BAB IV

KESIMPULAN

Perkembangan teknologi di Tiongkok mulai berkembang dengan pesat sejak awal Abad ke – 21, transisi ini sudah terasa sejak awal dari 1990an akhir hingga masuknya tahun 2000an. Pada saat itu sudah mulai berkembangnya teknologi dan beberapa sistem komputer pada Revolusi Industri 4.0, hingga berjalannya Tiongkok berusaha untuk meingkatkan sistem teknologinya yang dikembangkan dan diintegrasikan dengan sistem internet. Perangkat dan komputer mulai terintegrasi secara keseluruhan, dan secara matang konsep ini diperkenalkan pada tahun 2010an. Konsep ini secara umum disebut sebagai *Internet of Things* (IoT), seiring berkembangnya dalam IoT diperlukan juga banyaknya data untuk mengatur berjalannya IoT, konsep ini juga disebut sebagai *Big Data*. Namun, dalam Revolusi Industri 4.0 dengan terhubungan perangkat dengan internet dan memerlukan data yang banyak untuk dapat berjalannya konsep ini muncul sebuah ancaman dalam *Big Data Privacy* melalui penggunaan *malware* yang dapat masuk kedalam jaringan IoT tanpa diketahui, sehingga dalam penelitian ini berusaha menjawab pertanyaan penilitan yaitu "Bagaimana Dampak *Malware* yang digunakan oleh Tiongkok dalam *Big Data privacy* pada tahun 2010 – 2019?" yang menjadi landasan untuk dilakukannya penelitian ini.

Dalam Revolusi Industri 4.0 merupakan sebuah masa dimana negara-negara mulai mengembangkan teknologi domestiknya sebaik mungkin. Tiongkok sudah mulai meningkatkan teknologinya sejak berhenti kerjasama dengan Uni Soviet dan fokus dengan mengembangkan tekonologinya secara mandiri dengan memproduksi

penemuan negaranya. Namun setelah target dan tujuan diawal telah dianggap berhasil, Tiongkok memiliki tujuan tersendiri dalam teknologinya yaitu mengembangkan teknologi bersamaan dengan agenda militer mereka. Xi Jinping setelah menjadi pemimpin dari Tiongkok terus berusaha untuk memasukan agenda ini menjadi salah satu agenda prioritas. Lalu, agenda ini juga telah disebutkan di dalam salah satu poin PMS bahwa teknologi harus ditingkatkan agar bisa menjaga keamanan dalam dunia maya (*cyberspace*). Dengan peningkatan keamanan dalam dunia maya, Tiongkok melakukan beberapa operasi dan melakukan penyerangan sebagai *self-defense* bagi negaranya. Salah satunya, penyerangan yang sering dilakukan terhadap Amerika Serikat dan beberapa target yang “tidak diketahui”. Operasi terbesar yang dilakukan oleh Tiongkok dalam penggunaan *malware* pada operasi aurora, Google merupakan salah satu perusahaan yang menjadi target dari operasi ini. Data yang diambil dalam sebuah operasi dengan melakukan penyerangan secara besar terhadap perusahaan swasta di Amerika Serikat. Operasi Informasi dan Perang Informasi yang dilakukan oleh Tiongkok mencakup konsep dari "perang jaringan" dengan kisaran jumlah dari personel "tentara peretas" yang berada di Tiongkok berjumlah antara 50.000 hingga 100.000 orang.

Selain itu, Tiongkok juga memanfaat dari sektor perusahaan teknologi yang ada di dalam negaranya dengan menggunakan perusahaan WeChat dan Tecno Mobile. Kedua perusahaan ini diduga dengan beberapa data mendukung bahwa adanya *backdoor* dalam kedua perusahaan tersebut. WeChat terduga melakukan penyadapan terhadap wartawan BBC yang berada di Hong Kong, dan melakukan ancaman terhadap wartawan tersebut. Ancaman yang diberikan dimana untuk tidak menyebarkan foto-foto mengenai pemberontakan terhadap Tiongkok. Pada tahun

