FAKTOR-FAKTOR YANG MELATAR BELAKANGI KERJASAMA INDONESIA DENGAN INGGRIS DIBIDANG KEAMANAN SIBER TAHUN 2018

Bobby Firdaus Usman
Bobbyfirdausman10@gmai.com

Abstract
This study aims to analyze the factors behind the cooperation between Indonesia and the UK regarding cyber security 2018. The research method used is an explanative research method. The data collection technique is literature study. The results of this study illustrate that the 2018 Indonesian and British cyber cooperation, as an implementation of improving Indonesian cyber security strategies and tackling cybercrimes in Indonesia. The theory used in this study is bilateral cooperation, cybersecurity. Based on this theory, it can be concluded that cybercrimes that occurred in Indonesia occurred due to the weakness of the 5 principles in cybersecurity planting, as well as weak human resources and lack of awareness in cybersecurity planting in Indonesia. Indonesia.
Keywords: Cooperation, cyber security, Indonesia

Abstrak
Penelitian ini bertujuan untuk menganalisa Faktor- faktor yang melatarbelakangi kerjasama indonesia dan inggris terkait keamanan siber 2018. Metode penelitian yang digunakan adalah metode penelitian explanatif. Teknik pengumpulan data yaitu studi kepustakaan. Hasil penelitian ini menggambarkan bahwa Kerjasama siber Indonesia dan inggris tahun 2018, sebagai pelaksanaan peningkatan strategi keamanan siber indonesia dan penangulangan kejahatan siber di Indonesia. Teori yang digunakan dalam penelitian ini kerjasama bilateral, cybersecurity, di Berdasarkan teori tersebut, dapat disimpulkan bahwa kejahatan siber yang terjadi di Indonesia terjadi karena lemahnya 5 prinsip dalam penanaman keamanan siber, serta masih lemahnya Sumber daya manusia serta masih kurangnya kesadaran dalam penanaman keamanan siber di Indonesia.
Kata Kunci: Kerjasama, *cyber security*, indonesia

PENDAHULUAN

Setiap negara-negara pada dasarnya berupaya untuk memenuhi kebutuhannya. Kebutuhan tersebut akan mendorong negara-negara tersebut untuk melakukan kerjasama diharapkan mampu memenuhi kebutuhan, dan kepentingan negara-negara guna bertahan di dunia internasional. Hubungan kerjasama antar negara akan terus berkembang sesuai dengan kebutuhan yang dimiliki oleh Negara tersebut, misalnya terkait permasalahan keamanan(Frame, 2006).

Masalah keamanan dan keselamatan negara merupakan kepentingan nasional yang paling utama bagi setiap negara. Masalah ini menjadi salah satu dasar untuk landasan bagi negara dalam membuat suatu kebijakan politik luar negeri terhadap negara lain. Perkembangan teknologi dan informasi yang pesat saat ini membawa dampak yang besar dalam dunia hubungan internasional saat ini bukan hanya melanda negara-negara maju tetapi negara berkembang pun ikut mengembangkan teknologi dan informasi. Seiring dengan kemajuan yang sangat pesat negaranegara saling mengembangkan teknologi agar dapat bertahan dalam era globalisasi saat ini(Ghernaouti-Hélie, 2009).

Kemajuan teknologi pada saat ini mendorong perkembangan terhadap perangkat komputer yang didukung oleh perkembangan jaringan internet yang pesat, sehingga perkembangan komputer dan jaringan internet ini menyebabkan makin meningkatnya suatu resiko yang ditimbulkan dari penyalahgunaan *cyberspace* saat ini semakin meningkat

dan rumit yang dapat membajak infrastruktur vital suatu negara yang terintegrasi melalui jaringan internet(Piliang, 1999).

Masyarakat internasional saat ini sangat memperhatikan perkembangan ancaman *cybercrime.* Kekhawatiran tersebut dikarenakan *cybercrime* semakin mudah dilakukan oleh pihak-pihak tertentu. Serangan siber (*cyber-attack*) merupakan salah satu bentuk *cybercrime* dapat dilakukan untuk menyerang, baik secara individu maupun digunakan untuk menyerang suatu kelompok atau organisasi bahkan negara lain. Kemajuan teknologi komputer dan kemajuan internet yang saat ini terjadi menyebabkan semakin meningkatnya kasus yang ditimbulkan oleh peretas komputer *(computer hackers)*. Kegiatan para peretas komputer ini dapat dilakukan dalam hal positif maupun negatif.Dalam hal positif, para peretas computer biasanya memasuki suatu sistem dengan memanfaatkan kekurangan atau celah yang ada pada suatu sistem tersebut(Sterling, 2010).

