KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Ekonomi Manajemen Bisnis dan Akuntansi
Vol.2, No.3 Mei 2025
e-ISSN: 3047-6240, p-ISSN :3047-6232, Hal 329-338
DOI : https://doi.org/10.61722/jemba.v2i3.948

Analisis Keamanan Siber dan Hukum: Studi Kasus Bjorka

Radika Hanny Syah
Universitas Islam Negeri Sumatera Utara
Muhammad Irwan Padli Nasution
Universitas Islam Negeri Sumatera Utara
radikahannysyah123user@gmail.com [1], irwannst@uinsu.ac.id [2]

Abstrak. *Technology has always been a powerful tool in advancing human civilization. It allows us to become more organized, efficient, and connected. Since the advent of the Internet, we have increasingly relied on electronic communications as a means of conducting business. Cybersecurity, which also includes authentication, non-repudiation, and accountability, is an effort to protect the confidentiality, integrity, and availability of information in cyberspace. The process of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks falls under the category of cybersecurity. The following questions were used to evaluate the descriptive data in this paper, which uses a qualitative management approach: What triggers hackers to infiltrate Indonesia and how does the government respond to it?*

Keywords: cybersecurity, data privacy, cyber law

Abstrak. Teknologi selalu menjadi alat yang kuat dalam memajukan peradaban manusia.Teknologi memungkinkan kita menjadi lebih terorganisir, efisien, dan terhubung. Sejak munculnya Internet, kita semakin mengandalkan komunikasi elektronik sebagai sarana dalam menjalankan bisnis. Keamanan siber, yang juga mencakup otentikasi, non-repudiation (penyangkalan), dan akuntabilitas, merupakan upaya untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi di dunia maya. Proses perlindungan terhadap komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan berbahaya termasuk dalam kategori keamanan siber.Pertanyaan-pertanyaan berikut digunakan untuk mengevaluasi data deskriptif dalam makalah ini, yang menggunakan pendekatan manajemen kualitatif:Apa yang memicu para peretas untuk menyusup ke Indonesia dan bagaimana tanggapan pemerintah terhadap hal tersebut?

Keyword : cybersecurity, data privacy ,cyber law

PENDAHULUAN

Teknologi selalu menjadi alat yang kuat dalam memajukan peradaban manusia. Teknologi memungkinkan kita untuk menjadi lebih terorganisir, efisien, dan terhubung. Namun, seiring dengan semakin majunya teknologi, risiko penyalahgunaannya juga semakin besar. Hal ini menjadi masalah khusus ketika berkaitan dengan komunikasi elektronik.

Sejak munculnya Internet, kita semakin bergantung pada komunikasi elektronik sebagai sarana untuk menjalankan bisnis. Sayangnya, hal ini menjadikan internet sebagai tempat berkembang biaknya para peretas dan pelaku kejahatan yang mencari celah keamanan untuk dieksploitasi. Kenyamanan dalam menjalankan aktivitas bisnis seharihari secara online membawa risiko besar atas pencurian informasi pribadi dan rahasia oleh pihak yang berniat jahat. Hal ini bisa sangat merugikan, terutama bagi perusahaan. Kehilangan data sensitif perusahaan dapat merusak reputasi dan membahayakan stabilitas keuangan secara permanen.

Untuk mengatasi masalah ini, perusahaan teknologi berinvestasi besarbesaran dalam pengembangan langkahlangkah dan prosedur keamanan baru guna mencegah akses yang tidak sah. Ancamanancaman baru segera ditangani melalui penggunaan metode enkripsi canggih dan

Received Mei, 2025; Revised Mei , 2025;Mei , 2025
* radikahannysyah123user@gmail.com

algoritma komputer yang kompleks. Meskipun langkahlangkah pencegahan ini telah membuat penggunaan internet jauh lebih aman daripada sebelumnya, namun tetap tidak sepenuhnya aman dan masih terdapat celah dalam pertahanannya.

