Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024

E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id

Kebijakan dan Regulasi Spionase Siber di Indonesia

Mohamad Djafar Sodiq
Supono
Fahzal Hendri
Eci Marisna Ningsih
Universitas Jayabaya
Pos-el: emdeshodiq@pascajayabaya.ac.id

DOI: 10.32884/ideas.v10i4.1909

Abstrak

Spionase siber adalah kegiatan terlarang yang memanfaatkan jaringan internet untuk mengawasi entitas lain dengan cara menembus jaringan komputer mereka. Penelitian ini bertujuan untuk memaparkan secara komparatif kebijakan dan regulasi terkait spionase siber yang diterapkan oleh Indonesia dan Jerman. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, studi kasus, juga perbandingan hukum (comparative approach) dengan rumusan masalah bagaimana kebijakan dan regulasi terkait spionase siber yang diterapkan oleh Indonesia dan Jerman? Hasil dari penelitian ini menunjukkan bahwa Indonesia menunjukkan kekuatan dalam keamanan siber, yang ditandai dengan meningkatnya kesadaran terhadap masalah keamanan siber, peran kepemimpinannya di Asia Tenggara dalam domain ini, dan transformasi digitalnya yang cepat yang memfasilitasi adopsi langkah-langkah keamanan siber tingkat lanjut. Namun demikian, Indonesia bergulat dengan berbagai tantangan seperti kurangnya tenaga profesional keamanan siber yang terampil dan sumber daya yang terbatas untuk menerapkan strategi keamanan siber yang komprehensif, serta kerangka kerja peraturan dan hukum yang membutuhkan penyempurnaan dan adaptasi yang berkelanjutan. Sebaliknya, kerangka hukum Jerman yang kuat berperan sebagai benteng pertahanan terhadap ancaman siber. Ditambah dengan keahlian teknis yang substansial dan pendekatan inovatif terhadap keamanan siber, Jerman diuntungkan oleh kerangka hukum yang transparan yang memastikan kejelasan dan efisiensi dalam menangani ancaman siber. Meskipun demikian, Jerman juga menghadapi kelemahan, seperti ketergantungan pada teknologi dan rantai pasokan eksternal, prevalensi ancaman siber yang canggih, dan tantangan untuk menyelaraskan praktik keamanan siber di berbagai sektor.

Kata Kunci

Kebijakan regulasi, spionase siber, Indonesia, Jerman

Abstract

Cyber espionage is an illicit activity that utilizes the internet network to monitor other entities by penetrating their computer networks. This research aims to provide a comparative explanation of the policies and regulations related to cyber espionage implemented in Indonesia and Germany. This research uses normative legal research methods with a statutory and regulatory approach, case studies, as well as comparative law (comparative approach) with a problem formulation of what policies and regulations related to cyber espionage are implemented in Indonesia and Germany? The results of this research show that Indonesia is showing strength in cyber security, characterized by increasing awareness of cyber security issues, its leadership role in Southeast Asia in this domain, and its rapid digital transformation

E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id
Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024
that is driving the adoption of further levels of cyber security measures. However, Indonesia is grappling with various challenges such as a lack of skilled cybersecurity professionals and limited resources to implement a comprehensive cybersecurity strategy, as well as a legal and regulatory framework that requires continuous refinement and adaptation. In contrast, Germany's strong legal framework acts as a bulwark against cyber threats. Coupled with substantial technical expertise and an innovative approach to cyber security, Germany benefits from a transparent legal framework that ensures clarity and efficiency in dealing with cyber threats. Nonetheless, Germany also faces weaknesses, such as reliance on external technology and supply chains, the prevalence of sophisticated cyber threats, and the challenge of harmonizing cybersecurity practices across sectors.
Keywords
Regulatory policy, comparison, Indonesia, Germany

Pendahuluan

Perkembangan teknologi telah berhasil menunjukkan adanya pergantian bentuk-bentuk teknologi komunikasi yang terbaru dan informasi tradisional dengan media yang lebih baru dan lebih efisien (Nugroho, 2020). Salah satu dampak positifnya adalah peningkatan kecepatan dan kenyamanan di berbagai ranah. Misalnya, teknologi yang berhasil memfasilitasi pemilik bisnis dalam menghasilkan pendapatan melalui pemanfaatan beragam alat pemasaran, termasuk platform media sosial (Solomon & Klyton, 2020). Selain itu, perangkat inovatif seperti smartphone dan tablet telah menyederhanakan cara orang tua untuk tetap berhubungan dengan kerabat jauh (Drouin dkk., 2020). Bukan hanya itu, teknologi telah memberdayakan individu untuk berkomunikasi dengan orang lain secara global, mendobrak hambatan geografis, dan mendorong konektivitas global (Danping dkk., 2018).