Berdasarkan data yang ada menurut Menteri Kordinator Bidang Politik, Hukum dan Keamanan Republik Indonesia Wiranto, Indonesia dengan posisi siber nasional yang sangat terbuka ini, perlu mengembangkan strategi keamanan siber yang efektif dan mempunyai daya tangkal tinggi. Keamanan dunia siber nasional merupakan salah satu bidang yang perlu didorong dan diperkuat oleh pemerintah sebagai upaya meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional.Indonesia sebagai negara dengan pengguna internet terbesar nomor dua dunia, berperan penting dalam membentuk ketahanan masyarakat Indonesia yang multikultur serta menghormati demokrasi dan pluralisme (Indrawan, 2016).

Dengan pengguna internet yang cukup besar, Indonesia saat ini telah menjadi salah satu negara yang mengalami serangan siber yang cukup besar.Tercatat, serangan kepada laman-laman pemerintah mencapai sekitar 3000 serangan per hari.Serangan siber biasanya menyerang arus lalu lintas di bidang *e-commerce*, saham, perbankan dan menyangkut persoalan jasa keuangan.Serangan siber juga biasanya menyerang database database *online* pemerintah yang menyimpan data-data penting negara, seperti data penduduk, keuangan, dan sumber daya alam.

Telah banyak kasus yang diakibatkan dari serangan *cyber* yaitu seperti kasus Serangan *Ransomware WannaCry*.*WannaCry* adalah salah satu serangan cyber terbesar yang pernah terjadi di dunia.Tidak kurang dari 150 negara terkena dampak ransomware yang mengunci sistem komputer ini, termasuk Indonesia. Dibanding ransomware lain yang sebelumnya hanya menyebar secara relatif terbatas, *WannaCry* lebih "sakti" karena memanfaatkan *tool* senjata *cyber*dinas intel Amerika Serikat, *National Security Agency* (NSA), yang dicuri hacker dan dibocorkan di internet. Itulah mengapa *WannaCry* bisa menyebar luas dalam waktu relatif singkat. Hanya dalam beberapa jam, sang program jahat mampu menginfeksi ribuan sistem komputer di puluhan negara. Serangannya tak pandang bulu.Mulai dari industri otomotif, telekomunikasi, perbankan, hingga rumah sakit menjadi korban dan dipaksa membayar tebusan(New Forms of Governance, 2003).

Bahkan tidak hanya Negara Indonesia saja yang mendapatkan serangan cyber tersebut tetapi Negara Inggris pun juga mengalami serangan cyber tersebut. Jaringan *National Health Service* (NHS) di Inggris dibuat kerepotan karena ransomware mengunci dan "menyandera" data pasien di komputer rumah sakit.*National Cyber Security Center* (NCSC) Inggris berupaya memulihkan sistem komputer NHS.Sementara itu, pelayanan medis untuk pasien jadi tertunda. Ambulans terpaksa dialihkan ke

rumah sakit lain yang tak terdampak, sejumlah kegiatan operasi pun dibatalkan. Inggris mengumumkan ada setidaknya 45 organisasi kesehatan yang terdampak di negara itu.Data rekam medis pasien tidak ada yang dicuri, melainkan dikunci dan dimintai tebusan oleh ransomware (BBC, 2017).

KERANGKA ANALISIS

Proses kerjasama terbentuk dari perpaduan keanekaragaman masalah nasional, regional, global yang muncul dan memerlukan perhatian dari lebih satu Negara. Masing-masing pemerintah melakukan pendekatan dan memberikan saran, melakukan tawar-menawar atau mendiskusikan suatu masalah, mengumpulkan bukti-bukti tertulis untuk membenarkan suatu usul atau yang lainnya, dan mengakhiri perundingan dengan suatu perjanjian atau pengertian yang memuaskan semua pihak. Kerjasama merupakan suatu proses dimana pemerintah suatu Negara saling berhubungan dengan mengajukan pemecahan, perundingan atau pembicaraan mengenai masalah nasional, regional maupun global (Holsti, 1993).

