JURNAL IMAGINE
Vol. 3 No 2 – Desember 2023
p-ISSN 2684-947X (Print), e-ISSN 2684-9461 (Online)
Available Online at :
https://jurnal.std-bali.ac.id/index.php/imagine

ANCAMAN SPIONASE DALAM PENGGUNAAN WHATSAPP DI BIDANG PERTAHANAN INDONESIA

Abdul Razzaq Matthew Aditya[1], Amelia Widya Octa Kuncoro Putri[2], Anastasyia S. Kundhalini[3], David Yacobus[4]

[1234]Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan RI

e-mail: armatthewaditya1@gmail.com[1]

INFORMASI ARTIKEL

Received : April, 2023
Accepted : Desember, 2023
Publish online : Desember, 2023

A B S T R A C T

WhatsApp is a popular instant messaging app among Indonesians, but its data security and login access system have been a major concern. The vulnerability of the security system has led to an increase in cyber practices that can harm WhatsApp users, including espionage. The aim of this study is to identify the potential for espionage using WhatsApp in the virtual world. The research method used in this study was a literature review, including journals, articles, news, and websites related to espionage and WhatsApp. The findings of this study indicate that espionage is a cybercrime used as a military strategy to steal political, economic, and military information. Additionally, WhatsApp is one of the most widely used instant messaging apps among Indonesians and ranks second in terms of usage. Thirdly, potential espionage on the WhatsApp application includes spyware planting, hacking through calls, MP4 video formats, URL links, photo filter features, and malware planted through phone numbers, known as Pegasus spyware. Spyware Pegasus attacks the zero-day system of iOS and Android systems and smartphone applications, including the WhatsApp application currently used by Indonesian government agencies as a communication and work media. Finally, prevention measures that can be taken include protecting information, ensuring existing security measures, and planning for risks and threats.

Key words : *WhatsApp Application, Defense Sector, Cyber Crime, Espionage, Strategy*

A B S T R A K

WhatsApp merupakan salah satu aplikasi pesan instan yang populer di kalangan masyarakat Indonesia, namun keamanan data dan sistem akses login menjadi perhatian utama. Kelemahan sistem keamanan ini telah menyebabkan peningkatan praktik siber yang dapat merugikan pengguna WhatsApp, termasuk spionase. Tujuan dari penelitian ini adalah untuk mengidentifikasi potensi spionase menggunakan WhatsApp di dunia maya. Metode penelitian yang digunakan adalah tinjauan literatur, termasuk jurnal, artikel, berita, dan situs web terkait spionase dan WhatsApp. Hasil penelitian menunjukkan bahwa spionase adalah kejahatan siber yang digunakan sebagai strategi militer untuk mencuri informasi politik, ekonomi, dan militer. Selain itu, WhatsApp merupakan

salah satu aplikasi pesan instan yang paling banyak digunakan oleh masyarakat Indonesia dan menempati peringkat kedua dalam hal penggunaan. Potensi spionase pada aplikasi WhatsApp meliputi penanaman spyware, peretasan melalui panggilan, format video MP4, tautan URL, fitur filter foto, dan malware yang ditanam melalui nomor telepon, yang dikenal sebagai spyware Pegasus. Spyware Pegasus menyerang sistem zero-day dari sistem iOS dan Android serta aplikasi smartphone, termasuk aplikasi WhatsApp yang saat ini digunakan oleh lembaga pemerintah Indonesia sebagai media komunikasi dan bekerja. Terakhir, tindakan pencegahan yang dapat dilakukan termasuk melindungi informasi, memastikan keamanan yang ada, dan merencanakan risiko dan ancaman.

Kata Kunci: Aplikasi WhatsApp, Sektor Pertahanan, Kejahatan Dunia Maya, Spionase, Strategi

PENDAHULUAN

Perkembangan teknologi yang semakin cepat dan canggih dalam era globalisasi telah mempengaruhi berbagai aspek kehidupan di seluruh dunia. Salah satu dampaknya adalah perubahan cara berkomunikasi yang semakin mudah dan terhubung secara borderless, baik antar individu maupun negara. Perusahaan startup juga muncul dan berkembang dengan menciptakan aplikasi-aplikasi komunikasi seperti Line, Telegram, *WhatsApp*, dan lain-lain. Namun, meskipun aplikasi *WhatsApp* menjadi aplikasi pesan instan yang paling populer di Indonesia, masifnya penggunaan aplikasi ini juga memicu berbagai macam kejahatan cyber atau *cyber-crime* seperti penipuan, peretasan akun, penyadapan, dan spionase.

Proses globalisasi telah mempengaruhi seluruh dunia. Ini sebenarnya mempengaruhi setiap aspek kecil kehidupan di setiap negara di dunia. Karena globalisasi membuat perkembangan teknologi semakin cepat dan canggih. Masing-masing bidang kecanggihan tersebut mempengaruhi bidang komunikasi (Nurhaidah & Musa, 2015). Meskipun terjadi perubahan cara hidup masyarakat sesuai dengan globalisasi, salah satunya adalah cara berkomunikasi. Di era globalisasi, komunikasi menjadi lebih mudah. Sebuah artikel dari laman (tirto.id, 2021) menjelaskan bahwa globalisasi telah berkontribusi pada terciptanya alat komunikasi seperti telepon, internet dan banyak lagi lainnya, yang dapat mempermudah koneksi seluruh manusia di dunia. Padahal, komunikasi bisa terjadi di mana saja, kapan saja dan dengan jarak yang berbeda, baik dekat maupun jauh. Jenis komunikasi baru ini menjadikan jaringan komunikasi di era globalisasi tidak terbatas, yaitu tidak hanya memudahkan hubungan antar individu, tetapi juga hubungan antar negara (Zulkarnain et al, 2014)

Semakin majunya peralatan komunikasi dan internet di zaman globalisasi, bisnis mengalami perubahan arah dan memicu lahirnya perusahaan startup yang kini semakin populer dan berkembang pesat setiap tahunnya (Abdillah, 2019). Perusahaan startup memberikan kontribusi dengan menciptakan aplikasi-aplikasi untuk berkomunikasi baik secara pribadi maupun publik. Menurut (kompas.com, 2021), perusahaan startup fokus pada layanan atau produk berbasis teknologi. Beberapa startup telah menjadi perusahaan teknologi yang diakui secara global. Produk aplikasi komunikasi yang telah diakui dan populer di antaranya Line, Telegram, Kakaotalk, WeChat, Instagram, *Twitter*, *Facebook*, *WhatsApp*, dan banyak lagi. Aplikasi-aplikasi ini mempercepat penyebaran informasi dan membuat komunikasi menjadi lebih menarik karena memiliki fitur-fitur unggulan yang menarik banyak pengguna. Dilansir dari (cnnindonesia.com, 2021), aplikasi-aplikasi ini populer di kalangan masyarakat karena mudah digunakan dan memberikan kenyamanan.