Namun, munculnya teknologi baru mendatangkan tantangan baru bagi masyarakat (Khan dkk., 2020). Seiring dengan meningkatnya ketergantungan terhadap teknologi informasi, insiden kejahatan berbasis Internet, yang biasa disebut sebagai kejahatan dunia maya, diperkirakan akan meningkat (Caldwell dkk., 2020). Kegiatan kriminal ini memanfaatkan teknologi informasi sebagai media eksekusi. Dengan kemajuan teknologi, skala dan dampak kejahatan siber meluas dengan cepat, mempengaruhi individu, kelompok, dan negara (Lallie dkk., 2021). Kejahatan ini disebut spionase siber.

Spionase siber adalah kegiatan terlarang yang memanfaatkan jaringan internet untuk mengawasi entitas lain dengan cara menembus jaringan komputer mereka. Bentuk kejahatan ini sering kali menargetkan pesaing bisnis untuk mengakses dokumen atau data penting yang tersimpan di dalam sistem komputer mereka (Maskun dkk., 2020).

Selain itu, spionase siber sering kali melibatkan suatu negara yang bertindak sebagai pelaku. Tujuannya untuk mencuri informasi penting dan rahasia dari negara lain. Hal ini merupakan iterasi modern dari spionase tradisional, yang dilakukan untuk mengumpulkan data sensitif atau intelijen dari negara lawan. Informasi yang diperoleh digunakan untuk memprediksi tindakan negara lawan, terutama selama konflik. Akhirnya, operasi semacam itu menjadi hal yang biasa.

Kemajuan teknologi informasi telah memfasilitasi kemudahan dan kelaziman penyadapan untuk tujuan spionase di berbagai negara (Botua dkk., 2020). Bentuk spionase siber ini telah menjadi semakin meluas. Sebagian karena tidak memadainya peraturan yang mengatur

Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024
E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id

kegiatan penyadapan. Sangat penting untuk membedakan antara spionase yang dilakukan melalui konflik bersenjata dan spionase berbasis penyadapan yang terjadi di luar konteks perang fisik. Kurangnya sikap tegas dan kebijakan yang komprehensif dari pemerintah Indonesia mengenai spionase siber menunjukkan adanya kekurangan yang signifikan dalam menangani masalah ini secara efektif (Dewi, 2022).

Penyadapan, terutama di era modern, dianggap sebagai bentuk spionase karena risiko pendeteksian yang relatif rendah oleh target sehingga perlu digarisbawahi bahaya yang melekat pada spionase asing. Hal ini menimbulkan ancaman yang signifikan terhadap keamanan dan pertahanan nasional dengan potensi menyebabkan kerusakan dan destabilisasi (Rawat dkk., 2021). Contoh kasus spionase termasuk tindakan yang dilakukan oleh Amerika Serikat dan Australia terhadap pemerintah Indonesia. Marciano Norman, Kepala Badan Intelijen Negara (BIN), melaporkan bahwa Australia telah menyadap pembicaraan telepon beberapa pemimpin Indonesia dari tahun 2007 hingga 2009 (Mustameer, 2022).

Fenomena spionase tidak hanya terjadi di Indonesia; negara-negara lain, termasuk Jerman, juga menghadapi tantangan serupa. Pada tahun 2020, Nobelium, sebuah kelompok yang terkait dengan pemerintah Rusia, memprakarsai kampanye phishing tingkat lanjut yang menargetkan kementerian pemerintah Jerman dan entitas infrastruktur penting. Melalui kombinasi email spear-phishing dan serangan rantai pasokan, APT29 berhasil menyusup ke dalam sistem, yaitu menyusupkan informasi sensitif seperti dokumen pemerintah dan rencana strategis (BBC News, nd).

Selain badan-badan pemerintah, perusahaan Jerman dan lembaga penelitian telah menjadi fokus Ocean Lotus, kelompok spionase siber yang diyakini beroperasi di bawah naungan pemerintah Tiongkok. Memanfaatkan taktik seperti serangan spear-phishing, malware, dan email phishing, Ocean Lotus bertujuan untuk menyalahgunakan kekayaan intelektual dan rahasia dagang. Pada tahun 2018, APT32 terlibat dalam serangan siber terhadap perusahaan farmasi raksasa Jerman, Bayer, yang menyebabkan data rahasia mereka dibobol (Ray & Hayashi, 2019). Kasus ini menggarisbawahi tantangan rumit yang dihadirkan oleh persaingan global di era digital. Kemampuan teknologi informasi dan komunikasi yang canggih dapat dimanfaatkan oleh berbagai aktor, termasuk agen spionase.