2020, Tecno Mobile menjadi terduga dalam penggunaan *malware* yang terdapat pada *smartphone* yang diproduksi secara *entry-level*. Tindakan ini ditemukan di negara Ethiopia, Ghana, Kamerun dan Afrika Selatan. Menurut data yang disebutkan tindakannya ini telah dilakukan sejak tahun 2019. Perusahaan lainnya seperti Huawei dan ZTE, berdasarkan Amerika Serikat bahwa kedua perusahaan tersebut memiliki *backdoor* dalam produk ciptaannya yang berada di kawasan Amerika Serikat. Tentu saja, tindakan dengan memasang *backdoor* ini memerlukan *malware* agar dengan mudah dapat data-data yang diperlukan. Berbeda kasus dengan tindakan perusahaan-perusahaan dalam *local android app* seperti Tencent dan Baidu yang berbasiskan di Tiongkok. Tindakan ini memiliki tujuan dalam memperjualbelikan data untuk keuntungan pribadi. Dengan menciptakan kloningan aplikasi dan aplikasi yang tersematkan *malware* di dalamnya sebagai tindakan *phishing*.

Lalu, berdasarkan tindakan yang dilakukan oleh Tiongkok dan perusahaan swasta yang berbasiskan di Tiongkok maupun perusahaan s*tate-owned* memiliki dampak tersendiri bagi negaranya. Dalam tindakan yang dilakukan oleh perusahaan dengan berusaha untuk meningkatkan keuntungan pribadi berdasarkan konsep dari *surveillance capitalism*. Tindakan yang dilakukan tidak seutuhnya dapat dibenarkan, karena mereka melakukan tindakan tersebut tanpa adanya konsensus dengan pengguna dengan menjual data maupun melakukan transaksi tanpa adanya persetujuan dari pengguna. Dampak lainnya, Tiongkok sebagai aktor utama sebagai negara berdaulat melakukan penyerangan dan pengambilan data di beberapa wilayah yang disebutkan pada Bab 3. Hal ini tentu saja dapat memperkeruh suasana dalam politik internasional, dengan perusahaan yang menjadi terduga dalam

penggunaan *malware*. Oleh karena itu, Tiongkok sendiri menjadi permulaan dalam munculnya yang disebut sebagai *security dilemma* dalam Revolusi Industri 4.0 ini juga disebut sebagai *cybersecurity dilemma*. Dengan tindakannya akan berdampak terhadap negara lainnya, dimana negara akan berusaha untuk meningkatkan keamanan teknologinya untuk menghadapi *cyberthreat* yang dilakukan oleh Tiongkok sebelumnya. Jika kondisi ini terus berlanjut ke arah yang negatif (dalam hal ini terus adanya pencurian data) tidak menutup kemungkinan terburuknya akan terjadi *cyberwar* antara Tiongkok dengan negara oposisi.

DAFTAR PUSTAKA

4th ed., (Thousand Oaks: SAGE Publications Inc., 2014): 232

"An Undirected Attack Against Critical Infrastructure" (PDF). United States Computer Emergency Readiness Team (Us-cert.gov).

"A Brief History of Industry," Future of Industry, accessed April 9, 2021, https://www.sanayidegelecek.com/en/sanayi-4-0/tarihsel-gelisim/.

Alasdair Gilchrist, Industry 4.0: the Industrial Internet of Things (New York?: Apress, 2016).

Alex Pentland cited in "When There's No Such Thing As Too Much Information". The New York Times. 23 Apr. 2011

Archiveddocs, "Defining Malware: FAQ," accessed September 28, 2020, https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN.

"Big Data for Development: Opportunities and Challenges - White Paper • UN Global Pulse." Accessed April 22, 2021. https://www.unglobalpulse.org/document/big-data-for-development-opportunities-and-challenges-white-paper/.

Ball, Desmond. "China's Cyber Warfare Capabilities." Security Challenges 7, no. 2 (2011): 81-103. Accessed October 12, 2020. https://www.jstor.org/stable/26461991.

Ben Buchanan, The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations (Oxford, United Kingdom: Oxford University Press, 2017).

Ben Lutkevich and Ivy Wigmore, "What Is System Software? – Definition from WhatIs.Com," WhatIs.com (TechTarget, February 1, 2021), https://whatis.techtarget.com/definition/system-software.

