FENOMENA SERANGAN SIBER RUSIA TERHADAP UKRAINA: SEBAGAI PEMBELAJARAN BAGI INDONESIA DALAM PENGEMBANGAN PERTAHANAN SIBER

THE PHENOMENON OF RUSSIAN CYBER ATTACKS ON UKRAINE: LESSONS FOR INDONESIA IN CYBER DEFENSE DEVELOPMENT

Dina Anjelina

HASANUDDIN UNIVERSITY
(nadeenanjela02@gmail.com)

Abstrak – Rusia, sebagai negara great power, sukses melumpuhkan infrastruktur Ukraina melalui serangan siber untuk melakukan aneksasi. Serangan siber Rusia menarik perhatian utama dalam keamanan global, dengan potensi terjadi di negara lain, termasuk Indonesia. Diperlukan peningkatan bentuk pertahanan siber di setiap negara untuk mengantisipasinya. Penelitian ini bertujuan untuk menganalisis jenis serangan siber apa saja yang dilakukan oleh Rusia terhadap Ukraina. Selain itu, penelitian ini juga mengidentifikasi bagaimana upaya negara Indonesia dalam meningkatkan pertahanan siber sebagai bentuk kewaspadaan Indonesia. Metode penelitian yang digunakan adalah metode deskriptif melalui pendekatan kualitatif dengan data bersumber dari studi kepustakaan. Hasil penelitian ini adalah jenis serangan siber yang digunakan Rusia yaitu DDoS (*Distributed Denial of Service*), malware, ransomwar, dan phising. Adapun bentuk pengembangan pertahanan siber Indonesia yakni melalui teknik kriptografi, pembentukan tentara siber, dan bekerja sama dengan komunitas teknologi informasi.

Kata Kunci: Keamanan Nasional, perang, pertahanan siber, Rusia dan Ukraina, serangan siber

Abstract *– Russia, as a great power, successfully crippled Ukraine's infrastructure through a cyber-attack to facilitate annexation. The Russian cyber-attack has become a primary focus in global security, with the potential for similar incidents in other countries, including Indonesia. Enhancement of cyber defense measures in each nation is imperative to preempt such threats. This research aims to analyze the various cyber-attacks carried out by Russia against Ukraine. Additionally, the study identifies Indonesia's efforts to bolster its cyber defense as a manifestation of national vigilance. The research employs a descriptive method with a qualitative approach, drawing data from literature reviews. The findings reveal that Russia employed DDoS (Distributed Denial of Service), malware, ransomware, and phishing in their cyber-attacks. Indonesia's cyber defense development includes cryptographic techniques, the formation of a cyber army, and collaboration with information technology communities.*

Keywords: *National security, war, cyber defense, Russia and Ukraine War, cyber-attacks*

Pendahuluan

Dalam lanskap digital kontemporer, ranah hubungan internasional telah meluas melampaui batas-batas tradisional. Transformasi digital membawa perubahan signifikan dalam cara kita berinteraksi, berkomunikasi, dan membentuk koneksi lintas batas. Keterkaitan antarnegara tidak hanya terjadi dalam domain fisik tetapi juga

melibatkan dunia maya (Aleshkovski, Bondarenko, & Ilyin, 2020; Strømmen-Bakhtiar, 2020).

Abad ke-21 telah menyaksikan pergeseran paradigma dalam dunia konflik dan geopolitik, di mana medan pertempuran konvensional mulai beranjak menuju dunia siber yang kompleks. Fenomena ini menandai era di mana siber menjadi arena utama untuk konfrontasi geopolitik, mengubah cara negara-negara besar dan aktor internasional berinteraksi, berkompetisi, dan bahkan berperang (Douzet & Gery, 2021). Di tengah ketergantungan global pada teknologi informasi, siber tidak lagi hanya menjadi saluran komunikasi atau alat ekonomi, tetapi juga menjadi medan pertempuran yang memainkan peran kunci dalam menentukan keamanan suatu negara (Abaimov & Martellini, 2020).