WhatsApp merupakan salah satu aplikasi pesan instan yang populer di Indonesia. Menurut (databoks.katadata.co.id, 2021), Indonesia menempati peringkat ketiga di dunia dalam penggunaan WhatsApp dengan jumlah pengguna mencapai 84,8 juta pada Juni 2021. (Kontan.co.id, 2022) melaporkan bahwa WhatsApp adalah aplikasi nomor satu yang paling sering digunakan oleh masyarakat Indonesia. Namun, penggunaan aplikasi komunikasi instan seperti *WhatsApp* yang begitu luas tentu saja memicu kejahatan siber atau *cybercrime* yang merugikan para pengguna. Sehingga dapat dikatakan bahwa era globalisasi dan

teknologi informasi berdampak pada munculnya berbagai jenis kejahatan baru (*cybercrime*) (Didik M dkk, 2005). *Cybercrime* dapat terjadi dengan memanfaatkan kelemahan setiap aplikasi. Seperti dilansir dari (cnnindonesia.com, 2021), penipuan sering terjadi di aplikasi *WhatsApp*. Selain itu, (cnbcindonesia.com,2021) melaporkan tentang praktik peretasan akun di aplikasi WhatsApp. Ada juga praktek *cybercrime* lainnya, seperti dilansir oleh (cnbcindonesia.com,2022), yaitu penyadapan dengan mengirimkan *virus malware* melalui aplikasi *WhatsApp* yang bersangkutan. Berdasarkan fenomena kejahatan siber yang terjadi pada *WhatsApp*, dapat dikatakan bahwa ada berbagai jenis kejahatan siber yang sering terjadi pada aplikasi perpesanan instan, salah satunya adalah *WhatsApp* seperti *spyware*, serangan siber, peretasan, dan *spionase*.

Di Indonesia, spionase telah terjadi dalam beberapa kasus. Allen Lawrence Pope, misalnya, yang merupakan tentara yang berkoalisi dengan CIA pernah melakukan spionase terhadap Indonesia pada saat pemberontakan PRRI/Permesta (kompas.com, 2021). Pada tahun 1982, Rusia juga terbukti melakukan spionase di Indonesia melalui agen intelijennya, Sergei Egorov (detik.com, 2017). Tidak hanya itu, Negara Australia juga diketahui melakukan penyadapan terhadap percakapan telepon 7 petinggi negara Indonesia, termasuk presiden, pada tahun 2007-2009 (bbc.com, 2013). Banyak negara yang menentang praktik spionase dan mengusulkan PBB untuk segera mengeluarkan resolusi anti-spionase. Indonesia termasuk negara yang anti-spionase dan telah mencantumkan spionase sebagai salah satu jenis kejahatan *cyber* dalam undang-undang teknologi dan informasi. Namun, karena begitu banyaknya pengguna internet dan aplikasi komunikasi di Indonesia, maka aktivitas spionase dapat menjadi ancaman serius bagi negara.

Praktek spionase memiliki kaitan erat dengan politik global. Menurut Jemadu (2008), politik global menggantikan istilah politik internasional karena mencakup luasnya, tidak hanya antar negara tetapi juga aktor non-negara yang mempengaruhi secara global dan komunitas internasional. Politik global membahas berbagai isu seperti nuklir, terorisme, perubahan iklim, keamanan energi, cyber crime, dan lainnya. Dinamika politik global mempengaruhi setiap negara dengan dampak yang signifikan, termasuk Indonesia yang harus merumuskan kebijakan dalam menanggapi perkembangan politik global yang bisa menjadi ancaman, seperti spionase. Saat ini, spionase semakin canggih dengan memanfaatkan jaringan internet. Hal ini sangat berbahaya bagi Indonesia, terutama karena aplikasi WhatsApp yang digunakan secara massal oleh seluruh lapisan masyarakat untuk berkomunikasi menggunakan jaringan internet. WhatsApp memiliki banyak kelemahan sehingga telah terjadi banyak kasus cyber crime. Selain itu, server WhatsApp berada di luar negeri, sehingga meskipun telah dienkripsi end-to-end, potensi spionase masih ada. Militer, intelijen, instansi pemerintah, pejabat negara, bahkan Presiden Indonesia juga menggunakan WhatsApp untuk berkomunikasi, yang dapat memicu munculnya potensi spionase karena keamanan aplikasi tersebut masih relatif rendah dan berjalan menggunakan jaringan internet. Oleh karena itu, tulisan ini bertujuan untuk menjelaskan potensi praktek spionase terhadap penggunaan WhatsApp dalam bidang pertahanan Indonesia.

LITERATUR REVIEW

Spionase

Spionase adalah salah satu jenis kejahatan cyber yang dilakukan secara ilegal dengan cara mengumpulkan informasi atau data militer, ekonomi, hingga politik dari individu atau negara target melalui internet, perangkat lunak, atau komputer target dengan cara penyadapan atau pengawasan yang tidak sah (Subagyo, 2005). Spionase ini biasanya terjadi dalam konteks politik internasional dan digunakan sebagai salah satu strategi untuk mencari kelemahan serta celah dan mempersiapkan diri dalam menghadapi konflik dengan negara target. Oleh karena itu, spionase termasuk kejahatan *cyber* yang sangat berbahaya dan dapat mengancam kedaulatan sebuah negara.
Pertahanan Negara

Pertahanan

Konsep pertahanan sering kali diidentikkan dengan upaya untuk mempertahankan keberlangsungan hidup suatu negara dari ancaman dalam maupun luar negeri dengan tujuan menciptakan rasa aman. Syarifudin Tippe (2016) menyatakan bahwa objek studi ilmu pertahanan adalah perilaku negara dalam menjaga dan mengembangkan keberlangsungan hidupnya. Sejarah ilmu pertahanan berasal dari ilmu militer dan perang, yang mencakup konsep dan ide pengembangan organisasi, strategi, dan taktik militer untuk mencapai kepentingan negara (Tippe, 2016).

