e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 11 No 3 Tahun 2024 Hal. : 1026-1034

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

PENCURIAN DATA DAN INFORMASI DI INDONESIA SEBAGAI KEJAHATAN CYBER DALAM PERSPEKTIF PEPERANGAN ASIMETRIS

Iwan Setiawan, Fauzia G. Cempaka, Yono Reksoprodjo

Prodi Peperangan Asimetris, Fakultas Strategi Pertahanan,

Universitas Pertahanan Republik Indonesia

Abstrak

Pencurian data dan informasi dalam dunia maya merupakan bentuk kejahatan pelanggaran hukum, hal ini sangat berbahaya dan berpotensi mengakibatkan kerugian besar bagi korban baik individu maupun organisasi. Kejahatan dunia maya dilakukan dengan menggunakan peralatan komputer melalui jaringan oleh sebagian besar non-state actor yang memiliki tujuan tertentu dengan menguasai dan mengendalikan sistem komputer yang terkoneksi. Kejadian-kejadian pencurian data dan informasi di Indonesia merupakan fenomena tersendiri, mengapa kejadian tersebut bisa berulang, apabila tidak diantisipasi dengan tepat akan berimbas pada ancaman pertahanan dan keamanan negara. Sebelum dimulainya perang konvensional, peperangan asimetris didunia maya dilakukan untuk menguji kekuatan negara dan sebagai indikator dibidang pertahanan dan keamanan negara. Penelitian ini bertujuan untuk menganalisa fenomena kasus pencurian data dan informasi di Indonesia sebagai kejahatan cyber dalam perspektif peperangan asimetris. Metode penelitian ini mengunakan metode kualitatif. Data yang dikumpulkan berupa data primer dan data sekunder, yaitu dengan sumber literatur review, dalil hukum, dan teori. Hasil hypotesa menunjukkan ancaman kejahatan cyber sangat berbahaya karena dapat merugikan negara dan mengancam stabilitas pembangunan nasional baik secara politik, ekonomi dan militer. Pemerintah telah mengatur penanganan kejahatan cyber dalam UU ITE Nomor 19 Tahun 2016 namun belum optimal, sehingga diperlukan tindakan yang lebih efektif dan nyata.

Kata Kunci: Pencurian data dan informasi, kejahatan cyber, peperangan asimetris.

*Correspondence Address : iwansetiawan7898@gmail.com
DOI : 10.31604/jips.v11i3.2024. 1026-1034

PENDAHULUAN

Dalam era abad ke-21, ketergantungan manusia pada teknologi dan informasi menjadi suatu kebutuhan mendasar. Transaksi elektronik melalui perangkat seperti handphone, laptop, dan komputer telah memberikan kemudahan dalam pemenuhan berbagai kebutuhan hidup. Akan tetapi, untuk dapat melakukan transaksi ini, pengguna diharuskan mendaftarkan diri dan mengisi formulir data lengkap sebagai syarat untuk login ke dalam aplikasi yang dituju. Data pribadi yang dikumpulkan melalui proses ini memiliki berbagai tujuan, termasuk inventaris data, layanan konsumen, promosi produk, dan riset konsumen (Stallings and Bauer, 2012). Keamanan data pribadi menjadi aspek yang sangat penting dalam hubungan antara produsen dan konsumen, karena membangun kepercayaan yang esensial. Penyelenggara sistem elektronik memegang peran krusial dalam menjaga keamanan data dan informasi pelanggan. Namun, realitas menunjukkan adanya penyalahgunaan data pribadi oleh pihak tertentu, mengakibatkan kerugian kepercayaan masyarakat terhadap pemerintah.

Di sisi lain, perkembangan ilmu pengetahuan sistem informasi dan teknologi menjadi sumber eksploitasi untuk mencari celah kelemahan dalam sistem komputer dan aplikasi pada jaringan internet (Halder, 2011). Penggunaan teknologi sistem informasi diartikan sebagai alat untuk mencapai tujuan tertentu, yang memicu munculnya berbagai bentuk kejahatan cyber di seluruh dunia. Di Indonesia, pencurian data dan informasi, khususnya yang berkaitan dengan keamanan privasi, menjadi fokus perhatian, termasuk dokumen perusahaan swasta, BUMN, dan pemerintah.