Siber, sebagai medium di mana informasi dan data mengalir tanpa batas fisik, memberikan kekuatan baru dan menantang dalam dinamika geopolitik. Di dalamnya terdapat potensi untuk memenangkan pertempuran tanpa perlu pertempuran fisik, mengubah cara kita memahami keamanan nasional dan hubungan internasional.

Konflik berkelanjutan antara Rusia dan Ukraina mencerminkan pergeseran, di mana serangan siber memainkan peran sentral bersama strategi militer konvensional (Schulze, 2020).

Perang Rusia-Ukraina mencuri perhatian dunia karena dampaknya pada dinamika politik dan ekonomi global. Dimulai dari demonstrasi warga Ukraina anti-Rusia, konflik ini bertujuan menggulingkan Presiden Viktor Yanukovych yang menolak menandatangani *European Association Agreement* (EAA) pada November 2013, bentuk kerja sama antarnegara timur dan Uni Eropa di bidang ekonomi dan politik (Marples, 2017).

Situasi di Ukraina menunjukkan pergeseran keberpihakan menuju dukungan terhadap Rusia. Setelah menyaksikan aksi demonstrasi yang menentang kebijakan pro-Rusia, Rusia merasa terancam dan melakukan intervensi untuk mencegah Ukraina bergabung dengan Uni Eropa. Intervensi ini semakin memanas dengan munculnya rumor bahwa Ukraina berencana untuk bergabung dengan NATO, dengan tujuan untuk memperkuat kekuatan militer dan memberikan perlawanan terhadap agresi Rusia.

Bagi Rusia, potensi keanggotaan Ukraina di NATO menjadi ancaman serius, karena dikhawatirkan perbatasan antara Ukraina dan Rusia akan dimanfaatkan oleh NATO sebagai garda depan, dengan mendirikan pangkalan militer untuk mengancam keberlangsungan Rusia (Person & McFaul, 2022). Sebagai respons, Rusia melancarkan serangan terhadap beberapa kota besar di Ukraina, mengirim pasukan bersenjata kimia (Child, Gadzo, Rasheed, Harb, & Marsi, 2022), menutup akses bantuan (VOA News, 2022), dan menuntut Ukraina untuk mencabut permohonan bergabungnya dengan Uni Eropa dan NATO (Kotoulas & Pusztai, 2022). Tindakan ini mencerminkan eskalasi ketegangan antara kedua negara dan implikasinya terhadap keamanan regional dan global.

Serangan siber Rusia terhadap Ukraina sejak 2014, dalam konflik wilayah Krimea, memberikan pembelajaran berharga bagi Indonesia dalam mengembangkan pertahanan siber (Baezner, 2018; Jaitner & Geers, 2015; Rõigas, 2018). Krimea, yang dahulu merupakan bagian Uni Soviet, diberikan kepada Ukraina setelah keruntuhan Uni Soviet, tetapi konflik di Krimea memunculkan eskalasi dan keterlibatan Rusia dengan tindakan aneksasi yang menarik perhatian internasional.

Penggulingan Presiden Ukraina Viktor Yanukovych pada 2014, sebagai respons terhadap protes masyarakat, menyebabkan kekosongan kekuasaan dan ketidakstabilan politik di Ukraina. Dalam kondisi tersebut, Rusia campur tangan atas permintaan Perdana Menteri Krimea, didorong oleh pertimbangan etnis dan sejarah, serta kepentingan nasional terkait rencana Ukraina yang pro-Barat dan pro-Integrasi Eropa.

Rusia tidak hanya mengandalkan invasi militer, tetapi juga memanfaatkan serangan siber sebagai alat kekuatan. Serangan ini tidak hanya berdampak lokal, tetapi juga berdampak global, terlihat dari kenaikan harga minyak mentah Brent (Baezner, 2018; Zhang, Hu, Jiao, & Wang, 2024). Dengan menggabungkan serangan militer dan siber, Rusia menjadi pemain utama dalam menciptakan kompleksitas dan ketegangan dalam hubungan geopolitik global.