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah studi literatur atau kajian kepustakaan. Studi literatur adalah jenis penelitian yang dilakukan dengan mencari dan mengumpulkan informasi atau masalah yang

berkaitan dengan topik penelitian melalui buku dan majalah (Danial & Warsiah, 2009). Pengumpulan informasi dan data dilakukan dengan menggunakan sumber data sekunder dari buku, jurnal, atau artikel ilmiah yang terkait dengan tingkat nasional hingga internasional, berita, situs web resmi, dan majalah yang dapat diakses secara digital. Data dan informasi yang dikumpulkan berkaitan dengan kejahatan siber, khususnya praktik spionase, dan aplikasi WhatsApp yang digunakan di Indonesia. Tujuan dari studi literatur ini adalah untuk mengetahui potensi spionase terhadap penggunaan aplikasi WhatsApp dalam bidang pertahanan Indonesia.

HASIL DAN PEMBAHASAN

Perkembangan Spionase di Indonesia

Kejahatan dunia maya atau yang sering disebut sebagai cybercrime, merujuk pada tindakan kriminal yang menggunakan jaringan internet sebagai media pelakunya. Cybercrime merupakan kegiatan yang melanggar hukum dan merugikan pihak lain, yang dapat menghasilkan keuntungan atau tidak. Sebagaimana disebutkan oleh Arifah (2011), cybercrime dapat menimbulkan kerugian dalam berbagai bidang, seperti politik, ekonomi, sosial, dan budaya. Oleh karena itu, tindakan cybercrime dianggap lebih signifikan dan lebih berbahaya dibandingkan dengan kejahatan yang memiliki intensitas tinggi lainnya (Wahid & Labib, 2005). Cyber crime, yang juga disebut kejahatan maya, adalah sebuah tindakan kriminal yang menggunakan jaringan internet sebagai media aksinya. Cyber crime dapat menyebabkan kerugian dalam beberapa bidang, seperti politik, ekonomi, sosial, dan budaya, dan dapat dikategorikan menjadi empat kategori, menurut Yar dan Steinmetz (2019). Kategori pertama adalah cyber trespass, yaitu kejahatan cyber yang merusak properti atau hak milik orang lain, seperti hacking, penyebaran virus, dan tindakan perusakan lainnya. Kategori kedua adalah cyber deception and thefts, yaitu kejahatan cyber dengan tujuan mencuri uang atau properti, seperti penipuan kartu kredit atau pembajakan. Kategori ketiga adalah cyber pornography, yaitu kejahatan cyber yang melanggar hukum kesusilaan. Kategori keempat adalah cyber violence, yaitu kejahatan cyber dengan tujuan merusak psikologis atau menghasut sehingga mempengaruhi dan merugikan psikis orang lain, dan melanggar hukum perlindungan seperti hate speech dan stalking.

Beberapa jenis cyber crime termasuk di antaranya adalah hacking, yang merupakan aksi mengambil alih atau mengakses program komputer milik orang lain, dan dilakukan oleh seorang hacker yang memiliki obsesi dengan keamanan program. Sedangkan cracking adalah aksi hacking dengan tujuan yang tidak baik dan dilakukan oleh seorang cracker yang fokus pada hasil yang bisa diperoleh. Selain itu, terdapat juga cyber sabotage, yaitu aksi yang bertujuan merusak dan menghancurkan data, program, dan sistem jaringan internet. Sementara itu, cyber attack merupakan aksi yang dilakukan dengan sengaja untuk mengganggu kerahasiaan, integritas, dan ketersediaan data atau informasi. (Subagyo, 2015)

Carding adalah tindakan penipuan yang menggunakan nomor atau identitas kartu kredit orang lain untuk membeli barang atau jasa. Sedangkan Spyware adalah program yang secara diam-diam merekam aktivitas online pengguna dan mengirim data yang terkumpul ke pelanggan yang membayar. Di sisi lain, dalam aktivitas militer, ekonomi, dan politik, terdapat empat jenis serangan cyber yang dapat dikategorikan sebagai perang cyber (Subagyo, 2015). Salah satunya adalah serangan pada jaringan listrik yang dilakukan dengan mematikan pasokan listrik di wilayah target untuk mengganggu aktivitas ekonomi dan sebagai bagian dari strategi serangan militer untuk mengalihkan perhatian. Metode yang digunakan untuk melakukan serangan ini seringkali menggunakan program trojan horse.

Vandalisme merupakan tindakan merusak halaman web atau sumber daya komputer yang dilakukan melalui jaringan internet, komputer, dan program. Aktivitas ini dapat berbentuk propaganda atau pesan politik. Sementara sabotase dilakukan melalui media komputer dan satelit dengan tujuan untuk mengambil informasi tentang lokasi melalui perangkat militer musuh. Umumnya, program ini disembunyikan dalam hardware komputer. Sabotase juga dapat dilakukan dengan cara menyadap informasi dan mengganggu peralatan komunikasi, sumber energi, air, bahan bakar, dan transportasi.

Spionase cyber adalah kejahatan yang dilakukan secara diam-diam melalui jaringan, perangkat lunak, atau komputer negara target dengan tujuan memperoleh informasi militer, politik, atau ekonomi secara ilegal. Spionase merupakan jenis cybercrime karena dilakukan secara rahasia dan melanggar hukum, yang dapat merugikan pihak yang disasar. Kegiatan spionase menggunakan teknologi dan jaringan internet sebagai sarana pengumpulan informasi dari institusi tertentu, terutama dalam bidang ekonomi, politik, dan

militer. Kegiatan ini seringkali dilakukan oleh intelijen negara sebagai strategi militer atau politik untuk mendapatkan informasi tentang situasi dan kondisi negara lawan. Dalam hal ini, spionase merupakan fungsi utama dari intelijen (Kuswara, 2019).