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) menetapkan bahwa pemerintah dan penyelenggara sistem elektronikasi harus melindungi kepentingan umum dari gangguan penyalahgunaan informasi dan transaksi elektronik. Dengan memberlakukan sanksi pidana dan denda, UU ITE menegaskan perlunya perlindungan terhadap muatan pemerasan atau pengancaman dalam dokumen elektronik. Kejahatan berbasis komputer atau cyber crime, yang melibatkan komputer dan jaringan, menjadi ancaman serius (Moore, 2005). Ancaman cyber dapat merusak reputasi korban dan menyebabkan kerugian, baik secara langsung maupun tidak langsung, melalui berbagai platform telekomunikasi modern seperti internet, ruang chat, email, notice boards, dan group. Prediksi menunjukkan bahwa tren kejahatan cyber akan terus meningkat seiring dengan peningkatan penggunaan internet dan adaptasi kebiasaan baru oleh penggunanya.

Dalam konteks pertahanan negara, Undang-Undang No 3 Tahun 2002 tentang Pertahanan Negara menegaskan bahwa ancaman dalam sistem pertahanan negara tidak hanya berasal dari ancaman militer, tetapi juga dari ancaman non-militer, termasuk ancaman cyber. Eskalasi serangan cyber dapat mengancam kedaulatan negara, keutuhan wilayah, dan keselamatan bangsa. Oleh karena itu, formulasi kebijakan yang tepat dan sinergisitas antar lembaga terkait diperlukan untuk mempertahankan data dan informasi dari ancaman cyber crime di Indonesia (Warren G. Kruse, 2002; Halder, 2011). Dalam dunia hacker, terdapat beberapa jenis, antara lain Ethical Hackers, Threat Actors, Gray Hat Hackers, Red Hat Hackers, Blue Hat Hackers, Script Kiddies, dan Hacktivists. Ancaman cyber mencakup berbagai serangan dan aktivitas jahat yang bertujuan merusak, mengakses, dan mengganggu sistem

komputer dan jaringan. Beberapa contoh ancaman cyber yang sering dihadapi oleh individu atau organisasi melibatkan Malware, Injeksi SQL, Phishing, Serangan Man-in-the-Middle, dan Serangan Denial-of-Service.

Jenis keamanan cyber, seperti Cloud Security, Network Security, dan Application Security, menjadi krusial dalam melindungi data dan informasi dari ancaman cyber. Oleh karena itu, penelitian ini akan menganalisis faktor-faktor yang mempengaruhi pencurian data dan informasi di Indonesia, memahami kejahatan cyber dalam perspektif peperangan asimetris, serta mengevaluasi langkah-langkah pemerintah Indonesia dalam menangani ancaman kejahatan cyber.

Penelitian ini bertujuan untuk menyelidiki faktor-faktor yang berperan dalam mempengaruhi kasus pencurian data dan informasi di Indonesia. Selain itu, penelitian ini akan menggali pemahaman lebih mendalam mengenai kejahatan cyber dalam konteks perspektif peperangan asimetris di Indonesia. Melalui penelitian ini, akan dianalisis pula langkah-langkah yang telah diambil oleh pemerintah Indonesia dalam menanggulangi ancaman kejahatan cyber. Tujuan utama dari penelitian ini adalah untuk memberikan pemahaman yang lebih komprehensif terkait dengan dinamika dan tantangan yang terkait dengan keamanan data di tengah ancaman cyber yang semakin kompleks. Dengan demikian, diharapkan penelitian ini dapat memberikan kontribusi positif dalam pengembangan kebijakan serta strategi perlindungan data di era digital yang terus berkembang.

METODE PENELITIAN

Pada metode penelitian ini, penulis memaparkan jenis penelitian yang digunakan adalah metode kualitatif, dengan metode pendekatan melihat kasus pencurian data dan informasi yang sering terjadi di Indonesia oleh pelaku kejahatan cyber dihubungkan dengan kebijakan pemerintah melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektroknik (UU ITE). Sumber data berupa data primer dan sekunder, cara pengambilan data yaitu studi pustaka selanjutnya dianalisis untuk dapat dipahami dan mendapatkan kesimpulan dalam penelitian ini. Teknik analisis data yaitu narasi analisis

HASIL DAN PEMBAHASAN

Faktor yang mempengaruhi pencurian data dan informasi di Indonesia.