Skenario ini semakin menunjukkan kerentanan Indonesia sebagai target spionase yang potensial, yang sebagian besar disebabkan oleh kekurangan dalam kerangka hukumnya (Iqbal & Jaya, 2021). Spionase yang difasilitasi oleh penyadapan dan pemanfaatan teknologi membuat batas-batas negara menjadi tidak relevan, sehingga mengaburkan batas-batas kedaulatan. Informasi dan data sensitif dapat diakses tanpa batasan spasial dan temporal, sehingga menimbulkan ancaman yang signifikan terhadap kedaulatan nasional (Cristani, 2021). Akibatnya, muncul pertanyaan kritis mengenai kecukupan hukum Indonesia dalam menangani spionase siber dan langkah-langkah yang diterapkan Indonesia untuk menangkal ancaman tersebut, yang berpotensi membahayakan stabilitas pertahanan dan keamanan negara.

Sebelumnya, sudah ada beberapa penelitian tentang keamanan dunia maya. Sebagai contoh, Iqbal dan Jaya membahas evolusi kejahatan siber di Indonesia bersama dengan peraturan yang ada (2021). Raharjo dkk. menekankan pada birokrasi penegakan hukum

E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id
Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024

terhadap kejahatan siber di Indonesia, terutama kelemahan model pencegahan kejahatan yang ada dan terintegrasi dalam sistem peradilan pidana (2022).

Dalam eksplorasi yang lebih spesifik mengenai spionase siber, Mustameer telah melakukan penelitian tentang Penegakan Hukum Nasional dan Hukum Internasional terhadap Kejahatan Spionase Siber di Era Society 5.0. Mustameer menguraikan cara spionase siber menjadi ancaman bagi pertahanan dan keamanan di era Society 5.0 dan kesiapan kerangka hukum internasional dan nasional Indonesia untuk menghadapi ancaman tersebut (Mustameer, 2022). Penelitian terkait lainnya dilakukan oleh Dewi yang mengeksplorasi dimensi hukum spionase siber, termasuk kasus-kasus nasional dan internasional serta kerangka hukumnya (2022).

Penelitian ini berusaha membandingkan kerangka kerja legislatif Indonesia dan strateginya dalam melawan serangan siber, khususnya spionase siber, dengan Jerman. Perbandingan ini sangat penting untuk menilai efektivitas peraturan dan strategi hukum Indonesia saat ini dalam melawan kejahatan siber. Pemilihan Jerman sebagai subjek perbandingan dikarenakan negara ini merupakan negara maju dan sering mengalami serangan siber dari negara-negara seperti Rusia, Cina, Korea Utara, dan lainnya.

Dengan perkembangan dunia maya atau dunia digital yang cepat, kegiatan kriminal telah melampaui batas-batas fisik dan merambah ke ranah digital. Meskipun kemajuan teknologi memberikan hasil yang positif, dunia maya tetap rentan terhadap berbagai bentuk serangan, termasuk virus dan peretasan yang dilakukan oleh individu atau kelompok yang memiliki niat jahat.

Kejahatan dunia maya telah muncul sebagai tantangan yang signifikan, terutama karena sulitnya mengidentifikasi pelaku yang sering beroperasi di balik tabir anonimitas. Keahlian khusus sangat penting untuk menavigasi kompleksitas dunia maya dan mendeteksi kejahatan dunia maya secara efektif. Tantangan untuk mengekang kejahatan ini telah berkontribusi pada peningkatan yang konsisten dalam tingkat kejahatan siber, seperti yang dilaporkan oleh Badan Intelijen Negara.

Metode

penelitian ini menggunakan metode hukum normatif, dengan menggunakan pendekatan masalah multidimensi yang meliputi pendekatan perundang-undangan, konseptual, dan perbandingan. Bahan-bahan hukum yang mendukung penelitian ini dikategorikan ke dalam jenis bahan hukum primer dan sekunder. Bahan hukum primer terdiri atas peraturan perundang-undangan dan putusan pengadilan yang menjadi yurisprudensi, sedangkan bahan hukum sekunder meliputi publikasi hukum tidak resmi seperti buku, majalah, jurnal hukum, dan penelitian hukum yang relevan. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), dengan pengolahan bahan hukum yang menganut metode deduktif. Analisis dalam makalah ini dilakukan dengan menggunakan teknik analisis bahan hukum secara deskriptif kualitatif, yang melibatkan penafsiran secara sistematis dan komprehensif untuk menjelaskan temuan penelitian.

Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024
E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id

Hasil dan Pembahasan

Hasil

Indonesia telah memberlakukan berbagai kebijakan dan peraturan untuk memerangi ancaman spionase siber yang terus meningkat dan menjaga keamanan nasional. Langkah-langkah ini mencakup kerangka hukum yang komprehensif, inisiatif kebijakan strategis, dan mekanisme peraturan yang dirancang untuk meningkatkan kemampuan keamanan siber dan menangkal kegiatan spionase siber (Chotimah, 2019). Berikut ini adalah ikhtisar kebijakan dan peraturan tersebut.

Kerangka hukum utama yang mengatur dunia maya di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008, juncto Undang-Undang Nomor 16 Tahun 2019 tentang Informasi dan Transaksi Elektronik, yang umumnya dikenal sebagai Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

Spionase siber secara tidak langsung dirujuk dalam Pasal 31 UU ITE. Namun, dengan diberlakukannya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP), spionase siber sekarang secara eksplisit diatur dalam Pasal 258 dan 259 KUHP. Ketentuan tersebut menyatakan bahwa setiap orang yang secara tanpa hak atau melawan hukum melakukan kegiatan mendengarkan, merekam, melakukan pengalihan, memindahkan, mengubah, menghambat, dan/atau melakukan pendokumentasian transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dapat dipidana dengan pidana penjara paling lama sepuluh tahun atau denda paling banyak Rp200 juta (UU No. 1, 2023). Selain itu, orang yang menyiarkan atau menyebarluaskan hasil rekaman tersebut di atas dapat dipidana dengan pidana penjara paling lama tujuh tahun atau denda paling banyak Rp200 juta (UU No. 1, 2023).

Selain merekam aktivitas dan percakapan target, spionase siber juga bisa dilakukan dengan cara menembus atau membobol sistem informasi korban secara paksa. Melalui sistem ini, pelaku mencuri data rahasia yang sangat penting, kemudian diproses dan dianalisis untuk tujuan tertentu. Tindakan yang digambarkan ini sebagai metode kedua spionase siber dan diatur dalam KUHP tahun 2023, khususnya dalam Pasal 332—335.

Berdasarkan Pasal 332, akses tanpa izin ke komputer atau sistem elektronik orang lain sangat dilarang. Individu yang dengan sengaja dan melawan hukum mengakses sistem tersebut dapat menghadapi hukuman hingga enam tahun penjara atau denda hingga 500 juta Rupiah. Lebih lanjut, jika tujuan dari akses sistem tersebut untuk mendapatkan informasi atau dokumen elektronik, hukumannya meningkat menjadi maksimal tujuh tahun penjara atau denda paling banyak 500 juta Rupiah (UU No. 1, 2023).

Pasal 333 mengatur bahwa setiap orang yang tanpa izin yang sah atau di luar kewenangannya menggunakan atau mengakses komputer atau sistem elektronik dengan tujuan untuk mendapatkan, mengubah, merusak, atau menghapus informasi yang berkaitan dengan pertahanan negara atau hubungan internasional dan berpotensi mengganggu atau merugikan negara atau hubungannya dengan badan hukum internasional dapat dipidana dengan pidana maksimal tujuh tahun penjara atau denda paling banyak Rp200.000.000,00 (dua ratus juta rupiah).

E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id
Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024

Lebih lanjut, Pasal 335 mengatur bahwa setiap orang yang tanpa izin yang sah menggunakan atau mengakses komputer atau sistem elektronik dengan cara apa pun, dengan maksud untuk mendapatkan, mengubah, merusak, atau menghapus informasi yang diklasifikasikan atau dilindungi karena kepentingannya, diancam dengan pidana penjara paling lama dua belas tahun atau denda paling banyak lima miliar rupiah (UU No. 1, 2023).

UU ITE memainkan peran penting di era digital sehingga penting melakukan pengawasan penggunaan informasi elektronik agar memperkuat privasi dan perlindungan data pribadi (Lambi, 2023). Undang-undang tentang spionase siber di Indonesia diuraikan secara komprehensif yang membahas berbagai aspek transaksi elektronik dan aktivitas siber (Bawono, 2019). Undang-undang ini mengkriminalisasi aktivitas siber seperti akses sistem komputer yang tidak sah, penyadapan data, dan mendapatkan informasi rahasia (Hutabarat, 2023). Pasal-pasal yang diuraikan dalam regulasi tersebut tetap relevan dalam konteks spionase siber, mengingat spionase semacam itu biasanya melibatkan penangkapan dan pemantauan tindakan dan percakapan individu yang menjadi target.