Praktek spionase bertujuan untuk memperoleh informasi rahasia mengenai strategi politik terutama dalam politik luar negeri suatu negara dengan cara yang tidak sah, sehingga informasi tersebut dapat digunakan sebagai acuan untuk membuat strategi politik luar negeri yang baru (Salehun & Sulaiman, 2019). Penyadapan ilegal merupakan salah satu bentuk praktek spionase. Beberapa ciri khas dari praktek spionase meliputi: (1) akses yang tidak sah atau tidak diizinkan, (2) tidak ada unsur kekerasan, (3) keterlibatan fisik minimal, (4) penggunaan peralatan teknologi canggih, seperti jaringan global yang terdiri dari telekomunikasi, media, dan informatika, dan (5) dapat menyebabkan kerugian material dan non-material yang besar, termasuk kerahasiaan informasi (Zulkarnain et al., 2014).

Spionase cyber dapat dibagi menjadi dua jenis, yaitu spionase murni dan spionase abu-abu. Spionase murni bertujuan untuk memanfaatkan informasi dan data yang diperoleh untuk kegiatan kriminal seperti pencurian data, sabotase, atau pemalsuan data. Sedangkan spionase abu-abu dilakukan oleh programmer yang ingin mencoba kemampuannya dalam membobol sistem sasaran tanpa berniat merusak atau mencuri informasi (Nicko, 2011). Umumnya, spionase dilakukan dengan cara penyadapan. Proses spionase meliputi beberapa tahapan seperti footprinting (pencarian data), scanning (pemilihan sasaran), enumerasi (pencarian informasi), dan gaining access (mendapatkan akses ilegal) dengan berpura-pura sebagai pengguna biasa (Nicko, 2011).

Spionase termasuk dalam kategori kejahatan cyber dan diatur dalam Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE nomor 11 tahun 2008, khususnya di Bab VII tentang perbuatan yang dilarang. Pasal 31 ayat 1 dan 2 dari UU ITE nomor 19 tahun 2016 mengatur tentang intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain yang dilakukan dengan sengaja dan tanpa hak atau melawan hukum. Di Indonesia, spionase sangat dilarang dan ditentang. Sebagai contoh, pada tahun 2013, mantan pegawai NSA membocorkan dokumen tentang penyadapan yang dilakukan oleh Australia terhadap para petinggi Negara Indonesia melalui jaringan telepon. Para sasaran yang menjadi target spionase termasuk presiden, ibu presiden, wakil ketua presiden, juru bicara luar negeri, juru bicara dalam negeri, sekretaris negara, menko ekonomi, menko polkam, dan menteri agraria menggunakan berbagai jenis ponsel dan jaringan 3G (Muliana, 2018). Praktek spionase yang melibatkan penyadapan dan penyamaran di Indonesia terus berkembang.

Perkembangan WhatsApp di Indonesia

Sebanyak 83 persen dari total 171 juta pengguna internet di Indonesia terdeteksi menggunakan WhatsApp sebagai media komunikasi (Kominfo, 2019). WhatsApp termasuk dalam kategori aplikasi perpesanan instan yang populer bagi masyarakat Indonesia, khususnya para pengguna virtual. Dalam hal ini, aplikasi tersebut sangat membantu masyarakat dalam berinteraksi (Junawan & Laugu, 2020:52). Seperti yang dilaporkan di laman detik.com pada tanggal 4 Juni 2021, aplikasi WhatsApp sangat diminati oleh masyarakat Indonesia untuk berkomunikasi. Walaupun jumlah pengguna WhatsApp di Indonesia sangat tinggi, aplikasi ini memiliki beberapa kekurangan. Sebagaimana dilansir di laman kumparan.com pada tanggal 23 Februari 2022, kekurangan aplikasi WhatsApp antara lain penggunaan dan penyimpanan data yang besar, serta tidak bisa melakukan back up antar-platform. Selain itu, liputan6.com melaporkan pada tanggal 12 Januari 2021 bahwa WhatsApp memiliki celah yang rentan untuk kegiatan cyber crime

Strategi Pencegahan Potensi Ancaman Spionase pada WhatsApp di Bidang Pertahanan Indonesia

Potensi terjadinya spionase melalui penggunaan WhatsApp di bidang pertahanan Indonesia menjadi perhatian serius. Spionase termasuk salah satu metode dalam cyber warfare yang mengumpulkan informasi secara diam-diam. Tingginya penggunaan internet di Indonesia dan popularitas WhatsApp sebagai aplikasi media sosial meningkatkan risiko terjadinya spionase. Israel diketahui telah menggunakan cyber pegasus pada 1.400 pengguna WhatsApp, termasuk aktivis, politisi, dan jurnalis. Selain itu, spyware juga telah diperjualbelikan dan dioperasikan di Indonesia. WhatsApp rentan terhadap praktek cyber crime seperti spionase, yang dapat dilakukan melalui panggilan, tautan link URL, video, dan malware (kompas.com, 2020). Fitur baru pengguna untuk bergabung dalam video call meski video call sedang berjalan atau panggilan

grup juga dapat dimanfaatkan untuk melakukan penyadapan. Check Point Research (CPR) menemukan celah keamanan pada fitur filter foto di aplikasi WhatsApp for Android dan Bussines. Oleh karena itu, diperlukan strategi pencegahan untuk mengurangi risiko terjadinya spionase, termasuk meningkatkan kesadaran akan risiko tersebut, menggunakan aplikasi alternatif yang lebih aman, menghindari tautan link yang mencurigakan, menghindari membuka lampiran dari sumber yang tidak dikenal, dan memperbarui sistem keamanan secara teratur.

Dengan ditemukannya celah keamanan di WhatsApp, dapat disimpulkan bahwa ada potensi besar terjadinya spionase dalam aplikasi tersebut. Ini meningkatkan kekhawatiran para pengguna WhatsApp di Indonesia karena keamanan data dan aktivitas komunikasi masih lemah. Meskipun begitu, instansi pemerintah Indonesia masih menggunakan WhatsApp sebagai media komunikasi dan bahkan banyak menteri yang telah menggunakannya (Kemenkeu, 2020). Bahkan, WhatsApp juga dimanfaatkan selama pandemi COVID-19, sehingga penggunaannya meningkat di kalangan instansi pemerintah. Namun, pakar keamanan siber menyarankan agar presiden dan jajarannya tidak menggunakan WhatsApp untuk berkomunikasi karena adanya ancaman malware Pegasus (kompas.com, 2021).

