

## Referensi

- Ajayi, V. O. (2023). A Review on Primary Sources of Data and Secondary Sources of Data. *European Journal of Education and Pedagogy*, 2 (3).
- Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*.
- Alliance for Securing Democracy. (2014). *Russian government-connected hacktivist group CyberBerkut breaches Ukraine's Election Commission*.
- Alliance For Securing Democracy. Retrieved August 7, 2024, from <https://securingdemocracy.gmfus.org/incident/russian-government-connected-hacktivist-group-cyberberkut-breaches-ukraines-election-commission/>
- Anjelina, D. (2023). FENOMENA SERANGAN SIBER RUSIA TERHADAP UKRAINA: SEBAGAI PEMBELAJARAN BAGI INDONESIA DALAM PENGEMBANGAN PERTAHANAN SIBER. *Jurnal Pertahanan dan Bela Negara*, Volume 13 Nomor 3.
- AntaraNEWS. (2023, May 14). *Jangan terperosok kubangan perang informasi pada konflik Rusia-Ukraina*. *Antaraneews.com*. Retrieved June 18, 2024, from <https://www.antaraneews.com/berita/3537810/jangan-terperosok-kubangan-perang-informasi-pada-konflik-rusia-ukraina>
- Arikunto, & Suharsimi. (2006). *Prosedur Penelitian : Suatu Pendekatan Praktek*. Rineka Cipta.
- Army Cyber Institute. (2022). The Cyber Defense Review. *Russian Cyber Operations in the Invasion of Ukraine, No. 4 (FALL 2022)*. Retrieved September, 2024, from

[https://www.jstor.org/stable/pdf/48703290.pdf?refreqid=fastly-default%3A4b5e7a3d9891ef95263513e24cf22fe1&ab\\_segments=&initiator=&acceptTC=1](https://www.jstor.org/stable/pdf/48703290.pdf?refreqid=fastly-default%3A4b5e7a3d9891ef95263513e24cf22fe1&ab_segments=&initiator=&acceptTC=1)

Arquilla, J., & Ronfeldt, D. (1993). CYBERWAR IS COMING! *Vol 12*(No. 2).

Asmolov, G. (2022, Agustus 15). The transformation of participatory warfare: The role of narratives in connective mobilization in the Russia–Ukraine war. *Digital War*.

<https://link.springer.com/article/10.1057/s42984-022-00054-5>

Atlantic Council. (2022, Maret). *Russia's cyber statecraft*.

<https://www.atlanticcouncil.org/commentary/the-5x5-russias-cyber-statecraft/>

Atok, F. (2022). ANALISIS KONFLIK RUSIA DAN UKRAINA (STUDIKEPUSTAKAAN STATUS KEPEMILIKAN KRIMEA). *Jurnal Poros Politik*, 2528–0953, 11-15.

Bajraktari, Y., & Parajon, C. (2008, January). Media and Conflict Afghanistan as a Relative Success Story. *UNiteD StateS iNStitUte of PeaCe*.

Banasik, M. (2016). RUSSIA'S HYBRID WAR IN THEORY AND PRACTICE. *Journal on Baltic Security*, Vol 2, Issue 1.

Binus University. (2022, October 9). DDoS: Distributed Denial of Service – Cyber. Retrieved June 14, 2024, from <https://student-activity.binus.ac.id/csc/2022/10/ddos-distributed-denial-of-service/>

Binus University. (2024). *Mengenal Karakteristik dan Peran Mass Communication dalam Kehidupan Bermasyarakat*. BINUS UNIVERSITY.

Retrieved August 31, 2024, from <https://binus.ac.id/2024/05/peran-mass-communication-dalam-kehidupan-bermasyarakat/>

Bryman, A. (2012). *Social Research Methods*. OUP Oxford.