Perekaman dapat dilakukan melalui berbagai metode menggunakan teknologi canggih. Sebagai contoh, salah satu metode yang digunakan mata-mata adalah dengan menggunakan *Spyware* ke perangkat target, yang memungkinkan mereka untuk mengakses dan mengambil informasi yang direkam. *Spyware* ini kemudian mengirimkan data yang dikumpulkan kembali ke aktor spionase. Ini termasuk tindakan tidak sah yang mengarah pada kerusakan komputer atau sistem elektronik yang dilindungi negara melalui transmisi program, informasi, kode, atau perintah. Pasal ini juga mencakup penggunaan atau akses yang tidak sah atau berlebihan terhadap komputer atau sistem elektronik yang dilindungi negara, baik dalam maupun luar negeri, dengan tujuan untuk memperoleh informasi. Selain itu, pasal ini juga membahas penggunaan atau akses yang tidak sah terhadap komputer atau sistem elektronik milik pemerintah dan segala aktivitas yang mengganggu atau mengacaukan komputer atau sistem elektronik yang digunakan oleh pemerintah.

Mereka yang menyebarkan, memperdagangkan, atau mengeksploitasi kode akses atau informasi serupa yang dapat digunakan untuk mengkompromikan dan menyalahgunakan komputer atau sistem elektronik yang dilindungi oleh pemerintah, atau mereka yang menargetkan komputer atau sistem elektronik yang dilindungi oleh pihak asing di dalam yurisdiksi Indonesia dengan tujuan untuk menyebabkan kerusakan, juga akan dimintai pertanggungjawaban (UU No. 1, 2023).

Setiap orang yang: (1) tanpa izin yang sah atau di luar kewenangannya, menggunakan atau mengakses komputer atau sistem elektronik dengan tujuan untuk mendapatkan keuntungan finansial atau memperoleh informasi keuangan dari bank sentral, lembaga perbankan, lembaga keuangan, penerbit kartu kredit, atau penyedia kartu pembayaran, termasuk data laporan nasabah; (2) tanpa izin yang sah, menggunakan data atau mengakses kartu kredit atau kartu pembayaran milik orang lain dalam transaksi elektronik untuk kepentingan pribadi; (3) tanpa otorisasi yang tepat atau di luar kewenangannya, menggunakan atau mengakses sistem komputer atau sistem elektronik yang dilindungi dari bank sentral, lembaga perbankan, atau lembaga keuangan dengan maksud untuk menyalahgunakan atau memperoleh keuntungan darinya; dan (4) mendistribusikan, memperjualbelikan, atau mengeksploitasi kode akses atau

Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024
E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id

informasi serupa yang dapat membobol sistem komputer atau sistem elektronik dengan maksud untuk penyalahgunaan, yang berpotensi berdampak pada sistem elektronik bank sentral, lembaga perbankan, lembaga keuangan, serta bisnis domestik dan internasional.

Jerman telah memberlakukan kebijakan dan peraturan untuk mengatasi spionase siber dan aktivitas terkait secara efektif, menjaga keamanan nasional, melindungi infrastruktur penting, dan mengurangi ancaman siber (Barrinha & Renard, 2017). Inisiatif-inisiatif ini menggarisbawahi komitmen Jerman terhadap keamanan siber.

Elemen kuncinya adalah Kebijakan Pertahanan Siber Nasional, yang menggambarkan strategi keamanan siber Jerman, termasuk langkah-langkah untuk mencegah dan merespons spionase siber. Kebijakan ini menyoroti pentingnya melindungi infrastruktur penting, meningkatkan ketahanan siber, dan memperkuat kapasitas negara untuk mengidentifikasi dan mengatasi ancaman siber (Tumkevič, 2018).

Kerangka hukum Jerman untuk memerangi spionase siber dan pelanggaran terkait siber lainnya diwujudkan dalam Strafgesetzbuch (Kitab Undang-Undang Hukum Pidana Jerman (StGB)). KUHP Jerman menetapkan peraturan untuk berbagai aktivitas dunia maya, termasuk spionase dunia maya. Bagian-bagian terkait dari KUHP Jerman yang membahas spionase siber dan pelanggaran terkait adalah sebagai berikut (Radoniewicz, 2021).

1) Bagian 202a - Akses Tidak Sah ke Sistem Komputer: melarang akses tidak sah ke sistem komputer atau data. Ini menargetkan aktivitas seperti peretasan, penyusupan yang tidak sah, dan menghindari langkah-langkah keamanan untuk mengakses data atau mengganggu fungsionalitas sistem.
2) Bagian 202b-Pencurian Data berfokus pada akuisisi, pengungkapan, atau penggunaan data yang tidak sah yang tidak dapat diakses oleh publik. Hal ini mencakup intersepsi transmisi data yang tidak sah, pencurian rahasia dagang, atau pengaksesan informasi rahasia tanpa izin.
3) Bagian 202c - Mempersiapkan Spionase Data: mengkriminalisasi persiapan atau perencanaan pelanggaran spionase data, termasuk mengembangkan atau menggunakan alat atau perangkat lunak untuk akuisisi data tanpa izin.
4) Bagian 202d - Menyadap Transmisi Data Non-Publik: berkaitan dengan penyadapan tanpa izin atas transmisi data nonpublik. Bagian ini mencakup penyadapan komunikasi pribadi, penyadapan email, atau pengambilan data selama transmisi tanpa izin.
5) Bagian 202e - Memasok Perangkat Lunak Penyusupan: melarang pembuatan, distribusi, atau kepemilikan perangkat lunak atau alat yang ditujukan untuk penyusupan yang tidak sah ke dalam sistem komputer. Pasal ini menargetkan individu atau entitas yang terlibat dalam pembuatan dan pendistribusian perangkat lunak berbahaya, yang biasa disebut alat peretasan atau malware.