Pegasus adalah salah satu spyware atau trojan (script) yang dapat ditanam jarak jauh dan diinstal pada sistem iOS Apple dan Android. Spyware Pegasus memiliki teknologi terbaru yaitu "*zero link*" yang memungkinkan penanaman tanpa melalui tautan *link* (Chawla, 2021:2). Teknologi "*zero link*" dapat menyerang sistem iOS dan Android melalui kerentanannya yang disebut zero day, dimana celah dari *zero day* dimanfaatkan dengan mengirimkan malware melalui panggilan atau pesan teks. Malware tersebut kemudian akan tertanam dan menginstal secara otomatis (Chawla, 2021). *Zero day* mengacu pada penginstalan pertama kali dari aplikasi atau sistem yang termasuk dalam iOS Apple dan Android. Aplikasi WhatsApp juga memiliki *zero day*, sehingga risiko penanaman *malware* Pegasus atau spyware lainnya sangat tinggi saat menggunakan WhatsApp yang tidak pernah diperbarui atau ditingkatkan levelnya.

Menurut Babys (2021), penggunaan WhatsApp oleh pemerintah Indonesia dapat menimbulkan ancaman serius, dimana tujuan dari kejahatan siber adalah untuk menciptakan ketidakpercayaan masyarakat terhadap pemerintah dan membuat stabilitas nasional terganggu. Ardiyanti (2014) menambahkan bahwa Indonesia memiliki manajemen keamanan siber yang kurang kuat, sehingga pihak lain dapat dengan mudah menembus keamanan siber Indonesia melalui tindakan cyber espionage atau spionase. Hilangnya batas-batas negara akibat spionase ini, seperti yang dijelaskan oleh Hastri (2021), dapat berdampak besar pada kedaulatan negara. Oleh karena itu, diperlukan strategi dan penanganan maksimal oleh pemerintah Indonesia untuk melindungi negara dari segala ancaman siber yang mengancam kedaulatan dan pertahanan negara.

Diperlukan suatu strategi untuk mencegah spionase melalui aplikasi WhatsApp demi menjaga keamanan data dan kenyamanan dalam berkomunikasi. Strategi ini memerlukan pengembangan dan implementasi model tertentu. Beberapa model yang dapat digunakan telah dijelaskan oleh Vinietta (2016) antara lain: pertama, model informasi yang dilindungi, dimana bidang pertahanan perlu melakukan klasifikasi terhadap informasi yang harus dilindungi, terutama dalam hal pertahanan. Kedua, model keamanan eksisting, dimana bidang pertahanan perlu mempelajari celah-celah yang dapat dimasuki oleh pengguna atau pihak lawan, dan model ini dapat digunakan untuk memancing lawan. Ketiga, model risiko dan ancaman, dimana bidang pertahanan perlu menciptakan hipotesis mengenai pihak mana yang akan diuntungkan dari informasi yang akan diperoleh, serta metode yang akan digunakan oleh pihak lawan dalam menyerang.

Menurut Vinietta (2016), bidang pertahanan Indonesia memiliki empat jenis metode operasi yang dapat dilakukan dalam rangka menjaga keamanan siber, yaitu: defensif pasif (meliputi pertahanan, pengolahan, pemeriksaan, dan pengukuran keamanan), defensif aktif (menggabungkan perangkat keras dan perangkat lunak), ofensif pasif (pengumpulan informasi tentang lawan sampai pada tahap mata-mata siber), serta ofensif aktif (mengkonfigurasi dan melakukan perang siber).

Singapura adalah salah satu negara yang telah mengimplementasikan sistem keamanan cyber. Terdapat empat strategi keamanan cyber yang diterapkan oleh Singapura, yaitu national cyber security masterplan, cyber security research and development program, national cyber security center, dan Singapore's cybersecurity strategy (SCSS) (Muawwan, 2021). Pada dasarnya, strategi keamanan cyber di Singapura difokuskan pada beberapa aspek, seperti aktor negara, aplikasi atau hubungan antar warga, infrastruktur atau sarana

prasarana cyber, aktor selain negara, perkembangan ekonomi, kolaborasi antara aktor dan ahli, riset dan pengembangan, dan mitigasi (Muawwan, 2021). Namun, yang paling penting dari strategi keamanan cyber Singapura adalah mengurangi hambatan birokrasi dan administratif (Muawwan, 2021).

Dalam hal strategi keamanan cyber, Malaysia memiliki pendekatan yang berbeda dengan Singapura, yaitu lebih tertutup. Malaysia memiliki beberapa strategi keamanan cyber, antara lain modern threat (pengembangan teknologi dan informasi yang sesuai dengan perkembangan teknologi), policy enforcement (kebijakan yang jelas dan ketat), challenging (menghadapi tantangan dunia cyber untuk meningkatkan kompetensi dan pengetahuan), development of technology, dan social life (meningkatkan kapasitas dan kapabilitas keamanan bagi warga negara yang sangat tergantung pada teknologi) (Oktaviani & Silvia, 2021)

Jika dibandingkan dengan Singapura dan Malaysia, Indonesia saat ini sedang memperkuat sistem pertahanan siber untuk keamanan negara. Dalam aspek kebijakan, Indonesia telah beberapa kali melakukan perencanaan dan perubahan pada aturan mengenai pertahanan siber, seperti peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007, peraturan Kementerian Pertahanan Indonesia No.82 tahun 2014, dan peraturan Presiden Nomor 53 tahun 2017 dari Badan Siber dan Sandi Negara (BSSN). Dalam aspek struktur organisasi pemerintah, Indonesia memiliki beberapa lembaga pemerintahan yang mengurusi permasalahan siber seperti BSSN, Kominfo, BIN, Kemhan, POLRI dan institusi lainnya. Namun, dalam aspek tindakan prosedural, Indonesia masih belum cukup memadai dan terdapat tumpang tindih. Dalam aspek *capacity building*, Indonesia telah melakukan beberapa upaya, salah satunya dengan memberikan mata pelajaran teknologi dalam pendidikan formal. Indonesia juga menjalin kerja sama internasional dengan Australia dan empat negara lainnya dalam hal keamanan siber. Meskipun demikian, kesimpulan dari perbandingan strategi keamanan siber Indonesia dengan Singapura dan Malaysia adalah bahwa Indonesia masih belum memiliki strategi yang terfokus dan sentral seperti Singapura, serta kebijakan yang jelas dan kuat seperti Malaysia. Indonesia masih terus mengembangkan aspek-aspek strategi keamanan sibernya, namun masih terdapat aspek yang jauh dari layak, seperti aspek tindakan prosedural.