Kerjasama Internasional adalah hubungan antara negara yang memiliki tujuan berlandaskan kepentingan antar negara.Kerjasama Internasional terdiri dari, seperangkat aturan, prinsip-prinsip, norma-norma, dan prosedur pembuat keputusan yang mengatur jalannya rezim interasional. (Martin, 2007) Selain itu, negara-negara yang melakukan kerjasama internaisonal mempunyai tujuan bersama atau kepentingan bersama karena, ketidak beradaan kepentingan bersama di dalam kerjasama, merupakan sesuatu hal yang mustahil.(Keohane, 1989).

Kerjasama internasional adalah ketergantungan antar actor akan membuat mereka melakukan kerjasama untuk mengahadapi ancaman yang akan membahayakan kepentingan internasional (Betsill, 2006). Adanya kesamaan tujuan atau kepentingan bersama merupakan hal yang wajib dalam kerjasama.Tidak dipungkiri bahwa dalam kerjasama selalu terdapat benturan kepentingan masing-masing negara, namun selama tujuan bersama dapat disepakati, sejauh itu pula kerjasama dapat terus berjalan.

METODE PENELITIAN

Dalam menyusun penelitian ini, penulis menggunakan metode analisis data kualitatif dan model analisis data eksplanatif. Pengertian penelitian kualitatif dapat dirtikan sebagai penelitian yang menghasilkan data, mengenai kata-kata lisan maupun tertulis, dan tingkah laku yang dapat diamati dari apa yang diteliti (Steven, 1992). Model analisis data kualitatif menekankan kepada penyajian data non-statistik dengan cara menggambarkan dan menginterpretasikan suatu informasi ke dalam buku teks.

Sementara model analisis data eksplanatif digunakan untuk menghadirkan dua variable yang saling terkait dan mempengaruhi satu sama lainya. Kedua variable tersebut menurut Mochtar Mas'oed adalah unit analisis dan unit eksplanasi. Unit analisis yakni obyek yang perilakunya akan dianalisis atau disebut dengan variabel dependen. Sementara unit eksplanasi adalah obyek yang mempengaruhi unit analisa yang digunakan atau disebut juga sebagai variable independen

Adapun teknik pengumpulan data yang penulis lakukan dalam penelitian ini adalah teknik studi kepustakaan *(Library Research)* dan teknik wawancara *(Qualitative Interview).*Teknik studi kepustakaan merupakan teknik pengumpulan data dengan menemukan sumber referensi/literatur yang relevan bagi penelitian penulis (baik berupa buku, artikel jurnal, berita baik melalui media cetak atau elektronik, serta literatur lainya yang terkait dengan penelitian penulis), yang kemudian penulis menyaring dan

melakukan telaah terhadap informasi dari sumber sumber tersebut.

Dalam penelitian ini penulis menyaki bahwa dengan metode analisis data kualitatif dan model analisais dta exspanatif merupakan metode dan model analisa yang tepat digunakan dalam menganalisa Faktor-faktor yang melatarbelakangi kerjasama Indonesia dan Inggris dalam bidang keamanan siber tahun 2018.

PEMBAHASAN

Situasi saat ini menggarisbawahi keharusan bagi Indonesia untuk memiliki kebijakan dan strategi keamanan siber.Kebijakan dan strategi dunia maya harus didasarkan pada kepentingan nasional negara. Sebagaimana dinyatakan dalam pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, aspirasi nasional Indonesia bertujuan untuk melindungi semua rakyat Indonesia dan seluruh tanah air Indonesia, untuk memajukan kesejahteraan umum, untuk mengembangkan kehidupan intelektual bangsa, dan untuk berkontribusi pada implementasi tata dunia. Selain itu, tujuan-tujuan ini diperkuat oleh UU No. 3/2002 tentang pertahanan negara, yang bertujuan untuk melindungi kedaulatan negara, wilayah nasional, dan keselamatan bangsa dari semua jenis ancaman(UUD 45, 2002).

Serangan-serangan yang terjadi di indonesia tidak lepas dari para pengguna internet indonesia, Konvergensi itu sendiri adalah merupakan gejala yang mengemuka dalam industri jasa Teknologi Informasi Komunikasi (TIK) yang muncul sejalan dengan pesatnya kemajuan teknologi elektronika pada akhir abad 20. Dampak konvergensi secara sosial telah dirasakan masyarakat baik itu positif maupun negatif.Salah satu dampak negatif yang muncul dalam *cyberspace* adalah terjadinya *cybercrime*. Maraknya *cybercrime* memerlukan perhatian dan keseriusan dalam mengembangkan *cybersecurity* bagi sebuah negara termasuk Indonesia.