Pembahasan

Indonesia telah melakukan berbagai inisiatif penting untuk meningkatkan infrastruktur keamanan siber dan melindungi aset digital, infrastruktur penting, dan postur keamanan siber secara keseluruhan. Inti dari upaya ini adalah Badan Siber dan Sandi Negara (BSSN), yang bertindak sebagai koordinator utama untuk masalah keamanan siber nasional. BSSN

E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id
Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024

bertanggung jawab atas perumusan kebijakan dan mempelopori kolaborasi dengan lembaga pemerintah, lembaga penegak hukum, entitas sektor swasta, dan mitra internasional untuk meningkatkan kemampuan keamanan siber Indonesia (Sensuse dkk., 2022).

Indonesia telah memprioritaskan pengamanan sektor infrastruktur informasi yang penting, termasuk telekomunikasi, energi, transportasi, keuangan, dan layanan pemerintah. Indonesia telah mengembangkan dan menerapkan langkah-langkah keamanan yang kuat bekerja sama dengan sektor-sektor terkait. Selain itu, Indonesia telah membentuk Pusat Krisis Siber (C3) untuk mengelola dan mengoordinasikan respons terhadap insiden keamanan siber. C3 bekerja dalam kolaborasi erat dengan berbagai pemangku kepentingan, menawarkan panduan tentang respons insiden dan memfasilitasi pembagian intelijen ancaman (Aulianisa & Indirwan, 2020).

Indonesia mengakui peran penting kemitraan pemerintah-swasta dalam mengatasi tantangan keamanan siber dan secara proaktif mencari kolaborasi dan berbagi informasi dengan sektor swasta. Pemerintah menyoroti pentingnya pendidikan keamanan siber dan pengembangan tenaga kerja dalam memenuhi permintaan yang terus meningkat akan tenaga profesional yang terampil. Selain itu, kerja sama internasional juga sangat penting bagi Indonesia, karena Indonesia terlibat dalam perjanjian bilateral dan multilateral serta berkolaborasi dengan negara lain dalam masalah keamanan siber. Infrastruktur keamanan siber Indonesia terus berkembang untuk beradaptasi dengan ancaman yang muncul dan kemajuan teknologi. Pemerintah dan pemangku kepentingan terkait berdedikasi untuk meningkatkan kemampuan, melindungi infrastruktur penting, dan memastikan ketahanan secara keseluruhan dalam lanskap digital (Kalisz, 2023). Mengakui bahwa infrastruktur keamanan siber Indonesia terus berkembang, dengan tujuan untuk beradaptasi dengan ancaman yang muncul dan kemajuan teknologi sangat penting.

Bekerja sama dengan berbagai pemangku kepentingan, pemerintah berkomitmen untuk meningkatkan kemampuan keamanan siber, melindungi infrastruktur penting, dan memastikan ketahanan komprehensif kerangka kerja digital negara. Terlepas dari upaya-upaya ini, Indonesia menghadapi tantangan khusus dalam memerangi spionase siber secara efektif. Tantangan-tantangan ini mencakup kelangkaan tenaga profesional keamanan siber, keharusan untuk terus beradaptasi dengan ancaman yang terus berkembang, dan kekhawatiran terkait privasi dan tindakan pengawasan untuk mengatasi tantangan-tantangan ini, berbagai inisiatif yang sedang berjalan sedang dilaksanakan untuk meningkatkan kemampuan keamanan siber, berinvestasi dalam pendidikan dan pelatihan keamanan siber, serta merevisi kebijakan dan peraturan agar tetap selaras dengan lingkungan siber yang dinamis (Nugraha, 2016).

Sebagai kesimpulan, kebijakan dan peraturan Indonesia tentang spionase siber mencerminkan dedikasi pemerintah untuk memastikan keamanan nasional dan menjaga dari ancaman siber. Dengan menggunakan pendekatan multifaset yang mencakup kerangka hukum, inisiatif kebijakan, dan langkah-langkah regulasi, Indonesia bertujuan untuk memperkuat kemampuan keamanan sibernya, meningkatkan kesadaran, dan mendorong kerja sama internasional. Untuk melawan spionase siber secara efektif, sangat penting untuk terus berupaya mengatasi tantangan dan meningkatkan keefektifan kebijakan dan peraturan ini.

Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024
E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id

Bagian-bagian KUHP Jerman yang diuraikan di atas mencakup spektrum yang luas dari pelanggaran terkait siber, yang melampaui spionase siber hingga mencakup akses yang tidak sah, pencurian data, dan distribusi alat penyusupan. Selain itu, Undang-Undang Keamanan Siber tahun 2015, meskipun tidak secara eksplisit membahas spionase, menetapkan kerangka hukum yang kuat untuk keamanan siber di Jerman.

Undang-undang ini melindungi infrastruktur penting dan meningkatkan kemampuan keamanan siber negara. Undang-undang ini menekankan keamanan dan ketahanan sistem dan jaringan teknologi informasi, daripada secara langsung menangani kegiatan spionase. Kantor Federal untuk Keamanan Informasi (*Bundesamt für Sicherheit in der Informationstechnik* - BSI), sebagaimana ditetapkan oleh Undang-Undang Keamanan Siber, berfungsi sebagai otoritas pusat untuk masalah keamanan siber. Tanggung jawab BSI termasuk mempromosikan langkah-langkah keamanan siber, menawarkan panduan kepada entitas publik dan swasta, dan mengoordinasikan tanggapan terhadap insiden serangan siber. Oleh karena itu, ia memainkan peran penting dalam menjaga keamanan infrastruktur digital Jerman (Grotto & Schallbruch, 2021).

Undang-Undang Keamanan Siber menggambarkan tanggung jawab operator infrastruktur penting dalam melindungi sistem mereka, mengamanatkan penerapan langkah-langkah teknis dan organisasi yang sesuai untuk mempertahankan diri dari ancaman siber. Selain itu, UU ini memperkenalkan kerangka kerja untuk berbagi informasi dan kolaborasi antara Kantor Federal untuk Keamanan Informasi (BSI) dan operator infrastruktur penting, yang memfasilitasi komunikasi yang cepat tentang intelijen ancaman dan koordinasi tanggapan insiden.

Meskipun undang-undang ini ditujukan untuk melindungi infrastruktur penting dan meningkatkan langkah-langkah keamanan siber, undang-undang ini tidak secara tegas menangani kegiatan spionase. Kegiatan yang berkaitan dengan spionase biasanya diawasi oleh badan intelijen, otoritas penegak hukum, dan undang-undang keamanan nasional, bukan diatur secara langsung oleh peraturan keamanan siber (Schallbruch & Skierka, 2018).

Jerman telah memberlakukan peraturan untuk melindungi sektor-sektor yang dianggap sebagai infrastruktur penting, termasuk energi, air, telekomunikasi, transportasi, dan perawatan kesehatan. Operator sektor-sektor ini diwajibkan untuk menerapkan langkah-langkah keamanan siber yang tepat untuk melindungi dari ancaman siber, termasuk spionase. Penerapan Petunjuk Keamanan Jaringan dan Informasi (NIS), yang merupakan inisiatif dari Uni Eropa, menambah sikap keamanan siber Jerman. Arahan ini mengharuskan operator layanan penting dan penyedia layanan digital menerapkan langkah-langkah keamanan yang diperlukan dan memberi tahu pihak berwenang tentang insiden dunia maya yang signifikan. Dengan demikian, hal ini meningkatkan ketahanan keamanan siber Jerman terhadap spionase dan berbagai ancaman siber lainnya (Leinhos, 2020).

Badan intelijen Jerman, terutama Badan Intelijen Federal (BND), sangat terlibat dalam operasi intelijen dan kontra intelijen asing. Badan-badan ini berperan penting dalam mengidentifikasi dan menggagalkan upaya spionase siber dengan memantau dan menganalisis ancaman siber, melakukan investigasi, dan melindungi data sensitif (Schallbruch & Skierka, 2018).

E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id
Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024

Jerman sangat menghargai kerja sama internasional dalam menangani spionase siber dan ancaman siber lainnya. Jerman bekerja sama erat dengan negara lain, organisasi internasional, dan lembaga penegak hukum untuk berbagi informasi, bertukar praktik terbaik, dan mengoordinasikan upaya secara global untuk memerangi spionase siber secara efektif. Melalui penerapan kebijakan, peraturan, dan inisiatif kolaboratif yang menyeluruh (Vakulyk dkk., 2020).

Simpulan

Berdasarkan hasil dan pembahasan, berikut ini adalah simpulannya.