Teknologi sangat penting dalam menyediakan alat keamanan komputer yang dibutuhkan organisasi dan individu untuk melindungi diri dari serangan siber. Ada tiga entitas utama yang harus dilindungi: perangkat endpoint seperti kalkulator, perangkat pintar, dan

router; jaringan web; serta cloud. Teknologi umum yang digunakan untuk mempertahankan entitasentitas ini termasuk firewall generasi terbaru, pemfilteran DNS, keamanan malware, kode antivirus, dan solusi perlindungan email.

Namun, Indonesia pernah dibobol oleh peretas. Di sebuah forum dark web, seorang pengguna dengan nama Bjorka mengklaim telah meretas sistem keamanan pemerintah Indonesia dan mengambil datadata di dalamnya. Informasi yang dikumpulkan mencakup nama pengguna, alamat email, NIK, NPWP, nomor telepon, dan pengeluaran. Selain itu, disediakan pula tautan yang menunjukkan bukti berupa informasi akun dan transaksi yang dilakukan menggunakan data tersebut.

Bjorka juga diketahui memiliki akun di Twitter dan Telegram. Ia sering terlihat menyebarkan informasi yang ia peroleh melalui platform tersebut. Ia juga kerap menulis cuitan yang mengkritik lemahnya sistem keamanan yang dikelola oleh pemerintah Indonesia.

Sebelumnya, masyarakat Indonesia sempat dibuat terkejut oleh aksi yang dilakukan Bjorka dan bertanyatanya apa sebenarnya tujuan dari tindakannya tersebut. Mengejutkannya lagi, Bjorka membagikan motifnya, khususnya melalui cuitancuitan di Twitter yang tampak seperti ‘umpan’.

Di Warsawa, Polandia tempat asalnya diketahui Bjorka mengatakan bahwa ia memiliki seorang sahabat dari Indonesia di sana. Selain itu, Bjorka memperingatkan pemerintah Indonesia agar tidak mencoba mencari keberadaan sahabat dekatnya karena itu akan siasia melalui jalur kementerian luar negeri. Meskipun sahabatnya itu cerdas, ia bukan lagi warga negara Indonesia karena kebijakan tahun 1965.

Bjorka juga mengklaim bahwa ia menjalankan niat sahabat tercintanya tersebut. Dilaporkan bahwa temannya itu masih memiliki impian yang belum terwujud untuk kembali ke Indonesia tempat ia dilahirkan dan "melakukan sesuatu dengan teknologi meskipun ia sadar betapa menyedihkannya menjadi seorang Habibie."

Bjorka mengakui bahwa sulit baginya untuk melanjutkan impian sahabatnya, yang selama ini telah merawatnya sejak kecil, dengan cara yang sama. Oleh karena itu, Bjorka memutuskan untuk mencari solusi lain agar tanah kelahiran sahabatnya dapat mengalami perbaikan.

KAJIAN TEORI

Agus Subagyo dalam artikel jurnalnya yang berjudul Sinergi dalam Menghadapi Ancaman Perang Siber mengatakan bahwa di era globalisasi, sifat ancaman tidak hanya berasal dari aspek militer dan fisik saja, tetapi juga berasal dari ancaman non-militer dan non-fisik, salah satunya adalah ancaman siber. Dunia kini telah memasuki era ruang siber yang memunculkan kejahatan siber (cybercrime) dan berpotensi menimbulkan ancaman

perang siber. Indonesia membutuhkan pasukan siber untuk melawan ancaman perang siber. Kementerian Pertahanan Republik Indonesia harus berada di garis depan dalam proses penyusunan kebijakan pertahanan siber untuk menghadapi ancaman tersebut. Sinergi antara para pemangku kepentingan dan pihak-pihak terkait dalam melawan perang siber merupakan kunci keberhasilan.