Menurut John D. Howard (1997) dalam bukunya "An Analysis of Security Incidents on the Internet," keamanan komputer merupakan tindakan pencegahan terhadap serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Gollmann (1999) juga mengemukakan dalam bukunya "Computer Security" bahwa keamanan komputer terkait dengan pencegahan dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer. Dalam beberapa tahun terakhir, terjadi kasus pencurian data dan informasi di sektor pemerintahan, BUMN, dan swasta di Indonesia. Pencurian data dan informasi melibatkan eksploitasi dokumen rahasia untuk kepentingan pihak tertentu tanpa persetujuan pemiliknya. Proses pendaftaran di sistem elektronik seperti LinkAja, Gopay, ShopeePay, dan Isaku meminta pengguna untuk memasukkan data pribadi. Meski penyelenggara sistem elektronik wajib menyimpan data pribadi, risiko peretas menyerang situs web pemerintah dan swasta tetap ada. Informasi yang diperoleh dapat menjadi sasaran empuk untuk meretas akun dan mencuri data pribadi, menyebabkan kerugian finansial dan reputasi bagi korban. Dengan maraknya pencurian data secara online, penting untuk

menyadari bahaya pencurian data dan informasi. Risiko ini mencakup kerugian finansial dan reputasi, serta potensi penyalahgunaan data pribadi untuk kejahatan seperti pemalsuan identitas dan penipuan online. Ancaman pencurian data dapat mengintai siapa saja di kalangan pengguna internet yang tidak berhati-hati saat memberikan identitas online. Pengguna internet juga perlu waspada terhadap praktik phishing, di mana pelaku berusaha memancing korban dengan mengirimkan pesan atau email palsu dengan tautan yang mengandung virus. Selain itu, penipuan dengan menyamar sebagai pihak lain, baik melalui panggilan telepon atau pengiriman perangkat lunak ilegal, juga merupakan ancaman serius. Jenis pencurian data terakhir adalah cracking, yang melibatkan pembobolan sistem keamanan komputer untuk mendapatkan informasi sensitif seperti password dan nomor PIN. Semua tindakan kejahatan ini merupakan dampak dari penggunaan teknologi berbasis komputer dan jaringan telekomunikasi, yang meningkatkan kekhawatiran di kalangan pengguna jaringan. Hamzah (1992) dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" mendefinisikan kejahatan komputer sebagai kegiatan ilegal yang menggunakan komputer untuk tindakan pidana.

Keamanan komputer memiliki peran penting dalam menjaga kerahasiaan data, seperti yang diungkapkan oleh Wirdasari (2008). Dua faktor utama yang menjelaskan pentingnya keamanan komputer adalah: pertama, dalam masyarakat berbasis informasi, efisiensi dan akurasi penyajian informasi sangat vital bagi kinerja organisasi; kedua, infrastruktur jaringan komputer, termasuk LAN dan internet, menuntut penyajian informasi yang efisien, namun membuka peluang lubang keamanan (security hole). Beberapa faktor yang mempengaruhi pencurian data dan informasi di Indonesia termasuk keamanan jaringan, di mana peretas dapat mencuri data melalui jaringan yang terhubung, dan kurangnya kewaspadaan terhadap ancaman cyber. Kewaspadaan terhadap tanda-tanda ancaman cyber, seperti email spam atau website yang tidak aman, menjadi langkah mitigasi yang penting. Situasi di Indonesia juga memerlukan kewaspadaan terhadap cyberspace, mengingat peningkatan penggunaan internet dan kurangnya pembatasan serta pengawasan yang ketat, seperti yang diungkapkan oleh Mauludi (2018). Dengan meningkatnya pengguna internet di Indonesia, potensi kejahatan cyber juga semakin besar, memerlukan perhatian serius terhadap keamanan di wilayah operasi internet.