KESIMPULAN DAN REKOMENDASI

Semakin majunya teknologi di zaman sekarang menghasilkan beberapa peluang negatif dalam sistem pertahanan negara. Salah satu dampaknya adalah adanya potensi spionase pada aplikasi WhatsApp yang dapat membahayakan pertahanan negara Indonesia kapan saja. Tindakan kejahatan siber seperti cyber crime semakin rawan terjadi seiring dengan kemajuan teknologi, informasi, dan komunikasi. Spionase melalui aplikasi WhatsApp bisa dilakukan dengan beberapa cara, salah satunya melalui panggilan. Sebuah software bernama Spyware diketahui telah digunakan di Indonesia untuk kegiatan spionase. Potensi spionase lainnya adalah melalui membuka foto atau video tertentu yang dikirim melalui WhatsApp, karena foto atau video tersebut telah ditanam dengan software peretasan. Oleh karena itu, aplikasi WhatsApp dianggap cukup berisiko untuk terjadinya spionase, sehingga para pakar keamanan siber menyarankan Presiden dan stafnya untuk tidak menggunakan aplikasi ini dalam berkomunikasi.

Dalam bidang pertahanan Indonesia, ada beberapa rekomendasi untuk mengatasi potensi spionase pada pengguna aplikasi WhatsApp. Salah satunya adalah dengan meningkatkan keamanan dunia cyber melalui peningkatan sumber daya manusia yang ahli dan fasilitasi perangkat cyber secara maksimal. Selain itu, pelatihan dan pengembangan keterampilan dan teknologi harus dilakukan secara rutin, yang berdasarkan pada isu-isu dan globalisasi yang terus berkembang dan diperbarui. Kemudian, ada juga pentingnya untuk mengurangi kelonggaran administrasi yang tidak terlalu penting dan rumit sehingga tidak mengganggu performa para tenaga ahli dalam menangani kasus kejahatan siber di Indonesia.

DAFTAR PUSTAKA

Abdillah, Najib. (2019). Analisis Faktor yang Mempengaruhi Adopsi Scrum pada Startup Digital di Yogyakarta. Skripsi Thesis. Universitas Islam Indonesia. (http://hdl.handle.net/123456789/15702)

Agustini, P. (2021, September 12). Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya di Internet. Ditjen Aptika. https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/

Ancaman Militer dari Luar Negeri Sejak Kemerdekaan Indonesia Halaman all—Kompas.com. (n.d.). Retrieved February 24, 2022, from https://www.kompas.com/

stori/read/2021/06/03/133753179/ancaman-militer-dari-luar-negeri-sejak-kemerdekaan-indonesia?page=all

Ancaman Spyware Pegasus, Jokowi Disarankan Tak Gunakan WhatsApp Halaman all—Kompas.com. (n.d.). Retrieved February 24, 2022, from https://www.kompas.com/tren/read/2021/07/31/183200765/ancaman-spyware-pegasus-jokowi-disarankan-tak-gunakan-WhatsApp?page=all

Apa Itu Startup dan Contohnya? Halaman all—Kompas.com. (n.d.). Retrieved February 24, 2022, from https://money.kompas.com/read/2021/05/15/102503926/apa-itu-startup-dan-contohnya?page=all

Ardiyanti, Handrini. (2014). Cyber-Security dan Tantangan Pengembangannya di Indonesia. Jurnal Politica. 5 (1). 95-110. Doi: 10.22212/jp.v5i1.336

Arifah, Dista Amalia. (2011). Kasus Cybercrime Di Indonesia: Indonesia's Cybercrime Case. Jurnal Bisnis dan Ekonomi (JBE),Vol. 18 No. 2, Hal. 185 – 195, (https://www.unisbank.ac.id/ojs/index.php/fe3/article/view/2099)

Babys, Salmon A. M. (2021). Ancaman Perang Siber di Era Digital dan Solusi Keamanan Nasional Indonesia. Jurnal Oratio Directa. 3 (1). 425-442. E-ISSN 2615-07435.

Berbagai Cara Peretas Membajak Akun WhatsApp: Okezone techno. (n.d.). Retrieved February 24, 2022, from https://techno.okezone.com/read/2020/05/12/207/2212693/berbagai-cara-peretas-membajak-akun-WhatsApp

BIN: Australia menyadap Indonesia sejak 2007. (2013, November 20). BBC News Indonesia. https://www.bbc.com/indonesia/berita_indonesia/2013/11/131120_bin_sadap_australia

Black, Henry Campbell. (1979). Black's Law Dictionary, Fifth Edition. ST. Paul Minn: West Publishing co

Celah Keamanan di WhatsApp Bisa Ekspos Data Sensitif Pengguna. (n.d.). Retrieved February 24, 2022, from https://inet.detik.com/security/d-5708581/celah-keamanan-di-WhatsApp-bisa-ekspos-data-sensitif-pengguna

Chawla, A. (2021). Pegasus Spyware – 'A Privacy Killer'. SSRN. (DOI: 10.2139/ssrn.3890657).

Daftar Media Sosial yang Paling Populer Tahun 2022, Ada WhatsApp dan TikTok. (n.d.). Retrieved February 24, 2022, from https://lifestyle.kontan.co.id/news/daftar-media-sosial-yang-paling-populer-tahun-2022-ada-WhatsApp-dan-tiktok?page=all

Danial dan Wasriah. (2009). Metode Penulisan Karya Ilmiah. Bandung: Laboratorium Pendidikan Kewarganegaraan UPI.