Terkait hal tersebut, perubahan terus berlangsung dalam dunia yang dinamis, terkadang disertai gangguan yang mempengaruhi hubungan antar negara serta totalitas persoalan global yang berdampak pada sendi-sendi kehidupan berbangsa dan bernegara. Setiap peristiwa global di dunia akan selalu memengaruhi kehidupan negara secara menyeluruh di setiap negara, memaksa setiap negara untuk selalu mengamati dan menganalisis setiap peristiwa dalam lingkungan strategis baik di tingkat global, regional, nasional, maupun lokal.

Paulina Pannen dalam artikelnya pada jurnal Quality Assurance in Online Learning and Scale di Indonesia Cyber Education Institute menyatakan bahwa adopsi dan implementasi pendidikan daring bertujuan untuk meningkatkan kualitas proses belajar mengajar dengan mempertimbangkan perbedaan gaya belajar siswa, meningkatkan akses terhadap kesempatan belajar, meningkatkan fleksibilitas pembelajaran agar siswa dapat mengembangkan keterampilan dan kemampuan yang dibutuhkan, serta meningkatkan efisiensi biaya lembaga pendidikan. Pendidikan daring memungkinkan siapa pun untuk belajar kapan saja dan di mana saja, serta memungkinkan komunikasi dan kolaborasi virtual dari berbagai negara. Pengenalan dan implementasi pendidikan daring ini bertujuan untuk menyesuaikan kebutuhan abad ke-21 dan memberikan solusi pembelajaran yang lebih luas dan efektif.

METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif dengan pendekatan studi kasus. Pendekatan ini digunakan karena fokus penelitian adalah mendalami secara komprehensif fenomena kebocoran data dan pelanggaran keamanan siber yang terjadi dalam kasus Bjorka, serta menganalisis aspek hukum yang mengaturnya di Indonesia. Pertanyaan-pertanyaan berikut digunakan untuk mengevaluasi data deskriptif , yang menggunakan pendekatan manajemen kualitatif:

1. Apa yang mendorong para peretas untuk menyusup ke Indonesia?
2. Bagaimana tanggapan pemerintah terhadap peristiwa tersebut?

HASIL PENELITIAN DAN PEMBAHASAN

A. Kategori Keamanan Siber dan Bagian-bagiannya

Keamanan siber (cybersecurity), yang juga mencakup otentikasi, non-repudiation (ketidakmampuan menyangkal), dan akuntabilitas, adalah upaya untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi di ruang siber. Proses perlindungan terhadap komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan jahat termasuk dalam kategori keamanan siber. Keamanan ini sering disebut juga sebagai keamanan informasi elektronik atau keamanan teknologi

informasi. Istilah ini dapat dibagi ke dalam beberapa kategori luas dan digunakan dalam berbagai konteks, termasuk bisnis dan komputasi seluler. Ada enam kategori utama dalam keamanan siber, antara lain:

1. Keamanan Jaringan (Network Security): Merupakan proses perlindungan sistem komunikasi dari penyusup, seperti penyerang yang disengaja atau perangkat lunak berbahaya yang menyerang secara acak.
2. Keamanan Aplikasi (Application Security): Bertujuan untuk melindungi perangkat dan perangkat lunak dari ancaman. Aplikasi yang telah diretas dapat memberikan akses kepada pengguna terhadap informasi yang seharusnya dilindungi. Keamanan yang efektif dimulai jauh sebelum perangkat lunak atau mesin dibuat, yaitu dari tahap perancangan.
3. Perlindungan Data (Data Protection): Menjaga integritas catatan dan privasi baik saat data disimpan maupun saat ditransmisikan.
4. Keamanan Operasional (Operational Safeguards): Meliputi prosedur dan kebijakan dalam mengelola serta melindungi aset informasi. Ini termasuk protokol tentang di mana dan bagaimana data dapat disimpan atau ditransfer serta hak pengguna saat mengakses jaringan. Pemulihan Bencana dan Kelangsungan Bisnis (Disaster Recovery and Business Continuity): Menjelaskan bagaimana suatu organisasi merespons serangan siber atau kejadian lain yang menyebabkan hilangnya data atau gangguan operasional. Prosedur organisasi untuk mengembalikan data dan aktivitas ke kondisi sebelum insiden dijelaskan dalam kebijakan pemulihan bencana. Sementara rencana kelangsungan bisnis dijalankan ketika organisasi mencoba beroperasi tanpa sumber daya tertentu.
5. Pelatihan Pengguna Akhir (End-User Training): Melibatkan elemen manusia dalam keamanan siber, yang seringkali menjadi titik lemah. Siapa pun yang mengabaikan strategi keamanan yang baik bisa secara tidak sengaja memasukkan ancaman ke dalam sistem yang sebelumnya aman. Keamanan suatu organisasi sangat bergantung pada kemampuan para pegawainya dalam mengidentifikasi lampiran email mencurigakan, menghindari penggunaan perangkat USB asing, dan mengikuti praktik keamanan lainnya.