Breur, Tom (July 2016). "Statistical Power Analysis and the contemporary "crisis" in social sciences". Journal of Marketing Analytics. 4 (2–3): 61–65. doi:10.1057/s41270-016-0001-3. ISSN 2050-3318

"China's Growth through Technological Convergence and Innovation." In China 2030, 155–216. The World Bank, 2013. https://doi.org/10.1596/9780821395455_CH02.

"China Due to Introduce Face Scans for Mobile Users." BBC News. BBC, December 1, 2019. https://www.bbc.com/news/world-asia-china-50587098.

"Chinese Phones with Built-in Malware Sold in Africa," BBC News (BBC, August 25, 2020), https://www.bbc.com/news/technology-53903436.

Charles Cooper and Raphael Kaplinsky, Technology and Development in the Third Industrial Revolution (London: Frank Cass, 1989). Page, 16

Cheng, Dean. *Cyber Dragon: inside China's Information Warfare and Cyber Operations*. Santa Barbara, CA, Canada: Praeger, 2017.

Corinne Reichert. 2020. US finds Huawei has backdoor access to mobile networks globally, report says.CNET 12 February 2020. https://www.cnet.com/news/us-finds-huaweihas-backdoor-access-to-mobile-networks-globallyreport-says/

Corrinne Reichert. 2020. Huawei is backed by Chinese military, Trump administration finds. 2020. CNET 24 June 2020. https://www.cnet.com/news/huawei-is-backed-bychinese-military-trump-administration-reportedlyfinds/

Craig Silverman, "Chinese-Made Smartphones Are Secretly Stealing Money From People Around The World," BuzzFeed News (BuzzFeed News, August 26, 2020), https://www.buzzfeednews.com/article/craigsilverman/cheap-chinese-smartphones-malware.

"Cyberwarfare Statistics: A Decade of Geopolitical Attacks," PrivacyAffairs, May 9, 2021, https://www.privacyaffairs.com/geopolitical-attacks/#:~:text=Attacks%20originating%20in%20China%202009,sponsored%20attackers%2C%20targeting%2020%20countries.&text=32%25%20of%20China's%20attacks%20were,biggest%20target%20for%20Chinese%20hackers.

Dean Cheng, Cyber Dragon: inside China's Information Warfare and Cyber Operations (Santa Barbara, California ; Denver, Colorado: Praeger, 2017).

"Elderwood Project, Who Is behind Op. Aurora and Ongoing Attacks?" Security Affairs, August 27, 2017. http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html.

Eysenbach G. Infodemiology: tracking flu-related searches on the Web for syndromic surveillance. AMIA (2006)

Fu, Tao. "China's Personal Information Protection in a Data-Driven Economy: A Privacy Policy Study of Alibaba, Baidu and Tencent." Global Media and Communication 15, no. 2 (2019): 195–213. https://doi.org/10.1177/1742766519846644.

Ginsberg, Jeremy, Matthew H. Mohebbi, Rajan S. Patel, Lynnette Brammer, Mark S. Smolinski, and Larry Brilliant. "Detecting Influenza Epidemics Using Search Engine Query Data." Nature 457.7232 (2008): 1012-1014.

Glaser, Charles L. "The Security Dilemma Revisited." World Politics 50, no. 1 (1997): 171-201. Accessed June 3, 2021. http://www.jstor.org/stable/25054031.

Hart, O., A. Shleifer, and R. W. Vishny. “The Proper Scope of Government: Theory and an Application to Prisons.” *The Quarterly Journal of Economics* 112, no. 4 (1997): 1127–61. https://doi.org/10.1162/003355300555448.

“How the State Runs Business in China,” The Guardian (Guardian News and Media, July 25, 2019), https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei.

“How the Threat of 'Original Sin' Keeps China's Businessmen Awake at Night,” South China Morning Post, January 1, 2019, https://www.scmp.com/news/china/article/2180129/why-chinas-private-firms-arent-convinced-law-will-protect-them.

Helbing and Balietti. “From Social Data Mining to Forecasting Socio-Economic Crisis.”

Hugh Boyes et al., “The Industrial Internet of Things (IIoT): An Analysis Framework,” Computers in Industry 101 (2018): pp. 1-12, https://doi.org/10.1016/j.compind.2018.04.015.

“Industrial Revolution,” Encyclopædia Britannica (Encyclopædia Britannica, inc., February 21, 2021), https://www.britannica.com/event/Industrial-Revolution.