Pesatnya perkembangan teknologi informasi membuat pengguna internet kawasan Asia tumbuh pesat 1.319 persen sepanjang 2000-2015. Menurut data Internet Worlds Stats, pengguna internet Asia sat ini mencapai 1,62 miliar jiwa dengan penetrasi 40,2 persen dari total populasi sebesar 4 miliar jiwa. Sebanyak 674 juta jiwa pengguna internet Asia berasal dari Cina.Indonesia menempatkan peringakat 4 di Asia(Internet Worlds Stats, 2015).

Kebijakan *cyber-security* secara khusus di Indonesia telah diinisiasi sejak tahun 2007 dengan dikeluarkannya Peraturan Menteri Komunikasi dan Informatika No.26/ PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika No.16/PER/M.KOMINFO/10/2010 yang kemudian diperbaharui lagi dengan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010. Salah satu yang diatur dalam peraturan tersebut adalah pembentukan ID-SIRTII, yang merupakan kepanjangan dari *Indonesia Security Incident Response Team on Internet Infrastructure* adalah Tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet(kemifo, 2010).

Tugas dan fungsi dari ID-SIRTII diantaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-pihak terkiat di dalam maupun luar negeri di dalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan mengembangkan sistem database sistem

IDSIRTII, menyusun katalog-katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi contact point dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakn pekerjaan yang berkaitan dengan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet.

Kerangka hukum *cybersecurity* di Indonesia saat ini dibangun diantaranya berdasarkan atas dasar UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri. Terkait dengan upaya menjamin kepastian hukum dalam pengembangan *cybersecurity* telah dilakukan antara lain dengan melaksanakan serangkaian program yang sudah mulai berjalan diantaranya: menginisiasi peraturan perundangundangan yang terkait dengan *cybersecurity* seperti UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012, menyusun kerangka nasional *cyber-security* (UUD 45, 2012).

Pertahanan cyber yang lemah dapat menciptakan ketegangan di antara negara-negara dan mengganggu stabilitas keamanan, menciptakan dampak sosial, ekonomi, dan lingkungan, serta mengganggu hubungan antar negara (Ghernaouti-Hélie, 2009, hal. 24).

Keamanan dunia maya memiliki dua kata kunci: dunia maya dan keamanan. Berbicara tentang dunia maya berarti berbicara tentang informasi, koneksi (telekomunikasi, jaringan), gateway (komputer, perangkat, pengguna), ruang, atau ruang, dan ini tentang melibatkan, menggunakan, atau berkaitan dengan komputer, jaringan, dan internet.Sementara itu, keamanan biasanya terkait dengan aset dan perlindungan aset.Keamanan melindungi aset, melindungi komputer, jaringan, program, dan data dari akses, perubahan, atau perusakan yang tidak disengaja atau tidak sah, melindungi informasi dan sistem dari ancaman dunia maya yang besar (Ghernaouti-Hélie, 2009, p. 28).

Cyberspace menghadirkan manfaat dan tantangan bagi keamanan nasional, kemakmuran ekonomi dan kesejahteraan sosial negara, memengaruhi bisnis serta individu. Mengingat bahwa hari ini, negara semakin menjadi aktor di dunia maya, termasuk mengejar kepentingan keamanan nasional mereka, ada kebutuhan untuk berkolaborasi dan meningkatkan rasa saling percaya. Ini harus dibangun transparansi antara negara dan mengembangkan langkah-langkah untuk membantu mencegah risiko konflik yang disebabkan oleh kesalahan persepsi dan salah perhitungan antara negara di dunia maya. Beberapa forum internasional tentang tindakan membangun kepercayaan dunia maya (CBM)ditahan secara teratur oleh banyak negara, termasuk anggota ASEAN, serta organisasi regional lainnya. Tujuan kolaboratif tersebut kegiatannya adalah untuk mencapai pemahaman bersama dengan memberikan transparansi langkah-langkah untuk meningkatkan stabilitas di dunia maya.