B. Strategi Pemerintah Indonesia dalam Menghadapi "Peretasan"

Strategi nasional Indonesia mencakup enam area utama, yaitu:

1. Budaya dan kapabilitas keamanan informasi;
2. Risiko keamanan informasi;
3. Pengurangan risiko dalam hal keamanan informasi;
4. Penanganan insiden yang melibatkan keamanan informasi;
5. Kinerja dalam manajemen keamanan informasi;
6. Kapasitas penegakan hukum di bidang Informasi dan Transaksi Elektronik (ITE).

Visi dan misi dari rencana keamanan siber Kementerian Komunikasi dan Informatika juga dinyatakan. **Visinya** adalah memastikan terlaksananya transformasi digital dalam konteks pemerintahan berbasis elektronik, ekonomi digital, dan masyarakat berbasis pengetahuan. **Tujuannya** adalah menciptakan ekosistem informasi yang aman, andal, dan bertanggung jawab.

Misinya adalah membangun dan mengelola ruang siber secara andal, bertanggung jawab, dan aman, serta melindungi kepentingan negara Indonesia.

Terdapat juga tujuan-tujuan khusus dalam keamanan siber, yaitu:

1. Ketahanan Siber (Cyber Resilience): Membangun infrastruktur data nasional yang kritis agar tahan terhadap serangan dan tetap dapat menyediakan layanan publik meskipun sebagian rusak atau hancur.
2. Layanan Publik Siber (Cyber Public Service): Mengembangkan strategi, tindakan, dan prosedur dalam menangani serta memulihkan ancaman dari dalam maupun serangan siber melalui pertukaran informasi, kerja sama, dan taktik aksi.
3. Penegakan Hukum Siber (Cyber Law Enforcement): Membentuk kerangka hukum serta penerapan regulasi dan undang-undang untuk menciptakan lingkungan daring yang aman dan bersahabat.

   Keamanan Siber (Cybersecurity): Dalam hal ini, budaya merujuk pada standar penilaian dan cara berpikir dalam menghadapi tantangan keamanan informasi. Hal ini mencakup pembentukan budaya keamanan siber yang mendorong keselamatan serta penggunaan internet yang bertanggung jawab. Budaya ini menjadi landasan dalam membangun kesadaran, perilaku, dan kebiasaan baik dalam menjaga keamanan digital, baik di lingkungan individu, organisasi, maupun pemerintahan.

C. Beberapa Jenis Hacker Berdasarkan "Topi" Mereka

Hacker dibedakan menjadi beberapa jenis, termasuk **black hat**, **white hat**, dan **gray hat**.

1. **Black hat hackers** adalah penjahat dunia maya yang dengan sengaja membobol jaringan tanpa izin. Black hat hacking didefinisikan sebagai upaya untuk mendapatkan akses ke sistem komputer target secara ilegal. Setelah menemukan celah keamanan, mereka berusaha mengeksploitasinya, biasanya dengan menyisipkan malware seperti trojan atau virus.
2. Black hat hacker sering kali memulai sebagai "script kiddies" yang tidak berpengalaman, menggunakan alat peretasan komersial untuk mengeksploitasi kerentanan sistem. Beberapa di antaranya diajari oleh pihak yang ingin mendapat keuntungan cepat. Black hat yang paling dikenal biasanya adalah peretas ahli yang bekerja untuk kelompok kriminal terorganisir yang sangat canggih. Kelompok ini bahkan menyediakan alat komunikasi dan layanan pelanggan seperti halnya sebuah bisnis resmi.Kit malware yang dijual di dark web sering kali disertai dengan garansi dan dukungan pelanggan.