Tabel 1. Data Pengguna Internet di Indonesia

No.	Tahun	Jml Pengguna
1	2017	143,26 Jt
2	2018	171,17 Jt
3	2019	196,71 Jt
4	2021	202,6 Jt

Sumber: Diolah peneliti, 2023

Berdasarkan data di atas, peningkatan pengguna internet di Indonesia mencapai 29% setiap tahun. Pengaruh signifikan internet terlihat dalam berbagai sektor seperti ekonomi, sosial, budaya, politik, hukum, pendidikan, dan agama (Mauludi, 2018, p. xvii). Penggunaan internet memengaruhi cara berpikir, perilaku, dan interaksi sosial manusia, dengan dampak psikologis, sosiologis, dan budaya yang perlu diteliti lebih lanjut (Mauludi, 2018, p. xvii). Meskipun akses internet semakin mudah, masyarakat Indonesia masih memiliki literasi digital

rendah, menyebabkan ketidaksetaraan dan kerentanan terhadap kejahatan cyber (Mauludi, 2018, p. xviii). Media sosial, yang populer di Indonesia, memberikan dampak positif dan negatif, seperti pencemaran nama baik dan penyebaran konten berbahaya (Mauludi, 2018, p. xviii). Faktor-faktor yang mempengaruhi pencurian data di Indonesia mencakup penggunaan perangkat lunak tidak terupdate secara berkala, kata sandi yang lemah, dan ketidakjelasan dalam Undang-Undang ITE Tahun 2016 terkait kejahatan cyber (Kemenhan RI, 2019, p. 39; 16). Kelemahan dalam sistem keamanan informasi dan kurangnya kewaspadaan terhadap ancaman cyber crime juga menjadi faktor utama dalam pencurian data dan informasi di Indonesia.

Kejahatan Cyber dalam Perspektif Peperangan Asimetris.

Ancaman yang perlu diwaspadai dalam era digital saat ini adalah ancaman nonmiliter dari dunia cyber, yang dapat membahayakan pertahanan dan keamanan negara. Ancaman ini tidak hanya mengancam aspek fisik, ideologi, dan politik, tetapi juga mempengaruhi dimensi geografi, demografi, sumber daya alam, ideologi, politik, ekonomi, budaya, dan pertahanan (Kemenhan RI, 2017, p. 6). David L. Buffaloe menggambarkan peperangan asimetris sebagai bentuk konflik antara kekuatan populasi nontradisional dan kemampuan militer superior atau dengan kekuatan yang inferior melalui ancaman, operasi, pendekatan kultural, dan pembiayaan secara asimetris (Buffaloe, 2006). Ancaman cyber, khususnya dalam bentuk pencurian data dan informasi, menjadi kejahatan yang dilakukan melalui jaringan internet dengan biaya yang relatif murah. Ancaman ini dapat menjadi strategi peperangan asimetris yang digunakan untuk mencapai tujuan tertentu oleh negara atau kelompok tertentu. Cyber crime, melalui sarana komputer dan jaringan internet, mencakup berbagai bentuk seperti pencurian data, penipuan online, pemalsuan dokumen, serta kejahatan lainnya yang dapat mengubah bentuk kejahatan konvensional ke dalam ruang cyber (Tampubolon, 2019, p. 546).

Dalam perspektif peperangan asimetris, serangan cyber dianggap sebagai bagian dari gray zone area, yaitu wilayah di antara peperangan terbuka dan perdamaian penuh. Serangan ini dapat menyebabkan kerusakan serius seperti serangan militer konvensional, meskipun tidak terdeteksi secara langsung dan seringkali sulit dilacak ke sumber asalnya. Meskipun tidak terlihat sebagai serangan militer langsung, serangan cyber dapat menyebabkan kerusakan serupa, termasuk pada infrastruktur dan sistem pemerintahan. Taktik dan strategi serangan cyber dalam perspektif ancaman peperangan asimetris melibatkan negara atau kelompok sebagai subjek, menargetkan sistem komputer dan jaringan sebagai objek serangan, dan menggunakan metode seperti phishing dan remote access control. Sarana yang digunakan mencakup perangkat keras, perangkat lunak, dan jaringan internet. Motif serangan melibatkan tujuan ekonomi dan politik. Ancaman ini termasuk dalam kategori ancaman nonmiliter, dan dalam konteks penanggulangannya, partisipasi militer seperti Cyber Army Indonesia diperlukan untuk melibatkan pengawasan, pemantauan, dan perlindungan infrastruktur strategis negara dari serangan cyber (Kemenhan RI, 2014; UU No 3 Tahun 2002).

Langkah-langkah pemerintah Indonesia dalam menangani ancaman kejahatan cyber.