Namun hingga saat ini, upaya untuk mencapai pemahaman bersama tentang transparansi seperti yang diusulkan oleh forum-forum CBM dunia maya ini tampaknya jauh dari keadaan 'niat atau keinginan nyata untuk berbagi dan bertukar informasi penting. Ini mungkin terjadi karena kurangnya pemahaman tentang sifat ancaman, selain apa yang sebenarnya merupakan filosofi terbaik

untuk benar mengatur dunia maya. Ini penting karena kepentingan nasional mungkin berbeda di setiap negara.

KESIMPULAN

Perkembangan pesat teknologi dalam bidang informasi dan komunikasi telah menjadi lokomotif pemacu lahirnya globalisasi.Sifat global dari kemajuan teknologi ini pada gilirannya berbarengan dengan pesatnya kemajuan dan kecanggihan berbagai tindak pidana.Indonesia saat ini dalam keadaan yang sangat mengkhawatirkan dalam keamanan siber.

Dalam tataran kebijakan, penangganan cybercrime berbeda dengan penangganan kejahatan lainnya.Namun berbeda dengan penangganan kejahatan lainnya, cyber-security membutuhkan pemikiran yang komprehensif untuk menangganinya implementasi strategi nasional keamanan siber dari sisi sumber daya manusia, prosedur dan kebijakan pencegahan dan keamanan yang masih memerlukan koordinasi dengan seluruh pemangku kebijakan bagi dari sektor swasta, pemerintah, masyarakat, dan institusi luar negeri yang merupakan pengembang dari aplikasi-aplikasi yang seringkali dipergunakan sebagai media kejahatan siber, dan teknologi yang harus dikembangkan seiring dengan meningkatnya jenis serangan siber.

Permasalah terkait dengan pembangunan cyber-security yang tangguh di antaranya lemahnya pemahaman penyelenggara negara atan security terkait dengan dunia cyber yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya penggunaan secured system; belum adanya legalitas yang memadai terhadap penanganan penyerangan di dunia cyber,

Cyber-security ke depan hendaknya dibangun atas lima bidang dasar yaitu adanya kepastian hukum (undang-undang cybercrime); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); capacity building & pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman cybercrime terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman cyber).Karena keamanan siber merupakan sebuah ekosistem dimana aspek legal, organisasi, skill, kerjasama, dan implementasi teknik berjalan secara selaras untuk hasil yang efektif. Dan semua itu sangat diperlukan kerjasama dengan negara lain agar dapat meingkatkan strategi keamanan siber nasonal.

DAFTAR PUSTAKA

BUKU

APJII. (2017). Sejarah Internet di Indonesia.

BPRTIK. (2017). *Pengembangan dan Pelatihan Cybe Secuirty Indonesia*. jakarta.

Buzan, Barry. (1998). security: A New Framework For Analysis. Cororado: Lynne Rienner.

Buzan, Bary & Ole Waever. (2003). *Region And Power: The Structure Of International Security.* Cambridge: Cambridge Universiry Press.

Chendramata, A. (2018). *Indonesia Cybersecurity.* Jakarta: Direktorat Keamanan Informasi.

CSIS. (2017). *Cybercrime Global. Center For Strategic And International Studies* (CSIS).

Doughterty, J,E & Pfaltzgraff. R,L. (1997). *Contending Theory of International Relation: a Comperehensive Survey* (Four ed.). Addition Wesley Educational Publiser.

Drucker, P. F. (1999). *Management Challenges for 21st Century*. New York: HarperCollins.

Frame, J. D. (2006). *International Business and Global Technology*. Maryland: Lexington Books.

Ghernaouti-Hélie, S. (2009). *Cybersecurity Guide for Developing Countries (*Enlarged Edition ed.). Geneva: International Telecommunication Union.

Hidayat. (2016). *Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia*. Literatur Jurnal UI, 8-10.

Hufron, S. (2016). *Upaya Indonesia dalam Menangani Cyber Crime Sebagai Kejahatan Transnasional*. Malang: Universitas Muhammadiyah Malang.

Internet Worlds static. (2015). User internet Indonesia.

kemifo. (2010). Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/201. presiden RI.

keminfo. (2017). perkembangan pendidikan dan standarisasi cyber. jakarta.

Kenham. (2017). Peraturan Presiden Nomor 133 Tahun 2017. Presiden Republik Indonesia.

KOICA. (2014). seminar kerjasama koica dengan ITB. Bandung: koica.

Mcfee. (2010). "A Good Decade for Cybercrime". Mcfee report.