Didik M dkk. (2005). Cyber Law: Aspek Hukum Teknologi Informasi. Bandung: Refka Aditama

Fitur Baru WhatsApp Disebut Punya Celah Keamanan. (n.d.). Retrieved February 24, 2022, from https://www.jawapos.com/nasional/17/08/2021/fitur-baru-WhatsApp-disebut-punya-celah-keamanan/

Hastri, Evi Dwi. (2021). Cyber Espionage sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia. Law and Justice Review Journal. 1 (1). 12-25. http://dx.doi.org/10.11594/ lrjj.01.01.03

Hati-hati Klik "Link" di WhatsApp Web, Data di Komputer Bisa Dicuri. (n.d.). Retrieved February 24, 2022, from https://tekno.kompas.com/read/2020/02/06/19190517/hati-hati-klik-link-di-WhatsApp-web-data-di-komputer-bisa-dicuri

Hayati, D. S. N. (n.d.). 16 Media Sosial dengan Pengguna Terbanyak di Indonesia, WhatsApp Duduki Posisi Kedua—Portal Jember—Halaman 2. Retrieved February 24, 2022, from https://portaljember.pikiran-rakyat.com/iptek/pr-161917022/16-media-sosial-dengan-pengguna-terbanyak-di-indonesia-WhatsApp-duduki-posisi-kedua

Heboh Penyadapan Aplikasi WhatsApp, Ini Caranya Agar Selamat. (n.d.). Retrieved February 24, 2022, from https://www.cnbcindonesia.com/tech/20220114064135-37-307225/heboh-penyadapan-aplikasi-WhatsApp-ini-caranya-agar-selamat

Indonesia Pengguna WhatsApp Terbesar Ketiga di Dunia | Databoks. (2021, November 23). https://databoks.katadata.co.id/datapublish/2021/11/23/indonesia-pengguna-WhatsApp-terbesar-ketiga-di-dunia

Jemadu, Aleksius. Politik Global dalam Teori dan Praktik. Yogyakarta: Graha Ilmu.

Jumiatmoko. (2016). WhatsApp Messenger Dalam Tinjauan Manfaat Dan Adab. Wahana

Akademika, 3(1), 51–66. https://doi.org/10.21580/wa.v3i1.872

Junawan, Hendra&Laugu, Nurdin. (2020). Eksistensi Media Sosial, Youtube, Instagram dan WhatsApp Ditengah Pandemi Covid-19 Dikalangan Masyarakat Virtual Indonesia. Baitul Ulum: Jurnal Ilmu Perpustakaan dan Informasi, Vol. 4 No. 1, hlm 41-57. (DOI: https://doi.org/10.30631/baitululum.v4i1.46)

Kelebihan dan Kekurangan WhatsApp dan Telegram sebagai Aplikasi Pesan. (n.d.). kumparan. Retrieved February 24, 2022, from https://kumparan.com/berita-update/kelebihan-dan-kekurangan-WhatsApp-dan-telegram-sebagai-aplikasi-pesan-1xYsPxZJHWs

Kementrian Pertahanan Republik Indonesia. (n,d.). Tugas dan Fungsi. Website Resmi Kementrian Pertahanan Republik Indonesia. Retrieved February 28, 2022, from https://www.kemhan.go.id/tugas-dan-fungsi

KOMINFO, P. (n.d.). Kominfo, WhatsApp Kenalkan Literasi Privasi Dan Keamanan Digital. Website Resmi Kementerian Komunikasi Dan Informatika RI. Retrieved February 24, 2022, from http:///content/detail/22824/kominfo-WhatsApp-kenalkan-literasi-privasi-dan-keamanan-digital/0/sorotan_media

Kuswara, Yosa Bayu. (2019). Evaluasi Fungsi Kontra Intelijen Indonesia Dalam Menghadapi Spionase Intelijen Asing. Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 2 No.2, hlm 114-128. (http://jurnalpkn.ui.ac.id/index.php/jkskn/article/view/24/24)

Larasati, W.,dkk. (2013). Efektivitas Pemanfaatan Aplikasi WhatsApp sebagai Sarana Diskusi Pembelajaran Pada Mahasiswa (UIN Sunan Kalijaga Yogyakarta). (https://www.academia.edu/10886930/Efektivitas_Pemanfaatan_Aplikasi_WhatsApp_sebagai_Sarana_Diskusi_Pembelajaran_Pada_Mahasiswa_Survei_Pada_Mahasiswa_Ilmu_Komunikasi_Fakultas_Ilmu_Sosial_dan_Humaniora_Angkatan_2012_UIN_Sunan_Kalijaga_Yogyakarta_?auto=downl)

Liputan6.com. (2019, May 15). Cuma Lewat Panggilan WhatsApp, Peretas Bisa Kuasai Smartphone Korban. liputan6.com. https://www.liputan6.com/tekno/read/3966915/cuma-lewat-panggilan-WhatsApp-peretas-bisa-kuasai-smartphone-korban

Liputan6.com. (2021, January 12). Kelebihan dan Kekurangan WhatsApp Vs Telegram, Ketahui Keamanannya. liputan6.com. https://hot.liputan6.com/read/4454990/kelebihan-dan-kekurangan-WhatsApp-vs-telegram-ketahui-keamanannya

M, P. L. (n.d.). Kucing-kucingan Intel Indonesia dengan KGB. Detikx. Retrieved February 24, 2022, from https://news.detik.com/x/detail/intermeso/20171005/Kucing-kucingan-Intel-Indonesia-dengan-KGB/

Mengenal 4 Jenis Modus Penipuan WhatsApp yang Marak. (n.d.). Retrieved February 24, 2022, from https://www.cnnindonesia.com/teknologi/20210608174404-190-651843/mengenal-4-jenis-modus-penipuan-WhatsApp-yang-marak

Muawwan, (2021). Three Perspective Theory of Cyber Sovereignty dalam Strategi Keamanan Siber Singapura. Jurnal Kajian Ilmiah, Vol.21 No.2, hlm 171-184. (https://doi.org/10.31599/jki.v21i2.562)

Muliana, Rizky Pratama (2018) PERANG INTERNET (NETWAR) ANTARA INDONESIA DENGAN AUSTRALIA PASCA PENYADAPAN DI ERA PRESIDEN SUSILO BAMBANG YUDHOYONO. Undergraduate (S1) thesis, University of Muhammadiyah Malang. (https://eprints.umm.ac.id/39782/)

Nicko, Shelly. (2011) Tindak Pidana Cyber Espionage. Skripsi Thesis, Universitas Airlangga. (https://repository.unair.ac.id/14090/)

Nurhaidah&Musa, M.Insya. (2015). Dampak Pengaruh Globalisasi Bagi Kehidupan Bangsa Indonesia. Jurnal Pesona Dasar, Vol.3 No.3, hlm 1-14. http://jurnal.unsyiah.ac.id/PEAR/article/view/7506#:~:text=Dampak%20positif%20dari%20globalisasi%20adalah,kebarat%2Dbaratan%20serta%20kesenjangan%20sosial.