Budi, M. (2024, January 19). *Dua Peneliti Ini Unboxing Propaganda Medsos di Era 'Demokrasi Sesat'*. detikNews. Retrieved October 2, 2024, from <https://news.detik.com/berita/d-7149792/dua-peneliti-ini-unboxing-propaganda-medsos-di-era-demokrasi-sesat>

BUDIMAN, L. S. D. C. (2023). *Perang Rusia Ukraina dalam Perspektif Siber* (1st ed., Vol. 1). Politeknik Siber dan Sandi Negara.

Cahyani, I. (2012). Pendekatan Induktif Dan Deduktif.

Chin, W. (2018). Russia's Digital Awakening. *Connections: The Quarterly Journal*, QJ 17, no. 2. <https://www.jstor.org/stable/26936535>

CISA. (2022, October 28). *Understanding and Responding to Distributed Denial of Service Attacks*. CISA. Retrieved September 21, 2024, from [https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks\\_508c.pdf](https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf)

Clark, M. (2020, September 7). *RUSSIAN HYBRID WARFARE*. Institute for the Study of War. Retrieved October 2, 2024, from <https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf>

CliffsNotes. (2024, Maret 24). *Computer Network Defense*.

Cohen, S., Gowan, R., Gienger, V., Shah, P., Finucane, B., Prendergast, J., Wilson, D., Van Landingham, M., Wilde, G., Barrett, P. M., Graham, T., Hendrix, J., Jackson, D., Eisen, N. L., Klasfeld, A., Angel, S., Boone, C.,

Goodman, R., Barrilleaux, F., ... Berger, C. (2022, September 12). *AcidRain Malware and Viasat Network Downtime in Ukraine: Assessing the Cyber War Threat*. Just Security. Retrieved September 21, 2024, from <https://www.justsecurity.org/83021/acidrain-malware-and-viasat-network-downtime-in-ukraine-assessing-the-cyber-war-threat/>

Connell, M., & Vogler, S. (2017, Maret). *Russia's Approach to Cyber Warfare*. [https://www.cna.org/archive/CNA\\_Files/pdf/dop-2016-u-014231-1rev.pdf](https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf)

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

CSIRT Bappenas. (2021, October 26). *Layanan | Panduan Penanganan Insiden Serangan DDoS | CSIRT Kementerian PPN/Bappenas*. Retrieved June 14, 2024, from <https://csirt.bappenas.go.id/layanan/detail/bbd46f4f-bf6f-4e33-93bb-43b17528683c>

Danish Institute for International Studies. (2017). *Russian Hybrid Warfare : A Study Of Disinformation*. RUSSIAN HYBRID WARFARE. Retrieved October 2, 2024, from [https://pure.diis.dk/ws/files/950041/diis\\_rp\\_2017\\_6\\_web.pdf](https://pure.diis.dk/ws/files/950041/diis_rp_2017_6_web.pdf)

Darley, W. M. (2006). *Clausewitz's Theory of War and Information Operations*.

*DDoS Attacks*. (n.d.). Imperva a Thales Company. Retrieved 2024, from <https://www.imperva.com/learn/ddos/ddos-attacks/>

Delfia Balisa, Abigail Leffia, & Yamato Shino. (2023, oktober). *Memanfaatkan Fungsi Sistem Informasi Manajemen: Prospek dan*

Tantangan di Dunia Bisnis. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 2, no. 2. 10.33050/mentari.v2i2.452

Department of the Navy. (2009). *Computer Network Defense Roadmap*.

Deuze, M. (2020). THE ROLE OF MEDIA AND MASS COMMUNICATION THEORY IN THE GLOBAL PANDEMIC. *THE ROLE OF MEDIA AND MASS COMMUNICATION THEORY IN THE GLOBAL PANDEMIC*, Vol. 11(No. 2).

Djoyonegoro, N. (2022, Maret Kamis). *Mewaspada dampak serangan siber perang Rusia-Ukraina*.