Pemanfaatan serangan siber sebagai alat strategis dalam konflik modern disoroti oleh teori perang siber, yang menunjukkan bahwa serangan tersebut merupakan bagian integral dari perang proksi yang menggunakan alat

non-militer, khususnya teknologi. Rusia, dalam konteks konfliknya dengan Ukraina, telah meningkatkan serangan siber menjadi instrumen sah dalam strategi militer atau doktrin militer Rusia.

Dengan eskalasi serangan siber Rusia terhadap Ukraina yang terus meningkat hingga 2023, Indonesia, meskipun geografisnya jauh dari zona konflik, berpotensi terkena dampak. Pemerintah Indonesia secara tegas menekankan perlunya penguatan dan peningkatan sistem pertahanan siber nasional.

Era di mana teknologi informasi dan komunikasi berkembang pesat, memiliki dampak positif sekaligus menjadi ancaman terhadap keamanan nasional. Oleh karena itu, pengembangan sistem pertahanan siber Indonesia menjadi krusial sebagai langkah yang tidak bisa dihindari demi menjaga stabilitas nasional.

Sistem pertahanan siber Indonesia rentan terhadap serangan akibat kekurangan tenaga ahli keamanan siber, yang disebabkan oleh minimnya minat masyarakat pada bidang IT dan rendahnya kesadaran akan pentingnya keamanan siber pribadi.

Dalam konteks ini, penelitian ini akan membahas jenis serangan siber Rusia terhadap Ukraina, serta upaya pemerintah Indonesia dalam mengembangkan sistem pertahanan siber sebagai langkah kewaspadaan dan perhatian terhadap ancaman kedaulatan.

Hasil penelitian ini diharapkan dapat meningkatkan pemahaman pembaca tentang urgensi keamanan siber, mengajak lebih peka terhadap potensi ancaman siber yang dapat dihadapi oleh Indonesia, dan mendorong implementasi langkah preventif serta partisipasi aktif dalam mengidentifikasi kebutuhan untuk pengembangan solusi yang lebih efektif.

Metode Penelitian

Penelitian ini menggunakan metode kualitatif untuk mendalami dan mendeskripsikan fenomena yang dikaji, dengan mengumpulkan data sekunder dari dokumen resmi, seperti Berita Acara Keputusan Presiden, dan basis data pemerintah, termasuk Publikasi Badan Pusat Statistik Indonesia.

Metode penulisan kualitatif berbasis studi pustaka, di mana data dikumpulkan melalui analisis sumber referensi seperti buku, jurnal, dan riset sebelumnya, untuk menghasilkan pernyataan menjawab rumusan masalah yang ditetapkan (Zed, 2008). Hasil analisis data diinterpretasikan secara deskriptif

dan eksplanatif, menjelaskan hubungan sebab-akibat antar dua variabel dengan merujuk pada teori perang siber dan pertahanan siber.

Hasil dan Pembahasan

Serangan Siber Rusia Terhadap Ukraina

Sebagai negara *great power*, Rusia telah menggunakan kekuatan siber untuk mengekspresikan ketidakpuasannya. Pemimpin Rusia, Vladimir Putin, menganggap kemampuan sebagai kunci utama dalam mewujudkan tujuan politik luar negeri Rusia.

Pada periode 2014-2016, Rusia mencatat sejarah serangan siber awal terhadap Ukraina, yang terungkap melalui data dari *Center for Strategic and International Studies* (CSIS) (Mueller, Jensen, Valeriano, Maness, & Macias, 2023). Motivasi di balik penggunaan kekuatan siber ini adalah peluang besar keberhasilan di Ukraina, yang dianggap belum kuat dalam bidang teknologi.

Dalam serangan tersebut, Rusia mengincar infrastruktur internet Ukraina, merusak situasi menjelang pemilihan umum dengan menghancurkan citra kandidat nasionalis dan mendukung kandidat pro-Rusia. Serangan tersebut melibatkan pencurian informasi sensitif dari pemimpin Jerman, NATO, dan pejabat Demokrat yang akan disebarluaskan.

