DAFTAR PUSTAKA

Artikel Jurnal dan Jurnal Elektronik

Breen, M., & Geltzer, J. A. (2011). Asymmetric strategies as strategies of the strong. *Parameters*, *41*(1), 41.

Burk, R. A., & Kallberg, J. (2016). Bring on the Cyber Attacks–The increased predatory power of the restrained red queen in a nation-state cyber conflict. *The Cyber Defense Review*, *1*(2), 61-72.

Eun, Y. S., & Aßmann, J. S. (2016). Cyberwar: Taking stock of security and warfare in the digital age. *International Studies Perspectives*, *17*(3), 343-360.

Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research*, *11*(4), 517-525.

Haizler, O. (2017). The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking. Cyber, Intelligence, and Security, 1(1), 31-45.

Heginbotham, E. (2015). The US-China military scorecard: Forces, geography, and the evolving balance of power, 1996–2017. Rand Corporation.

Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. Journal of Strategic Security, 4(2), 1-24.

Iasiello, E., 2014., Is cyber deterrence an illusory course of action?. *Journal of Strategic Security*, 7(1), 54-67

Krekel, B. (2009). *Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation*. NORTHROP GRUMMAN CORP MCLEAN VA.

Lewis, J. A., & Hansen, S. (2014). *China's cyberpower: International and domestic priorities*. Australian Strategic Policy Institute

Liff, A. P. (2012). Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, *35*(3), 401-428.

Lynn, W. F. (2010). Defending a new domain-the Pentagon's cyberstrategy. *Foreign Aff.*, *89*, 97.

Mazanec, B. M. (2009). The art of (cyber) war. *Journal of International Security Affairs*, *16*, 84.

Mulvenon, J. (2009). PLA computer network operations: Scenarios, doctrine, organizations, and capability. *Beyond the strait: PLA missions other than Taiwan*, 257-259.

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict and Security Law*, *17*(2), 187-209.

Peng, G. & Yao, Y., 2005. *Science of military strategy*, Beijing: Military Science Publishing House.

Pinkston, D. A. (2016). Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the" Sŏn'gun" Era. *Georgetown Journal of International Affairs*, 60-76.

Pollpeter, K. (2015). Chinese writings on cyberwarfare and coercion. *China and cybersecurity: espionage, strategy, and politics in the digital domain*, 147.

Shaheen, S. (2014). Offense–defense balance in cyber warfare. In *Cyberspace and International Relations* (pp. 77-93). Springer, Berlin, Heidelberg.

Siboni, G. Y. R. (2012). What lies behind Chinese cyber warfare. *Military and Strategic Affairs*, *4*(2), 49-64.

Siboni, G., & Kronenfeld, S. (2012). Iran and Cyberspace Warfare. *Military and Strategic Affairs*, *4*(3), 86-91.

Spade, J. M. (2011). *China's cyber power and America's national security*. ARMY WAR COLL CARLISLE BARRACKS PA.

Stiennon, R. (2015). A short history of cyber warfare. In *Cyber Warfare* (pp. 7-32). Routledge.

Wortzel, L. M. (2014). *The Chinese People's Liberation Army and Information Warfare*. ARMY WAR COLLEGE CARLISLE BARRACKS PA STRATEGIC STUDIES INSTITUTE.

Wu, C. (2006). An Overview of the Research and Development of Information Warfare in China. In *Cyberwar, Netwar and the Revolution in Military Affairs* (pp. 173-195). Palgrave Macmillan, London.

Yancey, C. K. (2019). Cyber Security: China and Russia's Erosion of 21st Century United States' Hegemony. McNair Scholars Research Journal, 12(1), 9.

Zhang, L. (2012). A Chinese perspective on cyber war. *Int'l Rev. Red Cross*, *94*, 801.

Buku

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Carlin, J. P. (2018). *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. Hachette UK.

Cheng, D. (2016). *Cyber Dragon: Inside China's Information Warfare and Cyber Operations: Inside China's Information Warfare and Cyber Operations*. ABC-CLIO.

Clarke, R. A. (2010). *Cyber war*. Old Saybrook: Tantor Media, Incorporated.

CRAIG, A. J., & VALERIANO, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. *Realism in Practice*, *85*.

Green, J. A. (Ed.). (2015). *Cyber warfare: a multidisciplinary analysis*. Routledge.

Hagestad, W. (2012). *21st century Chinese cyberwarfare*. IT Governance Ltd.

Kozłowski, A. (2015). The "Cyber Weapons Gap." The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan. In *"On Their Own Paths. Japan and China Responses to the Global and Regional Challenges", eds. D. Mierzejewski, K. Żakowski, Łódź University Press, Łódź 2015;*. Wydawnictwo Uniwersytetu Łódzkiego.

