DAFTAR PUSTAKA

Buku

Andress, J., Winterfeld, S., Ablon, L., 2013. *Cyber Warfare Techniques, Tactics, and Tools for Security Practitioners*, Second Edition. Syngress Elsevier, Inc, USA.

Bernik, I., 2014. *Cybercrime and Cyberwarfare*. ISTE Ltd., London, UK.

Carr, J., 2009. *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media, Inc, Sebastopol.

Chossudovsky, M., 2005. *America War on Terrorism*. Global Research, Quebec.

Colarik, A.M., Zanczewski, L.J., 2008. *Cyber Warfare and Cyber Terrorism*. Information Science Reference, New York, USA.

Cunningham, Dr.C., 2020. *Cyber Warfare - Truth, Tactics, and Strategies*. Packt Publishing Ltd., Birmingham, UK.

Czosseck, C., Geers, K., 2009. *The Virtual Battlefield: Perspectives on Cyber Warfare*. IOS Press, Inc, Amsterdam, Netherlands.

Daras, N.J. (Ed.), 2019. *Cyber Security and Information Warfare*. Nova Science Publishers, Inc, New York.

Erbschloe, M., 2001. *Information Warfare: How to Survive Cyber Attacks*. The McGraw-Hill Companies, USA.

Geers, K., Kindlund, D., Moran, N., Rachwald, R., 2014. *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*. FireEye, Inc., Milpitas, CA.

Green, J.A., 2015. *Cyber Warfare: A Multidisciplinary Analysis*. Routledge, New York.

Jajodia, S., Shakarian, P., Subrahmanian, V.S., Swarup, V., Wang, C. (Eds.), 2015. *Cyber Warfare: Building The Scientific Foundation*. Springer International Publishing Switzerland, Virginia, USA.

Mazanec, B.M., Bradley, T.A., 2015. *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*. Palgrave Macmillan, United Kingdom.

Rosenzweig, P., 2013. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. ABC Clio, California.

Shakarian, P., Shakarian, J., Ruef, A., 2013. *Introduction to Cyber Warfare: A Multidisciplinary Approach*. Syngress Elsevier, Inc, USA.

Siboni, G., Kronenfeld, 2012. *Iran's Cyber Warfare*. Institute for National Security Studies.

Siboni, G., Kronenfeld, S., 2014a. *Developments in Iranian Cyber Warfare, 2013-2014*. Institute for National Security Studies.

Siboni, G., Kronenfeld, S., 2014b. *Iranian Cyber Espionage: A Troubling New Escalation*. Institute for National Security Studies.

Slavin, B., Healey, J., 2013. *Iran: How a Third Tier Cyber Power Can Still Threaten the United States*. Atlantic Council.

Springer, P.J. (Ed.), 2017. *Encyclopedia of Cyber Warfare*. ABC Clio, Santa Barbara, CA.

Springer, P.J., 2015. *Cyber Warfare: A Reference Handbook*. ABC Clio, Santa Barbara, California.

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Tzu, S. (2007). *The Art Of War*. Filiquarian. https://www.amazon.com/Art-War-Sun-Tzu/dp/1599869772

Vihul, L. (2013, April 15). The Tallinn Manual on the International Law applicable to Cyber Warfare. *EJIL: Talk!* https://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

Winterfeld, S., Andress, J., 2013. *The Basics of Cyber Warfare: Understanding the Fundamental of Cyber Warfare in Theory and Practice*. Syngress Elsevier, Inc, USA.

Yager, R.R., Reformat, M.Z., Alajlan, N. (Eds.), 2015. *Intelligent Methods for Cyber Warfare*. Springer International Publishing, New York.

Zanczewski, L.J., Colarik, A.M., 2005. *Managerial Guide for Handling Cyber Terrorism and Information Warfare*. Idea Group Publishing, USA.

Artikel dari Jurnal

Barzashka, I., 2013. Are Cyber-Weapons Effective?: Assessing Stuxnet's Impact on the Iranian Enrichment Programme. *The RUSI Journal*, 158(2), 48–56. https://doi.org/10.1080/03071847.2013.787735

Bahgat, G., 2020. Iran and Its Neighbors Face Risks and Opportunities in Cyber Security. *Orbis*, 64(1), 78–97. https://doi.org/10.1016/j.orbis.2019.12.006

Dalton, M. G., 2017. How Iran's hybrid-war tactics help and hurt it. *Bulletin of the Atomic Scientists*. https://www.tandfonline.com/doi/full/10.1080/00963402.2017.1362904

Kenney, M., 2015. Cyber-Terrorism in a Post-Stuxnet World. *Orbis*, 59(1), 111–128. https://doi.org/10.1016/j.orbis.2014.11.009

Rid, T., 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Artikel dalam Buku yang Diedit

Anderson, C., Sadjadpour, K., 2018a. Iran: Target and Perpetrator. *IRAN'S CYBER THREAT*, hlm. 9–16. Carnegie Endowment for International Peace. https://www.jstor.org/stable/resrep26913.8

Anderson, C., Sadjadpour, K., 2018b. Iran's Cyber Ecosystem: Who Are the Threat Actors? *IRAN'S CYBER THREAT*, hlm. 17–28. Carnegie Endowment for International Peace. https://www.jstor.org/stable/resrep26913.9

Munirathinam, S., 2020. Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT). Dalam P. Raj & P. Evangeline (Eds.), *Advances in Computers*, Vol. 117, hlm. 129–164. Elsevier. https://doi.org/10.1016/bs.adcom.2019.10.010

Martins, R. P., 2020. Punching Above Their Digital Weight: Why Iran is Developing Cyberwarfare Capabilities Far Beyond Expectations. Dalam *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*, hlm. 892–908. IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch054

Sumber dari Web

BBC, 2020. US-Iran relations: A brief history [WWW Document]. URL https://www.bbc.com/news/world-middle-east-24316661 (accessed 6.3.20).