“Internet of Things Meets the Military and Battlefield,” IEEE Computer Society Internet of Things Meets the Military and Battlefield Connecting Gear and Biometric Wearables for an IoMT and IoBT Comments, accessed May 1, 2021, https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt.

“Isaac Computer Science,” Isaac Computer Science, accessed April 14, 2021, https://isaaccomputerscience.org/concepts/sys_os_application_software#:~:text=General%20purpose%20software%20is%20software,software%20and%20word%20processing%20software.&text=Special%20purpose%20software%20is%20software,used%20for%20one%20particular%20task.

Joe Fitzsimmons, “Information Technology and the Third Industrial Revolution,” The Electronic Library 12, no. 5 (1994): pp. 295-297, https://doi.org/10.1108/eb045307.

Joe McReynolds, “China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy,” Jamestown, September 20, 2016,

https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy/.

Johan Sigholm, “Non-State Actors in Cyberspace Operations,” Journal of Military Studies 4, no. 1 (January 2013): pp. 1-37, https://doi.org/10.1515/jms-2016-0184.

John W. Creswell, “The Selection of a Research Design” dalam Research Design: Qualitative,

John W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches,

Julianna Wu Alice Tse, “Why 'Made in China 2025' Triggered the Wrath of President Trump,” South China Morning Post, September 11, 2018, https://multimedia.scmp.com/news/china/article/made-in-China-2025/index.html.

Kartasasmita, Giandi and Kurnadi, Andrea. “The Securitization of China’s Technology Companies in the United States of America.” Jurnal Ilmiah Hubungan Internasional 16, no. 2 (December 11, 2020): 159–78. https://doi.org/10.26593/jihi.v16i2.4204.159-178.

Kim, Gang-Hoon, Silvana Trimi, and Ji-Hyong Chung. “Big-Data Applications in the Government Sector.” Communications of the ACM 57, no. 3 (2014): 78–85. https://doi.org/10.1145/2500873.

Klaus Schwab, The Fourth Industrial Revolution (New York: Currency, 2017).

Lingling Wei, “China's Xi Ramps Up Control of Private Sector. 'We Have No Choice but to Follow the Party.',” The Wall Street Journal (Dow Jones & Company, December 10, 2020), https://www.wsj.com/articles/china-xi-clampdown-private-sector-communist-party-11607612531.

Litao ZHAO, “China’s Innovation-Driven Development under Xi Jinping,” East Asian Policy 08, no. 04 (2016): pp. 55-68, https://doi.org/10.1142/s1793930516000404.

Lyu Jinghua, “What Are China's Cyber Capabilities and Intentions?,” Carnegie Endowment for International Peace, accessed May 30, 2021, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

“Made in China 2025: 10-Year National Plan Unveiled,” FINDCHINA, May 20, 2015, https://findchina.info/made-china-2025-plan-unveiled-boost-manufacturing.

Mara Hvistendahl, “China's Hacker Army,” Foreign Policy, March 3, 2010, https://foreignpolicy.com/2010/03/03/chinas-hacker-army/.

Mert Onuralp Gokalp et al., “Big Data for Industry 4.0: A Conceptual Framework,” 2016 International Conference on Computational Science and Computational Intelligence (CSCI), 2016, https://doi.org/10.1109/csci.2016.0088.

Ning, Susan, and Han Wu. “International Legal Business Solutions - Global Legal Insights.” GLI - Global Legal InsightsInternational legal business solutions. Global Legal Group, 2020. https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/China.

PricewaterhouseCoopers, “Global Digital Operations 2018 Survey,” PwC, accessed April 9, 2021, https://www.strategyand.pwc.com/gx/en/insights/industry4-0.html.

Quantitative, and Mixed Methods Approaches, 3rd ed., (California: SAGE Publications Inc., 2009):8

Rao, Dr. Madanmohan. “Mobile Africa Report: Regional Hubs of Excellence and Innovation.” Mobile Monday (2011): 1-68. Mar. 2011

Robert Delaney. 2018. US slaps China’s ZTE with 7-year components ban for breaching terms of sanctions settlement. South China Morning Post 16 April 2018.

Robert L. Worden, Andrea Matles Savada, and Ronald E. Dolan, China: a Country Study (Washington, D.C.: The Division, 1988).