Menurut David L. Buffaloe (2006), serangan cyber lebih efektif melalui media informasi di dunia maya, memungkinkan penyebaran propaganda, penciptaan kebohongan,

dan pengembangan konspirasi. Respons masyarakat terhadap berita, apakah benar atau tidak, cenderung bergantung pada konfirmasi kebenaran yang ditemukan di media internet, dengan minimnya inisiatif mencari literatur kebenaran. Berdasarkan hukum Indonesia, kejahatan cyber diatur oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 27 hingga 30 UU ITE mengatur perbuatan yang dilarang, khususnya pasal 30 ayat (1), (2), dan (3) yang menyebutkan tentang hacking, termasuk akses tanpa hak, pemperoleh Informasi Elektronik dan/atau Dokumen Elektronik, serta akses dengan tujuan melanggar sistem pengaman. Pelanggaran UU ITE terkait kejahatan cyber dapat dikenai hukuman maksimal 6 tahun penjara dan denda hingga Rp.1 Milyar Rupiah..

Tabel 2. Data kasus kebocoran data pada sektor pemerintahan dan Swasta di Indonesia Tahun 2019-2022

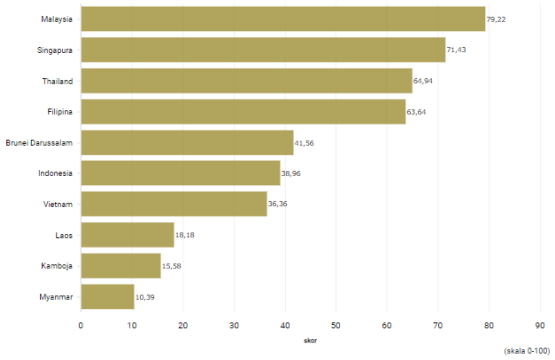
No.	Pemerintah/swasta	Jml data
1	Kemenkominfo (SIM Card)	1,3 M
2	PLN	17 Jt
3	KPU	105 Jt
4	Kemenkes (BPJS)	1,3 M
5	Indihome	26 Jt
6	BRI Life	2 Jt
7	Facebook	130,3 Rb
8	Bukalapak	13 Jt
9.	Tokopedia	91 Jt

Sumber: Diolah peneliti, 2023

Dari data di atas, sektor pemerintahan memunculkan tingkat kebocoran data tertinggi, khususnya dalam kasus SIM Card Kemenkominfo (1,3 milyar data) dan BPJS Kemenkes (1,3 milyar data). Sementara itu, sektor swasta mengalami tingkat kebocoran yang lebih rendah, yakni puluhan juta data. Hacker yang dikenal sebagai Bjorka memperoleh perhatian publik Indonesia pada tahun 2022 dengan menghebohkan sejumlah kasus pencurian data dan informasi. Bjorka mencantumkan sejumlah data pribadi masyarakat, mulai dari pelanggan IndiHome, registrasi SIM Card, hingga data KPU. Kasus pencurian data oleh Bjorka merupakan bentuk kejahatan cyber yang melanggar UU ITE Nomor 19 Tahun 2016.

Bjorka juga mencuri data rahasia Badan Intelijen Negara (BIN) yang ditujukan untuk Presiden Jokowi, serta melakukan doxing terhadap sejumlah pejabat publik Indonesia, termasuk Menkominfo Johnny G Plate, Puan Maharani, Semuel Abrijani Pangerapan, Luhut Binsar Pandjaitan, dan Erick Thohir. Meskipun Bjorka hanya menyebarkan data lama, kepolisian kesulitan mengungkap kasus ini, seiring dengan belum disahkannya rancangan Undang-Undang Perlindungan Data Pribadi. Kasus Bjorka menggambarkan kompleksitas penegakan hukum terhadap kejahatan cyber di tingkat internasional. Kejahatan cyber dapat merujuk pada berbagai tindakan tidak sah melalui teknologi informasi, seperti hacking, phishing, atau pencurian fisik media penyimpanan data. Meskipun telah ada perjanjian internasional yang mengatur tentang kejahatan cyber, kendala-kendala seperti perbedaan sistem hukum dan standar penegakan hukum antar negara masih menjadi tantangan. Untuk mengatasi hal ini, diperlukan kerjasama yang lebih erat antarnegara dalam menyelidiki dan menuntut pelaku kejahatan cyber.