Duguin, S., & Pavlova, P. (2023, September). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. *Euro Parliament*.  
[https://www.europarl.europa.eu/thinktank/en/document/EXPO\\_BRI\(2023\)702594](https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594)

DW News. (2022, January 14). *Ukrainian websites hacked in 'global attack'* – DW – 01/14/2022. DW. Retrieved September 21, 2024, from <https://www.dw.com/en/ukraine-government-websites-hacked-in-global-attack/a-60421475>

Dw News. (2022, February 22). *Latar Belakang Konflik Ukraina dan Invasi Rusia ke Donbas* – DW – 22.02.2022. DW. Retrieved August 31, 2024, from <https://www.dw.com/id/latar-belakang-konflik-ukraina-dan-invasi-rusia-ke-donbas/a-60872988>

Fortner, R. S., & Fackler, P. M. (2014). *The Handbook of Media and Mass Communication Theory* (Vol. Volume I). The Handbook of Media and Mass Communication Theory.

Fortuna, G. (2024, July 16). *Russia's ever-escalating hybrid war has the EU in its crosshairs*. Euronews.com. Retrieved September 2, 2024, from <https://www.euronews.com/my-europe/2024/07/16/russias-ever-escalating-hybrid-war-has-the-eu-in-its-crosshairs>

Fridman, O. (2019, March 4). *On the "Gerasimov Doctrine": Why the West Fails to Beat Russia to the Punch*. NDU Press. Retrieved October 1, 2024, from [https://ndupress.ndu.edu/Portals/68/Documents/prism/prism\\_8-2/PRISM\\_8-2\\_Fridman.pdf](https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Fridman.pdf)

Fridman, O. (2020). (PDF) *The Russian perspective on information warfare: conceptual roots and politicisation in russian academic, political, and public discourse*. ResearchGate. Retrieved October 26, 2024, from [https://www.researchgate.net/publication/324768132\\_The\\_Russian\\_perspective\\_on\\_information\\_warfare\\_conceptual\\_roots\\_and\\_politicisation\\_in\\_russian\\_academic\\_political\\_and\\_public\\_discourse](https://www.researchgate.net/publication/324768132_The_Russian_perspective_on_information_warfare_conceptual_roots_and_politicisation_in_russian_academic_political_and_public_discourse)

Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2023). Russian propaganda on social media during the 2022 invasion of Ukraine. *EPJ DATA SCIENCE*.

Glapiak, A. (2023). Implications of the war in Ukraine for the strategic communication system of the Polish Ministry of National Defence. *Security Defence*.

Gobel, T. (2020, October 27). *NotPetya, Malware Perusak yang Diduga Terafiliasi dengan Rusia*. Cyberthreat.id. Retrieved June 13, 2024, from <https://cyberthreat.id/read/8978/NotPetya-Malware-Perusak-yang-Diduga-Terafiliasi-dengan-Rusia>

Goemans, H., & Slantchev, B. (2023, May 17). *Premature Calls for Ukraine-Russia Talks Are Dangerous*. The Atlantic. Retrieved September 25, 2024, from <https://www.theatlantic.com/ideas/archive/2023/05/russia-ukraine-war-peace-talks-negotiations/674079/>

HAIG, Z. (2020). NOVEL INTERPRETATION OF INFORMATION OPERATIONS IN TODAY'S CHANGED OPERATIONAL ENVIRONMENT. *Scientific Bulletin, Vol. XXV, No. 2(50)*, 93-101.

Haigh, M., Haigh, T., & Matychak, T. (2019). Information Literacy vs. Fake News: The Case of Ukraine. *Open Information Science*. <https://doi.org/10.1515/opis-2019-0011>

Iliuk, K. (2023, Februari). *Kremlin Information Operations Before and After Ukraine Invasion*. Atlantic Council. Retrieved September 25, 2024, from <https://www.atlanticcouncil.org/event/kremlin-information-operations-before-and-after-the-february-2022-invasion/>

Joint Chief of Staff. (2016, agustus 19). *Public Affairs, Joint Publication 3-61*.

Joint Publication. (2011, agustus). Joint Publication. *Joint Operations, 3-0*.

Joint Publication. (2012, Januari 26). Military Deception. *Joint Publication*.