Rusia juga diduga meretas jaringan komputer Belanda untuk mendapatkan informasi rahasia terkait jatuhnya pesawat Malaysia Airlines MH17 di Ukraina pada tahun 2014 (de Hoon, 2019; De Hoon, 2017).

Selain itu, Rusia menyerang infrastruktur energi Ukraina dengan menutup jalur pipa yang mengakibatkan krisis energi di Uni Eropa dan melakukan pemadaman listrik, menciptakan ketidakstabilan dan merusak operasi militer Ukraina serta kepercayaan masyarakat terhadap pemerintah. Akibat dari serangan siber tersebut, beberapa koalisi internasional seperti NATO dan PBB memberikan kecaman agar Rusia menghormati kedaulatan Ukraina dengan mengakhiri serangannya.

Uni Eropa dan Amerika Serikat menjatuhkan sanksi ekonomi sebagai respons terhadap aneksasi Rusia terhadap Ukraina yang dianggap illegal (BAŞARAN, 2020; Silva & Selden, 2020). Sanksi ini mencakup pembekuan aset, larangan bertransaksi pada entitas tertentu, pembatasan ekspor dan layanan khusus, terutama yang berkaitan dengan ekspor minyak gas Ukraina ke Rusia. Sanksi ini juga diarahkan untuk

menyeimbangkan isi perjanjian Minsk, sebuah kesepakatan perdamaian yang ditandatangani pada tahun 2014 dan 2015 untuk mengatasi konflik di Ukraina Timur.

Perjanjian Minsk menetapkan persyaratan penting, termasuk pertahanan kedaulatan dan integritas teritorial Ukraina, prinsip non-intervensi, perlindungan hak asasi manusia, dan perdamaian di Ukraina Timur (Bentzen, 2020). Para pihak yang terlibat diharapkan mematuhi dan bekerja sama untuk mencapai stabilitas di Ukraina dan sekitarnya.

Meskipun mendapat kecaman internasional, Rusia melanjutkan serangan siber ke Ukraina pada tahun 2022. Serangan ini dimulai pada 13 Januari dan berlanjut dengan lebih dari 2.194 serangan. Target utamanya termasuk situs web pemerintahan dan lembaga keuangan Ukraina. Rusia menggunakan berbagai teknik, seperti serangan DDoS, malware, ransomware, dan phishing (Lewis, 2022)

Dampaknya melibatkan kelumpuhan sejumlah situs web dan institusi, termasuk bank besar Ukraina. Rusia juga meretas perusahaan satelit terbesar di dunia, menyebabkan kerugian besar dalam komunikasi internet di Ukraina (O'Neill, 2022). Namun, Ukraina berhasil merespons dengan membentuk pasukan ahli dalam teknologi informasi untuk melawan Rusia. Dengan serangkaian teknik yang digunakan, termasuk DDoS, malware, ransomware, dan phishing, Rusia terus menjadi ancaman serius di ranah siber global (Romandash, 2023).

Dalam perspektif teori perang siber, aksi penyerangan Rusia terhadap teknologi komunikasi dan jaringan informasi negara Ukraina menggambarkan bahwa serangan siber telah dijadikan sebagai alat militer untuk mengganggu layanan digital nasional melalui peretasan terhadap instansi pemerintah dan sarana prasarana masyarakat (Lehto, 2022; Li & Liu, 2021) . Rusia juga menjadikan serangan siber sebagai instrumen kegiatan spionase seperti mengumpulkan informasi rahasia negara-negara lain.

Contoh kasus pada tahun 2017, serangan siber NonPetya yang diduga menjadi malapetaka bagi sistem perekonomian negara Ukraina dikarenakan virus yang menargetkan sistem Windows ini telah menyebarluas di seluruh bisnis Ukraina (Marsh, 2018).

