang tidak sah.

Meningkatkan kesadaran dan pelatihan bagi karyawan juga merupakan kuncinya. Memberikan pelatihan rutin tentang kesadaran *cyber security* dan teknik rekayasa sosial serta melakukan simulasi serangan secara berkala akan membantu meningkatkan kesiapan dan respons karyawan terhadap ancaman siber. Selain itu, meningkatkan pemantauan dan deteksi dini dengan menggunakan sistem pemantauan keamanan yang canggih dan mengintegrasikan intelijen ancaman dapat membantu mendeteksi dengan cepat aktivitas yang mencurigakan.

KESIMPULAN

Tindakan yang dilakukan oleh kelompok UNC1549 diklasifikasikan sebagai *cyber espionage*, di mana metode yang digunakan adalah penanaman *malware*. Karakteristik *cyber espionage* meliputi akses yang tidak sah dan penggunaan teknologi. Pelaku *cyber espionage* seringkali sulit dilacak, dan kerangka hukum internasional yang ada saat ini tidak secara komprehensif menangani masalah ini. Namun, tindakan *cyber espionage* dapat diklasifikasikan sebagai pelanggaran terhadap prinsip-prinsip kedaulatan negara dan *non-intervention*.

Selain langkah-langkah yang telah disebutkan sebelumnya, AS dan Israel dapat membuat peraturan khusus dalam hukum nasional untuk mencegah munculnya aktivitas *cyber espionage*. Meningkatkan kemampuan penegakan hukum melalui pembentukan unit siber khusus dan memperkuat kolaborasi dengan badan-badan intelijen juga sangat penting. Selain itu, dengan memperkuat kerja sama internasional melalui perjanjian ekstradisi dan mengadvokasi standar *cyber security* global dapat memastikan bahwa penjahat siber dapat dituntut di mana pun lokasinya.

REFERENSI

Article VI Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (1966).

Assembly, G. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations. https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf?token=5vhktEHRNAAHURNb0j&fe=true

Aviation Organization, I. C. (n.d.). *Guidance Material*. Retrieved May 10, 2024, from https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

Cheng, B. (1998). Article VI of the 1967 Space Treaty revisited-'International responsibility', 'national activities', and 'the appropriate State. *Journal of Space Law*, *26*(1), 7–32.

Clark, R. M., & Hakim, S. (2016). *Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security*. Springer eBooks.

Dewi, M. C. (2022). Cyber Espionage in National and Global Perspective: How Indonesia Deal With This Issue? *International Law Discourse in Southeast Asia*, *1*(1), 1–22.

Donalds, C., & Osei-Bryson, K.-M. (2019). Toward a Cybercrime Classification Ontology: A Knowledge-based Approach. *Computers in Human Behavior*, *92*, 403–418.

Martellini, M. (2013). *Cyber Security Deterrence and IT Protection for Critical Infrastructures*. Springer Cham.

Nia Wati, L. T. C., Syahidullhaq, M. S., & Pramono, B. K. (2023). Comparative Analysis of Cyber Sovereignty: Case From Indonesia and Iran. *JUSS (Jurnal Sosial Soedirman)*, *6*(1).

Paddeu, F. (2017). To Convene or Not to Convene? The Future Status of the Articles on State Responsibility: Recent Developments. *Max Planck Yearbook of United Nations Law*, *21*, 83–123.

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press eBooks.

Schmitt, M. N. (2017a). *Cyber Operations Not per Se Regulated by International Law*. Cambridge University Press eBooks.

Schmitt, M. N. (2017b). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar*. Oxford University Press eBooks.

Warminsky, J. (2024, February 29). Suspected Iranian Cyber-espionage Campaign Targets Middle East Aerospace, Defense Industries. *Record Future News*. https://therecord.media/iran-cyber-espionage-campaign-targeting-middle-east-defense-aerospace.