Joint Publication. (2016, Januari 06). Operation Security. *Joint Publication, 3-13.3*.

Karisma, I., & Burhanuddin, A. (2023, Juni). Signifikansi Perang Siber dalam Konflik Modern Rusia-Ukraina Studi Kasus: Wizard Spider - It Army. *JISHUM (Jurnal Ilmu Sosial dan Humaniora)*, Vol. 1, No. 4.

Kementerian Pertahanan Republik Indonesia. (2017, Mei 15). *Psychological Operations (PsyOps) Adalah untuk Memenangkan Hati dan Pikiran Masyarakat*. <https://www.kemhan.go.id/2017/05/15/psychological-operations-psyops-adalah-untuk-memenangkan-hati-dan-pikiran-masyarakat.html>

Khateeb, S. A., & Agarwal, N. (2016). UNDERSTANDING STRATEGIC INFORMATION MANOEUVRES IN NETWORK MEDIA TO ADVANCE CYBER OPERATIONS: A CASE STUDY ANALYSING PRO-RUSSIAN SEPARATISTS' CYBER INFORMATION OPERATIONS IN CRIMEAN WATER CRISIS. *Journal on Baltic Security, Vol 2, Issue 1*.

Kirby, P. (2015, February 18). *Ukraine conflict: Why is east hit by conflict?* BBC. Retrieved September 2, 2024, from <https://www.bbc.com/news/world-europe-28969784>

Kirby, P. (2023). Why is Russia Invading Ukraine and What does Putin Wants.

Kizilova, K., & Norris, P. (2022, March 29). Assessing Russian Public Opinion on the Ukraine War. *RUSSIAN ANALYTICAL DIGEST, no 281*. 10.3929/ethz-b-000539633

Kuehl, D. D. (2004). Information Operations: The Hard Reality of Soft Power.



Kuehl, D. T. (2002). *Information Operations, Information Warfare, and Computer Network Attack Their Relationship to National Security in the Information Age*. 76(International Law Studies).

Kustiawan, W., Siregar, F. K., & Alwiyah, S. (2022). KOMUNIKASI MASSA. *JOURNAL ANALYTICA ISLAMICA*, 11(1).

Kuzio, T. (2022). *Why Russia Invaded Ukraine*. CIRSD. Retrieved September 22, 2024, from <https://www.cirsd.org/files/000/000/009/83/07c4011b79675bf82057e13d0f8669ff60d67441.pdf>

Lakshmanan, R. (2024, March 19). *Suspected Russian Data-Wiping 'AcidPour' Malware Targeting Linux x86 Devices*. The Hacker News. Retrieved September 21, 2024, from <https://thehackernews.com/2024/03/suspected-russian-data-wiping-acidpour.html>

Laksono, A. W. (2012, Januari 09). KONFLIK GEORGIA DAN RUSIA DI OSSETIA SELATAN PADA BULAN AGUSTUS 2008. *Konflik Georgia*.

Lee, C. (2023, May 11). *Russian Cyber Operations Against Ukrainian Critical Infrastructure*. Freeman Spogli Institute for International Studies. Retrieved October 14, 2024, from <https://fsi.stanford.edu/sipr/russian-cyber-operations-against-ukrainian-critical-infrastructure>

Libicki, & C, M. (1995). *What Is Information Warfare?*

Lonsdale, D. J. (2004). *The Nature of War in the Information Age: Clausewitzian Future*. Taylor & Francis.

Lucas, G. (2017). *Ethics and Cyber Warfare*.

M.A.G., D. H. A. M. (2015). *Pendekatan Kualitatif* (Cetakan 1 ed.). KALIMEDIA.

Matlock, J. F. (2022, February 15). *I was there: NATO and the origins of the Ukraine crisis*. Responsible Statecraft. Retrieved September 22, 2024, from <https://responsiblestatecraft.org/2022/02/15/the-origins-of-the-ukraine-crisis-and-how-conflict-can-be-avoided/>

McQuail, D. (2009, November). *McQuail's Mass Communication Theory, 6th edition*.