Grafik indeks keamanan cyber di Asia Tenggara



Sumber: National Cyber Security Index, Tahun 2022

Berdasarkan National Cyber Security Index (NCSI) per Juni/Kuartal II Tahun 2022, Indonesia menempati peringkat keenam dengan nilai indeks 38,96 dari 100, di bawah Malaysia, Singapura, Thailand, Filipina, dan Brunai Darussalam. Indeks ini mencakup evaluasi kebijakan hukum, kerja sama pemerintah, dan program lembaga pemerintah terkait keamanan cyber. Menghadapi ancaman pencurian data dan informasi serta bahaya terhadap stabilitas pembangunan nasional, pemerintah Indonesia perlu mengambil beberapa langkah strategis, antara lain:

1. Pertama, pengembangan kemampuan teknologi jaringan informasi dan komunikasi untuk deteksi dan pencegahan ancaman cyber serta penanganan kerusakan.
2. Kedua, memperkuat kerjasama internasional dalam menghadapi ancaman cyber.
3. Ketiga, menetapkan aturan dan regulasi ketat terkait keamanan cyber dengan sanksi tegas bagi pelaku kejahatan cyber dan perusahaan tanpa keamanan cyber memadai.
4. Keempat, meningkatkan literasi digital di masyarakat untuk responsif terhadap ancaman cyber.
5. Kelima, melakukan edukasi dan sosialisasi pentingnya keamanan cyber bagi masyarakat.
6. Keenam, koordinasi dengan instansi terkait, baik dalam negeri maupun luar negeri, di bawah BSSN.

Dalam bidang pertahanan cyber, Kementerian Pertahanan RI telah mengeluarkan Pedoman Pertahanan Cyber (Peraturan Menteri Pertahanan Republik Indonesia No. 82 Tahun 2014) untuk memastikan keamanan jaringan dan muatan di sektor pertahanan. Secara keseluruhan, pemerintah mendorong pengembangan diri pegawai, menetapkan pedoman dan sertifikasi, melakukan edukasi, serta menjalin kerjasama dan koordinasi untuk menangani keamanan cyber baik di dalam negeri maupun luar negeri.

SIMPULAN

Kesimpulan dari penelitian ini menunjukkan bahwa faktor-faktor yang mempengaruhi pencurian data dan informasi di Indonesia melibatkan lemahnya sistem keamanan informasi, kurangnya kewaspadaan terhadap ancaman cyber crime, penggunaan perangkat lunak yang tidak diupdate secara berkala, password yang kurang kuat, dan ketidakjelasan aturan penegakan hukum terhadap peretas data dan informasi. Dalam perspektif peperangan asimetris, langkah yang perlu diambil adalah melibatkan militer, seperti Cyber Army Indonesia, untuk melakukan pemantauan dan pengawasan terhadap aktivitas online yang dapat membahayakan keamanan negara.

Langkah-langkah pemerintah Indonesia untuk menangani kejahatan

cyber melibatkan pendorongan pegawai yang membidangi sistem informasi untuk mengembangkan kemampuan teknologi jaringan informasi dan komunikasi, pembuatan pedoman SNI dan sertifikasi SNI tentang sistem manajemen keamanan data dan informasi, edukasi dan sosialisasi tentang keamanan cyber, serta kerjasama dan koordinasi antar lembaga atau organisasi terkait baik dalam negeri maupun luar negeri. Berdasarkan hasil penelitian, saran kepada pemerintah dan stakeholder terkait melibatkan penyebarluasan informasi bahaya ancaman cyber crime kepada masyarakat umum untuk pencegahan dini, penerapan manajemen sistem keamanan data dan informasi secara ketat, pembuatan Undang-Undang tentang kejahatan cyber (cyber law) dengan sasaran pelaku hacker jahat yang mencuri data dan informasi secara ilegal, serta peningkatan peran Cyber Army dalam menjaga keselamatan, keamanan bangsa, dan kedaulatan NKRI.

DAFTAR PUSTAKA

10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-ramai Bantah - Halaman 2. (n.d.). Retrieved January 24, 2024, from https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah/2

Apa Motif Bjorka Bocorkan Data? Ini Kata Kriminolog | Republika Online. (n.d.). Retrieved January 24, 2024, from https://news.republika.co.id/berita/rict01396/apa-motif-bjorka-bocorkan-data-ini-kata-kriminolog?