3. Black hat hacker sering kali memiliki spesialisasi di bidang tertentu, seperti mengelola remote access tools atau melakukan phishing. Banyak dari mereka menemukan "pekerjaan" melalui forum dan tautan di dark web. Sebagian lainnya bekerja dengan sistem waralaba atau sewa, sedangkan ada juga yang membuat dan menjual program jahat secara langsung. Saat ini, pemerintah juga menggunakan peretasan sebagai alat penting untuk mendapatkan intelijen, meskipun black hat biasanya bekerja sendiri atau bersama kelompok kejahatan demi keuntungan cepat.
4. Karena skala operasinya yang besar, dunia peretasan dapat berfungsi seperti sebuah perusahaan besar, yang memudahkan penyebaran perangkat lunak berbahaya. Organisasi dalam ekosistem ini memiliki mitra, penjual, vendor, dan afiliasi, dan mereka membeli serta menjual lisensi malware kepada kelompok kriminal lain untuk digunakan di pasar atau wilayah baru.

Beberapa organisasi black hat bahkan memiliki pusat panggilan (call center) untuk melakukan panggilan keluar sambil menyamar sebagai karyawan perusahaan perangkat lunak terkenal seperti Microsoft. Dalam skema ini, hacker berusaha membujuk korban untuk mengunduh perangkat lunak atau memberikan akses penuh ke sistem mereka. Dengan memberikan akses atau menginstal perangkat lunak tersebut, korban secara tidak sadar memungkinkan penjahat mencuri kata sandi dan informasi perbankan, mengambil alih komputer secara diam-diam, dan menggunakannya untuk menyerang target lain. Kerugian korban diperparah dengan biaya "layanan" yang sangat mahal. Jenis serangan lainnya bahkan tidak melibatkan interaksi manusia dan bersifat cepat serta otomatis. Dalam kasus ini, bot serangan menjelajahi internet untuk mencari perangkat yang dapat dengan mudah diretas, biasanya melalui phishing, lampiran virus, atau tautan ke situs web yang telah diretas.
D. Pihak Mana yang Dipilih Bjorka, dan Reaksi Pemerintah Indonesia terhadap Aksinya

Seperti yang disebutkan pada bab pertama, Bjorka ingin memenuhi permintaan sahabat terbaiknya dari Indonesia. Sayangnya, kebijakan tahun 1965 menghalangi sahabat Bjorka untuk mewujudkan keinginannya sendiri. Dengan membagikan informasi dan data yang ia peroleh dari pemerintah dan perusahaan Indonesia, Bjorka berharap dapat membantu temannya meraih impiannya. Bjorka juga memperingatkan pemerintah bahwa sistem keamanan siber Indonesia sangat lemah.

Bjorka berperan sebagai Black Hat Hacker, dan tanpa disadari juga berubah menjadi Gray Hat Hacker. Ia membuat akun di Twitter dan Telegram, dan sering terlihat membagikan informasi yang telah diperolehnya di sana, serta membuat cuitan tentang buruknya pengelolaan sistem keamanan oleh pemerintah Indonesia.

Terlepas dari ke mana ia berpihak, Bjorka telah secara ilegal mengakses sistem keamanan milik pemerintah maupun perusahaan swasta Indonesia. Bjorka juga mengklaim bahwa dirinya menjual informasi yang diperolehnya dari forum gelap (dark forum). Jelas bahwa pemerintah Indonesia langsung menangani masalah ini. Akun Indonesia milik Bjorka segera dihapus oleh server, dan pihak berwenang mengambil tindakan lebih lanjut.