Media Indonesia. (2023, May 16). *Ini Pengertian dan Perbedaan Malware, Ransomware, Social Engineering, dan Ancaman Siber Lainnya*. Retrieved June 14, 2024, from <https://mediaindonesia.com/teknologi/581649/ini-pengertian-dan-perbedaan-malware-ransomware-social-engineering-dan-ancaman-siber-lainnya>

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook*. SAGE Publications.

Molander, R. C., Riddile, A. S., & Wilson, P. A. (1996). STRATEGIC INFORMATION WARFARE : A New Face of War. *National Defense Research Institute*.

Moleong, L. J. (2013). In *Metodologi Penelitian Kualitatif* (Vol. Cetakan 31, p. 330). Remaja Rosdakarya.

Monaghan, A. (2014, July 1). *NATO Review - The Ukraine crisis and NATO-Russia relations*. NATO. Retrieved September 2, 2024, from <https://www.nato.int/docu/review/articles/2014/07/01/the-ukraine-crisis-and-nato-russia-relations/index.html>

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023, July 13). *Cyber Operations during the Russo-Ukrainian War*. CSIS. Retrieved September 19, 2024, from <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>

Mulyana, R. (2024). *Computer Network Operations (CNO)*. RifqiMulyana.com. Retrieved 2024, from <https://rifqimulyawan.com/literasi/computer-network-operations-cno/>

Muur, M. K. M. K., Dr. Holger Molder, Dr. Vladimir Sazonov, & Prof. Dr. Pille Pruulmann-Vengerveldt. (2016). RUSSIAN INFORMATION OPERATIONS AGAINST THE UKRAINIAN STATE AND DEFENCE FORCES: APRIL-DECEMBER 2014 IN ONLINE NEWS. *Journal on Baltic Security, Vol 2, Issue 1,*.

Narula, S. (2004, Maret 21). Psychological operations (PSYOPs): A conceptual overview. *Strategic Analysis, Vol.28 No 1*.

NATO. (2020). *Media Disinformation Security [Information Warfare]*. [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf)

NATO. (2023, Januari). Allied Joint Doctrine for Information Operations. *Allied Joint Publication-10.1, Version 1*(Edition A).

Naval Csirt. (2024). *MALWARE 'ACIDPOUR' MENARGETKAN TELEKOMUNIKASI UKRAINA*. <https://naval-csirt.tnial.mil.id/malware-acidpour-menargetkan-telekomunikasi-ukraina/>

Nenad, P., & Branislav, M. (2021). Russian information operations in the Ukrainian armed conflict. 10.5937/bezbednost2101D0ABOUT62

Nowacki, L. (2019, November 09). How Ukraine Won the ‘#Like’ War with Russia Using Popular Mass Media – Dynamic Framing in Online Headlines in Poland. *Current Trends in Mass Communication*.

Nur Aini Adzan Nisa, & Rahman A Suwaidi. (2023). Analisis Potensi Dampak Artificial Intelligence (AI) terhadap Efisiensi Manajemen Operasional: Tinjauan Literatur. *Indonesian Journal of Social Sciences and Humanities, Vol. 3 No. 2*.

Oktaviano, D. R., & Fachri, Y. (2015, Juli). Kepentingan Rusia Me-Aneksasi Semenanjung Krimea Tahun 2014. *Jurnal Transnasional, Vol. 7*(No. 1).

Opperman, L. C. D. A. (2012). Strategy Research Project. *Information Operations and Public Affairs: A Union of Influence*.

Patton, M. Q. (2002). *Qualitative research and evaluation methods*. SAGE Publications.

Poerwandari, E. K. (1998). Poerwandari.

Polityuk, P. (2022, January 14). *EXCLUSIVE Hackers likely used software administration rights of third party to hit Ukrainian sites, Kyiv says*.