Menurut pakar ahli keamanan siber, Caton & Libicki (2024) dalam bukunya yang berjudul *"Cyberdetterence and*

Cyberwar," perang siber memiliki tujuan eksternal dan tujuan internal yang dipandang secara objektif. Tujuan eksternal umumnya menjadi penyebab perang siber tersebut terjadi, yakni menjatuhkan pihak lawan sesuai dengan keinginan. Sedangan tujuan internal berkaitan dengan pengelolaan konflik itu sendiri untuk menghindari ekskalasi menjadi kekerasan.

Meskipun pada dasarnya tujuan perang siber adalah menghancurkan musuh tanpa melibatkan pertempuran fisik, dampaknya dapat menciptakan ketidakstabilan nasional melalui kerusakan pada infrastruktur kritis. Contohnya, serangan siber Rusia terhadap Ukraina menunjukkan bahwa Rusia memiliki tujuan internal tertentu. Dalam konteks ini, Rusia berusaha memperingatkan Ukraina untuk tidak bergabung dengan NATO, yang dianggap sebagai ancaman keamanan dan dapat memicu eskalasi konflik internasional, menciptakan ketegangan antara NATO dan Rusia. Serangan siber menjadi alat untuk mencapai tujuan tersebut.

Pembelajaran Bagi Pengembangan Pertahanan Siber Indonesia

Seiring dengan kemajuan budaya dan peradaban manusia, perkembangan teknologi mengalami pertumbuhan yang pesat. Saat kebudayaan berkembang, teknologi pun semakin maju. Namun, dampak dari kemajuan teknologi tidak hanya positif, terutama dalam konteks keamanan siber yang menjadi isu krusial. Fenomena serangan siber antara Rusia dan Ukraina menjadi sorotan, tidak hanya karena mempengaruhi keamanan nasional kedua negara tersebut, tetapi juga merugikan stabilitas global. Hal ini menjadi pelajaran berharga bagi Indonesia untuk memperkuat pertahanan sibernya.

Data dari Kementerian Komunikasi dan Informatika (Kemkominfo) menunjukkan bahwa Indonesia menduduki peringkat kedelapan sebagai negara dengan jumlah pengguna internet terbanyak di dunia, mencapai 82 juta orang. Tingginya pengguna internet membuka peluang bagi serangan siber, terutama jika keamanan data tidak memadai. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa total serangan siber di Indonesia pada tahun 2022 mencapai 370,02 juta serangan, menunjukkan peningkatan sekitar 38,72% dibandingkan tahun sebelumnya (Pratiwi, 2023).

Beragam jenis serangan siber seperti *provocative, hate content, hate*

speech, pencurian data, dan pembobolan rekening (Zamir, 2020) semakin memperlihatkan kerentanan sistem pertahanan siber Indonesia. Dalam menghadapi tantangan ini, peran masyarakat sangat penting. Peningkatan kesadaran akan keamanan siber dan penerapan teknik penyandian atau kriptografi oleh individu dapat menjadi langkah awal dalam melindungi data dan informasi.

Namun, tantangan utama bagi Indonesia adalah kurangnya tenaga ahli keamanan siber, terutama dalam sektor strategis, pertahanan, dan bisnis. Pembentukan tentara siber menjadi solusi yang perlu dipertimbangkan untuk mengatasi serangan siber. Kerjasama antara Kementerian Pertahanan dan Kementerian Infomasi dan Komunikasi, serta kolaborasi dengan operator dan aktor keamanan, dapat memperkuat pertahanan siber Indonesia.

Langkah-langkah tersebut mencerminkan implementasi dari teori pertahanan siber (*cyber defense*), yang menekankan perlunya menjaga kerahasiaan, integritas, dan ketersediaan informasi negara. Upaya ini didukung oleh Kementerian Pertahanan Indonesia, 2014 tentang Pedoman Pertahanan Siber. Melalui langkah konkret ini, diharapkan Indonesia dapat terus mengembangkan pertahanan siber guna menghadapi ancaman dalam era teknologi informasi yang terus berkembang pesat.