Ryan Engelman et al., “The Second Industrial Revolution, 1870-1914,” US History Scene, October 25, 2020, https://ushistoryscene.com/article/second-industrial-revolution/.

Shahin, Saif, and Pei Zheng. “Big Data and the Illusion of Choice: Comparing the Evolution of India’s Aadhaar and China’s Social Credit System as Technosocial Discourses.” Social Science Computer Review 38, no. 1 (2018): 25–41. https://doi.org/10.1177/0894439318789343.

Shaun Rein, The End of Cheap China: Economic and Cultural Trends That Will Disrupt the World (Hoboken, NJ: Wiley, 2014).

Shoshana Zuboff, The Age of Surveillance Capitalism: the Fight for the Future at the New Frontier of Power (London, United Kingdom: Profile Books, 2019).

Shoubo Xu, Technological Economics (Singapore: Springer, 2020).

Soemon Takakuwa, Ivica Veza, and Stipe Celar, “‘Industry 4.0’ in Europe and East Asia,” Proceedings of the 29th International DAAAM Symposium 2018, 2018, pp. 0061-0069, https://doi.org/10.2507/29th.daaam.proceedings.009.

Stephen McDonell, “China Social Media: WeChat and the Surveillance State,” BBC News (BBC, June 7, 2019), https://www.bbc.com/news/blogs-china-blog-48552907.

Syndromic Surveillance (SS).” Centers for Disease Control and Prevention. 06 Mar. 2012

“The 5 V's of Big Data,” Watson Health Perspectives, December 3, 2020, https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/.

“The Fourth Industrial Revolution,” Encyclopædia Britannica (Encyclopædia Britannica, inc., March 23, 2021), https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734.

The social dilemma. Dir. Jeff Orlowski. Netflix, 2020. Documentary.

Third International Conference on Intelligent Control and Information Processing (ICICIP), 2012 (Piscataway, NJ: IEEE, n.d.).

“Tracking State-Sponsored Cyberattacks Around the World,” Council on Foreign Relations (Council on Foreign Relations), accessed May 30, 2021, https://microsites-live-backend.cfr.org/cyber-operations#Timeline.

Trevor J Barnes, “Big Data, Little History,” Dialogues in Human Geography 3, no. 3 (2013): pp. 297-302, https://doi.org/10.1177/2043820613514323.

Varian, Hal R. “Computer Mediated Transactions.” American Economic Review 100, no. 2 (May 2010): 1–10. https://doi.org/10.1257/aer.100.2.1.

Wang, Haoyu, Zhe Liu, Jingyue Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, Juan Tapiador, Jingcun Cao, and Guoai Xu. “Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets.” In Proceedings of the Internet Measurement Conference 2018, 293–307. Boston MA USA: ACM, 2018. https://doi.org/10.1145/3278532.3278558.

Wang, Lele. “Comparative Research on Germany QIndustrie 4.0q and q Made in China 2025q.” In Proceedings of 2016 2nd International Conference on Humanities and Social Science Research (ICHSSR 2016). Singapore: Atlantis Press, 2016. https://doi.org/10.2991/ichssr-16.2016.7.

“World Economic Forum: Global Risks Report 2019,” Computer Fraud & Security 2019, no. 2 (2019): p. 4, https://doi.org/10.1016/s1361-3723(19)30016-8.

Yongxin Liao et al., “The Impact of the Fourth Industrial Revolution: a Cross-Country/Region Comparison,” Production 28, no. 0 (2018), https://doi.org/10.1590/0103-6513.20180061.

Zetter, Kim. “Google Hack Attack Was Ultra Sophisticated, New Details Show.” Wired. Conde Nast, January 14, 2010. https://www.wired.com/2010/01/operation-aurora/.

Zuboff, S. (2020). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs.

Zuboff, Shoshana; Möllers, Norma; Murakami Wood, David; Lyon, David (March 31, 2019). "Surveillance Capitalism: An Interview with Shoshana Zuboff"

Zhou, Hongren. “Strategic Stability in Cyberspace: A Chinese View.” *China Quarterly of International Strategic Studies* 05, no. 01 (2019): 81–95. https://doi.org/10.1142/s2377740019500088.