Reuters. Retrieved September 21, 2024, from <https://www.reuters.com/world/europe/exclusive-hackers-likely-used-software-administration-rights-third-party-hit-2022-01-14/>

Prabowo, G., & Gischa, S. (2020, December 5). *Sejarah Krisis Crimea (2014)*. Kompas.com. Retrieved August 31, 2024, from

<https://www.kompas.com/skola/read/2020/12/05/134515369/sejarah-krisis-crimea-2014>

Pratiwi, A. (2023). KEPENTINGAN RUSIA DALAM PENGGERAHAN OPERASI MILITER KE UKRAINA TAHUN 2022.

President of Russia. (2022, February 24). *Address by the President of the Russian Federation*. President of Russia. Retrieved June 26, 2024, from <http://en.kremlin.ru/events/president/news/67843>

Proborini, D. (2016, Desember). Sisi Gelap Era Informasi: Information Warfare dan Perang Virtual. *Jurnal Globalisasi dan Masyarakat Informasi Minggu keduabelas*.

Przetacznik, J., & Tarpova, S. (2022, June 8). *Russia's war on Ukraine: Timeline of cyber-attacks*. European Parliament. Retrieved September 21, 2024, from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS\\_BRI\(2022\)733549\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf)

Putin, V. (2022, February 21). *Обращение Президента Российской Федерации • Президент России*. Президент России. Retrieved November 9, 2024, from <http://kremlin.ru/events/president/news/67828>

Putin, V. (2022, May 9). *Парад Победы на Красной площади • Президент России*. Президент России. Retrieved November 9, 2024, from <http://kremlin.ru/events/president/news/68366/videos>

RAND. (2023). PLA Social Media Warfare and the Cognitive Domain. *Volume 23*(Issue 16).

Rand Corporation. (2023, September). *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping w*. RAND. Retrieved September 25, 2024, from

[https://www.rand.org/content/dam/rand/pubs/perspectives/PEA2600/PEA2679-1/RAND\\_PEA2679-1.pdf](https://www.rand.org/content/dam/rand/pubs/perspectives/PEA2600/PEA2679-1/RAND_PEA2679-1.pdf)

RANGE OPERATIONS GROUP OPERATIONS SECURITY COMMITTEE. (2011, April). Operations Security Guide. *OPERATIONS SECURITY (OPSEC) GUIDE, RCC Document 600-11*.

Rany Purnama Hadi. S.IP., M.Hub.Int. (2016). Strategi Perang Informasi (Netwar) dan Perjuangan Non-violent dalam Upaya Pemisahan Diri Papua di Indonesia. *JURNAL TRANSFORMASI GLOBAL VOL 4 NO 1*.

Reeder, J. R., & Hall, C. T. (2021, August 7). *Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack*.

The Cyber Defense Review. Retrieved October 2, 2024, from [https://cyberdefensereview.army.mil/Portals/6/Documents/2021\\_summer\\_cdr/02\\_ReederHall\\_CDR\\_V6N3\\_2021.pdf?ver=6qlw1l02DXt1A\\_1n5KrL4g%3D%3D](https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf?ver=6qlw1l02DXt1A_1n5KrL4g%3D%3D)

Rid, T. (2011, October 5). *Journal of Strategic Studies Cyber War Will Not Take Place*. Center for Strategic Leadership. Retrieved October 1, 2024, from

<https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf>

Robinson, & Neil. (2024, July 30). *Cyber defence*. NATO. Retrieved October 26, 2024, from

[https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)