Bisnis Indonesia Daftar Kasus Kebocoran Data Indonesia, Sektor Pemerintah Juara? (n.d.). Retrieved January 24, 2024, from https://bisnisindonesia.id/article/daftar-kasus-kebocoran-data-indonesia-sektor-pemerintah-juara

Buffaloe, D. L. (2006). Defining Asymmetric Warfare. The Institute Land Warfare Papers (AUSA).

Gollmann,Dieter.(1999).ComputerSecurity.Jhon Willey &Son Inc Canada.

Hacker Bjorka is Back, Data Apa Saja yang Pernah Dibocorkan? (n.d.). Retrieved January 24, 2024, from https://www.cnbcindonesia.com/tech/20221111075351-37-386931/hacker-bjorka-is-back-data-apa-saja-yang-pernah-dibocorkan

Halder, D. &. (2011). Cyber Crime and the Victimization of Women Laws, Rights, and Regulations. Hershey PA, USA: IGI Global. ISBN 978-1-60960-830-9.

Hamdi, A.,dkk. (1992).Aspek-Aspek Pidana bidang Komputer.Jakarta:Sinar Grafika.

Howard, Jhon D.(1997).An analysis of security Incidents On The Internet.Software Engineering Insitute.

Kaelan, M. S. (2010). Pendidikan Pancasila. Yogyakarta: Paradigma.

Keamanan Siber Indonesia Peringkat ke-6 di Asia Tenggara. (n.d.). Retrieved January 24, 2024, from https://databoks.katadata.co.id/datapublish/2022/03/07/keamanan-siber-indonesia-peringkat-ke-6-di-asia-tenggara

Kebocoran data pribadi dan tanggungjawab pemerintah: “Tak perlu ada gugatan, kalau regulator berani dan tegas” - BBC News Indonesia. (n.d.). Retrieved January 24, 2024, from https://www.bbc.com/indonesia/articles/c19mdml39m2o

Kemenhan RI. (2014). Strategi Pertahanan Negara. Kementerian Pertahanan Republik Indonesia.

Kemenhan RI. (2017). Kewaspadaan Nasional, Bela Negara dan Integrasi Nasional. Puskom Publik Kemhan (WIRA) Edisi JULI-AGUSTUS 2017 - VOLUME 67/NOMOR 51.

Kemenhan RI. (2019). Pengetahuan Cyber: Dalam Gerakan Nasional Bela Negara. Jakarta: Kementerian Pertahanan Republik Indonesia.

Mauludi, S. (2018). Socrates Café: Bijak, Kritis & Inspiratif Seputar Dunia & Masyarakat Digital. PT Elex Komputindo.

Moore. (2005). Cyber Crime: Investigating High-Technology Computer Crime. Mississippi Cleveland: Anderson Publishing.

NEWS : 12 Kasus Kebocoran Data di Indonesia Sejak 2019. (n.d.). Retrieved January 24, 2024, from https://cyberthreat.id/read/12752/12-Kasus-Kebocoran-Data-di-Indonesia-Sejak-2019

Peraturan Menteri Pertahanan Republik Indonesia No. 82 Tahun 2014 tentang Pedoman Pertahanan Cyber.

Richard A. Clarke, d. R. (2010). Cyber War-The Next Threat to National Security and What to Do About It. Harper Collins Publishers.

Sari, Ika.Y.,dkk. (2020). Keamanan Data dan Informasi.Medan:Yayasan Kita Menulis

Stalling, W. (2005) Cryptography and Network Securty Principles and Pratices Fourth Edition. Prentice Hall.

Subagyo, A. (2015). Sinergi dalam Menghadapi Ancaman Cyber Warfare. Jurnal Pertahanan Vol 5, No 1 (2015).

Tampubolon, K. E. (2019). Perbedaan Cyber Attack, Cyber crime, dan Cyber Warfare. Jurist-Diction: Vol. 2 No. 2, Maret 2019.

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektroknik.

Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.

UNTERM. (n.d.). Retrieved January 24, 2024, from https://unterm.un.org/unterm2/DGAACS/unterm.nsf/WebView/BFDE24673F1B1F6E85256AFD006732A3?O.

Warren G. Kruse, J. G. (2002). Computer forensics: incident response essentials. Addison-Wesley ISBN 0-201-70719-5.

Wirdasari, D. (2008). Mengenal Teknik-Teknik Keamanan Komputer dan Model-Model Serangannya (Security Attack Models). Security Attack Models, 4(1), 111–119.