Kukkola, J., Nikkarila, J. P., & Ristolainen, M. (2017). Asymmetric frontlines of cyber battlefields. *GAME CHANGER Structural transformation of cyberspace*, 69.

McKenzie, T. M., 2017. Is Cyber Deterrence Possible?. Air University Press, Air Force Research Institute.

Mearsheimer, J. J. (2007). Structural realism. *International relations theories: Discipline and diversity*, *83*, 77-94.

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Broadway Books.

Springer, P. J. (2015). *Cyber Warfare: A Reference Handbook: A Reference Handbook*. Abc-Clio.

Media Cetak

Elegant, S. (2007). Enemies at the Firewall. Time Magazine, 170(25), 56-58.

Gady, F. S. (2015). Why the PLA Revealed Its Secret Plans for Cyber War. *The Diplomat*, *24*.

Pu, P. (2010). PLA unveils nation's first cyber center. *Global Times*, *22*.

Thornburgh, N. (2005). Inside the Chinese Hack Attack. *Times, August*, *25*.

Media Massa dan Website Online

Brenner, B. (2007). Experts doubt Russian government launched DDoS attacks. tersedia dalam: https://searchsecurity.techtarget.com/news/1255548/Experts-doubt-Russian-government-launched-DDoS-attacks [diakses pada Mei 2, 2020].

CBR. (2016). What is PLA Unit 61398 and who are the five Chinese hackers? *Computer Business Review*. Diakses pada: https://www.cbronline.com/what-is/what-is-pla-unit-61398-and-who-are-the-five-chinese-hackers-4271980/ [diakses pada Desember 20, 2020].

FBI, (2015). Five Chinese Military Hackers Charged with Cyber Espionage Against US,. tersedia dalam: https://www.fbi.gov/news/stories/five-chinese-military-hackers-charged-with-cyber-espionage-against-us [diakses pada Juli 13, 2020].

France-Presse, A., (2014). Xi wants China to be 'cyber power'. *DefenceTalk*. tersedia dalam: https://www.defencetalk.com/xi-wants-china-to-be-cyber-power-58886/ [diakses pada Desember 22, 2020].

Giandomenico, N. (2018). What is Spear-phishing? Defining and Differentiating Spear phishing from phishing. *Digital Guardian*. tersedia dalam: https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing [diakses pada Desember 24, 2020].

Hvistendahl, M. (2016). The Decline in Chinese Cyberattacks: The Story Behind the Numbers. tersedia dalam: https://www.technologyreview.com/2016/10/25/156465/the-decline-in-chinese-cyberattacks-the-story-behind-the-numbers/ [diakses pada Desember 22, 2020].

Jinghua, L. (2019). What Are China's Cyber Capabilities and Intentions? *Carnegie Endowment for International Peace*. tersedia dalam: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities and-intentions-pub-78734 [diakses pada Desember 22, 2020].

Lei, H., (2013). Foreign Ministry spokesperson Hong Lei's regular press conference. *Ministry of Foreign Affairs*. tersedia dalam: www.mfa.gov.cn/ce/ceke/eng/fyrth/t1047004.htm. [diakses pada Desember 22, 2020].

Mandiant, (2013). “APT1: Exposing One of China’s Cyber Espionage Units.” tersedia dalam: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [diakses pada Desember 22, 2020].

NBC News (2015), Exclusive: Secret NSA map shows China cyber attacks on US target. *NBC News*. tersedia dalam: https://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211 [diakses pada Desember 25, 2020].

PRC. (2014). The United States' Global Surveillance Record. tersedia dalam: http://www.china.org.cn/china/2014-05/27/content_32498950.htm [diakses pada Desember 22, 2020].

US DoD. (2011), *Department of Defense Strategy for Operating in Cyberspace*, tersedia dalam: www.defense.gov/news/d20110714cyber.pdf (diakses pada Desember 24, 2020).

US DoJ. (2015). US charges five chinese military hackers for cyber espionage against US corporations and a labor organization for commercial advantage.” tersedia dalam: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [diakses pada Desember 26, 2020].

Verton, D., (2016). Impact of OPM breach could last more than 40 years. *FedScoop*. Diakses pada: https://www.fedscoop.com/opm-losses-a-40-year-problem-for-intelligence- community/ [diakses pada Desember 22, 2020].

Skripsi, Tesis dan Disertasi

Ellis, J. M. (2015). *Chinese cyber espionage: a complementary method to aid PLA modernization*. Naval Postgraduate School Monterey CA.

Fritz, J. R. (2015). *China's Development of Cyber Warfare Doctrine: A Conceptual and Historical Investigation* (Doctoral dissertation, Bond University).