- Russia Today. (2022, Maret). *Leading experts warned NATO expansion would lead to conflict. Why did no one listen?* Russia Today world news. <https://www.rt.com/news/551225-nato-expansion-lead-conflict/>
- Saeri, M. (2023, Desember). KONFLIK RUSIA-UKRAINA TAHUN 2014-2022. *Jurnal Dinamika Global, Vol. 8 No. 2.*
- Samad, M. Y., & Persadha, P. D. (2022, Desember). Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara dalam Menangkal Ancaman Siber. *Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi), Vol. 24 No. 2.*
- Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.* Crown Publishing Group.
- Security Week. (2022, Februari). Cyberattacks Knock Out Sites of Ukrainian Army, Major Banks. <https://www.securityweek.com/cyberattacks-knock-out-sites-ukrainian-army-major-banks/>
- Sihombing, E. S., & Setiawan, M. E. (2022). Kerancuan Berpikir: Propaganda Publik Media Pro-Ukraina Dalam Situasi Perang Rusia-Ukraina 2022. *urnal Sosial Humaniora, Vol. 2, No. 2 (2022).*
- Smart, B., Watt, J., Benedetti, S., Mitchell, L., & Roughan, M. (2022, Agustus 20). #IStandWithPutin versus #IStandWithUkraine: The interaction of bots and humans in discussion of the Russia/Ukraine war. *#IStandWithPutin versus #IStandWithUkraine: The interaction of bots and humans in discussion of the Russia/Ukraine war.*

- Sorokin, M. A. (2023, November 24). *Future of the Russian Cyber Defense*. Future of the Russian Cyber Defense - PIR Center. Retrieved September 21, 2024, from <https://pircenter.org/en/editions/future-of-the-russian-cyber-defense/>
- States, J. C. o. (2014). *Informations Operations*. Joint Publication.
- Sugiyono. (2013). *Metode Penelitian Kuantitatif, Kualitatif, dan RD*. Alfabeta.
- Sunyoto, M. (2022, August 18). *Estonia tangkis serangan siber setelah pindahkan monumen Soviet*. ANTARA News. Retrieved October 1, 2024, from <https://www.antaraneews.com/berita/3066185/estonia-tangkis-serangan-siber-setelah-pindahkan-monumen-soviet>
- Sutisnawinata, K. (2023, October 23). *Advanced Persistent Threat (APT): Arti dan Langkah Perlindungan*. ASDF.ID. Retrieved June 14, 2024, from <https://www.asdf.id/pengertian-advanced-persistent-threat-apt/>
- Taylor, S. J., Bogdan, R., & DeVault, M. L. (2015). *Introduction to Qualitative Research Methods: A Guidebook and Resource*. Wiley.
- Thomas, T. L. (2015). Russia's Military Strategy and Ukraine. *The Journal of Slavic Military Studies*, vol. 28(no. 3).
- Tokariuk, O. (2023, February 21). *A Year of Lies: Russia's Information War Against Ukraine*. CEPA. Retrieved September 25, 2024, from <https://cepa.org/article/a-year-of-lies-russias-information-war-against-ukraine/>



Topor, L., & Tabachnik, A. (2021). Russian Cyber Information Warfare International Distribution and Domestic Control. *Journal of Advanced Military Studies, Vol. 12, No. 1.*

US Air Force. (2020, september). Air Force Doctrine Publication 3-61. *Public Affairs.*

U.S. Department of Justice. (2019, March 7). *Report on the Investigation into Russian Interference in the 2016 Presidential Election.* Department of Justice. Retrieved October 2, 2024, from <https://www.justice.gov/archives/sco/file/1373816/dl>

U.S. NAVY & U.S. MARINE CORPS. (2017). OPERATIONS SECURITY (OPSEC).

Vega, J. C. (2004). *Computer Network Operation Methodology.*

Vilnius. (2022, August 18). *Estonia tangkis serangan siber setelah pindahkan monumen Soviet.* ANTARA News. Retrieved June 13, 2024, from <https://www.antaraneews.com/berita/3066185/estonia-tangkis-serangan-siber-setelah-pindahkan-monumen-soviet>

Warzel, C. (2022, March 8). *The Information War Between Ukraine and Russia Is Far From Over.* The Atlantic. Retrieved September 25, 2024, from <https://www.theatlantic.com/technology/archive/2022/03/russia-ukraine-war-propaganda/626975/>

Zahid, H. (2024, September). *Understanding the Cyber Threat Landscape: Comprehensive Vulnerability Assessment Techniques.*

Zinatullin, L. (2016). *The Psychology of Information Security.*