Kesimpulan, Rekomendasi, dan Pembatasan

Dari hasil penelitian ini dapat disimpulkan jenis serangan siber oleh Rusia ke Ukraina yaitu DDoS *(Distributed Denial of Service)*, malware, ransomwar, dan phising. Mengevaluasi respons negara Indonesia dalam mengambil pembelajaran terkait keamanan dan pertahanan siber. Dengan merujuk pada teori serangan siber dan pertahanan siber, tulisan menyajikan analisis terstruktur terhadap kompleksitas perang siber dan peran masing-masing pihak. Eskalasi serangan siber antara Rusia dan Ukraina menyoroti kelemahan dalam sistem pertahanan siber Indonesia.

Meski adanya langkah-langkah konkret yang diambil oleh Indonesia dalam menghadapi ancaman siber, masih terdapat keterbatasan yang perlu diatasi. Beberapa kendala antara lain kurangnya kesadaran masyarakat tentang keamanan siber, keterbatasan tenaga ahli, dan masih adanya kerentanan dalam sistem pertahanan siber. Untuk mengatasi pembatasan ini, perlu

dilakukan tindakan lebih lanjut seperti peningkatan investasi dalam pelatihan dan pendidikan di bidang keamanan siber.

Rekomendasi meliputi peningkatan pelatihan tenaga ahli keamanan siber, penguatan kesadaran masyarakat, dan upaya bersama dalam membentuk tentara siber yang efektif.

Daftar Pustaka

Abaimov, Stanislav, & Martellini, Maurizio. (2020). *Cyber arms: security in cyberspace* (Myriam Dunn Cavelty & Andreas Wenger, Eds.). Retrieved from https://www.google.com/books?hl=id&lr=&id=ui3tDwAAQBAJ&oi=fnd&pg=PT5&dq=Cyber+is+no+longer+just+a+communication+channel+or+an+economic+tool,+but+also+a+battleground+that+plays+a+key+role+in+determining+a+country%27s+security.&ots=AAMfIwxQk1&sig=ZFmV2kYhJmbg-bHnpfYUr50Stuk

Aleshkovski, Ivan, Bondarenko, Valentina, & Ilyin, Ilya. (2020). Global values, digital transformation and development strategy for global society: conceptual framework. *International Journal of Foresight and Innovation Policy*, *14*(2/3/4), 120. https://doi.org/10.1504/IJFIP.2020.111243

Baezner, Marie. (2018). *Cyber and Information warfare in the Ukrainian conflict*. ETH Zurich.

BAŞARAN, Ali. (2020). Annexation Of Crimea By Russian Federation, United States And European Union's Economic Sanctions Against Russian Federation, 2014-2018. *Asya Studies*, *4*(11), 91–106. https://doi.org/10.31455/asya.686618

Bentzen, Naja. (2020). *Ukraine: The Minsk agreements five years on*. Retrieved from EPRS: European Parliamentary Research Service website: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2020)646203

Caton, Jeffrey L., & Libicki, Martin C. (2024). [Review of Cyberdeterrence and Cyberwar]. Strategic Studies Quarterly. *Strategic Studies Quarterly*, *5*(1), 148–150. Retrieved from http://www.jstor.org/stable/26270515

Child, David, Gadzo, Mersiha, Rasheed, Zaheena, Harb, Ali, & Marsi, Federica. (2022). Ukraine latest updates: NATO will 'respond' to chemical weapons Ukraine-Russia news from March 24: US President Joe Biden warns Russia against using chemical weapons in Ukraine. Retrieved October 22, 2023, from https://www.aljazeera.com/news/2022/3/23/us-president-biden-arrives-in-brussels-ahead-of-nato-summit-liveblog

de Hoon, Marieke. (2019). Pursuing Justice for MH17: The Role of the Netherlands. *Netherlands Yearbook of International Law 2018: Populism and International Law*, 245–270.

De Hoon, Marieke. (2017). Navigating the legal horizon: Lawyering the MH17 disaster. *Utrecht J. Int'l & Eur. L.*, *33*, 90.