BBC News. (2022, Juli 24). *How are "kamikaze" drones being used by Russia and Ukraine?* https://www.bbc.com/news/world-62225830 (accessed 6.28.24).

Center for Strategic & International Studies, 2019. Iran and Cyber Power [WWW Document]. URL https://www.csis.org/analysis/iran-and-cyber-power (accessed 6.3.20).

Cimpanu, C. (2021). *Iran updates budget to allocate $71.4 million to "cyberspace" operations*. https://therecord.media/iran-updates-budget-to-allocate-71-4-million-to-cyberspace-operations

Forbes, 2010. The Story Behind The Stuxnet Virus [WWW Document]. URL https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#1d50372351e8 (accessed 6.11.20).

Foreign Affairs, 2019. Iran's Green Movement Never Went Away [WWW Document]. URL https://www.foreignaffairs.com/articles/iran/2019-06-14/irans-green-movement-never-went-away (accessed 6.10.20).

Foreign Policy, Langner, R., 2013. Stuxnet's Secret Twin [WWW Document]. URL https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin (accessed 6.10.20).

Greenberg, A., 2022. Cyberwar: The Complete Guide. Wired.

History, 2019. September 11 Attacks [WWW Document]. URL https://www.history.com/.amp/topics/21st-century/9-11-attacks (accessed 6.4.20).

McAfee, 2020. What Is Stuxnet? [WWW Document]. URL https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html (accessed 6.11.20).

NJCCIC, 2017. Stuxnet: NJCCIC Threat Profile [WWW Document]. URL htpps://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/stuxnet (accessed 6.11.20).

Nye, J.S., 2012. Cyber War and Peace [WWW Document]. URL htpps://aljazeera.com/amp/indepth/opinion/2012/04/2012415102 42769575.html (accessed 4.21.20).

Stanford University, Holloway, M., 2015. Stuxnet Worm Attack on Iranian Nuclear Facilities [WWW Document]. URL https://large.stanford.edu/courses/2015/ph241/holloway1 (accessed 6.13.20).

The Guardian, 2020. Iran “revenge” could come in the form of cyber-attacks, experts warn.

The New York Times, 2008. Before the Gunfire, Cyberattacks [WWW Document]. URL htpps://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed 6.13.20).

the Secdev Group, 2009. Tracking GhostNet: Investigating a Cyber Espionage Network. Munk Centre for International Studies, University of Toronto.

Barnes-Dacey, H. A., Julien. (2024, Juni 5). Beyond proxies: Iran’s deeper strategy in Syria and Lebanon. ECFR. https://ecfr.eu/publication/beyond-proxies-irans-deeper-strategy-in-syria-and-lebanon/

Centre for Iranian Studies, & Rashid, Y. (2024). The Latest Status of the 25-Year Comprehensive Cooperation Agreement Between Iran and China—İRAN Center | Center for Iranian Studies in Ankara. https://iramcenter.org/en/the-latest-status-of-the-25-year-comprehensive-cooperation-agreement-between-iran-and-china-737

Clingendael Institute. (2024). The limit of Iran’s industrial resilience. Clingendael. https://www.clingendael.org/publication/limit-irans-industrial-resilience

CNN Transcripts. (2000, Januari 7). Public Papers of the Presidents of the United States: WILLIAM J. CLINTON (2000, Book I)—Remarks on the National Plan for Information Systems Protection and an Exchange With Reporters. https://www.govinfo.gov/content/pkg/PPP-2000-book1/html/PPP-2000-book1-doc-pg13-2.htm

Computer Fraud & Security. (2020). US-Iran conflict stokes fears of widespread cyberwar outbreak. *Computer Fraud & Security*, 2020(1), 1–3. https://doi.org/10.1016/S1361-3723(20)30001-4

Financial Times. (2016, April 26). Cyber warfare: Iran opens a new front. https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3

Sciarrone, M. O. (2017). Cyber Warfare: The New Front. The Catalyst Journal, 06. https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware/

Segal, S., & Gerstel, D. (2018). The Economic Impact of Iran Sanctions. https://www.csis.org/analysis/economic-impact-iran-sanctions

Starks, T., & DiMolfetta, D. (2023, Maret 14). Analysis | U.S. government provides cyber budget specifics. *Washington Post*. https://www.washingtonpost.com/politics/2023/03/14/us-government-provides-cyber-budget-specifics/

Stone, M. (2023, Januari 20). How Much is the U.S. Investing in Cyber (And is it Enough?). *Security Intelligence.* https://securityintelligence.com/articles/how-much-is-us-investing-in-cyber/

Loft, P. (2024). Iran’s influence in the Middle East. https://commonslibrary.parliament.uk/research-briefings/cbp-9504/

Laporan atau Publikasi dari Organisasi

Fassihi, F., 2012. Iran’s Censor Tighten Grip. *The Wall Street Journal*.