> *Jangan pernah memberikan informasi pribadi kepada seseorang yang mengaku dari pemerintah.* Jika menerima tautan dari nomor atau email yang tidak dikenal, jangan klik, karena peretas bisa melacak informasi pribadi Anda.

Pemerintah Indonesia merespons keberadaan Bjorka dengan menerbitkan Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Berdasarkan Pasal 3, undang-undang ini didasarkan pada asas keamanan, kualitas regulasi, kepentingan yang sah, efisiensi, kehati-hatian, keseimbangan, akuntabilitas, dan kerahasiaan.

Sri Mulyani Indrawati, Menteri Keuangan Republik Indonesia, menegaskan pentingnya keamanan siber di era serba digital saat ini. Alasannya adalah karena situs-situs web pemerintah kerap menjadi target serangan oleh peretas, yang tentunya berisiko menyebabkan pencurian informasi sensitif pemerintah. Bukan hanya Indonesia, negara lain pun sangat rentan terhadap peretasan, yang tentu dapat merugikan banyak orang atau pihak.

Inilah pentingnya keamanan siber.Keamanan siber adalah praktik melindungi sistem, jaringan, perangkat lunak, dan data dari bahaya daring serta akses tidak sah, terutama dari peretas. Ancaman siber tidak hanya menargetkan perusahaan besar, tetapi juga usaha kecil dan individu. Misalnya, mengakses informasi pribadi, mengubah data penting, atau bahkan menghapusnya.

- Pasal-Pasal Terkait dalam UU ITE
- Pasal 31 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menyatakan:
- (1) Setiap orang dengan sengaja melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain di dalam suatu komputer atau sistem elektronik lainnya secara tanpa hak atau melanggar hukum;
- (2) Setiap orang secara melawan hukum melakukan intersepsi atas aliran Informasi Elektronik atau Dokumen Elektronik yang tidak diperuntukkan bagi umum dari, ke, atau di dalam suatu komputer atau sistem elektronik tertentu milik orang lain.

Pasal 40 UU yang sama menyebutkan:

- (2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan akibat penyalahgunaan Informasi Elektronik dan/atau Dokumen Elektronik yang mengganggu ketertiban umum sesuai dengan ketentuan peraturan perundang-undangan;
- (2a) Pemerintah wajib menghentikan transmisi dan menghapus informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan;
- (2b) Untuk melaksanakan pencegahan sebagaimana dimaksud pada ayat (2a), pemerintah berwenang memutus akses terhadap informasi elektronik dan/atau dokumen elektronik yang bermuatan melanggar hukum, dan/atau memerintahkan kepada penyelenggara sistem elektronik untuk memutus akses.

KESIMPULAN

Teknologi selalu menjadi alat yang kuat untuk memajukan peradaban manusia. Ia memungkinkan kita menjadi lebih terorganisir, efisien, dan terhubung. Sejak munculnya Internet, kita semakin bergantung pada komunikasi elektronik dalam menjalankan aktivitas, termasuk bisnis. Sayangnya, hal ini juga menjadikan Internet sebagai lahan subur bagi peretas dan pelaku kejahatan siber yang memanfaatkan celah keamanan.

Untuk mengatasi masalah ini, perusahaan teknologi kini berinvestasi besar dalam pengembangan sistem keamanan baru dan prosedur untuk mencegah akses tidak sah. Saat ancaman baru muncul, perusahaan teknologi segera menanggapinya melalui teknologi enkripsi canggih dan algoritma komputer yang lebih pintar.

Namun, Indonesia telah berhasil dibobol oleh peretas. Meski kita mungkin merasa bahwa informasi pribadi kita aman, kenyataannya tidak selalu demikian. Meskipun telah diberikan otoritas, kita tidak selalu bebas dari tanggung jawab. Data yang dicuri dapat disalahgunakan oleh hacker dan cracker untuk kepentingan pribadi atau kelompok, baik untuk dijual, menyamar dengan identitas palsu, maupun untuk tujuan lain. Intinya adalah, kita masing-masing bertanggung jawab terhadap informasi pribadi kita sendiri.