Oktaviani, Putri B&Silvia, Anggraeni. (2021). Stretegi Keamanan Siber Malaysia. Jurnal Kajian Ilmiah, Vol.21 No.1, hlm 69-84. (https://doi.org/10.31599/jki.v21i1.447)

Pinontoan, Floriny Deasy V. (2013). Praktik Spionase Dalam Hubungan Diplomatik Antar Negara Ditinjau Dari Hukum Internasional. Skrispi Thesis. Universitas Hassanudin. (http://digilib.unhas.ac.id/uploaded_files/temporary/DigitalCollection/NWUxMjFhNDdkZDAxZWJjZjFlZWYwYmRlMzdkOTZjZDliNDRlNzQ0Zg==.pdf)

Pranajaya, & Hendra Wicaksono. (2017). Pemanfaatan Aplikasi WhatsApp (WA) Di Kalangan Pelajar (Studi kasus Di MTs Al Muddatsiriyah dan MTs jakarta Pusat). Prosiding SNaPP2017 Sosial, Ekonomi, Dan Humaniora, Vol 7, No.1, 98–109. Diakses dari (http://proceeding.unisba.ac.id/index.php/sosial/article/view/808)

Pratiwi, L.Ya Esty&Correia, Zezito Fatima M. (2020). Hukum Siber : Praktik Spionase Dalam Kedaulatan Negara Dan Hubungan Diplomasi Berdasarkan Ketentuan Hukum Internasional. Jurnal Pendidikan Kewarganegaraan Undiksha Vol. 8 No. 3, hlm 206-218. (https://ejournal.undiksha.ac.id/index.php/JJPP)

Prinada, Yuda. Pengertian Globalisasi dan Contohnya di Berbagai Bidang. (February 23, 2021). Retrieved Maret 03, 2022, from https://tirto.id/pengertian-globalisasi-dan-contohnya-di-berbagai-bidang-gas

Pusat Bantuan WhatsApp—Sistem Operasi yang Didukung. (n.d.). WhatsApp.com. Retrieved February 24, 2022, from https://faq.WhatsApp.com/general/download-and-installation/about-supported-operating-systems/?lang=id

Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi:-. Politeia: Jurnal Ilmu Politik, 14(1), 54-62.

roy. (n.d.). Awas! Pembajakan WhatsApp Marak Lagi, Ini Modusnya Hacker! CNBC Indonesia. Retrieved February 24, 2022, from https://www.cnbcindonesia.com/tech/20210125070455-37-218377/awas-pembajakan-WhatsApp-marak-lagi-ini-modusnya-hacker

Salehun, Lisna Wati&Sulaiman, Yohanes. (2019). Kebijakan Luar Negeri Indonesia Dan Kepemimpinan Susilo Bambang Yudhoyono: Studi Kasus Spionase Australia. JURNAL AGREGASI, Vol.7 No.2, (doi: 10.34010/agregasi.v7i2.2561)

Sejarah dan Perkembangan WhatsApp dari Masa ke Masa. (n.d.). Retrieved February 24, 2022, from https://www.cnnindonesia.com/teknologi/20210608100832-190-651585/sejarah-dan-perkembangan-WhatsApp-dari-masa-ke-masa

Serba-serbi Penggunaan Media Sosial di Instansi Pemerintah. (n.d.). Retrieved February 25, 2022, from https://www.djkn.kemenkeu.go.id/kanwil-jakarta/baca-artikel/13455/Serba-serbi-Penggunaan-Media-Sosial-di-Instansi-Pemerintah.html

Shanta Eki Ghossa (2018) Pemanfaatan WhatsApp Sebagai Media Interaksi Mahasiswa Komunikasi Uin Suska Riau Dalam Memperoleh Informasi Perkuliahan. Skripsi Thesis, Universitas Islam Negeri Sultan Syarif Kasim Riau. (http://repository.uin-suska. ac.id/15226/)

Sri Mulyani: Ada menteri yang tidak punya WA. (n.d.). Retrieved February 25, 2022, from https://nasional.kontan.co.id/news/sri-mulyani-ada-menteri-yang-tidak-punya-wa

Subagyo, Agus. (2015). Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy in Facing of Cyber Warfare Threat. Jurnal Pertahanan, Vol.5 No.1, hlm 89-108

Survei: 89% Orang Indonesia Pakai WhatsApp Untuk Komunikasi. (n.d.). Retrieved February 24, 2022, from https://inet.detik.com/mobile-apps/d-5594057/survei-89-orang-indonesia-pakai-WhatsApp-untuk-komunikasi

Tentang WhatsApp. (n.d.). WhatsApp.com. Retrieved February 24, 2022, from https://www.WhatsApp.com/about/?lang=id

Terungkap, Spyware Israel Incar Aktivis Indonesia Halaman all—Kompas.com. (n.d.). Retrieved February 24, 2022, from https://tekno.kompas. com/ read/2021/07/19/11010047/terungkap-spyware-israel-incar-aktivis-indonesia?page=all

Vinietta, Elsa. (2016). Strategi Operasi Kontra Intelijen Cyber Sebagai Upaya Peningkatan Ketahanan Negara Indonesia. (https://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf)

Wahid, Abdul& Labib, Mohammad. (2005). Kejahatan Mayantra (Cyber Crime). Bandung: PT Refika Aditama

WhatsApp Ternyata Bisa Diretas lewat Kiriman File Video. (n.d.). Retrieved February 24, 2022, from https://tekno.kompas.com/read/2019/11/19/08020017/WhatsApp-ternyata-bisa-diretas-lewat-kiriman-file-video

Yar, Majid&Steinmetz, Kevin F. (2019). Cybercrime and Society (Third Edition). London: Sage Publication Ltd

Zulkarnain, Rofi'a. (2014). Tindakan Spionase Melalui Penyadapan Antar Negara Sebagai Cybercrime. Jurnal Hukum, (http://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/781/768).