Midhio, I. W., Reksoprodjo, Y., & Zaelani, a. H. (2018). Pembangunan Kapasitas Cyber Security di Negara ASEAN: Analisis Komparatif Terhadap Brunei dan Indonesia. Unhan Journal, 79-81.

NCA. (2018). volume cyberattact on uk busnise. National cyber attact.

NCSC. (2017). *cybersecurity cost.* National Cyber Security Center (NCSC) .

NCSN. (2018). cybersecurity global. National Cyber Security Center (NCSC) .

Ooredoo, P. I. (2015). *Menerima Sertifikasi ISO 27001 Dari Standar Inggris Lembaga Untuk Sistem Manajemen Keamanan Informasin.*

Othman, A. U. (2017). Analisis Penggunaan Media Siber terhadap Keamanan Nasional: Suatu Studi di Malaysia. Unhan Journal, 65-66.

Piliang, Y. A. (1999). *Introduction. In M. Slouka, Ruang yang Hilang: Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan* . Bandung: Mizan.

Sterling, B. (2010). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam Books.

Steven, R. B. (1992). *Introduction To Quaitative Research Methods: A Pheomenological Approach To The Social Sciences*. Surabaya: Usaha Nasional.

DOKUMEN

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikas. Jakarta: Presiden Republik Indonesia.

Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. .

Undang-Undang Nomor 23 Tahun 2006 tentang *Administrasi Kependudukan.*

Undang-Undang Nomor 25 Tahun 2009 Tentang *Layanan Publik Mengidentifikasi Sektor-Sektor Penting Atau Strategis*.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. PRESIDEN RI.

Undang-undang UU No. 3/2002 tentang pertahanan negara. Presiden RI.

Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri.

Warana, A. C., Pedrason, R., & Prasetyo, a. T. (2017). Implementasi Digital Forensik Brunei Darussalam Dalam Membangun Keamanan Siber. Unhan Journal, 12-15.

WEBSITE

Dirjen Aplikasi telematika. (2013, Oktober 23). . Indeks Keamanan Informasi. Retrieved from https://www.kominfo.go.id/content/detail/3326/indeks-keamanan-informasikami/0/kemanan_informasi

New Forms of Governance. (2003). Social Regulations of the Global Market, Univ. of Marryland. Retrieved from http://web2.law.buffalo.edu/faculty/meidinger/823/Haufler.pdf

Indrawan, A. (2016, October 12). Republika. Retrieved from Republika.co.id: https://www.republika.co.id/berita/dunia-islam/fatwa/17/04/30/nasional/hukum/16/10/12/oew6e8365-menko-polhukam-bangun-badan-siber-antisipasi

International Telecommunication Union. (2017). peringkat cybersecurity di dunia. Retrieved from https://www.google.com/search?q=International+Telecommunication+Union&rlz=1C1CHBF_enID838ID838&oq=International+Telecommunication+Union&aqs=chrome.69i57j0l5.2213j0j9&sourceid=chrome&ie=UTF-8

Internet Worlds Stats. (2015). pengguna internet di Indonesia. Retrieved from https://www.google.com/search?q=Internet+Worlds+Stats&rlz=1C1CHBF_enID838ID838&oq=Internet+Worlds+Stats&aqs=chrome..69i57j0l5.1233j0j7&sourceid=chrome&ie=UTF-8

APJII. (2018). Retrieved from APJII STATISTIK: https://nandonurhadi.wordpress.com/2013/02/20/jumlah-pengguna-internet-indonesia-tahun-1998-2012-versi-apjii/

APNIC. (2009). History protocol of Internet Indonesia.

BBC. (2017, October 27). BBC. Retrieved from BBC.com: https://www.bbc.com/news/technology-41753022

BSSN. (2018, agustus 18). Retrieved from https://bssn.go.id/bssn-tandatangani-nota-kesepahaman-kerjasama-di-bidang-keamanan-siber-dengan-pemerintah-inggris-raya/

global cybersecurity index. (2018). global security index 2018. Retrieved from https://www.google.com/search?q=global+cybersecurity+index&rlz=1C1CHBF_enID838ID838&oq=global+cybersecurity+index&aqs=chrome.69i57j35i39l2j0l3.1266j0j9&sourceid=chrome&ie=UTF-8

cyber security statistic. (2017). nitizen worldwide. index cyber security statistic.

ID-CERT. (2017, 9 27). laporan standarisasi pendidikan cyber indonesia. Retrieved from from cert.or.id: https://www.cert.or.id/tentang-kami/id