Jangan pernah memberikan akses terhadap informasi sensitif Anda kepada orang asing, bahkan jika mereka adalah teman dekat Anda

DAFTAR PUSTAKA

"UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi," peraturan.bpk.go.id. [Online]. Available: https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27- tahun-2022. .Database Peraturan | JDIH BPK

CNN Indonesia, "Siapa Bjorka dan Kenapa 'Mengacak-acak' Indonesia?,"

teknologi, Oct. 12, 2022. [Online]. Available: https://www.cnnindonesia.com/teknologi/20220912053812-192-846395/siapa- bjorka-dan-kenapa-mengacak-acak-indonesia. .

Kaspersky, "What is Cyber Security?," 2019. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. .

R. K. Siregar, "Perbedaan Hacker dan Cracker," www.djkn.kemenkeu.go.id, Sep. 27, 2022. [Online]. Available: https://www.djkn.kemenkeu.go.id/kanwil-rsk/baca-artikel/15422/Perbedaan-Hacker-dan-Cracker.html. .

Kaspersky, "Black hat, White hat, and Gray hat hackers – Definition and Explanation," Apr. 09, 2021. [Online]. Available: https://www.kaspersky.com/resource- center/definitions/hacker-hat-types. .

O. Buxton, "Hacker Types: Black Hat, White Hat, and Gray Hat Hackers," Oct. 12, 2022. [Online]. Available: https://www.avast.com/c-hacker-types. .

"UU No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," peraturan.bpk.go.id. [Online].
Available: https://peraturan.bpk.go.id/Home/Details/37582/uu-no-19-tahun-2016. [Accessed: Dec. 28, 2022].

A. Chendramata, "Indonesia Cyber Security Strategy," dephub.go.id. [Online]. Available: https://dephub.go.id/public/files/uploads/posts/posts/postbody/strategi_cs_nasiona l_desember2016.pdf. [Accessed: Dec. 28, 2022].

I. R. Dewi, "Hacker Bjorka is Back, Data Apa Saja yang Pernah Dibocorkan?," CNBC Indonesia, Nov. 11, 2022. [Online]. Available: https://www.cnbcindonesia.com/tech/20221111075351-37-386931/hacker-bjorka- is-back-data-apa-saja-yang-pernah-dibocorkan. [Accessed: Dec. 28, 2022].

A. Subagyo, "SINERGI DALAM MENGHADAPI ANCAMAN CYBER WARFARE,"
Jurnal Pertahanan & Bela Negara, vol. 5, no. 1, Aug. 2018. [Online]. Available: https://doi.org/10.33172/jpbh.v5i1.350.

P. Pannen, "Quality Assurance in Online Learning at Scale at the Indonesia Cyber
Education Institute," Education in the Asia-Pacific Region: Issues, Concerns and Prospects, pp. 121–134, 2021. [Online]. Available: https://doi.org/10.1007/978- 981-16-0983-1_9.

"Menyingkap Tabir Istilah Hacker dan Cracker," www.djkn.kemenkeu.go.id. [Online].
Available: https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/15368/Menyingkap-Tabir-Istilah-Hacker-dan-Cracker.html. .Kemenkeu

"Permen Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik," peraturan.bpk.go.id. [Online]. Available: https://peraturan.bpk.go.id/Download/142743/Permen%20Kominfo%20Nomor%2 020%20Tahun%202016.pdf. .Database Peraturan | JDIH BPK

"Personal Data Protection Authority Institute," Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Personal_Data_Protection_Authority_Institute . . Wikipedia

"Perpres Nomor 49 Tahun 2024 tentang Pelaksanaan UU No. 27 Tahun 2022," peraturan.bpk.go.id. [Online].
Available:https://peraturan.bpk.go.id/Download/341380/Perpres%20Nomor%20 49%20Tahu n%202024.pdf. .