1. Indonesia menunjukkan kekuatan dalam keamanan siber, yang ditandai dengan meningkatnya kesadaran akan masalah keamanan siber, peran kepemimpinannya di Asia Tenggara dalam domain ini, dan transformasi digitalnya yang cepat yang memfasilitasi adopsi langkah-langkah keamanan siber tingkat lanjut. Namun demikian, Indonesia bergulat dengan berbagai tantangan seperti kurangnya tenaga profesional keamanan siber yang terampil dan sumber daya yang terbatas untuk menerapkan strategi keamanan siber yang komprehensif, serta kerangka kerja peraturan dan hukum yang membutuhkan penyempurnaan dan adaptasi yang berkelanjutan.
2. Pembentukan peraturan khusus yang menargetkan keamanan siber menjadi sangat penting bagi Indonesia. Sebaliknya, kerangka hukum Jerman yang kuat berperan sebagai benteng pertahanan terhadap ancaman siber. Ditambah dengan keahlian teknis yang substansial dan pendekatan inovatif terhadap keamanan siber, Jerman diuntungkan oleh kerangka hukum yang transparan yang memastikan kejelasan dan efisiensi dalam menangani ancaman siber. Meskipun demikian, Jerman juga menghadapi kelemahan, seperti ketergantungan pada teknologi dan rantai pasokan eksternal, prevalensi ancaman siber yang canggih, dan tantangan untuk menyelaraskan praktik keamanan siber di berbagai sektor.

Daftar Rujukan

BBC News. “German Cyber Officials Defend Handling of Mass Data Attack.” https://www.bbc.com/news/world-europe-46768990.

Chotimah, Hidayat Chusnul. (2019). “Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara.” *Jurnal Politica Dinamika Masalah Politik dalam Negeri dan Hubungan Internasional.* Volume 10, No. 2 (2019): 113–128.

Cristani, Federica. (2021). “Economic Cyber-Espionage in the Visegrád Four Countries: A Hungarian Perspective.” *Politics in Central Europe* 17, No. 4: 697–721.

Dewi, Maharani Chandra. (2022). “Cyber Espionage in National and Global Perspective: How Indonesia Deal with This Issue?” *International Law Discourse in Southeast Asia* 1, No. 1 (2022): 1–22.

Drouin, Michelle, Brandon T. McDaniel, Jessica Pater, and Tammy Toscos. (2020). “How Parents and Their Children Used Social Media and Technology at the Beginning of the COVID-19 Pandemic and Associations with Anxiety.” *Cyberpsychology, Behavior and Social Networking* 23, No. 11 (2020): 727–736.

Grotto, Andrew J. and Martin Schallbruch. (2021). "Cybersecurity and the Risk Governance Triangle: Cybersecurity Governance from a Comparative U.S. German Perspective." *International Cybersecurity Law Review* 2, No. 1 (2021): 77–92.

Hutabarat, Sumiaty Adelina (2023) *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. Jambi: Sonpedia Publishing Indonesia.

Iqbal, Muhammad and Nyoman Serikat Putra Jaya. (2021). "Development of Cyber Crime and Its Regulations in Indonesia." *International Journal of Social Science and Human Research* 4, No. 2: 141–147.

Kalisz, Aleksander. (2023). "Public-Private Partnerships on Cybersecurity and International Law: Finding Multilateral Solutions." In Tomoko Ishikawa and Yarik Kryvoi (ed.) *Public and Private Governance of Cybersecurity: Challenges and Potential* Cambridge: Cambridge University Press.

Khan, W.Z. (2020) "Industrial Internet of Things: Recent Advances, Enabling Technologies and Open Challenges." *Computers & Electrical Engineering* 81 (2020): 106522.

Lallie, Harjinder Singh (2021) "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic." *Computers & Security* 105: 1-20.

Lambi, Manuel. (2023). *Sistem Informasi Manajemen Al (Artificial intelligence) as the Future Management Information System*. Ponorogo: Uwais Inspirasi Indonesia.

Leinhos, Ludwig. (2020). "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr." *Connections: The Quarterly Journal* 19, no. 1: 9–19.

Maskun (2020) *Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional*. Makassar: Nas Media Pustaka.

Rawat, Romil (2021) "Artificial Cyber Espionage Based Protection of Technological Enabled Automated Cities Infrastructure by Dark Web Cyber Offender." In Fadi Al-Turjman, Anand Nayyar, Ajantha Devi, and Piyush Kumar Shukla. *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations*. Cham: Springer International Publishing.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana

E-ISSN: 2656-940X
P-ISSN: 2442-367X
URL: jurnal.ideaspublishing.co.id
Volume: 10
Nomor : 4
Bulan : November
Tahun : 2024