Douzet, Frédérick, & Gery, Aude. (2021). Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in

cyberspace. *Journal of Cyber Policy*, *6*(1), 96–113. https://doi.org/10.1080/23738871.2021.1937253

Jaitner, Margarita, & Geers, Kenneth. (2015). Russian information warfare: Lessons from Ukraine. *Cyber War in Perspective: Russian Aggression against Ukraine*, 87–94.

Kementerian Pertahanan Indonesia. *Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Sibe.* , (2014).

Kotoulas, Ioannis E., & Pusztai, Wolfgang. (2022). Geopolitics of the War in Ukraine. *Foreign Affairs Institute*.

Lehto, Martti. (2022). Cyber-attacks against critical infrastructure. In *Cyber Security: Critical Infrastructure Protection* (pp. 3–42). Springer.

Lewis, James Andrew. (2022). *Cyber War and Ukraine*. Retrieved from https://www.csis.org/analysis/cyber-war-and-ukraine

Li, Yuchong, & Liu, Qinghui. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Marples, David R. (2017). Ukraine in Conflict An Analytical Chronicle. In *E-International Relations*. Retrieved from https://www.e-ir.info/wp-content/uploads/2017/05/Ukraine-in-Conflict-E-IR.pdf

Marsh, Sarah. (2018). US joins UK in blaming Russia for NotPetya cyber-attack. In *Cybercrime*. Retrieved from https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine

Mueller, G., Jensen, Benjamin, Valeriano, Brandon, Maness, R., & Macias, J. (2023). Cyber operations during the Russo–Ukrainian war. In *Center for Strategic Int. Studies, Washington, DC, USA*. Retrieved from JSTOR website: https://www.jstor.org/stable/resrep52130

O'Neill, Patrick Howell. (2022). *Russia hacked an American satellite company one hour before the Ukraine invasion*. Retrieved from https://www.technologyreview.com/supertopic/about/

Person, Robert, & McFaul, Michael. (2022). What Putin fears most. *Journal of Democracy*, *33*(2), 18–27. Retrieved from https://www.journalofdemocracy.org/articles/what-putin-fears-most/

Pratiwi, Febriana Sulistya. (2023). *BSSN Catat 370,02 Juta Serangan Siber ke Indonesia pada 2022*. Retrieved from https://dataindonesia.id/internet/detail/bssn-catat-37002-juta-serangan-siber-ke-indonesia-pada-2022

Rõigas, Henry. (2018). Cyber war in perspective: lessons from the conflict in Ukraine. *A Civil-Military Response to Hybrid Threats*, 233–257.

Romandash, Anna. (2023). *Ukraine's IT Army: Digital Resistance to Russian Propaganda*. https://doi.org/10.7274/qr46qz24c90

Schulze, Matthias. (2020). Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *2020 12th International Conference on Cyber Conflict (CyCon)*, *1300*, 183–197.

https://doi.org/10.23919/CyCon49761.2020.9131733

Silva, Paul M., & Selden, Zachary. (2020). Economic interdependence and economic sanctions: a case study of European Union sanctions on Russia. *Cambridge Review of International Affairs*, *33*(2), 229–251. https://doi.org/10.1080/09557571.2019.1660857

Strømmen-Bakhtiar, Abbas. (2020). *Introduction to Digital Transformation: and its impact on society*. Informing Science Press.

VOA News. (2022). Ukraine Demands Russia Allow Aid into Mariupol and Open a Corridor for Safe Civilian Passage. Retrieved November 23, 2023, from VOA News website: https://www.voanews.com/a/biden-russia-may-use-cyberattacks-chemical-weapons-/6495562.html

Zamir, Hassan. (2020). Cybersecurity and Social Media. *Cybersecurity for Information Professionals: Concepts and Applications*, 153.

Zed, Mestika. (2008). *Metode penelitian kepustakaan*. Yayasan Pustaka Obor Indonesia.

Zhang, Qi, Hu, Yi, Jiao, Jianbin, & Wang, Shouyang. (2024). The impact of Russia–Ukraine war on crude oil prices: an EMC framework. *Humanities and Social Sciences Communications*, *11*(1), 8. https://doi.org/10.1057/s41599-023-02526-9